15. Tätigkeitsbericht 2007/2008

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Tätigkeitsbericht 2007/2008
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 2007 und 31. März 2008 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. 410.015.d/f

Inhaltsverzeichnis

* Originaltext auf Französisch

* Originaltext auf Französisch

* Originaltext auf Französisch

* Originaltext auf Französisch

Vorwort

Im letzten Tätigkeitsbericht habe ich die Rolle des Datenschützers mit jener des Sisyphos verglichen, der tragischen Gestalt aus der griechischen Mythologie, die immer wieder vergeblich denselben Stein den Berg hinauf stösst: Kaum glaubt man ein Datenschutzproblem gelöst, taucht ein neues auf. Auch wenn sich am Bild grundsätzlich nichts ändert, so gibt der jährliche Tätigkeitsbericht doch die Gelegenheit, Rückschau zu halten und sich an den Erfolgen zu freuen. Man kann es so auf den Punkt bringen: Vernünftiger Datenschutz ist erfolgreich.

Das beginnt beim Gesundheitsbereich, wo nach unseren Empfehlungen in Sachen CSS einiges in Bewegung geraten ist. Die Schweizerische Gesellschaft der Vertrauensärzte hat im Dezember 2007 mit unserer Unterstützung Empfehlungen für die Tätigkeit der Vertrauensärzte verabschiedet, die darauf abzielen, deren Unabhängigkeit gegenüber ihren Versicherungen zu stärken. Der Datenfluss innerhalb des vertrauensärztlichen Dienstes wurde klarer geregelt und die administrative Unabhängigkeit besser organisiert. Der Umstand, dass Krankenversicherer im Rahmen weit verzweigter Holdings verschiedene Produkte wie Taggeldversicherung und Lebensversicherungen anbieten, ruft nach Klärung der Rolle der nach KVG eingesetzten Vertrauensärzte, die auch im Bereich der nichtobligatorischen Versicherungen tätig sind. Unklar ist ferner nach wie vor die Rolle der Case Manager und die Frage, ob es zur Klärung beiträgt, wenn sie in den vertrauensärztlichen Dienst eingegliedert werden.

Positiv ist sodann, dass ein gemeinsames Projekt zwischen dem Bundesamt für Gesundheit und uns zustande gekommen ist, mit dem versucht wird, einen Überblick über den Stand des Datenschutzes im Gesundheitsbereich zu schaffen und Lösungsansätze zu formulieren. Angesichts der Entwicklungen auf diesem Gebiet – als Stichwort sei hier nur die Einführung des DRG genannt – ist diese Arbeit ausserordentlich wichtig. Die Resultate sind im Verlaufe dieses Jahres zu erwarten. Ebenfalls erfreulich ist, dass die CSS bereit ist, sich einem regelmässigen externen Datenschutzaudit zu unterziehen. Das fordern wir seit langem für den gesamten Gesundheitsbereich, um das Vertrauen in die Bearbeitung von hochsensiblen Daten nachhaltig zu stärken.

Mit dem neuen Datenschutzgesetz wurde gerade in diesem Bereich mit der Möglichkeit zur Datenschutzzertifizierung ein wichtiges neues Instrument geschaffen. Wir setzen uns dafür ein, dass solche Audits insbesondere bei der Bearbeitung von besonders schützenswerten Personendaten zum Standard werden. Derzeit sind wir daran, mit den interessierten Kreisen die in der Zertifizierungsverordnung vorgesehenen

Richtlinien zu erarbeiten. Ziel muss sein, ein möglichst einfaches und kundenfreundliches Verfahren zu etablieren, das auf der Grundlage der ISO 27001-Norm abgewickelt werden kann.

Überhaupt zeigt das per 1. Januar 2008 in Kraft gesetzte revidierte Datenschutzgesetz erste positive Auswirkungen. Wir stellen fest, dass sich vor allem die grossen Wirtschaftsunternehmen, deren Datenschutzverantwortliche im Verein Unternehmens-Datenschutz (VUD) zusammengeschlossen sind, mit grosser Ernsthaftigkeit an die Umsetzung der neuen Bestimmungen gemacht und dabei eine konstruktive Zusammenarbeit mit dem EDÖB gesucht haben.

Im Rahmen der Erarbeitung des neuen Gesetzes über die polizeilichen Informationssysteme ist es uns gelungen, im Nachgang zu einem Urteil des Europäischen Gerichtshofs für Menschenrechte die Rechtsstellung von Einsichtsuchenden in die Datenbanken Janus und Gewa markant zu verbessern. Die gleiche Verbesserung muss nun auch beim Bundesgesetz über die Massnahmen zur Wahrung der inneren Sicherheit, dessen Revisionsentwurf sich derzeit in der parlamentarischen Behandlung befindet, vollzogen werden. Auch sonst wird uns dieses Gesetz wegen seiner gefährlichen Stossrichtung dieses Jahr besonders beschäftigen.

In Sachen SWIFT ist positiv zu vermerken, dass sich diese Organisation entschieden hat, sämtliche Geldtransaktionen, die nicht direkt mit den USA zu tun haben, organisatorisch und technisch so zu abzutrennen, dass das amerikanische Recht darauf nicht mehr anwendbar ist, so dass die Transaktionsdaten dem Zugriff durch US-Behörden entzogen werden. In diesem Sinne werten wir es als richtigen Schritt, dass sich SWIFT entschlossen hat, zu diesem Zweck ein Operation Center in der Schweiz zu etablieren und die Geldtransaktionen, welche mit den USA nichts zu tun haben, hier abzuwickeln.

Das Öffentlichkeitsgesetz ist nun bald zwei Jahre in Kraft und eine erste Beurteilung ist möglich. Es zeichnet ein allmählicher Mentalitätswandel vom Geheimhaltungs- zum Öffentlichkeitsprinzip in den Bundesämtern ab. In unserer Funktion als Schlichtungsstelle haben wir in den allermeisten Fällen, in denen der Zugang zu amtlichen Dokumenten durch ein Bundesamt ganz oder zum Teil abgelehnt wurde, eine für die Gesuchstellenden günstigere Lösung erzielen können. Gleichzeitig wurde in dieser ersten Phase des Öffentlichkeitsprinzips aber auch deutlich, dass die Ämter noch eine gewisse Zeit benötigen werden, um sich mit dieser neuen Situation vertraut zu machen. Positiv festzuhalten ist, dass die von uns angesprochene Ressourcenproblematik dadurch entschärft werden konnte, dass sich die Bundeskanzlei bereit erklärte, uns zwei Stellen – allerdings nur befristet – zur Verfügung zu stellen, um die im ersten

Jahr gehäuft aufgetretenen Schlichtungsanträge abzutragen. Wir sind zuversichtlich, dass somit die Rückstände bis Ende Jahr aufgearbeitet werden können. Es wird sich dann die Frage stellen, welche Ressourcen für einen geordneten Betrieb definitiv zur Verfügung gestellt werden müssen.

In Hinblick auf den Beitritt der Schweiz zu den Abkommen Schengen/Dublin und deren Umsetzung hat unser Land eine Evaluation seines datenschutzrechtlichen Systems zu bestehen. In diesem Zusammenhang besuchte uns im März während mehrerer Tage eine 13-köpfige EU-Delegation unter der Führung der slowenischen Datenschutzbeauftragten. Untersucht wurde der Stand des Datenschutzes auf der Ebene von Bund und Kantonen. Inzwischen liegt der Bericht der EU-Experten vor, der eine Reihe von Empfehlungen enthält. Die Experten stellten fest, dass insbesondere die administrative und finanzielle Unabhängigkeit der Datenschutzbehörden nicht ausreichend gewährleistet sei und namentlich für die Bewältigung der neuen Aufgabe zu wenig Ressourcen zur Verfügung stünden. In den nächsten sechs Monaten wird die Schweiz erklären müssen, wie sie die Empfehlungen umsetzen wird. Der EDÖB hat in den letzten Jahren wiederholt auf diese Problematik hingewiesen, insbesondere auch mit Blick auf die bevorstehenden internationalen Abkommen. Er wird mit den zuständigen Stellen versuchen, eine gangbare Lösung zu finden, damit die Schweiz den Anforderungen der EU genügt. Eine weitere Empfehlung zielt darauf hin, im Hinblick auf die sich überschneidenden Aufsichtsaufgaben von Bund und Kantonen die Zusammenarbeit zwischen dem EDÖB und den kantonalen Datenschutzbehörden festzulegen.

Dass Datenschutzfragen durchaus auf Interesse stossen, zeigte der am 11. Januar 2008 mit der Universität Freiburg gemeinsam organisierte erste Datenschutzrechtstag. Die sehr gut besuchte Veranstaltung befasste sich schwergewichtig mit der einige Tage zuvor in Kraft getretenen Revision des Datenschutzgesetzes, beleuchtete die Rechtsprechung der ehemaligen Datenschutzkommission und setzte sich mit Blick auf das 2006 in Kraft getretene Öffentlichkeitsgesetz mit dem Thema «Öffentlichkeitsprinzip versus Datenschutz» auseinander. Im gleichen Zusammenhang zu erwähnen ist der am 28. Januar 2008 zum zweiten Mal durchgeführte europäische Datenschutztag, der erneut in Kooperation mit dem Europa Institut an der Universität Zürich durchgeführt werden konnte. Zum gleichen Anlass konnte ausserdem eine Zusammenarbeit mit den Radiosendern DRS und RSR realisiert werden, die sich den ganzen Tag mit journalistisch hervorragend aufbereiteten Aspekten des Datenschutzes befassten, begleitet von einem von uns gestellten Expertenteam, das den Hörerinnen und Hörern während dieser Zeit für zahlreich eingegangene telefonische Anfragen zur Verfügung stand.

In all diesen Fällen zahlte sich eine intensive Zusammenarbeit mit interessierten Akteuren ausserhalb des engen Bereichs des Datenschutzes aus und führte zu beachtlichen Resultaten im Interesse des Schutzes der Privatsphäre. Vernünftiger Datenschutz ist vor allem dann erfolgreich, wenn er in einem möglichst breiten Feld mit potentiellen Interessenten kooperiert.

Hanspeter Thür

Abkürzungsverzeichnis

ADAMS	Anti Doping Administration and Management System
AHVG	Bundesgesetz über die Alters- und Hinterlassenenversicherung
AS	Amtliche Sammlung des Bundesrechts
ATSG	Bundesgesetz über den allgemeinen Teil des Sozialversicherungsrechts
BAG	Bundesamt für Gesundheit
BAV	Bundesamt für Verkehr
BAZL	Bundesamt für Zivilluftfahrt
BBl	Bundesblatt
BFS	Bundesamt für Statistik
BGÖ	Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung
BIT	Bundesamt für Informatik und Telekommunikation
BJ	Bundesamt für Justiz
BK	Bundeskanzlei
BPG	Bundespersonalgesetz
BStatG	Bundesstatistikgesetz
BSV	Bundesamt für Sozialversicherungen
BUR	Betriebs- und Unternehmensregister
BVGer	Bundesverwaltungsgericht
BWIS	Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit
DSG	Bundesgesetz über den Datenschutz
DSMS	Datenschutz-Managementsystem
EAN	European Article Number
EDA	Eidgenössischen Departement für auswärtige Angelegenheiten
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter

EDPS	European Data Protection Supervisor
EJPD	Eidgenössisches Justiz- und Polizeidepartement
EPA	Eidgenössisches Personalamt
fedpol	Bundesamt für Polizei
GK	Gemeinsame Kontrollinstanz Schengen
GUMG	Bundesgesetz über genetische Untersuchungen beim Menschen
HFG	Bundesgesetz über die Forschung am Menschen
ICAO	Die International Civil Aviation Organization
IPRG	Bundesgesetz über das Internationale Privatrecht
ISMS	Informationssicherheitsmanagementsystem
IVG	Bundesgesetz über die Invalidenversicherung
IVV	Verordnung über die Invalidenversicherung
IWGDPT	International Working Group on Data Protection in Telecommunications
KVG	Bundesgesetz über die Krankenversicherung
PNR	Passenger Name Record
RHG	Bundesgesetz über die Harmonisierung der Einwohnerregister und anderer amtlicher Personenregister
SAA	Schengen-Assoziierungsabkommen
SAS	Schweizerische Akkreditierungstelle
SchKG	Bundesgesetz über Schuldbetreibung und Konkurs
Sedex	secure data exchange
SIS	Schengener Informationssystem
UID	Unternehmens-Identifikationsnummer
UVG	Unfallversicherungsgesetz
VAD	Vertrauensärztlicher Dienst
VBS	Departement für Verteidigung, Bevölkerungsschutz und Sport
VDSG	Verordnung zum Bundesgesetz über den Datenschutz

VDSZ	Verordnung über die Datenschutzzertifizierungen
VVG	Bundesgesetz über den Versicherungsvertrag
VWIS	Verordnung über Massnahmen zur Wahrung der inneren Sicherheit
VwVG	Bundesgesetz über das Verwaltungsverfahren
WADA	World Anti Doping Agency
ZentG	Bundesgesetz über die kriminalpolizeilichen Zentralstellen des Bundes
ZIS	Zentrales Informationssystem (zur Bekämpfung des Versicherungsmissbrauchs)

1. Datenschutz

1.1 Grundrechte

1.1.1 Verordnung über die Datenschutzzertifizierungen

Im Rahmen der Anhörung und der zweiten Ämterkonsultation haben wir zur Verordnung über die Datenschutzzertifizierungen Stellung genommen. Wir sprachen uns klar für ein offizielles Datenschutz-Qualitätszeichen aus, was nicht berücksichtigt wurde. Dagegen sieht die Verordnung nun ausdrücklich vor, dass wir Richtlinien über die Mindestanforderungen an ein Datenschutzmanagementsystem zu erlassen haben.

Zum Verordnungsentwurf für die Datenschutzzertifizierung (VDSZ) haben wir sowohl im Rahmen der Anhörung als auch anlässlich der zweiten (bundesinternen) Ämterkonsultation Stellung genommen. Dabei stellten wir mit Bedauern fest, dass die aktuellen Verordnungsentwürfe kein Datenschutz-Qualitätszeichen mehr enthielten. Unseres Erachtens drängt sich ein solches indessen aus Transparenzgründen auf und würde es dem Konsumenten erlauben, sofort zu erkennen, ob er es mit einer Zertifizierung nach DSG durch ein akkreditiertes Unternehmen zu tun hat oder nicht. Das zertifizierte Unternehmen seinerseits hätte die Möglichkeit, das offizielle Label nach erfolgter Zertifizierung ohne zusätzliche Kosten zu benützen. Auch hielten wir fest, dass die Arbeitsgruppe (vgl. Ziff. 1.1.1 unseres 14. Tätigkeitsberichts 2006/2007) ein offizielles Datenschutz-Qualitätszeichen nie in Frage gestellt hatte. Zudem würde ein solches zusätzlich zu allfälligen privaten Qualitätszeichen bestehen. Weiter wiesen wir darauf hin, dass zwischen Datenschutz und Informationssicherheit zu unterscheiden sei, weshalb ein reiner Verweis auf internationale Standards und Normen betreffend Managementsysteme und insbesondere Informationssicherheitsmanagementsysteme (ISMS) nicht genügen würde. Aus diesem Grund sei uns in der VDSZ die Kompetenz zu erteilen, Richtlinien betreffend die speziellen Datenschutzanforderungen im Rahmen einer Zertifizierung zu erlassen, wie der Entwurf dies bereits für die Datenschutzzertifizierung von Produkten vorsehe. Schliesslich sprachen wir uns dafür aus, dass die Kompetenz, ausländische Zertifizierungsstellen anzuerkennen, nicht uns, sondern der Schweizerischen Akkreditierungsstelle oder dem Bundesamt für Justiz zugesprochen werden sollte. Wir begründeten dies damit, dass uns das DSG keine Verfügungskompetenz zuschreibe.

Unsere Bemerkungen betreffend offizielles Datenschutzlabel und Anerkennung ausländischer Zertifizierungsstellen wurden nicht berücksichtigt. Dagegen sieht die definitive Version der VDSZ ausdrücklich vor, dass der EDÖB Richtlinien über die Mindestanforderungen an das Datenschutzmanagementsystem zu erlassen habe (vgl. Ziff. 1.1.2 des vorliegenden Tätigkeitsberichts.

Das revidierte Datenschutzrecht und damit auch die VDSZ sind auf den 1. Januar 2008 in Kraft getreten.

1.1.2 Richtlinien des EDÖB für die Zertifizierung von Organisationen

Gemäss der Verordnung über die Datenschutzzertifizierungen hat der EDÖB Richtlinien über die Mindestanforderungen an das Datenschutzmanagementsystem zu erlassen. Er stützt sich dafür auf die internationalen Normen für Managementsysteme, insbesondere ISO/IEC 27001:2005. Diese Richtlinien beinhalten die wesentlichen Elemente der Norm 27001 mit Schwerpunkt auf dem Datenschutz und gleichzeitig basierend auf einem ergänzenden Leitfaden zur Umsetzung. Diese Broschüre, die nach neun allgemeinen Grundsätzen des DSG aufgebaut ist und derzeit rund zwanzig konkrete Massnahmen enthält, ist das auf den Datenschutz anwendbare Gegenstück zur Norm 27002 (Leitfaden für die Informationssicherheit) in Verbindung mit der Norm 27001.

Im Anschluss an die Einführung des neuen Artikels 11 DSG betreffend das Zertifizierungsverfahren ist am 1. Januar 2008 die Verordnung über die Datenschutzzertifizierungen (VDSZ) in Kraft getreten. Laut Art. 4 Abs. 3 VDSZ (Zertifizierung von Organisation und Verfahren) erlässt der oder die Beauftragte «Richtlinien über die Mindestanforderungen an das Datenschutzmanagementsystem. Er oder sie berücksichtigt dabei internationale Normen und Standards für die Errichtung, den Betrieb, die Überwachung und die Verbesserung von Managementsystemen, insbesondere die Normen ISO 9001:2000 und ISO 27001:2005.»

Um dem zu entsprechen, geht es in einem ersten Schritt darum, von ISO 27001 die allgemeinen Anforderungen an Managementsysteme zu übernehmen, die ihrerseits aus den grundlegenden Vorgaben von ISO 9001 für das Qualitätsmanagement stammen, wie dem informativen Anhang C von ISO 27001 zu entnehmen ist. Die Hauptschwierigkeit bestand darin, den Akzent mehr auf den Datenschutz als auf die Informationssicherheit zu setzen. Über Art. 7, der die vom DSG vorgeschriebenen Voraussetzungen für die Datensicherheit umschreibt, kann glücklicherweise der Datenschutz

im weiteren Sinne als Gesamtziel an Stelle des mit ISO 27001 angestrebten Ziels der Informationssicherheit betrachtet werden. Auf diesem Wege soll ein Datenschutz-Managementsystem (DSMS) aufgebaut werden, das unter anderem eine Politik des Datenschutz-Managementsystems, eine Auswahl von Massnahmen für die Behandlung von Nichtkonformitäten, eine Erklärung zur Anwendbarkeit der umgesetzten Massnahmen mit einer Begründung der gegebenenfalls ausgeschlossenen Massnahmen, einen Plan für die Behandlung der Nichtkonformitäten, eine Überprüfung der Datenschutzverletzungen oder -zwischenfälle und Korrektur- oder Vorbeugungsmassnahmen zur Verbesserung des DSMS vorschreibt.

Ein zweiter Schritt bestand in der Übernahme des normativen Anhangs A von ISO 27001, der eigentlich aus dem Inhaltsverzeichnis der Norm ISO/IEC 27002:2005, auch bekannt unter der Bezeichnung «Leitfaden zum Management der Informationssicherheit», besteht. Dieser umfasst 15 Kapitel, von denen die letzten 11 «Kontrollgruppen» bilden, die ihrerseits in 39 «Kontrollziele» unterteilt sind und zu insgesamt 133 «Kontrollmassnahmen» führen. Die Betonung auf dem Datenschutz ist hier offenkundig aufgrund der Massnahme 15.1.4, welche den «Datenschutz und [die] Vertraulichkeit von personenbezogenen Informationen» betrifft und im Wesentlichen vorschreibt, dass «diese gemäss den Rechtsnormen, Reglementen und allfällig anwendbaren Vertragsbestimmungen gewahrt» werden müssen.

Mit Blick auf eine Datenschutzzertifizierung von Organisationen oder Verfahren muss diese sehr generelle Massnahme natürlich genauer ausgeführt und in Zielsetzungen unterteilt werden, die ihrerseits durch konkrete Schutzmassnahmen erreicht werden können. Dies ist nun im Rahmen eines «Umsetzungsleitfadens» bzw. «Leitfadens zum Datenschutz-Management» im Anhang zu den «Richtlinien über die Mindestanforderungen an das DSMS» vorgesehen. Entsprechend dem Beispiel der OECD und anderer Länder wie Australien, Grossbritannien und Kanada haben wir «9 Datenschutzgrundsätze» als Hauptziele dieses «Leitfadens für die Umsetzung der DSMS-Richtlinien» definiert. Diese Ziele sind bisher in 20 konkrete Datenschutzmassnahmen umgesetzt worden, die in nicht abschliessender Form die wichtigsten Anforderungen aus dem Gesetz oder seiner Vollzugsverordnung aufgreifen. Für eine bessere Lesbarkeit und zum leichteren Verständnis dieses Anhangs ist jede Massnahme gemäss dem Standard ISO 27002 strukturiert, da sie dessen spezifische Ausweitung auf den Datenschutz bildet. Ebenso wie die Massnahme 15.1.4 die ISMS auf die DSMS überträgt, ist die 7. Zielsetzung «Datensicherheit» mit den damit verbundenen Massnahmen nichts anderes als der Verweis der DSMS auf die ISMS. Unter den nach ISO 27002 vorgeschlagenen 133 Sicherheitsmassnahmen wurde eine Vorauswahl der datenschutzrelevantesten Massnahmen getroffen.

Obgleich es natürlich nicht darum geht, für die Erlangung einer DSMS-Zertifizierung eine ISMS-Zertifizierung vorauszusetzen, muss der Zertifizierer dennoch den Umfang der Anerkennung einer bereits vorhandenen ISMS-Zertifizierung, namentlich betreffend die Anforderungen an die «Datensicherheit», von Fall zu Fall beurteilen und darüber entscheiden. Was dagegen die Akkreditierung durch die Schweizerische Akkreditierungsstelle (SAS) anbelangt, so wird die DSMS-Akkreditierung wahrscheinlich als eine Erweiterung der ISMS-Zertifizierung (ISO 27001) vorgesehen, da ein enger und ausdrücklicher Bezug zu den Anforderungen dieser Norm gegeben ist.

Für alle betroffenen Akteure (Akkreditierungsstellen, Zertifizierungsstellen, Zertifizierte, Prüfer, Kontrolleure, usw.) ist hervorzuheben, dass der derzeitige enge Zusammenhang mit den internationalen Normen ISO 27001 und 27002, und nicht zu vergessen den künftigen Normen 27003, 27004, 27005, 27006 und 27007, sinnvoll und vorteilhaft ist in Anbetracht ihrer weit reichenden Anerkennung und Verbreitung im Weltmarkt wie auch ihres wertvollen terminologischen, strukturellen und systematischen Beitrags.

Um die Meinungen der betroffenen Kreise einzuholen, haben wir Ende 2007 eine Vernehmlassung bei den Bundesämtern und eine externe Anhörung eröffnet. Im Allgemeinen wurden die vorgeschlagenen Richtlinien sowie der Umsetzungsanhang eher positiv aufgenommen. Im Lichte der eingegangenen Stellungnahmen arbeiten wir derzeit an einer redaktionellen Neugestaltung der Richtlinien, um ihre Transparenz und Lesbarkeit durch die Einfügung der wesentlichen Elemente aus der ISO-Norm 27001 unter gleichzeitiger Beachtung der urheberrechtlichen Einschränkungen zu verbessern. Auf diese Weise sollte der EDÖB in der Lage sein, diese Richtlinien im Laufe des Frühjahrs 2008 herauszugeben.

1.1.3 Einführung biometrischer Daten in Ausweisen

Die begrenzte und geregelte Verwendung biometrischer Daten für eine bessere Personen-Authentifizierung im Rahmen von Identitätskontrollen und für eine verstärkte Sicherheit der Ausweispapiere widerspricht den Datenschutzprinzipien nicht. Die Verwendung dieser Daten für Identifikationszwecke ist dagegen problematischer und stösst bei uns auf Vorbehalte.

Im Rahmen der Ämterkonsultation zum Bundesbeschluss über die Genehmigung und Umsetzung des Notenaustauschs zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Verordnung (EG) 2252/2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten hatten wir mehrere Bemerkungen betreffend die Ver-

wendung biometrischer Daten anzubringen. Wir haben unseren Standpunkt auch den Staatspolitischen Kommissionen des Ständerates und des Nationalrates unterbreitet. Das Parlament hat indessen unseren Bemerkungen nicht Rechnung getragen und den vom Bundesrat vorgelegten Entwurf verabschiedet.

Die Verordnung (EG) 2252/2004, die im Rahmen der Entwicklung des Besitzstands von Schengen übernommen werden muss, ebenso wie die Empfehlungen der International Civil Aviation Organization (ICAO) und die Gesetzesvorschriften der Vereinigten Staaten sehen die Aufnahme biometrischer Daten (Gesichtsfotografie und Fingerabdrücke) in den Pässen und Reisedokumenten zu Authentifizierungswecken (1:1-Vergleich) vor. Unter Authentifizierung versteht man den Vorgang, mit dem anhand eines Lesegeräts überprüft wird, ob die bei der Ausweiskontrolle erhobenen biometrischen Daten einer Person den Referenzdaten auf dem in dem Dokument enthaltenen elektronischen Datenträger entsprechen. Das Authentifizierungsverfahren erfordert keine zentrale Speicherung der Daten, da die Überprüfung unmittelbar mit Hilfe des Geräts am Kontrollposten erfolgen kann. Eine Aufbewahrung der biometrischen Daten im Informationssystem Ausweise (ISA-Datei) und im Informationssystem zur Ausstellung von schweizerischen Reisedokumenten und von Rückreisevisa an ausländische Personen (ISR-Datei), die über die für die Ausstellung der Dokumente notwendige Zeit hinaus andauert, würde in diesem Fall die Grundsätze der Zweckbindung und der Verhältnismässigkeit verletzen. Wir lehnen jedoch die durch neue Technologien wie der Biometrie gebotenen Möglichkeiten für eine bessere Authentifizierung der Personen im Rahmen von Identitätskontrollen sowie für eine erhöhte Sicherheit der Ausweise nicht ab.

Wir haben dagegen erhebliche Vorbehalte gegenüber der Verwendung biometrischer Daten zu Identifikationszwecken (1:n-Vergleich), die zwangsläufig mit einer zentralen Speicherung der Daten verbunden ist. Eine derartige Bearbeitung sensibler Daten ist zulässig, wenn die Zweckbindung und die Zugriffsrechte auf diese Daten in einer Gesetzesgrundlage im formellen Sinn (Ausweisgesetz) genügend ausführlich geregelt sind. Nur mit einem starren Gesetzesrahmen lassen sich nämlich Risiken von Missbrauch und Auswüchsen sowie die Gefahr einer Verwendung der biometrischen Daten als Zugangsschlüssel zu diversen Datenbanken und damit der Verknüpfung verschiedener Datensätze einschränken. Unseres Erachtens erfüllt die im Rahmen des oben erwähnten Bundesbeschlusses vorgeschlagene Änderung des Ausweisgesetzes die hier genannten Bedingungen nicht. Aus diesem Grund haben wir die Aufbewahrung der biometrischen Daten in den ISA- und ISR-Dateien zu Identifikationszwecken nicht unterstützt.

Auf Ebene der Europäischen Union hat die gemäss Artikel 29 der Richtlinie 95/46/EG eingesetzte Arbeitsgruppe zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten in einem vom 30. September 2005 datierten Gutachten Vorbehalte gegenüber einer nationalen oder europäischen Datenbank für biometrische Elemente geäussert. Das europäische Parlament hat sogar ein Verbot einer zentralisierten Datenbank für Pässe und Reisedokumente mit den biometrischen und anderen persönlichen Daten von sämtlichen Inhabern eines Reisepasses innerhalb der Europäischen Union gefordert.

1.1.4 Vollzugsverordnung zum Registerharmonisierungsgesetz

Wir wurden aufgefordert, im Rahmen von zwei Vernehmlassungsverfahren betreffend die Vollzugsverordnung zum Registerharmonisierungsgesetz Stellung zu nehmen. Es bestehen weiterhin Divergenzen, namentlich betreffend die Sicherheitsmassnahmen für den Datenaustausch auf Kantons- und Gemeindeebene sowie die Modalitäten für die Qualitätskontrolle der Daten. Ausserdem werden gewisse Datenströme nicht erwähnt.

Das am 1. November 2006 in Kraft getretene neue Registerharmonisierungsgesetz (RHG) ist eine der Gesetzesgrundlagen für die Volkszählung 2010. Die Vollzugsverordnung zu diesem neuen Gesetz wurde vom Bundesamt für Statistik (BFS) zwei Vernehmlassungsverfahren unterzogen.

Nach Abschluss dieser Verfahren, in denen wir zu Stellungnahmen aufgefordert waren, bleiben folgende Divergenzen bestehen:

- Sicherheitsmassnahmen für den Datenaustausch auf Kantons- und Gemeindeebene: während die Kommunikationsplattform Sedex (vgl. Ziffer 1.1.7) ein sehr hohes Sicherheitsniveau für den Datenaustausch auf Bundesebene gewährleistet, sind auf Kantons- und Gemeindeebene nicht die gleichen Garantien vorgesehen. Die Kantone und Gemeinden sind nämlich nicht verpflichtet, dasselbe Sicherheitsniveau zu garantieren, wie es die Sedex-Plattform bietet.

- Kontrollmodalitäten für die Datenqualität: der Verordnungsentwurf des BFS sieht die Möglichkeit einer Qualitätsprüfung bei den eingegangenen Daten vor, enthält aber keine genaue Umschreibung der Einzelheiten. Unseres Erachtens ist zu präzisieren, dass die Qualitätskontrolle ausschliesslich auf der Grundlage der zu statistischen Zwecken für die eidgenössische Volkszählung erhobenen Daten erfolgen darf.

Überdies stellt sich bei einem Validierungsdienst für die Qualitätskontrolle von Daten die Frage, welche Datenströme vorliegen, falls fehlerhafte Daten festgestellt werden. Der Entwurf des BFS hat bisher noch keine Antwort darauf geliefert.

1.1.5 Volkszählung 2010

Im Rahmen der Vorbereitungsarbeiten für die Volkszählung von 2010 haben wir die zu berücksichtigenden Datenschutzaspekte im Bereich der Statistik, der Registerharmonisierung und der Zählung untersucht. Wir haben mit dem Bundesamt für Statistik zusammengearbeitet und zu den Entwürfen des Gesetzes über die eidgenössische Volkszählung und der Verordnung über die Registerharmonisierung Stellung bezogen.

Im Jahre 2010 wird die eidgenössische Volkszählung nach einer neuen Methode durchgeführt; zum ersten Mal in der Schweiz erfolgt damit die Volkszählung auf der Grundlage von Informationen aus den Verwaltungsregistern und von Umfragen in ausgewählten Haushalten.

Im Rahmen der Vorbereitungsarbeiten für die Volkszählung 2010 hatten wir zahlreiche Kontakte mit dem Bundesamt für Statistik (BFS) in Form von schriftlichen Stellungnahmen oder Besprechungen, um unseren Beitrag zu den in diesem Amt angestellten Überlegungen zum Schutz von Personendaten zu leisten.

Anlässlich der verschiedenen Vernehmlassungen betonten wir insbesondere die Bedeutung der Einhaltung des Zweckbindungsprinzips, des Sicherheitsniveaus (technische und organisatorische Massnahmen) für den Datenaustausch im Rahmen des Gesetzes über die Registerharmonisierung und des Gesetzes über die Volkszählung, sowie die Modalitäten der Qualitätskontrolle der Daten und den Datenstrom in die Kantone und Gemeinden im Falle von fehlerhaften Daten.

Im Kontext der Volkszählung 2010 sind die Hauptthemenbereiche in Sachen Datenschutz: die Anonymisierung und Löschung der Personendaten, die Einhaltung des Zweckbindungsgrundsatzes (Unterscheidung zwischen statistischen und administrativen Zwecken), die Datensicherheit, das Auskunftsrecht, der Verkehr von Personendaten mit den mit der Durchführung der Umfragen betrauten Drittpersonen oder der Datenrückfluss in die Kantone und Gemeinden, die Registerharmonisierung und die Verwendung der AHV-Nummer als Identifikationselement.

1.1.6 Identifikationsnummer für Unternehmen

Das Bundesamt für Statistik sieht die Einführung einer Identifikationsnummer für Unternehmen vor. Dieses Vorhaben dient gleichzeitig statistischen und administrativen Zwecken. Wir verstehen die Vorteile eines solchen Systems sehr wohl; die geplante Gesetzesgrundlage ist indessen nicht zufriedenstellend. Überdies nehmen mit gewissen Anwendungen, insbesondere den Business-to-Business-Anwendungen, die Möglichkeiten für eine Überwachung und Persönlichkeitsverletzung deutlich zu.

Im Rahmen einer Ämterkonsultation hat uns das Bundesamt für Statistik (BFS) seinen Entwurf für eine Unternehmens-Identifikationsnummer (UID) unterbreitet. Das Vorhaben, das im Jahr 2010 umgesetzt werden sollte, bezweckt eine Vereinfachung des Informationsaustausches innerhalb der Verwaltung (Government to Government, G2G), zwischen Unternehmen und Verwaltung (Business to Government, B2G) sowie zwischen den verschiedenen Unternehmen (Business to Business, B2B). Über die statistische Verwendung hinaus dient das Vorhaben auch administrativen Zwecken.

Das BFS plant, sich bei diesem Vorhaben auf das Betriebs- und Unternehmensregister (BUR) zu stützen. Die gesetzliche Verankerung der Verordnung über das BUR ist im Bundesstatistikgesetz (BStatG) zu finden.

Die mit dem Projekt geplante Zweckbestimmung und Verwendung reichen indessen weit über den statistischen Rahmen hinaus. Es muss daher eine rechtliche Grundlage in Form eines Gesetzes im formellen Sinn erarbeitet werden. Um die Existenz einer solchen Gesetzesgrundlage bei der für 2010 vorgesehenen Inbetriebnahme des Systems sicherzustellen, sollten die Gesetzgebungsarbeiten unverzüglich und gleichzeitig mit den Arbeiten zur technischen Konzeptualisierung des Projekts an die Hand genommen werden.

Die vorgeschlagene Anwendung ist mit Risiken der Persönlichkeitsverletzung verbunden. Die verschiedenen Tätigkeiten der betroffenen Personen könnten nämlich auf der Basis der UID korreliert und zu Profilierungszwecken genutzt werden.

Was die Verwendung der UID innerhalb der Verwaltung sowie zwischen den Unternehmen und der Verwaltung anbelangt, so entsprechen die Anwendungen G2G und B2G gemäss den gelieferten Erklärungen nachweislich dem Verhältnismässigkeitsprinzip. Die ergänzende Verwendung der UID zwischen verschiedenen Unternehmen schafft dagegen sehr viel grössere Möglichkeiten einer Überwachung und Persönlichkeitsverletzung. Diese Risiken sind mit denjenigen vergleichbar, denen anlässlich der letzten

Revision des Bundesgesetzes über die Alters- und Hinterlassenenversicherung Rechnung getragen wurde (Art. 50e AHVG schränkt die Verwendung der neuen AHV-Nummer ein). In der vorgelegten Dokumentation werden jedoch die Risiken betreffend die möglichen Anwendungen im Bereich B2B, wie etwa der Profilierung, nicht analysiert oder auch nur erwähnt. Unseres Erachtens müsste die Verwendung der UID für die B2B-Anwendungen im Rahmen der auszuarbeitenden Bestimmungen untersagt oder zumindest eingeschränkt werden.

1.1.7 Kommunikationsplattform Sedex

Um die elektronische Datenübertragung im Rahmen der Registerharmonisierung und der Volkszählung 2010 zu ermöglichen, hat das Bundesamt für Statistik eine Kommunikationsplattform eingerichtet. Bei der Ausgestaltung des Systems wurde das Schwergewicht auf den Schutz und die Sicherheit der Daten gelegt. Das Endprodukt entspricht in allen Teilen den Datenschutzanforderungen.

Die Registerharmonisierung und die Volkszählung 2010 sind mit der elektronischen Übermittlung einer Vielzahl von Personendaten zwischen den verschiedenen Akteuren (Bundes-, Kantons- und Gemeindebehörden) verbunden. Die fraglichen Daten betreffen sämtliche Aspekte im Leben der Bürgerinnen und Bürger und sind in diesem Kontext verstärkt schützenswert. Die Notwendigkeit, jeden missbräuchlichen Zugriff auf die Daten zu verhindern, ist offenkundig. In diesem Rahmen hat das Bundesamt für Statistik (BFS) die Datenaustauschplattform Sedex (secure data exchange) entwickelt.

Sedex beruht auf einer Public-Key-Infrastruktur (PKI) und einer robusten Verschlüsselung der ausgetauschten Informationen, so dass die Vertraulichkeit der Daten gewährleistet ist. In der Praxis wird jeder Akteur seinen eigenen asymmetrischen Schlüssel besitzen (d.h. einen öffentlichen, allen betroffenen Akteuren bekannten Teil, und einen privaten Teil).

Es gilt nicht nur, die Vertraulichkeit der Daten zu gewährleisten, sondern auch sich zu vergewissern, dass der Datenabsender tatsächlich die Person ist, für die er sich ausgibt. Dank der im Rahmen von Sedex vorgesehenen PKI-Infrastruktur kann der Absender mit Hilfe des privaten Teils seines Schlüssels seine Nachrichten digital signieren, während die Empfänger anhand des öffentlichen Schlüsselteils die Identität des Absenders überprüfen können.

Schliesslich ist sicherzustellen, dass die Nachrichten ihren Bestimmungsort auch wirklich erreichen und dass dem Absender gegebenenfalls die Nichtzustellung der Nachricht mitgeteilt wird. Zu diesem Zweck bewahrt die Sedex-Plattform sämtliche

noch nicht zugestellten Nachrichten in einem zentralen Server auf. In der Praxis wird eine versendete Nachricht dem Empfänger nicht unmittelbar zugestellt, sondern in einem individuellen Postfach (der nur durch den Empfänger geöffnet werden kann) bei einem zentralen Server hinterlegt. Mit periodisch ergehenden Aufforderungen kann der Empfänger die allfällige Präsenz von ihn betreffenden Nachrichten überprüfen. Wird die Nachricht vom Empfänger nicht binnen einer gewissen Frist gelesen, wird sie beim Server gelöscht und der Absender wird über das Problem informiert, damit er entsprechend reagieren kann. Ein solches Vorgehen ermöglicht die Kontrolle über die Zustellung der Nachrichten.

In Anbetracht der Eigenschaften des Sedex-Systems können wir eine weitgehend positive Beurteilung abgeben. Diese Feststellung hat sich bei der öffentlichen Vorführung eines betriebsbereiten Prototyps des Systems bestätigt.

1.1.8 Schwarze Listen und Persönlichkeitsschutz

Hotel- und Restaurantbetreiber müssen sich regelmässig mit Kunden auseinandersetzen, die sich ungebührlich benehmen, ihre Rechnungen nicht bezahlen, Schäden verursachen oder sich anderen Kunden gegenüber aggressiv verhalten. Geschädigte Gastwirte, Betreiber von Nachtclubs oder Hoteliers sind mit der Anfrage an uns gelangt, ob sie eine gemeinsame Datenbank für ähnliche Betriebe schaffen könnten, um sich unangenehme Überraschungen zu ersparen. Nachdem wir zum Schluss gelangt sind, dass ein überwiegendes privates Interesse an der Einrichtung einer solchen Datensammlung bestehen kann, haben wir genauer ausgeführt, unter welchen Voraussetzungen eine solche Massnahme zulässig ist.

Aufgrund der ungebührlichen Verhaltensweisen von Seiten gewisser unangenehmer Kunden haben uns Verantwortliche von Hotels und Gaststätten und verwandten Betrieben angefragt, ob sie eine Datenbank einrichten könnten, um den durch diese Personen verursachten Schaden zu verhindern und ihre Betriebe so weit wie möglich zu schützen.

Die Beschaffung von Informationen über Personen, die sich ungebührlich verhalten, und ihre Registrierung in einer Datenbank stellen eine Datenbearbeitung im Sinne des DSG dar. Da diese für die betroffenen Personen eine Persönlichkeitsverletzung bedeuten kann, muss die Person, welche die Daten erhebt, einen Grund zur Rechtfertigung dieser Bearbeitung geltend machen können. Im vorliegenden Fall kann das überwiegende private Interesse der Betreiber eine Bearbeitung von Personendaten

grundsätzlich rechtfertigen. Die Person, welche die Daten bearbeitet, muss sich jedoch an die allgemeinen Grundsätze des DSG halten. Sie muss namentlich die betroffenen Personen über den Zweck und die Bedingungen der Datenbearbeitung klar informieren (Transparenzprinzip) und darf nur die für den Zweck der Datenbearbeitung geeigneten und notwendigen Personendaten bearbeiten (Grundsatz der Zweckbindung und Verhältnismässigkeit).

In diesem Kontext haben wir eine Anzahl Regeln definiert, um sicherzustellen, dass die geplante Massnahme im Einklang mit dem DSG und seinen Prinzipien steht, und wir haben den Betreibern empfohlen, vor der Einführung einer solchen Massnahme ein Datenbearbeitungskonzept zu entwickeln. Diese Regeln sind im Anhang 4.1 zu finden.

1.1.9 Postmortaler Persönlichkeitsschutz

Datenschutz ist Persönlichkeitsschutz. Die juristischen Diskussionen rund um die Persönlichkeit und die Persönlichkeitsverletzung sind für unsere Behörde daher von grosser Bedeutung. Eine Streitfrage, die in diesem Rahmen immer wieder auftaucht, betrifft den Schutz der Persönlichkeit über den Tod hinaus. Sie ist für uns vor allem im Zusammenhang mit dem Auskunftsrecht relevant: Der Fall der Auskunft nach dem Tod ist in der Verordnung zum Datenschutzgesetz zwar geregelt, in der praktischen Anwendung der Bestimmung gibt es aber immer wieder offene Fragen.

Am einfachsten lässt sich die juristisch komplexe Problematik anhand eines praktischen Beispiels verdeutlichen. So stellt sich die Frage nach dem postmortalen Persönlichkeitsschutz etwa dann, wenn eine Person um Einsicht in Akten einer Versicherungsgesellschaft nachsucht, die einen verstorbenen Angehörigen betreffen, der Versicherer die Herausgabe mit dem Hinweis auf den Datenschutz aber verweigert.

Grundsätzlich ist die Zurückhaltung des Versicherers aus der Optik des Datenschutzes zu begrüssen. Im vorliegenden Falle kann man sich mit diesem Hinweis aber nicht begnügen, da die Verordnung zum Datenschutzgesetz (VDSG) den Angehörigen einen Anspruch auf die Datenherausgabe einräumt, wenn sie ein Interesse daran nachweisen können und keine überwiegenden Interessen Dritter auszumachen sind. Dabei müssen all jene Personen keinen Interessennachweis erbringen, die mit dem/der Verstorbenen nahe verwandt oder verheiratet sind (Art. 1 Abs. 7 VDSG).

Auch an dieser Stelle der Prüfung darf man es sich nicht zu einfach machen: Dass der Interessennachweis beim Vorliegen eines Verwandtschaftsverhältnisses oder einer Ehe entfällt, bedeutet nicht, dass deswegen eine Interessenabwägung überflüssig wäre. Man muss nach den Motiven der Parteien fragen, sowohl was das Ansinnen der Datenherausgabe als auch deren Verweigerung angeht.

Die Rechtsprechung ist bezüglich der Datenherausgabe an Angehörige eher zurückhaltend. Werden die Daten für eine rechtliche Auseinandersetzung gebraucht, ist die Datenbekanntgabe auf jene Informationen zu beschränken, die sich auf den künftigen Prozessgegenstand beziehen. Bei medizinischen Akten ist ausserdem zu berücksichtigen, ob und inwieweit der Persönlichkeitsschutz der Verstorbenen gewahrt werden kann, indem man zwar keine direkte Einsichtnahme in die Akten zulässt, die Informationen aber durch einen Arzt mit Akteneinsicht kommunizieren lässt (Filterfunktion).

Die Interessenabwägung kann nur unter Berücksichtigung der fallbezogenen Gegebenheiten vorgenommen werden. Wir können deshalb Herausgabegesuche nicht abschliessend beurteilen. Im eingangs erwähnten Beispiel haben wir immerhin eine Auslegeordnung der wichtigsten Argumente erstellt, um damit eine einvernehmliche Lösung zwischen den Parteien nach Möglichkeit zu befördern.

1.2 Datenschutzfragen allgemein

1.2.1 Einsatz von Überwachungsgeräten an der Schweizer Grenze

Die Verordnung über den Einsatz von Bildaufnahme-, Bildaufzeichnungs- und anderen Überwachungsgeräten durch die Eidgenössische Zollverwaltung, die auf den 1. Mai 2007 in Kraft getreten ist, schafft detaillierte Ausführungsbestimmungen für den Einsatz von Überwachungsgeräten an der Schweizer Grenze. Sie bezeichnet die zulässigen Geräte sowie deren Einsatzbereiche und regelt die Verantwortlichkeiten und die Aufbewahrungsdauer der Aufzeichnungen.

Zum dritten Mal in Folge beschäftigten wir uns mit dem Einsatz von Überwachungsgeräten (wie Drohnen oder mit Infrarot-Systemen ausgerüstete Helikopter) an der Schweizer Grenze (s. 13. Tätigkeitsbericht 2005/2006; Ziffer 2.2.1, 14.Tätigkeitsbericht 2006/2007, Ziffer 1.2.2). Der von der Zollverwaltung in die Ämterkonsultation geschickte Entwurf zur «Verordnung über den Einsatz von Bildaufnahme-, Bildaufzeichnungs- und anderen Überwachungsgeräten durch die Eidgenössische Zollverwaltung» bedurfte aus datenschutzrechtlicher Sicht zahlreicher Verbesserungen.

So stellten wir uns beispielsweise gegen die zu allgemeine Umschreibung, wonach die zulässigen Geräte «statische oder bewegte visuelle Signale» und «akustische Signale aufnehmen und aufzeichnen» können. Stattdessen forderten wir aus Transparenz- und Verhältnismässigkeitsgründen eine klare, abschliessende Bezeichnung aller Einsatzgeräte, die zur Überwachung eingesetzt werden dürfen (wie beispielsweise Fotokameras, Wärmebildgeräte, Bewegungsmelder, Funkpeilung). Darüber hinaus verlangten wir, dass die Verordnung den Einsatzbereich für jedes einzelne Überwachungsgerät klar bezeichnet und abschliessend regelt, zu welchen Zwecken es eingesetzt werden darf. Weiter stellten wir uns gegen eine Aufbewahrungsdauer von drei Monaten und einigten uns schliesslich mit der Zollverwaltung darauf, dass die Aufzeichnungen grundsätzlich nach einem Monat zu löschen sind.

Wir regten eine Bestimmung an, die zwei wichtige Grundsätze für jeden Einsatz festhält: Erstens ist jeder mobile Einsatz zeitlich zu befristen. Zweitens muss mit Blick auf die im revidierten Datenschutzgesetz statuierte Informationspflicht die Öffentlichkeit durch geeignete Massnahmen auf den Einsatz der Überwachungsgeräte hingewiesen werden (beispielsweise durch Hinweisschilder, vorgängige Ankündigung im Internet oder in lokalen Medien). Dieser Hinweis darf lediglich unterbleiben, wenn er den Zweck des Einsatzes gefährden würde.

Die Zollverwaltung kam unseren Forderungen mehrheitlich nach und passte die Bestimmungen entsprechend an. Nicht durchgedrungen sind wir mit unserer Forderung, wonach die Verordnung jene Bereiche (z.B. dicht besiedelte Gebiete, das Landesinnere) hätte bezeichnen müssen, in denen überhaupt keine Überwachung stattfinden darf. Wir hatten uns dabei an einer Stellungnahme des Bundesrates zur Motion 05.3804 orientiert, in der er sich explizit dagegen ausspricht, dass Drohnen in diesen zwei Einsatzbereichen zum Einsatz gelangen sollen. Bedauerlich ist das Nichtbeachten unserer Forderung vor allem deshalb, weil die Verordnung nun nicht mehr nur den Einsatz von Drohnen, sondern von zahlreichen Überwachungsgeräten zulässt.

1.2.2 Überwachung mittels Mikrodrohnen

Das Bundesamt für Zivilluftfahrt wandte sich in Zusammenhang mit dem Einsatz von Mikrodrohnen, die mit Kameras ausgerüstet sind, an uns. Allgemein gilt, dass Personen, die solche Mikroüberwachungsdrohnen in Betrieb nehmen wollen, die Datenschutzgesetzgebung beachten müssen.

Das BAZL wurde wiederholt mit dem möglichen Betrieb von so genannten Mikrodrohnen konfrontiert. Dabei handelt es sich um unbemannte Luftfahrzeuge unter 30 kg, für die in der heutigen Gesetzgebung keine Bewilligungspflicht besteht. Das BAZL überlegt sich nun, ob und wie diese Mikrodrohnen einer Bewilligungspflicht unterstellt werden sollen. Da diese auch mit Kameras ausgerüstet werden können, wandte sich das Bundesamt an uns. Allgemein kann festgehalten werden, dass Personen, die Mikrodrohnen mit Kameras in Betrieb nehmen wollen, die Datenschutzgesetzgebung beachten müssen, sobald bestimmte oder bestimmbare Personen von der Kamera erfasst werden. Gegenüber dem BAZL hielten wir fest, dass wir es begrüssen würden, wenn auch seinerseits nach Möglichkeit auf die zu beachtende Datenschutzgesetzgebung hingewiesen würde, sei dies im Zusammenhang mit einer allfälligen Bewilligung, sei es auf andere Weise. Das BAZL wird nun betreffend Mikrodrohnen ein Grobkonzept ausarbeiten und uns in Hinblick auf Datenschutzaspekte beiziehen.

1.2.3 Der Einsatz von datenschutzfreundlichen Technologien bei der Videoüberwachung

Grundsätzlich soll aus Sicht des Datenschutzes nur auf Videoüberwachung zurückgegriffen werden, wenn keine weniger stark in die Persönlichkeit eingreifende Massnahmen verfügbar sind. Wird eine Videoüberwachung durchgeführt, so sind – insbesondere im öffentlichen Bereich und im Dienstleistungssektor – möglichst datenschutzrechtliche Technologien anzuwenden.

Gegen eine Videoüberwachung im Dienste der Sicherheit ist auch aus datenschutzrechtlicher Sicht nichts einzuwenden, solange bei ihrem Einsatz die Rechte und Freiheiten bezüglich der Bearbeitung von Personendaten garantiert bleiben. Datenschutzfreundliche Technologien bei der Videoüberwachung haben stets dem Verhältnismässigkeitsprinzip zu genügen. Nach diesem Grundsatz dürfen jeweils nur die Personendaten – in diese Kategorie gehören auch Bilder von Personen – bearbeitet werden, die geeignet und notwendig sind, um den vorgängig genau definierten Zweck zu erfüllen.

Inzwischen existieren im Bereich der Videoüberwachung Technologien, die es ermöglichen, die aufgenommenen Objekte – insbesondere Personen – zur Unkenntlichkeit zu verwischen, mithin die Daten zu verschlüsseln. Bei Bedarf – z. B. bei Vorliegen einer strafbaren Handlung – können die verwischten Objekte nachträglich entschlüsselt und differenziert erkennbar gemacht werden. Dank dieser Technologie ist es nun möglich, öffentliche Räume im Dienst der Sicherheit zu überwachen, ohne den Schutz der Privatsphäre zu beeinträchtigen.

Auch eine solche datenschutzfreundlichere Videoüberwachung bietet indessen keine Garantie dafür, dass Personendaten nicht unrechtmässig bearbeitet werden. Wichtig beim Einsatz dieser Technologien ist insbesondere, dass die Entschlüsselung der verwischten Objekte tatsächlich nur einer beschränkten Anzahl vertrauenswürdiger Personen zusteht. Am zweckdienlichsten ist es, die Verantwortung entsprechend dem «Vier-Augen-Prinzip» auf mindestens zwei Personen zu verteilen. Nur so kann dem Risiko einer unrechtmässigen Datenbearbeitung wirkungsvoll begegnet werden.

1.2.4 Bundesgesetz über die militärischen Informationssysteme

Die neueste Fassung des Entwurfs für das Bundesgesetz über die militärischen Informationssysteme, der im September 2007 in die Ämterkonsultation ging, unterscheidet sich von den früheren Fassungen durch eine detailliertere Regelung der Verwendung von Überwachungsmitteln.

Im Rahmen der Arbeiten zur Revision der Militärgesetzgebung (vgl. unseren 14. Tätigkeitsbericht 2006/2007, Ziff. 1.2.3), haben wir beim Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) unsere ablehnende Haltung gegenüber einer knappen Regelung der Verwendung von Überwachungsmitteln zum Ausdruck gebracht. Jegliche Form der staatlichen Überwachung bedeutet einen schwerwiegenden Eingriff in die Grundrechte und muss auf einer klaren und genügend ausführlichen Gesetzesgrundlage beruhen. Das VBS hat im September 2007 eine neue Fassung des Entwurfs für das Bundesgesetz über die militärischen Informationssysteme, der die Verwendung von Überwachungsmitteln ausführlicher regelt, in die Ämterkonsultation gegeben. Diese Bestimmungen definieren das für den Einsatz der Überwachungsmittel verantwortliche Organ, aber auch die mit diesen Massnahmen verfolgten Zwecke sowie die Vorschriften betreffend die Bearbeitung von Personendaten (Beschaffung, Bekanntgabe und Aufbewahrung). Der Gesetzesentwurf wurde dem Parlament vorgelegt.

1.2.5 Nachkontrolle im Sportzentrum KSS und Verwendung von Systemen für biometrische Erkennung

Bei der Nachprüfung der Umsetzung unserer Empfehlungen konnten wir uns davon überzeugen, dass sämtliche Empfehlungen angenommen und befolgt worden sind, mit Ausnahme der Forderung nach einer dezentralisierten Speicherung, deren Einführung bisher noch ungewiss ist.

Im Anschluss an die Kontrolle in den «KSS Sport- und Freizeitanlagen Schaffhausen» veröffentlichten wir im Jahre 2006 einen Bericht mit fünf Empfehlungen betreffend das dort für die Zutrittskontrolle verwendete System der biometrischen Erkennung.

In diesen Empfehlungen ging es um Folgendes: Vorschlag für eine preisgleiche Ersatzlösung für Personen, welche die Erhebung ihrer biometrischen Daten ablehnen; dezentralisierte Speicherung der Daten auf einem Chip auf der Abonnentenkarte; automatische Löschung der Kundendaten binnen 18 Monaten ab dem letzten Kontakt; Anonymisierung der Kundenverkehrsdaten; Löschung der noch in der Datenbank gespeicherten biometrischen Daten binnen einer Frist von drei Monaten.

Im Laufe des vergangenen Jahres haben wir das KSS-Zentrum zweimal aufgesucht, um den Fortschritt bei der Umsetzung der Empfehlungen zu überprüfen. Dabei konnten wir feststellen, dass mit Ausnahme der dezentralisierten Speicherung die Empfehlungen übernommen und befolgt worden sind.

Wie die letzte Besprechung ergab, sollte die Umsetzung der Empfehlung betreffend die dezentralisierte Speicherung ab Januar 2009 möglich sein. Die KSS haben indessen im Februar bestätigt, dass Sie unsere Empfehlung nicht akzeptieren. Wir werden nun die weiteren Schritte in dieser Angelegenheit prüfen.

In diesem Kontext haben wir den Einfluss der Systeme für biometrische Erkennung auf die persönliche Freiheit eingehend analysiert.

Unsere Arbeiten beziehen sich im Wesentlichen auf die Funktionsweise der heute eingesetzten verschiedenen Technologien, die Regelung und die Evaluationskriterien für die zur Privatsphäre gehörenden Faktoren im Zusammenhang mit den Systemen der biometrischen Erkennung.

Darüber hinaus haben wir an einem Symposium teilgenommen, bei dem die wichtigsten Fragen behandelt wurden, die sich aufgrund der zunehmenden Verwendung von Systemen der biometrischen Erkennung zur Identifizierung oder Authentifizierung von Personen und der Einrichtung von Biobanken mit einer wachsenden Anzahl biologischer Proben stellen.

1.2.6 Die Aussagekraft von Betreibungsregisterauszügen

Die Kreditwürdigkeit ist für die Teilnahme am Wirtschaftsleben von zentraler Bedeutung. Da der Betreibungsregisterauszug zu diesem Thema Auskunft gibt, ist er ein brisantes Dokument. Es wird bisweilen aber nicht richtig verstanden, dass einige der Einträge auf dem Auszug mit der Kreditwürdigkeit nichts zu tun haben. Der Versuch, die Gefahr von Fehlinterpretationen mittels einer parlamentarischen Initiative zu beseitigen, scheiterte an der Vielfalt der Auffassungen, auf welche Weise dies geschehen müsste.

Eine Betreibung ist zunächst einmal nichts anderes als die Behauptung einer Geldschuld. Wer sich gegen diese Behauptung mit Erfolg zur Wehr setzt, hat ein grosses Interesse daran, dass der Betreibungsauszug über diesen Vorgang keine Auskunft gibt. Das Gleiche gilt auch dann, wenn die Behauptung nach dem Rechtsvorschlag der betroffenen Person nicht bekräftigt wird und die Betreibung deshalb nach Ablauf eines

Jahres nicht mehr fortgesetzt werden kann. Die entsprechenden Einträge auf dem Betreibungsregisterauszug geben keine Auskunft über die Kreditwürdigkeit, da der Vorgang nicht auf eine mangelnde Liquidität der betroffenen Person schliessen lässt.

Auf Betreiben des damaligen Nationalrats Jean Studer wurde eine parlamentarische Initiative lanciert (04.467s Pa. Iv.), mit der die Gefahr von Missverständnissen wenigstens minimiert werden sollte. Der Vorschlag bestand darin, die Anzeigedauer von nicht fortgesetzten Betreibungen auf dem Auszug zu verkürzen (Revision von Art. 8a SchKG). Die für die Behandlung der Initiative zuständige Rechtskommission des Ständerats holte daraufhin eine Stellungnahme des EDÖB sowie verschiedener Fachorgane im Bereich der Schuldbetreibung ein.

Wir haben die Rechtskommission darauf hingewiesen, dass eine Verkürzung der Anzeigedauer das Problem nicht aus der Welt schafft, da die einmal eingeholten Betreibungsregisterauszüge im Privatsektor weiter kursieren. Dies geschieht namentlich über die Bonitätsauskünfte von Kreditauskunfteien. Diese sind sich offenbar nicht alle bewusst, dass die Weitergabe veralteter Betreibungsregisterauszüge mit dem Datenschutzgesetz nicht vereinbar ist (Datenaktualität als Aspekt der Datenrichtigkeit).

Wir sind vor diesem Hintergrund der Auffassung, dass ein zuverlässiger Schutz vor kreditschädigender Fehlinterpretation nur dann besteht, wenn die oben problematisierten Einträge auf den Auszügen gar nicht aufgeführt werden. Wir haben der Rechtskommission empfohlen, diesen Punkt im Rahmen der Revision von Art. 8a SchKG zu berücksichtigen.

Die anderen Vernehmlassungsteilnehmer waren zumeist ebenfalls der Meinung, die Aussagekraft der Betreibungsregisterauszüge sei mangelhaft, sie hatten aber andere Vorstellungen, auf welche Weise dies sinnvollerweise geändert werden könnte. Vereinzelt wurde auch die Meinung vertreten, die Interessen der Schuldner seien schon heute sehr stark gewichtet und diese bedürften keines zusätzlichen Schutzes. Angesichts dieser teils erheblich voneinander abweichenden Stellungnahmen wurde die parlamentarische Initiative Jean Studer schliesslich abgeschrieben. Wir werden unsere Bemühungen für einen Schutz vor kreditschädigender Datenbearbeitung mittels Massnahmen im Privatbereich fortführen (vgl. auch Ziff. 1.8.3 des vorliegenden Tätigkeitsberichts).

1.2.7 Anmeldung von Flugpassagieren bei Zoll- und Polizeibehörden im Fall von Flughäfen ohne Zoll

Im Rahmen von grenzüberschreitenden Flügen nach schweizerischen Flugplätzen, die nicht über einen Zoll verfügen, muss der Pilot die Passagiere anhand eines auf der Website des Flugplatzes auszufüllenden Formulars anmelden. Die Daten werden danach ungesichert per E-Mail an die Zoll- und Polizeibehörden gesandt. Aufgrund der begrenzten Anzahl betroffener Personen und der Tatsache, dass es auf zahlreichen Flugplätzen einen Zoll gibt, sind wir der Meinung, dass eine Datenschutzerklärung eine angemessene Massnahme darstellt.

In der Schweiz gibt es an einigen kleinen Flugplätzen keinen Zoll. Aus dem Ausland kommende Flugzeuge sind dort landeberechtigt, die Zollformalitäten müssen jedoch vor dem Abflug erledigt werden. Der Pilot muss insbesondere sämtliche Passagiere (sich selbst eingeschlossen) anhand eines auf der Website des Flugplatzes auszufüllenden Formulars anmelden. Die Daten werden danach ungesichert per E-Mail den Zoll- und Polizeibehörden zugesandt. Während es bis vor kurzem noch möglich war, diese Formalität über Telefax zu erledigen, schreibt nunmehr ein neues Zollreglement ihre Abwicklung auf elektronischem Weg vor. Es stellt sich die Frage, ob eine ungesicherte Übermittlung dieser Daten per E-Mail zulässig ist.

Unter Berücksichtigung der Tatsache, dass die Passagiere einen der zahlreichen mit einem Zollposten ausgestatteten Flugplätze wählen könnten und dass die Zahl der betroffenen Personen sehr begrenzt ist, halten wir die Einrichtung eines gesicherten elektronischen Nachrichtenübermittlungssystems für unverhältnismässig. Wir haben dagegen verlangt, dass die betreffenden Flugplätze auf ihren Websites und auf den Zollmeldeformularen eine Datenschutzerklärung veröffentlichen.

Nach Massgabe des Bundesgesetzes über den Datenschutz (DSG) muss die Datenschutzerklärung möglichst transparent sein und mindestens folgende Informationen enthalten: den Bearbeitungszweck, zu dem die Daten beschafft werden, die Kategorien der Datenempfänger, die Dauer der Datenaufbewahrung und die Tatsache, dass die Datenübertragung nicht sicher ist.

1.2.8 Datenschutz bei Unternehmensgründern im Bereich elektronischer Medien

Durch die Verwendung von elektronischen Medien entstehen immer neue Geschäftsideen, bei welchen personenbezogene Daten bearbeitet werden. Die Unternehmensgründer tragen den Anforderungen des Datenschutzes im Rahmen ihrer Geschäftsmodelle allerdings nicht immer genügend Rechnung, so dass teilweise ein erhöhtes Risiko einer Persönlichkeitsverletzung durch einen unsachgemässen Gebrauch der angebotenen elektronischen Produkte oder Dienstleistungen bestehen kann. Daher mahnen wir vor allem bei innovativen Geschäftsideen in der digitalen Welt zu einer erhöhten Aufmerksamkeit im Hinblick auf datenschutzrechtliche Probleme.

Elektronische Medien bieten heute immer vielfältigere Möglichkeiten, neue Geschäftsmodelle zu entwerfen sowie digitale Produkte und Dienstleistungen über das Internet oder mobile Informationskanäle anzubieten. Oft wird allerdings hierbei von Unternehmensgründern dem Datenschutz zu wenig Beachtung geschenkt. Auch wenn bei digitalen Produkten und Dienstleistungen manchmal aufgrund des Geschäftsmodells kein absoluter Datenschutz gewährleistet werden kann, so muss der Anbieter dennoch das Risiko einer Persönlichkeitsverletzung, die sich durch einen unsachgemässen Gebrauch seines Angebots ereignet, minimieren. Im konkreten Fall bietet eine Unternehmung einen Service an, mit welchem an registrierte Verkehrsteilnehmer anhand des Fahrzeugkennzeichens SMS versendet werden können. Die Registrierung bei diesem Service kann ebenfalls via SMS durchgeführt werden, indem man eine entsprechende Kurznachricht, welche auch das Fahrzeugkennzeichen enthält, an den Service schickt. Auf diese Weise wird dem Fahrzeugkennzeichen eine Mobiltelefonnummer zugeordnet und der vermeintliche Fahrer bzw. Fahrzeughalter kann somit über diesen SMS-Service von nun an Nachrichten empfangen.

Aus datenschutzrechtlicher Sicht birgt dieses Geschäftsmodell das Risiko, dass eine dritte Person auf seine Mobiltelefonnummer das Kennzeichen eines Fahrzeugs registriert, dessen Halter er nicht ist oder welches er nicht benutzt. Dies könnte sogar ohne Wissen und Einverständnis des Halters oder Fahrers geschehen. So ist es beispielsweise denkbar, dass ein eifersüchtiger Freund das Fahrzeug seiner Freundin auf seine Mobiltelefonnummer registrieren lässt, um zu erfahren, ob sie von anderen Autofahrern angesprochen wird. Ein solches Vorgehen könnte je nach Ausmass den Charakter einer teilweisen Überwachung des Fahrzeuglenkers annehmen. Um dies zu verhindern sind daher in Bezug auf die Registrierung für diesen Service entsprechende Sicherheitsmassnahmen zu ergreifen.

Auf der anderen Seite kann dieser SMS-Service nur funktionieren, wenn er einfach und schnell zu handhaben ist. Er würde wohl nicht nachgefragt werden, wenn er aufwändige Registrierungen erfordern würde. Daher wurde nach Lösungsmöglichkeiten gesucht, um einen solchen Missbrauch bestmöglich zu unterbinden und das Risiko einer Persönlichkeitsverletzung zu minimieren, ohne dabei das Geschäftsmodell des Anbieters zu zerstören. Daher haben wir dem Anbieter empfohlen, nach der Registrierung eines Fahrzeugkennzeichens die Namen der registrierten Person mit dem öffentlich zugänglichen Namen des Fahrzeughalters zu vergleichen sowie die Anzahl der auf eine Mobiltelefonnummer registrierbaren Fahrzeugkennzeichen zu beschränken. Zudem hat der Anbieter die Möglichkeit einer exklusiven Registrierung geschaffen, bei welcher die Identitätsdaten verifiziert werden.

Das Risiko einer Persönlichkeitsverletzung konnte mit diesen Massnahmen zwar verringert, nicht aber vollkommen ausgeschlossen werden. Weitergehende Massnahmen hätten das Geschäftsmodell wohl verunmöglicht. Im Falle einer Persönlichkeitsverletzung kann sich der Anbieter des Services also dennoch mit einer Zivilklage konfrontiert sehen. Er trägt somit beim Angebot seines Services nach wie vor ein nicht unerhebliches Risiko.

1.3 Internet und Telekommunikation

1.3.1 Internet-Tauschbörsen und Datenschutz

Wir haben die Datenbearbeitung eines im Bereich der Bekämpfung von Urheberrechtsverletzungen tätigen Unternehmens untersucht und festgestellt, dass die Datenbeschaffung in den Peer-to-Peer-Tauschbörsen den Grundprinzipien des DSG nicht gerecht wird. Dabei stellen wir aber die Legitimität der strafrechtlichen Verfolgung von Urheberrechtsverletzungen keineswegs in Frage. Wie wir jedoch bemerkt haben, missbrauchen in der Praxis die Urheberrechtsinhaber ihr Akteneinsichtsrecht im Rahmen eines Strafverfahrens, um die Identität der Inhaber des Internetzugangs zu erfahren, und so umgehen sie das Telekommunikationsgeheimnis im Bereich des Privatrechts. Unseres Erachtens erfordert eine Verletzung des Telekommunikationsgeheimnisses im zivilen Bereich eine ausdrückliche Gesetzesgrundlage. Wir haben dem betreffenden Unternehmen empfohlen, die Datenbearbeitung einzustellen.

Im Auftrag der Medienindustrie forscht ein schweizerisches Unternehmen (im Folgenden X AG) in den Peer-to-Peer-Netzwerken (P2P) nach Urheberrechtsverletzungen in den Tauschbörsen für Musik- und Video-Dateien im Internet. Speziell für diesen Zweck hat das betreffende Unternehmen eine Software entwickelt, welche im Geheimen und automatisch die elektronischen Spuren ermittelt, die der Benutzer der P2P-Software hinterlässt, mit der die urheberrechtlich geschützten Werke illegal verfügbar gemacht werden. Diese Daten, die namentlich die IP-Adressen umfassen, werden ohne Wissen der betroffenen Personen (einschliesslich des möglicherweise gutgläubigen Inhabers des Internetzugangs) registriert und in regelmässigen Abständen den Inhabern des Urheberrechts an dem betreffenden Werk oder ihren gesetzlichen Vertretern, in den meisten Fällen im Ausland, bekannt gegeben.

Die im Besitz der Anbieter von Telekommunikationsdiensten befindlichen Daten betreffend die IP-Adresse (wie Name und Adresse des Inhabers des Internetzugangs) sind durch das Telekommunikationsgeheimnis geschützt. Nur im Rahmen einer Strafuntersuchung darf die Identität des Inhabers des Internetzugangs den Untersuchungsbehörden bekannt gegeben werden. Aus diesem Grunde reichen die Urheberrechtsinhaber oder ihre gesetzlichen Vertreter bei den zuständigen Untersuchungsbehörden Strafklage gegen Unbekannt unter Vorlage der von der Firma X AG erhobenen Daten ein. Sie erhalten sodann im Rahmen des Strafverfahrens Akteneinsicht und beschaffen

sich auf diese Weise die Adresse des Inhabers der IP-Adresse (der nicht unbedingt mit dem Urheber der Rechtsverletzung identisch ist). In der Folge machen sie noch vor der strafrechtlichen Verurteilung des Urhebers der Zuwiderhandlung ihre zivilrechtlichen Ansprüche in Form von Schadenersatzforderungen für die Verfügbarmachung des Werkes geltend.

Die erhobenen Daten (insbesondere die IP-Adresse) sind insofern Personendaten, als mit ihrer Hilfe bestimmte Personen indirekt identifiziert werden können. Die Bearbeitung dieser Daten untersteht dem DSG. Da die von der Firma X AG angewendeten Bearbeitungsmethoden die Privatsphäre zahlreicher Personen ohne deren Wissen verletzen können, haben wir den Sachverhalt untersucht.

Wir prüften, ob die Grundsätze des Datenschutzes, insbesondere die Prinzipien der Rechtmässigkeit, der Zweckbindung, von Treu und Glauben und der Transparenz, sowie der Verhältnismässigkeitsgrundsatz eingehalten werden. Wir untersuchten auch die Frage, ob ein Grund – insbesondere ein überwiegendes privates Interesse – vorliegt, der eine solche Datenerhebung rechtfertigen würde.

Gemäss dem Rechtmässigkeitsgrundsatz dürfen Personendaten nur auf gesetzlich zulässige Weise bearbeitet werden. Aufgrund der geltenden Gesetzgebung ist eine systematische Beschaffung von IP-Adressen in den Tauschbörsen weder ausdrücklich erlaubt noch untersagt. Wir sind indessen der Ansicht, dass eine solche Datenbearbeitung – die ohne Wissen der betroffenen Personen, proaktiv und zu Strafverfolgungszwecken erfolgt – in einer ausdrücklichen Gesetzesgrundlage geregelt sein sollte.

Dem Grundsatz der Zweckbindung zufolge dürfen Personendaten nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist. Im vorliegenden Fall werden die Verbindungsdaten zugänglich gemacht, um den Austausch der Inhalte zu ermöglichen. Die systematische Beschaffung und Registrierung von Daten, um Urheberrechtsverletzungen aufzuspüren, sind nicht im Einklang mit dem ursprünglich verfolgten Ziel: Diese Zweckänderung ist nicht in einem Gesetz vorgesehen und auch nicht erkennbar für die Softwarebenutzer – und keinesfalls für den Inhaber der IP-Adresse. Die Firma X AG verstösst mit ihrem Vorgehen gegen das Zweckbindungsprinzip.

Nach dem Transparenzprinzip muss eine Datenbearbeitung für die betroffene Person erkennbar sein; sie hat darüber informiert zu werden oder muss aufgrund der Umstände damit rechnen können. Im vorliegenden Fall erfolgt die Datenbeschaffung ohne Wissen der betroffenen Personen (ob das nun der Inhaber des Internetzugangs oder die Person ist, welche die geschützten Dateien tatsächlich zur Verfügung stellt), und diese haben grundsätzlich nicht damit zu rechnen. Unter diesen Voraussetzungen beachtet die Firma X AG auch nicht den Transparenzgrundsatz.

Eine Datenbearbeitung muss auch den Grundsatz von Treu und Glauben befolgen. Im vorliegenden Fall beschafft die Firma X AG die Daten zwecks Identifizierung des Inhabers des Internetzugangs, um in der Folge zivilrechtliche Forderungen gegen ihn zu erheben. Die Daten betreffend die IP-Adresse sind durch das Telekommunikationsgeheimnis geschützt, und die Identifikation des Inhabers eines solchen Zugangs ist derzeit nur ihm Rahmen eines Strafverfahrens möglich. Durch Einreichung einer Strafklage mit dem alleinigen Ziel, die Identität des Internetzugangsinhabers festzustellen (der wie schon erwähnt guten Glaubens sein kann), um von ihm Schadenersatzleistungen zu verlangen, umgehen die Urheberrechtsinhaber oder ihre gesetzlichen Vertreter das im zivilen Bereich geltende Telekommunikationsgeheimnis. Wir sind zu der Auffassung gelangt, dass ein solches Vorgehen als Verstoss gegen den Grundsatz von Treu und Glauben zu betrachten ist. In der Praxis nutzen die Urheberrechtsinhaber das Akteneinsichtsrecht im Strafverfahren dazu, gegenüber dem Inhaber der IP-Adresse zivilrechtliche Forderungen geltend zu machen, ohne den Abschluss des Strafverfahrens und die Verurteilung des Urhebers der Zuwiderhandlung abzuwarten. Dieses Vorgehen ist unserer Ansicht nach rechtsmissbräuchlich. In der Gesetzgebung ist die Möglichkeit der Aufhebung des Telekommunikationsgeheimnisses im Privatrecht nicht vorgesehen, und diese Lücke wurde anlässlich der letzten Revision des Urheberrechtsgesetzes nicht behoben.

Was die Prüfung des Verhältnismässigkeitsgrundsatzes anbelangt, so kann eine Datenbearbeitung als verhältnismässig gelten, wenn sie notwendig und dem angestrebten Ziel angemessen ist und wenn die getroffenen Massnahmen in einem vernünftigen Verhältnis zur Persönlichkeitsverletzung der betroffenen Person stehen. Vorliegend ist die Bearbeitung durch die Firma X AG eine Massnahme, die dazu geeignet ist, den Kreis der einer Urheberrechtsverletzung verdächtigten Personen einzugrenzen und den Tatbestand einer solchen Rechtsverletzung zu ermitteln, um danach eine Klage mit guten Erfolgsaussichten einreichen zu können. Diese Massnahme ist auch notwendig, um eine Urheberrechtsverletzung festzustellen und die Zuwiderhandlung nachweisen zu können. Die Urheberrechtsinhaber müssen jedoch die Identität des gutgläubigen Inhabers des Internetzugangs nicht unbedingt kennen, um ihre Parteirechte im Rahmen eines Strafverfahrens wahrzunehmen, und unter diesen Umständen kann lediglich die Beschaffung von Personendaten zum Zwecke einer Strafverfolgung als verhältnismässig erachtet werden.

Nur ein überwiegendes privates Interesse könnte als Rechtfertigung für die Datenbearbeitung durch die Firma X AG herangezogen werden. Bei der von den Urheberrechtsinhabern (in diesem Fall der Firma X AG) vorgenommenen Datenbearbeitung steht einerseits das Interesse der Urheberrechtsinhaber an einer gerichtlichen Verfolgung der Personen, die ihre Rechte verletzen, den Interessen der betroffenen Personen an der Wahrung ihrer Persönlichkeitsrechte andererseits gegenüber.

In der Praxis zeigt sich in diesem Fall, dass das Einsichtsrecht missbräuchlich genutzt wird, um gegen die gutgläubigen Inhaber eines Internetzugangs zivilrechtliche Forderungen geltend zu machen. Für diesen Rechtsmissbrauch gibt es keinerlei Rechtfertigungsgründe. Da keine Gewähr dafür geboten werden kann, dass sich die Beschaffung und die Bearbeitung der Daten durch die Firma X AG auf die Strafverfolgung und auf die allein gegen die Urheber der Rechtsverletzung gerichteten zivilrechtlichen Forderungen begrenzen, sind wir zu der Auffassung gelangt, dass die Datenbearbeitung eingestellt werden muss.

Zusammenfassend können wir festhalten, dass die Datenbearbeitung durch die Firma X AG nicht im Einklang mit den Grundprinzipien des DSG steht und dass das legitime private Interesse der Urheberrechtsinhaber nicht als ausreichender Rechtfertigungsgrund gelten kann, solange keine Garantie dafür besteht, dass die Identität der gutgläubigen Inhaber eines Internetzugangs im Rahmen eines Strafverfahrens geschützt ist.

Wir haben der Firma X AG empfohlen, ihre Datenbearbeitung unverzüglich und so lange einzustellen, als keine angemessene Rechtsgrundlage ausgearbeitet worden ist. Das Unternehmen liess innerhalb der anberaumten Frist verlauten, dass es unsere Empfehlung nicht akzeptiert. Wir haben die Angelegenheit daher dem Bundesverwaltungsgericht zum Entscheid vorgelegt.

1.3.2 Datenschutz im Rahmen der Internet-Telefonie (Voice over IP)

Da die Internet-Telefonie seit einigen Jahren einen grossen Aufschwung erlebt, haben wir uns entschlossen, diesen Bereich zu analysieren und uns dabei besonders mit den potenziellen Problemen der Persönlichkeitsverletzung zu befassen. Wir haben sechs kostenlose Softwarepakete für die Internet-Telefonie mit dem Ziel geprüft, den Benutzern und Entwicklern nützliche Ratschläge zu erteilen. Ein Auszug des Bericht befindet sich im Anhang 4.2, der vollständige Bericht auf unserer Website (www.derbeauftragte.ch).

1.3.3 Versehentliche Bekanntgabe von Personendaten im Internet

Ein in Ausmass und Sensibilität der Daten sehr aussergewöhnlicher Fall von versehentlicher Veröffentlichung im Internet zeigt einmal mehr, wie wichtig es ist, die vom Datenschutzgesetz verlangten technischen und organisatorischen Massnahmen sorgfältig umzusetzen.

Regelmässig erhalten wir Hinweise, dass Personendaten wegen ungenügender Datensicherheitsmassnahmen unbeabsichtigt via Internet zugänglich gemacht werden. 2007 mussten wir von einem Fall Kenntnis nehmen, der sowohl von der Anzahl der betroffenen Personen als auch von der Sensibilität der Daten her aussergewöhnlich war. Es handelte sich um eine über 50 Megabyte grosse Textdatei, die frei zugänglich auf einem Webserver lag; sie enthielt zehntausende Einträge von Personen. Neben Namen, Adressen, E-Mail-Adressen und Geburtsdaten waren auch heikle Daten über die Gesundheit der betroffenen Personen enthalten. Dabei handelt es sich um besonders schützenswerte Personendaten im Sinne des Datenschutzgesetzes.

Die Datei lag auf einem Webserver eines Internet-Dienstleisters und wurde von einem Kunden irrtümlich hochgeladen. Mehrere Wochen hat niemand dieses Versehen bemerkt. Nachdem wir von einer Person über den Fall informiert wurden, haben wir uns an die betreffende Firma gewandt und verlangt, dass die Daten umgehend vom Netz genommen werden, was auch sogleich geschah. Weiter verlangten wir die Ergreifung angemessener Massnahmen, damit ein solchen Vorfall in Zukunft verhindert wird.

Wie uns versichert wurde, ergab die Auswertung des Logfiles, dass glücklicherweise nur sehr wenige Zugriffe auf die Daten aus dem Internet erfolgt sind.

1.4 Justiz/Polizei/Sicherheit

1.4.1 Datenschutz im Rahmen der Schengen-Evaluation

Die Umsetzung des Schengen-Assoziierungsabkommens wird von der Europäischen Union einer Evaluation unterzogen, bevor das Schengener Informationssystem (SIS) in der Schweiz zur Anwendung kommt. Anlässlich des Evaluationsbesuchs bei den schweizerischen Datenschutzbehörden werden die Kompetenzen des EDÖB und mehrerer kantonaler Datenschutzbehörden geprüft.

Das Schengen-Assoziierungsabkommen (SAA) – von der Schweiz im März 2006 ratifiziert – ist am 1. März 2008 in Kraft getreten. Seine Anwendung setzt einen Beschluss des EU-Rates voraus. Der Beschluss muss von den am Raum Schengen beteiligten Staaten einstimmig gefasst werden, nachdem die Fähigkeit der Schweiz zur Umsetzung dieses Abkommens einer Evaluation unterzogen wurde. Erst danach kommt die nationale SIS-Datei in der Schweiz zum Einsatz. Die Evaluation wird von Teams vorgenommen, die sich aus Sachverständigen des Europäischen Rates, der Europäischen Kommission und der Mitgliedstaaten zusammensetzen. Sie betrifft die polizeiliche Zusammenarbeit, den Datenschutz, die Kontrolle an den Aussengrenzen, die Visa, die konsularische Zusammenarbeit und die Verwaltung der nationalen SIS-Datei (N-SIS).

Die Evaluation des Datenschutzes umfasst die Umsetzung des SAA, insbesondere die Kompetenzen der eidgenössischen (also des EDÖB) und der kantonalen Kontrollbehörden im Bereich Datenschutz. Diese werden auf der Grundlage eines Fragebogens und von Inspektionen vor Ort beurteilt. Die Evaluation erstreckt sich insbesondere auf die Aufsichts-, Ermittlungs- und Eingriffsbefugnisse der Kontrollbehörden sowie auf ihre Unabhängigkeit. Analysiert werden die rechtlichen Grundlagen und speziell die Kontrollbefugnisse bezüglich des SIS und die an seiner Verwaltung beteiligten Dienste. Die Rechte der betroffenen Personen und die Datensicherheit sind ebenfalls Gegenstand einer Evaluation.

Wir haben uns intensiv mit der Vorbereitung dieser Evaluation befasst, in enger Zusammenarbeit namentlich mit dem Bundesamt für Justiz, dem Bundesamt für Polizei, dem Bundesamt für Migration und den kantonalen Datenschutzbehörden. Es ging dabei um die Beantwortung des von der EU an die Schweiz gerichteten Evaluationsfragebogens (Februar 2008) und um unsere Vorbereitung auf die Inspektionen vor Ort (erstes Halbjahr 2008). Der Evaluationsbesuch im Bereich Datenschutz bei den schweizerischen Kontrollbehörden fand im März 2008 statt. Die europäischen Experten prüften die Kompetenzen des EDÖB und mehrerer kantonaler Datenschutzbehörden. Die Kantone Zürich, Freiburg, Waadt und Tessin standen auf dem Besuchsprogramm.

In der Folge werden wir unsere Aktivitäten auf die Einführung von Kontrollen über die Bearbeitung von Personendaten im Rahmen des SIS konzentrieren, insbesondere beim Bundesamt für Polizei (dem Inhaber der N-SIS-Datensammlung) und bei den eidgenössischen Dienststellen, die das SIS benutzen, ebenso wie bei den schweizerischen Vertretungen im Ausland. Überdies werden wir unsere Rolle als Koordinator der schweizerischen Datenschutzbehörden ausgestalten. In dieser Eigenschaft übernehmen wir das Präsidium und das Sekretariat der Koordinationsgruppe, in welcher der EDÖB und die kantonalen Datenschutzbehörden zusammengeschlossen sind. Wir haben diese Koordinationsgruppe eingesetzt, um auf schweizerischer Ebene eine einheitliche Haltung der 27 Datenschutzbehörden gegenüber den Ansuchen des Europäischen Datenschutzbeauftragten (EDPS) zu gewährleisten und um allen schweizerischen Behörden rasch und in koordinierter Form vollständige Informationen zukommen zu lassen. Im Übrigen werden wir in Zusammenarbeit mit den kantonalen Behörden unsere Informations- und Sensibilisierungsarbeit in der Öffentlichkeit zu Datenschutzthemen im Rahmen der Umsetzung des SIS in der Schweiz ausdehnen. Wir planen namentlich die Ausarbeitung von Broschüren zuhanden der SIS-Benutzer und der von den Datenbearbeitungen im Rahmen des SIS betroffenen Personen und die Mitwirkung an einer Informationskampagne. Schliesslich beteiligen wir uns zusammen mit den kantonalen Datenschutzbehörden an verschiedenen internationalen Ausschüssen und Arbeitsgruppen. Die Schweiz entsendet namentlich zwei Vertreter, den EDÖB und einen Vertreter der kantonalen Datenschutzbehörden, an Tagungen der gemeinsamen Kontrollinstanz (GK), die mit der Überwachung der zentralen technischen Unterstützungsfunktion des SIS betraut ist.

1.4.2 Hooliganismusbekämpfung

Im Bereich Hooliganismusbekämpfung sind in der Berichtsperiode verschiedene Gesetzgebungsarbeiten weitergeführt worden. Wir wurden in diesem Zusammenhang eingeladen, zu verschiedenen Vorlagen Stellung zu nehmen, die auf unterschiedlichen Stufen der Gesetzgebung – vom Entwurf zu einer Bestimmung in der Bundesverfassung bis zu Richtlinien über Datenbearbeitungen durch Private – angesiedelt waren.

Verschiedene der im Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (BWIS) und der zugehörigen Verordnung (VWIS) vorgesehenen Massnahmen wurden vom Parlament nur für die begrenzte Zeit bis Ende 2009 in Kraft gesetzt. Dies geschah deshalb, weil dem Bund auf dem Gebiet der sicherheitspolizeilichen Massnahmen keine Gesetzgebungskompetenz zusteht. Um sicherzustellen, dass die entsprechenden Bestimmungen auch nach dem erwähnten Zeitpunkt weiterhin Gültigkeit behalten können, fallen zwei Möglichkeiten in Betracht: Einerseits könnten die Kantone

ein Konkordat schliessen, worin sie die oben erwähnten Massnahmen vorsehen. Dieser Weg wurde von den Kantonen eingeschlagen, er könnte sich aber als recht langwierig erweisen. Da zusätzlich das Resultat bis auf weiteres ungewiss ist, soll andererseits gewissermassen als Absicherung eine neue Bestimmung für die Bundesverfassung formuliert werden, die dem Bund die entsprechende Kompetenz zuweist. Der Unterschied zwischen den beiden Vorgehensweisen ist unter dem Gesichtspunkt der Kompetenzen wesentlich. Eine spezifische Relevanz für den Datenschutz ist indessen – anders als bei den Bestimmungen auf den nachgeordneten Stufen der Gesetzgebung – nicht vorhanden. Dementsprechend haben wir zum Entwurf einer Verfassungsbestimmung keine inhaltliche Stellungnahme abgegeben, was an unseren bisherigen Bemerkungen zu den Bestimmungen tieferer Stufe selbstverständlich nichts ändert.

Wir erwähnen hier nochmals unsere Kritik an der zu offenen Definition des Gewaltbegriffs sowie unsere Feststellung, dass für einen allfälligen Einsatz biometrischer Gesichtserkennungssysteme eine formellgesetzliche Bestimmung erforderlich ist und daher die Stufe Verordnung nicht genügt. Letzteres ist insbesondere dadurch zu begründen, dass mit solchen Systemen die Daten nicht bloss von Hooligans, sondern sämtlicher Stadionbesucher bearbeitet würden.

Weiter wurden wir in der Berichtsperiode eingeladen, zur Richtlinie für die Verwendung und Bearbeitung von Daten des Informationssystems HOOGAN durch die Organisatoren von Sportveranstaltungen und deren Sicherheitsverantwortliche Stellung zu nehmen. Es hat uns mit Befriedigung erfüllt, dass aufgrund unserer Bemerkungen in verschiedener Hinsicht Klärung erreicht werden konnte. Dies gilt insbesondere in Bezug auf die Vorgehensweise bei der Datenvernichtung vor Ort bzw. in den Stadien. Weiter haben wir mit Genugtuung zur Kenntnis genommen, dass der Einsatz eines so genannten elektronischen Personenerkennungssystems nicht vorgesehen ist. Leider besteht zwischen der erwähnten Richtlinie einerseits und Gesetz und Verordnung andererseits eine Ungereimtheit, welche durch Artikel 2 Absatz 3 der Richtlinien geschaffen wurde. Dessen Formulierung «Die Richtlinie gilt sinngemäss für Übertragungen von Sportveranstaltungen mittels Grossbildleinwänden (Public-Viewing)» will den Anwendungsbereich von Gesetz und Verordnung über deren Wortlaut hinaus erweitern. Im Gesetz und in der Verordnung ist nämlich die Rede von «Sportveranstaltungen», was nach allgemeinem Sprachgebrauch die Vorführung dieser Veranstaltungen auf Grossleinwänden nicht umfasst.

Die Situation ist hier aus zwei Gründen, auf welche wir bloss hinweisen können, unbefriedigend. Erstens kann eine derartige Ausweitung des Anwendungsgebiets gerade im Zusammenhang mit freiheitsbeschränkenden Massnahmen in formeller Hinsicht nicht funktionieren. Dies ist insofern störend, als gerade im Hinblick auf die EURO 08 auch für das Public Viewing Sicherheitsmassnahmen erforderlich sind und also

eine gewisse Ausdehnung der Anwendbarkeit inhaltlich durchaus sinnvoll erscheint. Und zweitens werden soweit wir sehen durch die Formulierung «sinngemässe Anwendung» Unsicherheiten geschaffen, weil nicht klar scheint, was dies in der Praxis genau bedeuten soll. Beispielsweise dürften nicht unbedeutende Unterschiede aus der Tatsache entstehen, dass «Public Viewing» in erster Linie auf öffentlichem Grund stattfindet, während beispielsweise Fussballstadien in der Schweiz in der Regel in Privatbesitz sind. Ein Unterschied zwischen den beiden Konstellationen liegt beispielsweise darin, dass das Betreten eines Stadions trotz eines Stadionverbotes ein Hausfriedensbruch darstellt, während dieselbe Situation auf öffentlichem Grund schwerlich denkbar scheint.

1.4.3 Aktivitäten im Zusammenhang mit der EURO 08

Die EURO 08 bringt verschiedenste Bearbeitungen von Personendaten sowohl durch Behörden als auch durch Private mit sich. Unsere Aktivitäten in diesem Zusammenhang waren schon Inhalt unseres Tätigkeitsberichts in den vergangenen zwei Jahren. In der Berichtsperiode wurden wir zu zwei Punkten angefragt.

Die erste Anfrage betraf die Vorschriften, welche die Bearbeitung der durch Drohnen aufgenommen Bilder regeln. Wie im letzten Tätigkeitsbericht beschrieben (vgl. 14. Tätigkeitsbericht 2006/2007, Ziff. 1.3.5), hatten wir das VBS beim Erarbeiten der angesprochenen Regeln unterstützt. Zwar ist der entsprechende Bundesratsbeschluss nicht im vollen Wortlaut publiziert, alle seine inhaltlichen Elemente sind jedoch beschrieben in der Botschaft zum Bundesbeschluss über den Einsatz der Armee im Assistenzdienst zur Unterstützung der zivilen Behörden anlässlich der Fussball-Europameisterschaft 2008 (UEFA EURO 2008). Für die datenschutzrechtliche Betrachtung ist insbesondere bedeutsam, dass der Bundesrat den Einsatz der Aufklärungsmittel der Luftwaffe mit Beschluss vom 13. September 2006 genehmigt hat, «unter der Bedingung, dass eine Aufzeichnung der Daten untersagt ist» (BBl 2006 8179, letzter Absatz vor Ziff. 4).

Die zweite Anfrage kam von einer Person, die in der Ticketverlosung vom März 2007 erfolglos geblieben war. Sie wollte wissen, was nun mit ihren Daten geschehen werde und ob sie allenfalls die Möglichkeit habe, diese Daten löschen zu lassen. Unsere Abklärungen bei der UEFA haben ergeben, dass die Daten der Bewerber grundsätzlich in einer Warteliste gespeichert bleiben, um für weitere Verlosungen benutzt zu werden. Betroffene Personen können ihre Daten löschen lassen; die UEFA verlangt dafür gemäss den Angaben auf ihrer Webseite jedoch eine schriftliche Eingabe. Der Nutzen der Warteliste ergibt sich aus den verschiedenen Möglichkeiten, auch nach der Ver-

losung noch zu Tickets zu kommen. Dies kann passieren, wenn erstens Personen, die Tickets zugeteilt erhalten haben, dafür nicht bezahlen; wenn zweitens ein Verlosungsgewinner beim Abgleich mit einer Liste von Gewalttätern aus Sicherheitsgründen ausgeschlossen wird; oder wenn drittens während des Turniers ein nationaler Verband in einem Spiel der KO-Phase, wofür die teilnehmenden Mannschaften heute ja noch nicht bekannt sind, nicht sein gesamtes Kontingent ausschöpfen sollte. Nach dem Turnier werden sämtliche Bewerberdaten, die nicht aus rechtlichen Gründen noch benötigt werden, gelöscht. Darunter versteht die UEFA einerseits Fälle, in welchen die Informationen für steuerliche Zwecke noch benötigt werden. Andererseits geht es um Fälle, in welchen die Angaben im Zusammenhang mit vertraglichen Streitigkeiten oder aufgrund von sicherheitsrelevanten Vorfällen weiterhin benötigt werden.

1.4.4 Bundesgesetz über die polizeilichen Informationssysteme des Bundes

Der Nationalrat hat den Entwurf des Bundesgesetzes über die polizeilichen Informationssysteme des Bundes verabschiedet. Die von uns zu zahlreichen Punkten in dem Entwurf eingebrachten Vorschläge wurden indessen nicht berücksichtigt. Was die besondere Frage des so genannten «indirekten» Auskunftsrechtes anbelangt, so wurde die beschlossene Regelung vom Eidgenössischen Justiz- und Polizeidepartement und vom Bundesamt für Polizei vorgeschlagen. Diese Regelung stellt eine Verbesserung gegenüber der heutigen Situation dar, welche mit Artikel 13 der Bundesverfassung und den Artikeln 8 und 13 der Europäischen Menschenrechtskonvention, in denen der Schutz der Privatsphäre gewährleistet wird, nicht vereinbar ist. Unbefriedigend ist für uns indessen die Tatsache, dass die Information der betroffenen Person automatisch um drei Jahre aufgeschoben wird, wenn über sie keine Daten bearbeitet werden.

Wir erwähnten in unserem 14. Tätigkeitsbericht 2006/2007 (Ziff. 1.3.7) eine Reihe von Bemerkungen zum Entwurf des Bundesgesetzes über die polizeilichen Informationssysteme des Bundes. In erster Linie bedauerten wir die Beibehaltung des Systems des so genannten «indirekten Auskunftsrechts». Wir kritisierten auch die Tatsache, dass eine spätere Information der betroffenen Personen nur vorgesehen ist, wenn die Daten unmittelbar (und ohne Wissen der Betroffenen) von der Bundeskriminalpolizei erhoben worden sind. Wir äusserten zudem Zweifel betreffend den Online-Zugriff der Eidgenössischen Spielbankenkommission auf das automatisierte Polizeifahndungssystem sowie der Meldestelle für Geldwäscherei auf das Staatsschutz-Informations-

System (ISIS). Schliesslich sprachen wir uns auch dagegen aus, dass der nationale Polizeiindex Angaben über den Grund für den Eintrag bezüglich einer erkennungsdienstlich behandelten Person sowie über das Informationssystem oder die Art von System, aus dem die Daten stammen, enthalten soll. Nach der Behandlung des Gesetzesentwurfs im Nationalrat hat dieser einen Text verabschiedet, der unseren verschiedenen Bemerkungen nicht Rechnung trägt.

Im Rahmen der Arbeiten der Kommission für Rechtsfragen des Nationalrats wurde eine neue Regelung betreffend den Zugriff der betroffenen Personen auf die im Informationssystem Bundesdelikte enthaltenen Daten erarbeitet. Diese Daten werden derzeit im Informationssystem JANUS der Bundeskriminalpolizei bearbeitet. Die neue Regelung wurde vom Eidgenössischen Justiz- und Polizeidepartement und vom Bundesamt für Polizei (fedpol) vorgeschlagen. Eine Person kann Auskunft darüber verlangen, ob die Bundeskriminalpolizei Daten über sie im oben erwähnten Informationssystem bearbeitet. Das fedpol schiebt diese Auskunft auf, wenn betreffend die bearbeiteten Daten überwiegende Interessen der Strafverfolgung an einer Geheimhaltung bestehen. Die Auskunft wird ebenfalls aufgeschoben, wenn über die Person keine Daten bearbeitet werden. Das fedpol teilt der gesuchstellenden Person den Aufschub der Auskunft mit und weist sie darauf hin, dass sie das Recht hat, vom EDÖB zu verlangen, dass er prüfe, ob sie betreffende Daten rechtmässig bearbeitet werden und ob überwiegende Geheimhaltungsinteressen den Aufschub rechtfertigen. Der EDÖB führt auf Verlangen der gesuchstellenden Person die Prüfung durch und teilt ihr mit, dass entweder in Bezug auf sie keine Daten unrechtmässig bearbeitet werden oder dass er im Falle von Fehlern bei der Datenbearbeitung oder betreffend den Aufschub der Auskunft eine Änderungsempfehlung an das fedpol gerichtet hat. Er weist die betroffene Person auch darauf hin, dass sie vom Bundesverwaltungsgericht (BVGer) verlangen kann, diese Mitteilung oder den Vollzug der Empfehlung zu überprüfen. Das BVGer führt auf Verlangen der gesuchstellenden Person die Prüfung durch und teilt ihr anschliessend mit, dass sie im begehrten Sinne durchgeführt worden ist. Im Falle von Fehlern bei der Datenbearbeitung oder betreffend den Aufschub der Auskunft richtet das BVGer eine Verfügung zu deren Behebung an das fedpol. Das gleiche Verfahren gilt, wenn die Empfehlung des EDÖB nicht befolgt wird. Dieser kann gegen diese Verfügung beim Bundesgericht Beschwerde führen. Die oben erwähnten Mitteilungen sind stets gleich lautend und werden nicht begründet. Sie können nicht mit einem Rechtsmittel angefochten werden. Sobald das Geheimhaltungsinteresse dahingefallen ist, spätestens aber nach Ablauf der Aufbewahrungsdauer, erteilt das fedpol der gesuchstellenden Person Auskunft, sofern dies nicht mit übermässigem Aufwand verbunden ist. Personen, über die keine Daten bearbeitet wurden, informiert das fedpol drei Jahre nach Eingang ihres Gesuches über diese Tatsache. Legt eine

Person glaubhaft dar, dass ihr bei einem Aufschub der Auskunft ein erheblicher, nicht wieder gutzumachender Schaden erwächst, so kann der EDÖB empfehlen, dass das fedpol ausnahmsweise sofort Auskunft erteilen soll, soweit damit keine Gefährdung der inneren oder der äusseren Sicherheit verbunden ist.

Diese neue Regelung stellt zwar eine Verbesserung gegenüber der heutigen Situation dar, welche mit Artikel 13 der Bundesverfassung und den Artikeln 8 und 13 der Europäischen Menschenrechtskonvention, in denen der Schutz der Privatsphäre gewährleistet wird, nicht vereinbar ist. Unbefriedigend ist dagegen für uns die Tatsache, dass die Information der betroffenen Person automatisch um drei Jahre aufgeschoben wird, wenn über sie keine Daten bearbeitet werden. In den meisten Fällen entsteht kein besonderes Risiko für die innere und die äussere Sicherheit, wenn die Auskunft über diese Situation sofort erteilt wird. Sollte eine generelle Frist eingeführt werden, dürfte sie sechs Monate nicht überschreiten. Die Vorlage wird zur Zeit im Ständerat behandelt.

1.4.5 Videoüberwachung zu Sicherheitszwecken an öffentlichen Orten

Unter der Leitung des EJPD wurde ein Bericht betreffend die Videoüberwachung zu Sicherheitszwecken im öffentlichen Raum ausgearbeitet. Wir haben diese Arbeiten als Beobachter begleitet. Zur im Bericht vorgeschlagenen Verlängerung der Aufbewahrungsdauer hielten wir fest, dass dabei das Verhältnismässigkeitsprinzip beachtet werden müsse. Weiter kritisierten wir, dass der Bericht zu wenig auf die Nachteile und die Gefahren der Videoüberwachung hinweist.

Zur Thematik der Videoüberwachung zu Sicherheitszwecken im öffentlichen Raum wurde unter der Leitung des EJPD ein Bericht ausgearbeitet. Wir begleiteten diese Arbeiten als Beobachter. Der Bericht kommt hauptsächlich zum Schluss, dass die für den Bundessicherheitsdienst geregelte Aufbewahrungsdauer von 24 Stunden für Videoaufzeichnungen zu kurz sei, und schlägt vor, die entsprechende Rechtsgrundlage anzupassen. An den Sitzungen sowie in unserer Stellungnahme zum Berichtsentwurf hielten wir fest, dass bei einer Verlängerung der Aufbewahrungsdauer für den Bundessicherheitsdienst die allgemeinen Datenschutzgrundsätze, insbesondere das Verhältnismässigkeitsprinzip, beachtet werden müssten. So wäre eine allfällige Verlängerung auf beispielsweise 100 Tage auf jeden Fall unverhältnismässig. Im Übrigen hielten wir fest, dass der Bericht insgesamt zu einseitig ausgefallen ist, das heisst, dass überwiegend die Vorzüge der Videoüberwachung, kaum aber die damit verbundenen Gefahren erwähnt wurden. Die Videoüberwachung kann in bestimmten Fällen sicher

sinnvoll und nützlich sein. Allerdings kann damit die Kriminalität nicht ganz verhindert werden, sondern wird häufig einfach an andere Orte verdrängt. Zudem führt die Überwachung oft dazu, dass vor allem das subjektive Sicherheitsempfinden der überwachten Personen, nicht aber die tatsächliche Sicherheit erhöht wird. Vor dem Einsatz von Videoüberwachungsgeräten und der Schaffung entsprechender Rechtsgrundlagen muss jeweils im Einzelfall sorgfältig geprüft werden, ob die datenschutzrechtlichen Voraussetzungen (wie das Verhältnismässigkeits- und das Zweckbindungsprinzip) erfüllt sind. Insbesondere muss geprüft werden, ob nicht eine mildere Massnahme als die Videoüberwachung zum gleichen Ziel führt. Zudem muss die Videoüberwachung von bestimmten Massnahmen (wie Löschung der Daten, sobald diese nicht mehr gebraucht werden, Einsatz datenschutzfreundlicher Technologien begleitet werden.

1.4.6 Abkommen zwischen der Schweiz und Frankreich über die grenzüberschreitende Zusammenarbeit in Justiz-, Polizei- und Zollsachen

Das revidierte Abkommen mit Frankreich über die grenzüberschreitende Zusammenarbeit in Justiz-, Polizei- und Zollsachen schafft gegenüber dem ursprünglichen Abkommen von 1998 einen verstärkten Datenschutz. Die Datenschutzbestimmungen dieses revidierten Abkommens sind denjenigen ähnlich, die in den Abkommen mit Deutschland und mit Österreich und Liechtenstein enthalten sind.

Die Datenschutzbestimmungen des im Laufe des Jahres 2007 revidierten Abkommens sind vollständiger als diejenigen in dem ursprünglichen Abkommen von 1998 und verstärken damit den Schutz der im Rahmen der grenzüberschreitenden Zusammenarbeit in Justiz-, Polizei- und Zollsachen mit Frankreich bearbeiteten Personendaten. Sie übernehmen zum Teil die Normen des Schengener Durchführungsübereinkommens und lehnen sich an die Datenschutzbestimmungen im Abkommen mit Deutschland und denjenigem mit Österreich und Liechtenstein an. Diese Bestimmungen behandeln die Zweckbindung der Bearbeitung von Personendaten, die Berichtigung, die Vernichtung sowie die Bekanntgabe dieser Daten. Das revidierte Abkommen enthält auch eine Bestimmung über das Auskunftsrecht.

Im Rahmen der Ausarbeitung des Entwurfs zu dem revidierten Abkommen nahm das Bundesamt für Polizei mehrmals mit uns Verbindung auf. Es trug allen unseren Bemerkungen und insbesondere der Forderung Rechnung, in dem Abkommen darauf hinzuweisen, dass die Kontrolle über die von den Beamten der Zentren für Polizei- und Zollzusammenarbeit verwendeten gemeinsamen Datenbank in einem Zusatzprotokoll geregelt wird. Die Zuständigkeiten der verschiedenen Datenschutzbehörden (Commis-

sion Nationale de l'Informatique et des Libertés, EDÖB und kantonale Datenschutzbehörden) müssen nämlich, je nachdem ob die französischen oder die schweizerischen Behörden (Bundes- und Kantonsbehörden) in diesen gemeinsamen Zentren tätig sind, entsprechend definiert werden.

1.4.7 Indirektes Auskunftsrecht

Am 1. Januar 2007 hat das Bundesverwaltungsgericht die Aufgaben der Eidgenössischen Datenschutz- und Öffentlichkeitskommission im Bereich des indirekten Auskunftsrechts übernommen. Gemäss Artikel 18 Abs. 2 des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit (BWIS) und Artikel 14 Abs. 3 des Bundesgesetzes über kriminalpolizeiliche Zentralstellen des Bundes (ZentG) überprüft der Präsident der auf dem Gebiet des Datenschutzes zuständigen Abteilung I des Bundesverwaltungsgerichts auf Verlangen der betroffenen Person die Mitteilung des EDÖB oder gegebenenfalls den Vollzug der von diesem abgegebenen Empfehlung. Der Präsident teilt der Person anschliessend in einer stets gleich lautenden Antwort mit, dass die Prüfung im begehrten Sinn durchgeführt wurde.

Für die Personen, die Gesuche zu bearbeiten haben, die aufgrund von Artikel 18 BWIS und Art. 14 ZentG eingegangen sind, haben wir in Zusammenarbeit mit dem Bundesverwaltungsgericht – und auf dessen Begehren hin – eine Informationssitzung über die verschiedenen Aspekte des indirekten Auskunftsrechts organisiert. Der Präsident der ehemaligen Eidgenössischen Datenschutz- und Öffentlichkeitskommission nahm ebenfalls an dieser Sitzung teil.

Im Rahmen der Prüfung des Entwurfs für das Bundesgesetz über die polizeilichen Informationssysteme des Bundes durch die Kommission für Rechtsfragen des Nationalrates wurden neue Modalitäten für die Ausübung des Auskunftsrechts vorgesehen. Ausführlichere Informationen zu dieser Frage sind in Ziffer 1.4.4 des vorliegenden Tätigkeitsberichts zu finden.

1.4.8 Nachträgliche Information der betroffenen Personen

Im Zusammenhang mit seinem Entscheid vom 15. August 2006 betreffend die nachträgliche Information der betroffenen Personen im Polizeibereich vertritt das EJPD die Meinung, dass es sich hier nicht um eine eigentliche Verfügung handelt. Daher sei dieser auch nicht zu veröffentlichen. Wir haben das EJPD aufgefordert, eine Verfügung gemäss Art. 5 VwVG zu treffen und diese in anonymisierter Form zu veröffentlichen. Das EJPD klärt nun ab, ob wir die Befugnis haben, eine solche Verfügung zu verlangen.

In unserem letzten Tätigkeitsbericht haben wir bereits den Entscheid des EJPD vom 15. August 2006 im Zusammenhang mit der nachträglichen Information der betroffenen Personen im Polizeibereich und unsere entsprechenden Empfehlungen erwähnt (vgl. 14. Tätigkeitsbericht 2006/2007, Ziff. 1.3.8). Der Entscheid sah unter anderem vor, dass ein Auszug im Bundesblatt publiziert werden sollte. Dagegen vertraten wir die Auffassung, dass der gesamte – anonymisierte – Entscheid oder aber ein Auszug mit den wesentlichen Elementen inklusive Rechtsmittelbelehrung zu veröffentlichen sei. Das EJPD stellte sich seinerseits auf den Standpunkt, dass es sich bei seinem Entscheid nicht um eine Verfügung gemäss Art. 5 des Bundesgesetzes über das Verwaltungsverfahren (VwVG), sondern um eine interne Massnahme handle. Aus diesem Grund werde er nun doch nicht publiziert. Wir waren mit dieser Auslegung nicht einverstanden und blieben dabei, dass das EJPD den Entscheid veröffentlichen müsste. Sollte das EJPD daran festhalten, dass hier keine eigentliche Verfügung gemäss Art. 5 VwVG vorliegt, muss es nach unserer Auffassung eine solche treffen und sodann in anonymisierter Form im Bundesblatt sowie auf seiner Internetseite veröffentlichen. Das EJPD klärt nun ab, ob wir die Befugnis haben, eine solche Verfügung von ihm zu verlangen.

1.5 Gesundheit

1.5.1 Die Erstellung von DNA-Profilen im Rahmen der Familienzusammenführung

Die Einführung von DNA-Tests für nachziehende Familienangehörige im Einwanderergesetz hat in Frankreich zu heftigen Diskussionen geführt. In der Schweiz existiert diese Praxis bereits: Ausnahmsweise kann die Erteilung einer Bewilligung von der Erstellung von DNA-Profilen abhängig gemacht werden, sofern die betroffene Person schriftlich zustimmt. Diese Praxis darf aber unseres Erachtens nur äusserst restriktiv angewandt werden.

Am 1. April 2007 ist das Bundesgesetz über genetische Untersuchungen beim Menschen (GUMG) in Kraft getreten. Danach können im Verwaltungsverfahren die Erteilung von Bewilligungen oder die Gewährung von Leistungen von der Erstellung von DNA-Profilen abhängig gemacht werden, wenn begründete Zweifel an der Abstammung oder der Identität einer Person bestehen und sich diese Zweifel nicht auf andere Weise ausräumen lassen. Diese DNA-Profile dürfen nur erstellt werden, wenn die betroffenen Personen schriftlich zustimmen.

Es muss sich somit um Ausnahmefälle handeln, deren Klärung mittels DNA-Profilen unter Berücksichtigung des Verhältnismässigkeitsprinzips zu erfolgen hat. Dies ist beispielsweise der Fall, wenn Zivilstandsurkunden aus Ländern mit einem wenig ausgebauten und nicht immer zuverlässigen Zivilstandswesen stammen.

Bei einem Gesuch um Familiennachzug kann sich die Untersuchung auf das Verhältnis zwischen Mutter und Kind beschränken, um eine private Tragödie zu vermeiden. Eine nicht zu unterschätzende Zahl von Kindern ist zwar in einer Ehe geboren und hat demzufolge den Ehemann der Mutter zum rechtlichen Vater, der biologische Vater ist aber ein anderer Mann.

Die Diskussionen in Frankreich haben auch eine Debatte in der Schweiz ausgelöst. So beauftragte der Nationalrat Carlo Sommaruga in einer Motion vom 5. Oktober 2007 den Bundesrat, einen Bericht zum Umgang mit DNA-Tests im Falle des Familiennachzuges vorzulegen. Wir haben diese Motion unterstützt, da wir der Meinung sind, dass ein Bericht in diesem komplexen und heiklen Bereich sehr nützlich wäre. Nationalrat Alfred Heer seinerseits hat am 20.12.2007 eine parlamentarische Initiative eingereicht, welche zwingende DNA-Tests für den Familiennachzug aus Problemländern vorsieht.

Aus Sicht des Datenschutzes muss die Durchführung einer DNA-Analyse unbedingt verhältnismässig sein und nur als Ultima Ratio angeordnet werden. Die Freiwilligkeit des Tests ist relativ, denn im Verweigerungsfall riskiert der Gesuchsteller, kein Visum zu erhalten. Ausserdem muss er auch für die Kosten aufkommen.

Im Gegensatz zur Schweiz werden in Frankreich DNA-Tests durch einen Richter angeordnet und vom Staat bezahlt. Die gesetzliche Grundlage für die Anordnung von DNA-Tests ist in der Schweiz mit dem GUMG gegeben.

1.5.2 Die Übermittlung von biologischen Proben in die USA im Rahmen der medizinischen Forschung

Biologische Proben können in die USA ausgeführt werden, wenn die betroffenen Personen vorab ihre Einwilligung gegeben haben. Ohne diese Einwilligung darf eine Datenbekanntgabe nur stattfinden, wenn ein angemessener Datenschutz im Empfängerland gewährleistet werden kann.

Die geltende Gesetzgebung zur Forschung am Menschen (d.h. sowohl mit Personen als auch mit biologischen Materialien) ist in der Schweiz leider noch lückenhaft. Mit zwei Motionen beauftragt das Parlament den Bundesrat, diesen Bereich durch einen Verfassungsartikel und ein Bundesgesetz über die Forschung am Menschen zu regeln (vgl. Ziffer 1.4.1 unseres 14. Tätigkeitsberichtes 2006/2007). Auf Bundesebene bestehen spezifische Regelungen nur für Teilbereiche der Medizin, namentlich für klinische Versuche mit Heilmitteln. Bei solchen wird vermehrt biologisches Material zu Analysezwecken ins Ausland geschickt, unter anderem in die USA.

Die Übermittlung von biologischen Proben ins Ausland birgt ein erhöhtes Risiko für Persönlichkeitsverletzungen der betroffenen Personen. Liegen keine spezialgesetzliche Regelungen vor, findet bei jeder Bearbeitung von Personendaten und somit auch bei der Ausfuhr von biologischen Proben das Datenschutzgesetz (DSG) Anwendung.

Das revidierte Datenschutzgesetz, welches am 1. Januar 2008 in Kraft getreten ist, verlangt als grundsätzliche Voraussetzung die Datenübermittlung ins Ausland, dass die Gesetzgebung im Bestimmungsland einen angemessenen Schutz gewährleistet. Dies ist den USA, im Gegensatz zu den Mitgliedstaaten der Europäischen Union, nicht der Fall. Fehlt also ein angemessener Schutz, so ist durch hinreichende Garantien sicherzustellen, dass die Datenbekanntgabe die Persönlichkeit der betroffenen Personen nicht schwerwiegend gefährdet. Diese Garantien können in einem Vertag (Datenschutzklauseln) festgelegt sein oder sich aus einem Verhaltenskodex ergeben. Ein solches Regelwerk, dem sich Private freiwillig unterstellen, ist beispielsweise das «Safe

Harbor Privacy Framework», das von der Europäischen Kommission und den USA ausgehandelt wurde. Wer sich auf solche Garantien stützt, bleibt für den Datenschutz aber selber verantwortlich und muss uns über die Garantien informieren.

Eine Bekanntgabe ist im Einzelfall auch möglich, wenn die betroffene Person eingewilligt hat. Diese Einwilligung muss nach angemessener Information freiwillig und ausdrücklich erfolgen; d.h. die betroffene Person muss wissen, welche Daten zu welchem Zweck an welchen Empfänger bekannt gegeben werden. Sie ist ebenfalls darüber zu informieren, dass ein angemessener Datenschutz fehlt.

1.5.3 Internationaler Datenaustausch bei der Dopingbekämpfung

Die World Anti Doping Agency (WADA) befasst sich mit der Koordination und der Unterstützung von Massnahmen zur Dopingbekämpfung. Da in diesem Zusammenhang von der WADA auch in der Schweiz Daten gesammelt werden, haben wir diejenigen Tätigkeiten der WADA analysiert, die vom Schweizer Datenschutzgesetz (DSG) tangiert werden könnten. Wir kommen zum Schluss, dass eine Unterstellung der WADA unter das DSG in Teilbereichen nicht ausgeschlossen werden kann, und haben daher im Rahmen der Revision des Sportförderungsgesetzes eine gesetzliche Grundlage angeregt, um die internationale Zusammenarbeit in der Dopingbekämpfung zu vereinfachen.

Bei der Dopingbekämpfung nimmt die WADA unter anderem drei wesentliche Aufgaben wahr. Sie fungiert erstens als zentrale Clearingstelle für Daten und Resultate von Doping-Tests für Sportler auf internationaler und nationaler Ebene. In diesem Rahmen werden ihr alle Tests der ihr zugeteilten Sportler während und ausserhalb eines Wettkampfes gemeldet. Ihre zweite wichtige Aufgabe ist die selbständige Durchführung von Dopingkontrollen und deren Koordination. Drittens betreibt sie ein zentrales elektronisches Datenbanksystem, in welchem die Personenprofile sämtlicher bei ihr registrierter Sportlerinnen und Sportler (inklusive deren Gesundheits- und Dopinghistorie) geführt werden. Diese drei Aufgabenbereiche wurden im Rahmen eines für die WADA verfassten Gutachtens von uns im Hinblick auf unsere Zuständigkeit und die Unterstellung unter das Schweizer Datenschutzgesetz näher analysiert.

Grundsätzlich richtet sich die Anwendung des DSG und damit die Zuständigkeit des EDÖB nach dem Territorialitätsprinzip. Dies bedeutet, dass das DSG nur für eine Datenbearbeitung anwendbar ist, die in der Schweiz stattfindet. Betrifft die Datenbearbeitung allerdings einen internationalen Kontext, so hat der Betroffene gemäss dem internationalen Privatrechtsgesetz (IPRG) die Wahlmöglichkeit zwischen dem Recht des

Staates, in dem der Urheber der Verletzung seine Niederlassung oder seinen gewöhnlichen Aufenthalt hat, und dem Recht des Staates, in dem der Erfolg der verletzenden Handlung eintritt, sofern der Schädiger mit dem Eintritt des Erfolges in diesem Staat rechnen musste. Damit sind einem Datenbearbeiter die Möglichkeiten weitgehend genommen, sich durch eine Sitzverlegung ins Ausland datenschutzrechtliche Vorteile zu verschaffen, indem er sich einer anderen Rechtsordnung unterstellt. Vor diesem Hintergrund war in den drei oben genannten Aufgabenbereichen zu prüfen, ob und in wieweit die WADA dem DSG unterstellt ist.

Im Hinblick auf ihre Funktion als Clearingstelle werden der WADA von nationalen (z.B. in der Schweiz tätigen) Anti-Doping-Organisationen besonders schützenswerte Personendaten (in der Regel Kontrollergebnisse) ins Ausland (nach Kanada) gemeldet. Ein solcher Datentransfer ist nach DSG nur dann möglich, wenn die Gesetzgebung im Ausland ein angemessenes Datenschutzniveau aufweist oder auf andere Weise ein angemessener Schutz gewährleistet werden kann. Da die WADA eine nichtkommerzielle Stiftung ist und das Datenschutzgesetz Kanadas für nichtkommerzielle Institutionen keinen angemessenen Schutz gewährleistet, müssen die Schweizer Anti-Doping-Organisationen für eine Datenübermittlung nach Kanada selbst für ein angemessenes Datenschutzniveau sorgen, beispielsweise durch einen Vertrag mit der WADA. Der umgekehrte Datentransfer von Kanada in die Schweiz hingegen unterliegt nicht dem Schweizer Datenschutzregime.

Bei der Durchführung von Dopingkontrollen bearbeitet die WADA personenbezogene Daten. Somit unterliegen diese Kontrollen, falls sie in der Schweiz durchgeführt werden, der Schweizer Datenschutzgesetzgebung.

Da die WADA ihre elektronische Datenbank (ADAMS) ausschliesslich in Kanada betreibt und auch die von ihr vorgenommenen Bearbeitungsprozesse nicht in der Schweiz stattfinden, ist für deren Betrieb keine Zuständigkeit der Schweizer Datenschutzgesetzgebung gegeben.

Im Rahmen unserer Abklärungen kamen wir insgesamt zum Ergebnis, dass eine Unterstellung der WADA unter das Schweizer Datenschutzgesetz nicht in allen Fällen ausgeschlossen werden kann. Zur Vereinfachung der internationalen Zusammenarbeit im Bereich der Dopingkontrollen und des internationalen Datentransfers bei der Dopingbekämpfung haben wir daher angeregt, im Rahmen der Revision des Sportförderungsgesetzes eine entsprechende gesetzliche Grundlage zu schaffen (vgl. dazu auch Ziffer 1.5.4).

1.5.4 Revision des Bundesgesetzes über die Förderung von Turnen und Sport

Der internationale Datentransfer zur Dopingbekämpfung und die Durchführung von Dopingkontrollen sind heute in der Schweiz noch nicht gesetzlich geregelt, was bei den beteiligten Akteuren häufig zu Rechtsunsicherheit führt. Mangels einer gesetzlichen Grundlage kann heute ein internationaler Datenaustausch zwischen einzelnen Dopingbekämpfungsstellen nur durchgeführt werden, wenn ein angemessener Datenschutz vertraglich oder gesetzlich gewährleistet wird. Auf der anderen Seite beruhen Dopingkontrollen in der Schweiz rein rechtlich auf einer freiwilligen Zustimmung des jeweiligen Sportlers, welche er in Form einer Erklärung abgibt. Diese Praxis ist umstritten, da eine Verweigerung zum Ausschluss des Sportlers von der Veranstaltung führt und daher von Freiwilligkeit keine Rede sein kann. Um diesen beiden Problematiken zu begegnen, haben wir zwei Gesetzesvorschläge in die Revision des Sportfördergesetzes eingebracht.

Zur effizienten internationalen Dopingbekämpfung ist ein Datenaustausch zwischen den einzelnen nationalen Dopingbekämpfungsorganisationen von grosser Wichtigkeit. Vor allem bezüglich der Koordination von Massnahmen in der Dopingbekämpfung (Durchführung von Kontrollen) und der Meldung von Dopingmissbräuchen existieren heute in der Schweiz noch keine gesetzlichen Normen, weshalb die allgemeinen Regelungen des Datenschutzgesetzes (DSG) zur Anwendung kommen. Daher kann es bei der grenzüberschreitenden Übermittlung dieser besonders schützenswerten Personendaten derzeit zu Schwierigkeiten kommen, wenn diese Daten an einen Staat übermittelt werden, welcher keinen angemessenen Datenschutz gewährleistet. Um diesen Schwierigkeiten zu begegnen, ist es denkbar, dass die einzelnen nationalen Anti-Doping-Organisationen der am Austausch beteiligten Länder untereinander entsprechende Verträge abschliessen. Da das Aushandeln einer Vielzahl von Verträgen in der Praxis allerdings umständlich und problematisch sein kann, haben wir die Schaffung einer entsprechenden gesetzlichen Grundlage angeregt. Gemäss dieser Grundlage, die in das Vernehmlassungsverfahren zur Revision des Sportfördergesetz aufgenommen wurde, wären die zuständigen Stellen berechtigt, personenbezogene Daten zum Zweck der Dopingbekämpfung mit anerkannten ausländischen oder internationalen Organisationen auszutauschen, wenn dies für Dopingkontrollen, deren Koordination oder zur Meldung von Dopingverstössen notwendig ist. Mit der angestrebten Regelung soll vor allem für die nationalen Anti-Doping-Organisationen Rechtssicherheit geschaffen und deren Arbeit erleichtert werden.

Heutzutage beruhen Dopingkontrollen auf der Basis einer freiwilligen Einverständniserklärung der Sportlerinnen und Sportler. Allerdings führt die Nichtabgabe einer solchen Erklärung oder die Verweigerung einer Dopingkontrolle in der heutigen Praxis des Leistungssports entweder zum Ausschluss vom jeweiligen Wettkampf oder zum Verlust der Sportlerlizenz. Daher kann aus unserer Sicht die von den Sportlern gegebene Zustimmung zu den Dopingkontrollen und der nachfolgenden Datenbearbeitung nicht als freiwillig angesehen werden. Aus diesem Grund haben wir eine gesetzliche Grundlage angeregt, welche Dopingkontrollen legitimiert. Der von uns eingebrachte Gesetzesvorschlag, wonach Sportler, die regelmässig an Wettkämpfen teilnehmen, jederzeit Dopingkontrollen unterzogen werden können, wurde in den Entwurf zur Revision des Sportförderungsgesetzes aufgenommen. Damit soll auch im Bereich der Dopingkontrollen für Sportler und Veranstalter Rechtssicherheit geschaffen werden.

1.5.5 Datenschutzanforderungen bei generellen Bewilligungen in der medizinischen Forschung

Sofern ein Spital über eine generelle Bewilligung der Expertenkommission für das Berufsgeheimnis in der medizinischen Forschung verfügt, müssen die entsprechenden Auflagen umgesetzt werden. Kontrollmechanismen sind einzurichten, die sich nicht nur auf die Überprüfung des Forschungsprojektantrages beziehen, sondern auch im Forschungsprojekt selber in der entsprechenden technischen und organisatorischen Form einzubauen sind.

Bei Organisationseinheiten wie z.B. Universitätsspitälern, die eine grosse Anzahl von Forschungsprojekten durchführen, ist ein vereinfachtes Bewilligungsverfahren vorgesehen, so dass nicht für jedes Forschungsprojekt eine Sonderbewilligung eingeholt werden muss. Diese generelle Bewilligung muss bei der Expertenkommission beantragt werden, ist fünf Jahre gültig und kann danach erneuert werden. Aufgrund der Bewilligung können Forscher und Doktoratskandidaten der betreffenden Institution die Patientendaten für die betriebsinterne Forschung verwenden.

Der Bewilligungsnehmer muss Kontrollmechanismen einrichten, damit ein wirksamer Schutz der Patientendaten gewährleistet werden kann. Diese Mechanismen sind nicht nur für die Prüfung und Freigabe des internen Projektes wichtig, sie müssen auch im Forschungsprojekt selber vorhanden sein, damit nachvollzogen werden kann, ob die Auflagen der Expertenkommission eingehalten wurden.

Heute werden in den Spitälern EDV-gestützte und/oder Papierarchive eingesetzt, in denen die Daten von Patienten jeweils ungefähr zwei Wochen nach deren Austritt aus dem Spital festgehalten werden. Die Forschenden greifen für ihre Arbeiten in den

meisten Fällen auf die archivierten Daten zu. Die technischen und organisatorischen Auflagen der Expertenkommission sind insbesondere in diesem Bereich zu dokumentieren und umzusetzen. Der gesamte Prozess von der Erhebung der archivierten Daten (inklusive der Protokollierung) bis zu ihrer Löschung ist aufzuführen. Dabei ist aufzuzeigen, mit Hilfe welcher Informationen und Aufgabenträger der Forschende auf die Daten zugreifen kann, welche Daten er extrahiert und wann er sie wie anonymisiert oder pseudonymisiert. Zudem ist festzuhalten, auf welchen Sachmitteln er die erhobenen Daten für sein Forschungsprojekt weiterbearbeitet und sichert, sofern die Daten nicht vollständig anonymisiert sind (bei einer vollständigen Anonymisierung entfallen die Vorgaben des Datenschutzes). Meist sind die erhobenen Daten pseudonymisiert festgehalten, so dass auch aufgezeigt werden muss, wie eine Reidentifikation möglich und kontrollierbar ist.

Im medizinischen Bereich werden besonders schützenswerte Personendaten bearbeitet, die aufgrund der normativen Vorgaben gemäss dem Stand der Technik zu schützen sind. Für Forschungsarbeiten mit Hilfe von Papierarchiven erachten wir namentlich das folgende Vorgehen als angemessen:

- Die gewünschten Papierdossiers werden dem Forschenden von einem Mitarbeiter des Archivs ausgehändigt, der in einem Protokoll festhält, welche Dossiers dem Forschenden zur Verfügung gestellt wurden.

- Der Forschende übernimmt die Daten meist in einen Laptop. Dabei ist darauf zu achten, dass die Daten zumindest in pseudonymisierter Form übernommen werden, wenn sie nicht von Anfang an anonymsiert wurden. Ausserdem dürfen sich die identifizierenden Daten, die dem jeweiligen Pseudonym zugeordnet sind, nicht im Klartext auf dem Laptop befinden, d.h. sie werden durch gute Chiffrierverfahren geschützt oder gar nicht erst auf dem Laptop gespeichert. Die Informationen aus den Dossiers sollten möglichst in den Archivräumen auf den Laptop übernommen werden. Als weitere Sicherheitsmassnahme empfiehlt sich, den Laptop während den Forschungsarbeiten nicht an ein Datennetzwerk anzuschliessen.

Für Forschungsarbeiten, die auf Archivdatenbanken zurückgreifen, gelten grundsätzlich auch die oben aufgeführten Gesichtspunkte. Bei der Gestaltung der Bildschirmmasken und der Ausdrucksmöglichkeiten ist vom Grundsatz auszugehen, dass ausschliesslich die für die Aufgabenerfüllung notwendigen Personendaten zu bearbeiten sind. Sofern der Forscher nicht auch noch Kontakt mit den Patienten aufnehmen muss, wird es genügen, dass mit anonymisierten Daten oder mit Pseudonymen gearbeitet

wird. Je nach Forschungsvorhaben könnten so z.B. unterschiedliche Forschungsaccounts in einer Klinik eingerichtet werden, die den Forschenden für ihre Arbeiten zur Verfügung gestellt werden. Sofern die Forschenden die Abfragen selber vornehmen können, bestünde unseres Erachtens keine Notwendigkeit, Archivmitarbeitende einzubeziehen; eine möglichst pseudonymisierte und revisionssichere Protokollierung und deren Auswertung wäre aber, sofern bestimmte oder bestimmbare Personendaten bearbeitet werden, notwendig.

Uns ist bei den Augenscheinen vor Ort auch noch aufgefallen, dass nicht nur die Forschenden, sondern auch die Ärzte bei ihrer täglichen Arbeit im Spital auf das elektronische Archivsystem zugreifen können. Dies ist insbesondere notwendig, um festzustellen, ob ein ins Spital eintretender Patient schon einmal dort behandelt wurde, und ob allenfalls bereits wichtige Informationen über ihn im Archiv vorhanden sind. Ein möglicher Lösungsansatz, um den Zugriff auf diese Archivdatenbank entsprechend der Aufgabenerfüllung zu regeln, wäre, dass man den Zugriff nur erlaubt, wenn der Patient bereits im Patientenaufnahmesystem registriert ist. Durch einen solchen präventiven Kontrollmechanismus hat man den Zugriff auf die Archivdatenbank für die tägliche Arbeit schon recht gut geregelt. Zusätzlich ist das System so zu gestalten, dass bei Notfällen ein Zugriff auf die Archivdatenbank möglich ist. Zudem sind Zugriffe auf sensitive Personendaten gemäss den oben aufgeführten Kriterien zu protokollieren.

Wir erachten es auch als wichtig darauf hinzuweisen, dass die Datenschutzberatung in Spitälern eine wesentliche Aufgabe ist, die nicht noch irgendwie nebenbei zu zehn Prozent wahrgenommen werden kann. Neben der Beharrlichkeit, die ein solcher Aufgabenträger für die Aufgabenerfüllung mitbringen muss, sind die Anforderungen an die Fachkunde dieses Mitarbeiters umfassend. Es wird immer wieder darauf hingewiesen, dass namentlich Grundkenntnisse in den Bereichen Informatik, Organisation, Betriebswirtschaft, Informationssicherheit, Didaktik und Recht für die Aufgabenerfüllung notwendig sind.

1.5.6 Medizinische Forschungsprojekte, die aufgrund der Einwilligung der Betroffenen durchgeführt werden

Die Einwilligung des Patienten ist nur dann wirksam, wenn dieser ausreichend informiert ist und sich dadurch ein klares Bild über die Datenbearbeitung machen kann. Die Einwilligung ist freiwillig und darf somit nur dann eingeholt werden, wenn der Betroffene nicht unter Druck oder Zwang steht.

Grundsätzlich darf man die Daten von Patienten nur dann für die Forschung verwenden, wenn ihre schriftliche Einwilligung oder, je nach Situation, diejenige des gesetzlichen Vertreters oder von näheren Angehörigen vorliegt. Kann die Einwilligung nicht eingeholt werden, so besteht die Möglichkeit, bei der Expertenkommission für das Berufsgeheimnis in der medizinischen Forschung eine Bewilligung für das entsprechende Forschungsvorhaben zu beantragen.

Bei Forschungsprojekten, die aufgrund der Einwilligung der Betroffenen durchgeführt werden, gilt es namentlich die folgenden Kriterien zu berücksichtigen:

Eine Einwilligung des Patienten ist nur dann wirksam, wenn sie freiwillig erfolgt und der Betroffene ausreichend informiert ist. Die Freiwilligkeit ist nur gegeben, wenn nicht Druck oder Zwang ausgeübt wird. Soweit möglich ist beispielsweise eine Einwilligung erst nach einer wichtigen Operation einzuholen und nicht schon im Voraus, sonst wird der Patient einem Zwang ausgesetzt. Auch hat der Patient das Recht, seine Einwilligung jederzeit zu widerrufen, jedoch nur mit Wirkung auf die Zukunft.

Der Betroffene ist erst dann ausreichend informiert, wenn er im Voraus weiss, welche seiner Daten durch welche Stellen zu welchem Zweck auf welche Weise bearbeitet werden. Ausserdem ist ihm aufzuzeigen, welche technischen und organisatorischen Massnahmen zum Schutz der Daten getroffen wurden. Die Information des Patienten muss bei der Erhebung der Daten beginnen und endet bei deren Löschung oder Anonymisierung. Macht sich der Betroffene aufgrund der Informationen eine falsche Vorstellung über Art, Umfang und Zweck der Bearbeitung oder über die verantwortliche Stelle, so ist die Einwilligung unwirksam und die Datenbearbeitung nicht rechtskonform.

1.6 Versicherungen

1.6.1 Die Umsetzung der 5. IV-Revision

Das revidierte Bundesgesetz über die Invalidenversicherung (IVG) und die zugehörige Verordnung (IVV) sind per 1. Januar 2008 in Kraft getreten. Eine der wesentlichen Neuerungen ist das Modell der Früherfassung von Invaliditätsfällen. Die Regelung der Anmeldung für Früherkennungsmassnahmen ist aus Sicht des Datenschutzes verbesserungswürdig.

Die datenschutzrechtliche Diskussion über die Revision des Invalidenversicherungsgesetzes wurde bereits vor der hier zu besprechenden Tätigkeitsperiode abgeschlossen (vgl. unseren 13. Tätigkeitsbericht 2005/2006, Ziff. 5.1.2). Zu beurteilen blieb lediglich die Konkretisierung des Gesetzes auf Verordnungsstufe. Wir haben dazu im Rahmen der Ämterkonsultation Stellung genommen.

Anlass zu Kritik gab die Regelung der Meldebefugnis bei möglicherweise invalidisierenden Gesundheitsstörungen. Eine solche Meldung darf nicht nur dann erfolgen, wenn Arbeitnehmer 30 Tage in Folge arbeitsunfähig sind, sondern auch schon dann, wenn jemand aus gesundheitlichen Gründen innerhalb eines Jahres wiederholt jeweils während kürzerer Zeit der Arbeit fernbleiben muss (Art. 1ter Abs.1 lit. b IVV). Im Unterschied zu einer einmonatigen Absenz ist ein mehrmaliges gesundheitsbedingtes Fernbleiben vom Arbeitsplatz während eines Jahres nicht derart ungewöhnlich, dass die Gefahr einer Invalidisierung offensichtlich wäre. Damit beruht die Meldung einer Person bei der IV hier viel stärker auf Verdachtsmomenten, als dies bei einer 30tägigen Absenz der Fall ist.

Die datenschützerische Skepsis ergibt sich aus der Sorge um die Datenrichtigkeit: Der Grundsatz der Datenrichtigkeit bedeutet nicht nur, dass Fakten richtig registriert werden müssen, sondern auch, dass nach Möglichkeit eine Datenbearbeitung nicht auf einen blossen Verdacht hin erfolgen soll. Es ist in diesem Zusammenhang allerdings einzuräumen, dass es legitime Bemühungen um Risikoprävention unentbehrlich machen, einen Verdacht zu überprüfen. Der Gesetzgeber muss sich hier aber immerhin bemühen, das ausschlaggebende Verdachtsmoment so genau wie möglich zu umschreiben. Entsprechend haben wir uns dafür eingesetzt, dass der Fall der mehrmaligen kurzen Absenzen genauer definiert wird, indem eine Mindestanzahl von Krankheitstagen je Kalenderjahr genannt wird. Das BSV hat diese Forderung als federführendes Amt aber verworfen.

1.6.2 Die Neuregelung des Zentralen Informationssystems (ZIS)

Das zentrale Informationssystem der Versicherer zur Bekämpfung des Versicherungsmissbrauchs (ZIS) war bereits früher Gegenstand unserer Tätigkeitsberichte. Die Aktualität früherer Bezugnahmen wird nun relativiert, da das Reglement zum ZIS neu geregelt werden soll. Bislang sind noch nicht alle datenschutzrechtlichen Bedenken ausgeräumt.

Ein wichtiges Mittel der Bekämpfung von Versicherungsmissbrauch ist das zentrale Informationssystem (ZIS). Es ist seit 1995 beim EDÖB (damals EDSB) als Datensammlung angemeldet und soll nun revidiert werden. Die für das ZIS verantwortlichen Organe haben uns das neue Reglement zur Stellungnahme vorgelegt. Als wichtigste Änderungen aufgefallen sind die Verbesserung der Transparenz und die Neufassung der Eintragungstatbestände.

Ersteres haben wir in unserer Stellungnahme ausdrücklich begrüsst. Dagegen haben wir bezüglich der Neuregelung der Erfassungsgründe Vorbehalte angemeldet. Dies deshalb, weil neu auch jene Fälle in der Zentraldatenbank erfasst werden sollen, bei denen der entsprechende Verdacht noch nicht per Gerichtsurteil bestätigt worden ist.

Aus der Sicht des Datenschutzes besteht gegenüber einer Datenbearbeitung, die auf Verdachtsmomenten beruht, stets eine gewisse Skepsis. Verstösse gegen die allgemeinen Datenschutzgrundsätze sind zwar schlecht fassbar, deswegen aber nicht unwahrscheinlich. Als Knackpunkt erweist sich vor allem die Verhältnismässigkeit der Datenbearbeitung; diese lässt sich erst dann aussagekräftig beurteilen, wenn feststeht, ob die Erfassung von Verdachtsfällen für die Missbrauchsbekämpfung einen namhaften Beitrag leisten kann oder nicht.

Wir haben die Vertreter der Versicherungswirtschaft darauf hingewiesen, dass die Erfassung von Verdachtsfällen durchaus eine persönlichkeitsverletzende Datenbearbeitung darstellen kann, und dass uns wesentliche Elemente für eine endgültige Beurteilung noch fehlen. Einzuräumen ist, dass die Versicherungswirtschaft über diese Elemente erst Auskunft geben kann, wenn sie eine verdachtsbasierte Datenbearbeitung während einer bestimmten Zeit umsetzt. Der auf diese Probleme bezogene Dialog zwischen der Assekuranz und uns ist derzeit noch nicht abgeschlossen.

1.6.3 Schweige- oder Auskunftspflicht der privaten Unfallversicherer gegenüber der Steuerverwaltung

Aus dem Kanton St. Gallen wurden wir angefragt, das Verhältnis zwischen verschiedenen gesetzlichen Bestimmungen zu untersuchen. Die Frage lautete, ob es möglich sei, dass die kantonale Steuerverwaltung Daten aus dem Vollzug des AHVG erhalte, während ihr dies im Rahmen des UVG-Vollzuges nicht gewährt werde. Aufgrund der Entstehungsgeschichte der Bestimmungen erwies sich, dass dieser Unterschied gesetzgeberisch gewollt ist. Im Übrigen hat die Steuerverwaltung auch im Bereich des UVG eine zielführende Möglichkeit, indem sie eine Ermessensveranlagung vornimmt und so dem Steuerpflichtigen die Beweislast für die Unrichtigkeit dieser Veranlagung auferlegt.

Die zu prüfende Frage lautete, ob ein privater Unfallversicherer im obligatorischen Bereich Personendaten gegenüber dem Steueramt bekannt geben dürfe bzw. müsse oder ob er in dieser Beziehung der Schweigepflicht nach Art. 33 des Bundesgesetzes über den Allgemeinen Teil des Sozialversicherungsrechts (ATSG) unterliege. Die St. Gallischen Veranlagungsbehörden können gemäss Art. 172 Abs. 1 lit. c und Abs. 2 des St. Gallischen Steuergesetzes (nachfolgend StG SG) dann vom Versicherer Bescheinigungen über ausbezahlte Leistungen verlangen, wenn der Steuerpflichtige die Bescheinigung trotz Mahnung nicht einreicht. Es fragt sich zunächst, ob diese kantonale Bestimmung die Schweigepflicht gemäss Art. 33 ATSG aufheben und den Unfallversicherer zu einer Datenbekanntgabe ermächtigen kann. Diese Frage könnte gemäss Art. 49 Abs. 1 der Bundesverfassung, wonach Bundesrecht entgegenstehendem kantonalem Recht vorgeht, nur dann bejaht werden, wenn der Gesetzgeber im Bundesgesetz über die Unfallversicherung (UVG) die Möglichkeit weiterer gesetzlicher Ermächtigungen zur Datenbekanntgabe vorgesehen hätte. Weil dem aber nicht so ist (weder im ATSG noch im UVG wird auf weitere gesetzliche Ermächtigungen zur Datenbekanntgabe verwiesen), ist in Art. 172 Abs. 1 lit. c in Verbindung mit. Abs. 2 StG SG keine Ausnahmebestimmung zu Art. 33 ATSG zu erblicken. Für dasselbe Resultat scheint unseres Erachtens auch der zweite Satz von Art. 172 Abs. 2 StG SG zu sprechen, der das «gesetzlich geschützte Berufsgeheimnis» vorbehält. In Bezug auf diese Bestimmung haben wir uns jedoch zurückhaltend geäussert, weil es sich hierbei um eine kantonale Bestimmung handelt.

Als nächstes war zu prüfen, weshalb im Bereich der Unfallversicherung eine Schweigepflicht bestehen soll, während die Steuerbehörde beim Vollzug des Bundesgesetzes über die Alters- und Hinterlassenenversicherung (AHVG) Daten einfordern kann. Die geltenden Regelungen von Art. 50a AHVG und Art. 97 UVG zur Datenbekanntgabe (bzw.

zu den Ausnahmen von der Schweigepflicht) weisen verschiedene Parallelen auf, unterscheiden sich aber dennoch in einigen Punkten. Beide führen eine Reihe von Fällen auf, in welchen die Organe der Sozialversicherungen «im Einzelfall und auf schriftlich begründetes Gesuch hin (…) Daten in Abweichung von Artikel 33 ATSG bekannt geben» dürfen. Dabei handelt es sich um Art. 50a Abs. 1 lit. e AHVG und um Art. 97 Abs. 1 lit. i UVG. Die UVG-Regelung enthält in ihren vier Ziffern wortwörtlich denselben Text wie die ersten vier Ziffern unter dem entsprechenden Buchstaben in der Bestimmung des AHVG. Auffällig ist, dass im AHVG noch eine Ziff. 5 figuriert, welche zu Datenbekanntgaben an Steuerbehörden ermächtigt, «wenn die Daten für die Anwendung der Steuergesetze erforderlich sind». Dieser Punkt findet im UVG keine Entsprechung, und man kann sich fragen, ob es sich hierbei um ein gesetzgeberisches Versehen handelt, oder ob der Unterschied vom Gesetzgeber so gewollt war. Wir sind dieser Frage nachgegangen und haben festgestellt, dass die Regelungen von AHVG und UVG zur Datenbekanntgabe in jüngerer Zeit zweimal im gleichen Zug revidiert worden sind. Die letzte Revision erfolgte auf den 1.1.2003 im Rahmen der Einführung des ATSG, während die vorletzte auf den 1.1.2001 durchgeführt wurde im Zusammenhang mit der Anpassung und Harmonisierung der gesetzlichen Grundlagen für die Bearbeitung von Personendaten in den Sozialversicherungen an die Regeln des Bundesgesetzes über den Datenschutz. Die Revision von 2001 zielte gemäss den Aussagen in der Botschaft (BBl 2000 255) nicht auf Änderungen der Regelungen ab. Vielmehr verfolgte diese das Ziel, die Anforderungen des Datenschutzgesetzes zu erfüllen und die vorher grossteils auf Verordnungsstufe vorgesehenen Ermächtigungen zu Datenbekanntgaben auf die Regelungsstufe eines formellen Gesetzes zu heben (Ziffern 1.2.2 und 1.3 der erwähnten Botschaft). Angesichts der Formulierungen in der Botschaft ist davon auszugehen, dass die unterschiedlichen Regelungen vom Gesetzgeber durchaus so gewollt sind und im Übrigen auch schon vor der Revision auf Verordnungsstufe ebenso bestanden haben. So wird in Ziffer 1.3.3 der Botschaft gesagt, in den verschiedenen Sozialversicherungen sei die Liste der Fälle der Datenbekanntgabe «so weit wie möglich vereinheitlicht worden». Und in Ziffer 2.1.4 wird mit Bezug auf die Datenbekanntgabe an Steuerbehörden ausgeführt, diese erfahre «gegenüber den geltenden Bestimmungen und der heutigen Praxis keine materiellen Änderungen». Auch die zweite der erwähnten Revisionen hat den Unterschied zwischen AHVG und UVG nicht eingeführt. So wurde Art. 50a Abs. 1 lit. e AHVG im Rahmen der Revision abgesehen von kleinen redaktionellen Änderungen und der Erwähnung von Art. 33 ATSG aus dem bisherigen Art. 50a Abs. 1 AHVG übernommen (Buchstaben a bis e dieses Absatzes entsprechen den neuen Ziffern 1 bis 5, vgl. den Wortlaut der alten Bestimmung in AS 2000 2749). In Bezug auf das UVG präsentiert sich die Angelegenheit abgesehen von einer geänderten Artikelnummer identisch: Der neue Art. 97 Abs. 1 lit. i entspricht mit seinen vier Ziffern den Buchstaben a bis d des alten Art. 102a Abs. 1 UVG (AS 2000 2760). Diesel-

be Aussage – dass also der fragliche Unterschied nicht im Rahmen dieser Revision eingeführt wurde – ergibt sich auch aus den Ziffern 2.1.1.5 und 2.1.5.6 der Botschaft über die Anpassung des Anhangs zum ATSG, wonach die bisherigen Bestimmungen unverändert gelten sollen (BBl 2002 803).

Aufgrund der dargelegten Überlegungen sind wir zum Ergebnis gekommen, dass der UVG-Versicherer der Veranlagungsbehörde gegenüber zur Verschwiegenheit verpflichtet ist. Das muss jedoch nicht bedeuten, dass die Behörde in ihrer Arbeit blockiert ist, weil sie die Beweislast für steuerbegründende und steuervermehrende Tatsachen trägt. Art. 177 StG SG sieht nämlich die Möglichkeit einer Ermessensveranlagung gerade auch für die Fälle vor, in denen der Steuerpflichtige seine Verfahrenspflichten trotz Mahnung nicht erfüllt hat. Das Wesen der Ermessensveranlagung besteht nun gerade darin, dass dem Steuerpflichtigen der Gegenbeweis auferlegt werden kann, wenn begründete Anhaltspunkte dafür bestehen, dass er Einkommensquellen besitzt, die nicht in der Steuererklärung erscheinen.

1.6.4 Sachverhaltsabklärung beim vertrauensärztlichen Dienst im obligatorischen Krankenversicherungsbereich

Im Verlaufe des Jahres 2006 haben wir beim vertrauensärztlichen Dienst der CSS Kranken-Versicherung AG eine Sachverhaltsabklärung durchgeführt und dabei Mängel festgestellt. Das hat uns veranlasst, im Frühjahr 2007 sechs Empfehlungen zuhanden der CSS zu erlassen.

Anfang 2006 wurde in der Presse über mögliche Datenschutzverletzungen in der CSS, namentlich im Bereich des vertrauensärztlichen Dienstes (VAD), berichtet. Insbesondere wurde gemeldet, dass eine unverhältnismässig grosse Zahl von CSS-Mitarbeitenden – die Rede war von rund 400 Personen – Zugriff auf sensitive Versichertendaten hätte. Im Rahmen unserer Aufsichtstätigkeit haben wir entschieden, den Sachverhalt abzuklären. Dabei stellten wir fest, dass der Datenschutz beim VAD der CSS tatsächlich Mängel aufwies. Wegen des fehlenden standardisierten Verfahrens für die Berechtigungsvergabe konnte rückwirkend indessen nicht mehr festgestellt werden, ob auch Unberechtigte Zugang zum sensiblen Bereich des VAD erhalten hatten. Dies ist im Rahmen des vom BAG im Mai 2006 eingeleiteten Strafverfahrens abzuklären. Die Frage, ob tatsächlich rund 400 Personen Zugang zu diesem Bereich hatten, muss also vorerst offen bleiben.

Gestützt auf die Ergebnisse der Sachverhaltsabklärung sahen wir uns im Frühjahr 2007 veranlasst, sechs Empfehlungen zuhanden der CSS zu erlassen, um die Datenschutzkonformität ihres VAD zu gewährleisten.

Die erste Empfehlung zielte auf einen besseren Schutz der Patientendossiers. Diese werden zum überwiegenden Teil auch heute noch in Papierform bearbeitet und entsprechend aufbewahrt. Die Räumlichkeiten der VAD-Mitarbeitenden waren von den Arbeitsplätzen der übrigen CSS-Mitarbeitenden nicht getrennt, so dass auch keine systematische Zugangskontrolle erfolgen konnte. Wir haben dem VAD empfohlen, die notwendigen getrennten Räumlichkeiten und Infrastrukturmittel zur Verfügung zu stellen und dafür besorgt zu sein, dass die Daten des VAD gegenüber der Versicherung und gegenüber Dritten stets vertraulich gehalten werden können.

Die zweite Empfehlung galt der Stärkung der Unabhängigkeit des VAD. Der vertrauensärztliche Dienst kam bei der CSS nämlich nicht nur – wie es das Krankenversicherungsgesetz (KVG) vorschreibt – in der Grundversicherung zum Einsatz, sondern wurde auch als gesellschaftsärztlicher Dienst für Fälle im Bereich der Zusatzversicherungen (VVG) beigezogen. Daraus ergab sich klar ein Interessenskonflikt, und die vorgeschriebene Unabhängigkeit im Bereich der Grundversicherung wurde unseres Erachtens nicht genügend gewahrt. Eine strikte personelle Trennung des VAD im KVG-Bereich vom Gesellschaftsarzt im VVG-Bereich haben wir deshalb stets als unerlässlich erachtet.

Auch die dritte Empfehlung zielte auf die Stärkung der Unabhängigkeit des VAD. So haben wir empfohlen, dass der Leiter des VAD künftig nicht mehr wie bis anhin dem Leiter Geschäftsbereich Leistung unterstellt sein sollte, sondern direkt der Geschäftsleitung beizuordnen sei.

Die Empfehlungen vier und fünf befassten sich mit der Zugriffsvergabe im elektronischen Anfragebewirtschaftungssystem des VAD. So forderten wir in der vierten Empfehlung, es sei sicherzustellen, dass Mitarbeitende der Administration bei Ablehnungsentscheiden keinen Zugriff auf sensitive Informationen über Versicherte haben dürften. In der fünften Empfehlung verlangten wir, dass die Aufgaben und Pflichten der medizinischen Expertinnen und Experten mit Zugang auf sensitive Bereiche möglichst detailliert zu beschreiben seien. Die Anzahl der Zugangsberechtigten mit solch erweiterten Rechten sei möglichst klein zu halten und ständig zu überprüfen.

In unserer sechsten Empfehlung schliesslich forderten wir die CSS auf, ihren VAD im Rahmen eines externen Audits auf seine Datenschutzkonformität hin zu überprüfen. Uns erschien nämlich die von der CSS angegebene Anzahl von ungefähr 120 Zugriffsberechtigten zum sensiblen Bereich des VAD als zu hoch. Die im Hinblick auf Verhältnis- und Zweckmässigkeit angemessene Zahl muss stets durch eine detaillierte und fundierte Analyse der internen Prozesse festgelegt werden. Während der Sachverhaltsabklärung vermochte die CSS selber weder über die effektive, noch über die notwendige Anzahl Zugriffsberechtigungen genaue Angaben zu liefern. Dieser Umstand hat unseres Erachtens die Notwendigkeit einer unabhängigen, externen und systema-

tischen Auditierung deutlich aufgezeigt. Wir vertraten diesbezüglich auch die Ansicht, dass eine derartige Überprüfung wegen der Komplexität der Sache, der möglichen Veränderungen und des hohen Gefährdungspotentials in regelmässigen zeitlichen Abständen zu wiederholen ist.

Die CSS hat sämtliche Empfehlungen anstandslos angenommen. Wie von uns empfohlen liess sie ein externes Audit durchführen. Unter Beilage eines Berichts wurde uns sodann mitgeteilt, dass das Audit durch die Schweizerische Vereinigung für Qualitäts- und Managment-System (SQS) durchgeführt worden sei. Wichtig erscheint uns in diesem Zusammenhang, dass sich die CSS nunmehr in regelmässigen Abständen diesem externen Audit unterziehen will. Wir haben diese Initiative der CSS begrüsst und erwarten, dass auch andere Institutionen und Firmen dem Beispiel folgen. Auf Ende Jahr hat die CSS sodann den Vollzug aller Massnahmen zu unseren Empfehlungen mitgeteilt.

Die Sachverhaltsabklärung bei der CSS stellt einen Wendepunkt in unserer Zusammenarbeit mit dem BAG dar. Insbesondere die laufende Erhebung über die datenschutzrechtliche Organisation des vertrauensärztlichen Dienstes der Krankenversicherer bezweckt eine zukünftig gemeinsame Ausrichtung in Datenschutzfragen (siehe auch Ziffer 1.6.5).

1.6.5 Erhebung über die datenschutzrechtliche Organisation des vertrauensärztlichen Dienstes der Krankenversicherer

Zusammen mit dem BAG führen wir seit Anfang Dezember 2007 eine Erhebung über die datenschutzrechtliche Organisation bei allen Krankenversicherern durch. Die Aktion hat insbesondere zum Ziel, die Aufsichtsorgane dabei zu unterstützen, Kriterien für eine datenschutzkonforme Organisationsstruktur der Versicherer zu erarbeiten.

In der Öffentlichkeit wurden in den letzten Jahren mehrmals Vorwürfe über missbräuchliche Bearbeitungen von Personendaten durch die Krankenversicherer erhoben. Dies hatte entsprechende Aufsichtstätigkeiten des BAG und unsererseits sowie parlamentarische Vorstösse zur Folge. Sowohl das BAG als auch wir führten bei einzelnen Krankenversicherern entsprechende Abklärungen durch. Diese haben ergeben, dass tatsächlich datenschutzrechtliche Mängel bestehen, die einen Missbrauch von Personendaten ermöglichen. Als Antwort auf einen parlamentarischen Vorstoss beauftragte der Bundesrat bereits im vergangenen Jahr das BAG, künftig vermehrt die Datensammlungen der Versicherer zu prüfen und dabei auch den EDÖB mit einzubeziehen. Verschiedene Krankenversicherer haben zudem von sich aus den Wunsch geäussert, dass beide Aufsichtsorgane vertiefter zusammenarbeiten sollten. Aus die-

sem Grund führen wir nun zusammen mit dem BAG bei allen anerkannten sozialen Krankenversicherern eine Erhebung durch, die Fragen zur Organisation und zum Datenschutz beinhalten. Alle Versicherer haben einen ausführlichen Fragebogen erhalten, der in Zusammenarbeit mit dem EDÖB entstanden ist. Die Versicherer wurden aufgefordert, diesen bis zum 15. Februar 2008 zu beantworten und mit Dokumenten zu belegen.

Wichtiger Zweck der Untersuchung ist es, die Aufsichtsorgane dabei zu unterstützen, Kriterien für eine datenschutzkonforme Organisationsstruktur der Versicherer zu erarbeiten. Zudem sollen aufgrund der Erhebung auch die Kontrollprozesse über die Leistungen datenschutzrechtlich optimiert werden. Es ist vorgesehen, die Kriterien im Herbst 2008 in Form von Empfehlungen festzulegen. Diese sollen die Krankenversicherer dabei unterstützen, ihre Verantwortung für die Einhaltung des Datenschutzes wahrzunehmen.

1.6.6 Identitätsnachweis bei Auskunftsbegehren für den Datenpool der santésuisse

Wir haben im Sommer 2007 auf Anfrage von santésuisse den Prozess der Auskunftserteilung im Zusammenhang mit ihrem Datenpool datenschutzrechtlich beurteilt, jedoch bloss in abstrakter Weise. Obwohl santésuisse allen unseren Bemerkungen Rechnung getragen hatte, wurde das Vorgehen zur Identitätsprüfung kurz darauf aufgrund der Anfrage eines betroffenen Arztes abgeändert.

Santésuisse bearbeitet unter dem Namen «Datenpool» eine grosse Menge von Daten der Krankenversicherer, unter anderem mit dem Ziel, die Wirtschaftlichkeit der Tätigkeit von Leistungserbringern bzw. Ärzten zu beurteilen. Anfang Juli 2007 hat uns diese Institution angefragt, ob wir das Vorgehen bei der Auskunftserteilung nach Art. 8 des DSG beurteilen könnten. Die diskutierte Auskunftserteilung betrifft eine Datensammlung aus dem Vollzug des Bundesgesetzes über die Krankenversicherung (KVG). Dementsprechend ist für die Bearbeitung an sich eine Rechtsgrundlage erforderlich. Gerade die Bestimmungen betreffend Wirtschaftlichkeitskontrolle sind im KVG sehr interpretationsbedürftig formuliert. Es war für uns daher bedeutsam darauf hinzuweisen, dass der EDÖB sich in seiner Tätigkeit primär mit Datenschutzfragen zu den Informationen betreffend Patienten befasst. In Bezug auf Fragen im Zusammenhang mit Daten der Leistungserbringer geht der EDÖB davon aus, dass diese in erster Linie durch die Tarifpartner und allenfalls durch das BAG zu beurteilen sind. Im vorliegenden Fall war aufgrund der uns zur Verfügung gestellten Informationen festzustellen, dass die bearbeiteten Daten keinen Patientenbezug aufweisen.

Bezogen auf den Inhalt der Auskunft hielten wir zunächst fest, dass aus der gesetzlichen Formulierung «alle über die betroffene Person vorhandenen Daten» (vgl. Art. 8 Abs. 2 lit. a DSG) für den vorliegenden Zusammenhang vor allem zwei Dinge folgen: Zunächst sind nicht nur so genannte Rohdaten, sondern auch abgeleitete, berechnete Informationen den Betroffenen mitzuteilen. Und zweitens müssen diese Angaben unabhängig von der physischen Darstellung der Daten beim Inhaber der Datensammlung – elektronisch oder in Papierform – den Betroffenen mitgeteilt werden. Es schien uns jedoch angemessen, dass im Zusammenhang mit der Auskunftserteilung zum Datenpool den betroffenen Ärzten ihre Korrespondenz mit santésuisse nicht in Kopie zugestellt wird. Dies deshalb, weil davon ausgegangen werden kann, dass die entsprechenden Dokumente bei den betroffenen Ärzten schon vorhanden sind. Allerdings dürfte es je nach Formulierung des Auskunftsbegehrens aufgrund von Treu und Glauben erforderlich sein, diese Einschränkung ausdrücklich zu erwähnen.

Was die Identitätsprüfung des um Auskunft ersuchenden Arztes betrifft, so hatten wir santésuisse zu Beginn die Standardvorgehensweise empfohlen, wie sie in der Botschaft zum DSG, in verschiedenen veröffentlichten Dokumenten des EDÖB sowie in den beiden Auflagen des Kommentars beschrieben ist: Die betroffene Person legt ihrem schriftlichen Auskunftsbegehren eine Kopie eines Personalausweises bei, um ihre Identität nachzuweisen. Ein betroffener Arzt hatte sich über diese Anforderung bei uns beschwert und dies gleich mehrfach begründet. Etwas abgekürzt lautete seine Argumentation, dass eine solche Identitätsprüfung erstens nicht erforderlich sei, da santésuisse die Informationen betreffend Adresse, Praxisbewilligung, Konkordatsnummer und EAN-Nummer besitze. Der Pass jedoch enthalte abgesehen von Name und Geburtsdatum keine Angaben, welche für die Berechtigungsprüfung durch santésuisse relevant wären. Zweitens wären Angaben auf einer Kopie einfach zu fälschen, weshalb eine beigelegte Kopie in Hinblick auf die gewonnene Sicherheit wertlos sei. Drittens enthalte der Pass auch Angaben zu physischen Merkmalen, welche der Empfänger des Auskunftsbegehrens nicht zu kennen brauche. Und viertens hänge die sichere Zustellung an den richtigen Empfänger einzig von einer korrekten Adressierung der entsprechenden Sendung ab. Da uns die beschriebene Begründung stichhaltig erschien, haben wir uns mit santésuisse in Verbindung gesetzt, welche sich umgehend bereit erklärt hat, das Verfahren zur Auskunftserteilung anzupassen. Im abgeänderten Verfahren wird nun in der Regel keine Identitätsprüfung mehr vorgenommen, weil die um Auskunft ersuchende Person der santésuisse bekannt ist. Einzig bei Zweifeln betreffend die Zustelladresse scheint es sinnvoll, weitere Abklärungen zur Identität des um Auskunft ersuchenden Arztes zu tätigen.

1.7 Arbeitsbereich

1.7.1 Die Videoüberwachung bei der Post

Die Post kämpft mit dem Phänomen der durch eigene Angestellte begangenen Diebstähle. Ein Videoüberwachungssystem soll dabei Abhilfe schaffen. Durch den Einsatz moderner Verschlüsselungstechniken und dank restriktiver Entschlüsselung der Aufnahmen wird das Problem des Verhaltensüberwachungsverbots am Arbeitsplatz weitgehend gelöst.

Die Videoüberwachung bei der Post war bereits 1999 Gegenstand einer Intervention unserer Dienststelle (vgl. unseren 7. Tätigkeitsbericht 1999/2000, Ziffer 6.1). Damals kamen wir zum Schluss, dass die Videoüberwachung nicht rechtskonform war, weil das Verhaltensüberwachungsverbot verletzt wurde. Die Post ist 2007 mit einem neuen Videoüberwachungsprojekt an uns gelangt und hat uns ersucht, es aus datenschutzrechtlicher Sicht zu beurteilen.

Den Auslöser des neuen Videoüberwachungsprojektes stellen Diebstähle, die durch eigene Angestellte begangen werden, dar. Die Post und ihre Kundschaft erleiden durch diese Delikte einen grossen Schaden. Nach Wunsch des Unternehmens sollen folglich die Briefzentren der Post zukünftig mit Videokameras systematisch überwacht werden. Die heute vorhandenen Sicherheitsmassnahmen haben nach Ansicht der Post zu einem grossen Teil lediglich präventiven Charakter, decken die Sicherheitsbedürfnisse der Briefzentren aber nur ungenügend. Nach Angaben der Firma zählen zu den bestehenden Massnahmen unter anderem Sicherheits-Audits, sporadische Personen- und Effektenkontrollen sowie geschützte Sonderkanäle für spezielle Kunden, die erwiesenermassen regelmässig Opfer von Diebstählen sind. In Zukunft sollen zudem Mechanismen zur automatischen Postverteilung sowie die RFID-Technologie für das Nachverfolgen bestimmter Sendungen zum Einsatz kommen. Die Post begründet das neue Videoüberwachungsprojekt hauptsächlich mit besserer Prävention, effizienterer Überführung von Tätern und Entlastung Unschuldiger. Im Handsortierbereich sollen die Angestellten zum Teil während der gesamten Tagesarbeitszeit im Aufnahmefeld der Videoüberwachungskameras stehen. Es besteht jedoch eine wöchentliche Rotation an nicht überwachte Stellen. Eine ständige Überwachung (Livebildmonitoring) ist nicht vorgesehen. Die 100-tägige Aufbewahrungsdauer der Aufnahmen rechtfertigt die Firma mit der Möglichkeit, spät gemeldete Verluste (z. B. in Zusammenhang mit internationalen Sendungen) zu rekonstruieren. Das Personal wird über bestehende bzw. geplante Sicherheitsmassnahmen gebührend informiert. Das Unternehmen hat bestätigt, dass die Personalverbände involviert worden sind.

Wir haben das Projekt untersucht und der Post zuerst den Schutz des Verhaltens als Bestandteil des Persönlichkeitsbegriffs erläutert. Wir haben diesbezüglich insbesondere hervorgehoben, dass das negative Gefühl, ständig unter Beobachtung zu stehen, einen Druck verursachen kann, der mit der Zeit zu gesundheitlichen Problemen führen kann.

Wir haben der Post gegenüber weiter erläutert, dass Videoüberwachungen zur Beweiserhebung und -sicherung aufgrund der Schwere des Persönlichkeitseingriffs ausschliessliche Aufgabe der Strafjustiz sind. Damit wird die Verantwortung für eine bestimmte Videoüberwachung den öffentlichen Behörden übertragen, in der Annahme, diese können neutraler und rechtmässiger entscheiden. Das Verhaltensüberwachungsverbot lässt somit eine systematische Überwachung durch den Arbeitgeber nicht zu, seien seine Interessen noch so überwiegend. Nur in einer Notstandssituation darf der Arbeitgeber von sich aus das Verhalten der Arbeitnehmer mit einem System überwachen.

Wir haben gegenüber der Post festgehalten, dass diese rechtliche Lage praktische Schwierigkeiten bereitet. Die zuständigen Behörden sind nämlich kaum in der Lage, dem allseits vorhandenen Bedürfnis Privater nach Beweissicherung durch Videoüberwachung nachzukommen. Die Praxis zeigt, dass die an die zuständigen Behörden gerichteten Überwachungsgesuche oft kurzerhand dem Gesuchsteller überlassen werden. Wir haben der Post jedoch zugesichert, dass dank der heutigen Technologie dieser praktischen Schwierigkeit Abhilfe geschaffen wird. Wir haben erläutert, dass systematische Videoüberwachungen nunmehr als gesetzeskonform betrachtet werden können, wenn sie verschlüsselt erfolgen. Die systematische Verschlüsselung der Aufnahmen und die Beschränkung der Entschlüsselung auf konkrete Verdachtsfälle reduziert nämlich das Gefühl der systematischen Verhaltensüberwachung auf ein Minimum. Zu dieser Schlussfolgerung sind wir vor allem nach Gleichstellung der Videoüberwachung mit der Internet- und E-Mail-Überwachung durch die Arbeitnehmer gekommen, wo systematische, jedoch pseudonymisierte Verhaltensüberwachungen unter bestimmten Bedingungen als rechtmässig betrachtet werden können.

Wir haben der Post ausserdem empfohlen, den Zugriff auf die Aufnahmen und deren Entschlüsselung durch ein Doppelschlüssel-System restriktiv zu gestalten. Dabei soll das Unternehmen den ersten, ein Dritter (z. B. eine Arbeitnehmervertretung) den zweiten Teil des Zugriffsschlüssels besitzen. Dadurch soll die Entschlüsselung der Aufnahmen auf konkrete Verdachtsfälle unter Einhaltung des Vieraugenprinzips beschränkt werden. Zentral ist schliesslich die vorherige Information der betroffenen Personen über Verschlüsselung und restriktive Entschlüsselung.

Wir haben der Post schliesslich mitgeteilt, dass durch den Einsatz solcher technischen Lösungen das Problem des Verhaltensüberwachungsverbots durch Videoüberwachung am Arbeitsplatz weitgehend gelöst werden kann (vgl. dazu Ziffer 1.2.3 des vorliegenden Berichts).

1.7.2 Die Bearbeitung von Randdaten des Telefonverkehrs durch das Bundesamt für Informatik und Telekommunikation

Die Bearbeitung, vor allem aber die Bekanntgabe von Randdaten des Telefonverkehrs der Bundesverwaltung an Untersuchungsbehörden und Kostenträger des Bundes durch das Bundesamt für Informatik und Telekommunikation (BIT) setzt Rechtsgrundlagen voraus. Zu deren Schaffung hat der Bund eine Arbeitsgruppe eingesetzt. Bis zur Erarbeitung und Inkraftsetzung der Rechtsgrundlagen haben wir dem BIT empfohlen, sich an unsere Übergangslösung zu halten. Danach sind die Randdaten des privaten Telefonverkehrs bei der Bekanntgabe an die Kostenträger des Bundes auf die Ortskennziffern zu beschränken. Den Untersuchungsbehörden dürfen Randdaten des Telefonverkehrs nur bei begründeten Verdachtsmomenten bekannt gegeben werden.

Das BIT stellt das Bindeglied zwischen der Telekommunikationsdienstanbieterin Swisscom und den einzelnen Bundesorganen dar. In dieser Funktion kommuniziert das Bundesamt regelmässig Randdaten des Telefonverkehrs an die Kostenträger und, auf Anfrage, an Untersuchungsbehörden des Bundes. Mangels einer gesetzlichen Regelung sieht sich das BIT vor allem in Zusammenhang mit Dateneinsichtsbegehren von Untersuchungsbehörden oft mit der Frage seiner Berechtigung zur Datenbekanntgabe konfrontiert. Das Amt hat uns somit ersucht, die Voraussetzungen für einen datenschutzkonformen Umgang mit diesen Daten abzuklären. Wir haben die Problematik differenziert betrachtet und zwischen der regelmässigen Datenbekanntgabe an Kostenträger und der Bekanntgabe an Untersuchungsbehörden im Einzelfall unterschieden.

Wir haben festgehalten, dass für die regelmässige Datenbekanntgabe an die Einheiten der Bundesverwaltung zur Kostenverrechnung Rechtsgrundlagen erforderlich sind; solche sind zurzeit nicht vorhanden. Diesbezüglich ist eine interdepartementale Arbeitsgruppe unter der Leitung des Bundsamtes für Justiz kreiert worden mit dem Auftrag, die Gesetzeslücke zu schliessen. Sowohl das BIT als auch wir sind an dieser Arbeitsgruppe beteiligt.

Die Fernmeldegesetzgebung lässt zu, dass der Vertragspartner vom Anbieter von Telekommunikationsdienstleistungen bei der Rechnungsstellung vollständige Randdaten des Telefonverkehrs erhält. Vollständige private Zielnummern sind jedoch unseres Erachtens für die Fakturierung nicht erforderlich. Wir haben daher dem BIT empfohlen, die Randdaten privater Telefonate bei der Swisscom auf die Ortskennziffern abkürzen zu lassen.

Bei der Festnetztelefonie erfolgt die Unterscheidung zwischen privaten und geschäftlichen Telefonaten in der Regel durch Drücken einer entsprechenden Telefontaste. Voraussetzung dafür ist, dass eine Telefonzentrale besteht, die eine solche Funktion vorsieht. Dies ist beim Bund der Fall. Bei der mobilen Telephonie erfolgt die Unterscheidung zwischen privaten und geschäftlichen Telefondaten am einfachsten durch Benutzung jeweils zweier SIM-Karten.

In Zusammenhang mit der Bekanntgabe von Telefonranddaten an Untersuchungsbehörden bei bundesinternen Straf- oder Administrativuntersuchungen haben wir ebenfalls festgestellt, dass entsprechende gesetzlichen Grundlagen fehlen. Wir haben dem BIT empfohlen, Telefonranddaten an die Untersuchungsbehörde nicht systematisch bei jeder Anfrage, sondern erst bei Vorliegen begründeter und konkreter Verdachtsmomente eines untersuchungsrelevanten Verhaltens bekannt zu geben. Unbegründete Behauptungen, vage Gefühle, persönliche Eindrücke, Vermutungen oder der blosse Mangel an Vertrauen gegenüber einem Angestellten stellen in der Regel keine ausreichende Grundlage für die Einleitung einer Untersuchung und folglich für eine Datenbekanntgabe durch das BIT an die Untersuchungsbehörde dar.

1.7.3 Empfehlung zu den Drogentests der SBB

Im Frühjahr 2007 hat die Presse über Drogentests bei den SBB berichtet. Danach werden unter 40-jährige Mitarbeitende mit sicherheitsrelevanten Funktionen auf den Konsum illegaler Drogen getestet. Im Falle eines positiven Resultats müssen Betroffene eine Vereinbarung unterschreiben, nach der sie künftig auch in der Freizeit auf den Konsum von Cannabis verzichten. Wir haben u. a. empfohlen, Grenzwerte für Drogen- und Alkoholtests einzuführen, bei deren Unterschreitung keine Datenbearbeitungen erfolgen sollen.

Zunächst haben wir festgestellt, dass derzeit keine ausreichende gesetzliche Grundlage für die Vornahme der Drogentests besteht. Weder die geltenden Bestimmungen noch die Bahnreform 2 sehen Urin-, Blut- und andere invasive Tests auf Drogenkonsum ohne entsprechende Indikation vor. Vielmehr ermöglichen die künftigen Bestim-

mungen der Bahnreform 2 nur Atem-Alkoholtests ohne konkreten Verdacht. Die heutige Praxis zeigt jedoch, dass Mitarbeitende verdachtsunabhängig zum Drogentest gezwungen werden.

Gestützt auf die Ergebnisse unserer Abklärung haben wir den SBB empfohlen, sich für die Vornahme von Drogentests an den entsprechenden Bestimmungen der Bahnreform 2 zu orientieren. Wir haben ebenfalls empfohlen, Grenzwerte für Drogen- und Alkoholtests einzuführen, bei deren Unterschreitung keine Datenbearbeitungen erfolgen sollen.

Das Bundesamt für Verkehr (BAV) hat sich daraufhin bereit erklärt, für den Zeitraum bis zum Inkrafttreten der entsprechenden Rechtgrundlagen mittels einer Richtlinie Grenzwerte zu prüfen und einzuführen.

Die Empfehlung ist im Anhang 4.4 dieses Tätigkeitsberichts zu finden.

1.7.4 Revision des Bundespersonalgesetzes

Das Bundespersonalgesetz wird zurzeit einer umfassenden Revision unterzogen. Dabei sollen auch die neuen Aufgaben des Personalinformationssystems der Bundesverwaltung (BV PLUS) gesetzlich verankert werden. Zu den neuen Aufgaben des BV PLUS zählen u. a. die Mitarbeiterbeurteilungen sowie die Zeiterfassung. Das entsprechende Abrufverfahren (E-Gate) und die neu zugriffsberechtigten Stellen sind ebenfalls im Bundespersonalgesetz vorzusehen.

Wir haben im Rahmen der Ämterkonsultation zur Revision des Bundespersonalgesetzes (BPG) festgehalten, dass die Erweiterung des Datenbearbeitungssystems BV PLUS mit teils bereits wahrgenommenen, teils noch zu implementierenden neuen Aufgaben vom Gesetzgeber nicht mehr ignoriert werden kann. Wir haben insbesondere verlangt, dass die Mitarbeiterbeurteilungen, die Zielvereinbarungen sowie die Zeiterfassung als neue Funktionen von BV PLUS explizit im Gesetzestext aufzunehmen sind. Weiter haben wir gefordert, die Zugriffe auf solche besonders schützenswerte Personendaten und Persönlichkeitsprofile auf die jeweiligen Mitarbeiter und ihre Vorgesetzten zu beschränken und sie entsprechend im Gesetz zu verankern. Das Zugriffsrecht der Personaldienste hat sich dabei auf die Beurteilungsstufe und allenfalls auf administrative Daten zu beschränken.

In Zusammenhang mit dem entsprechenden Abrufverfahren (E-Gate) haben wir eine höhere Regelungsdichte sowie, technisch, die Verschlüsselung gefordert. Schliesslich haben wir beantragt, die Zugriffsrechte des Eidgenössischen Personalamtes und der technischen Support-Stellen auf die Daten im BV PLUS explizit und restriktiv zu regeln.

1.7.5 Personalbewirtschaftungssystem der Bundesverwaltung

Wir nehmen zurzeit eine Überprüfung der Einhaltung des Datenschutzes bei der Benutzung des Personalbewirtschaftungssystems der Bundesverwaltung BV PLUS vor. Ziel der Kontrolle ist die Gegenüberstellung des technischen und organisatorischen Ist-Zustandes von BV PLUS mit den einschlägigen gesetzlichen Grundlagen.

Wir werden lediglich die Einhaltung der wesentlichen datenschutzrechtlichen Vorgaben kontrollieren und nur stichprobenartig detaillierte Untersuchungen vornehmen. Als Kontrollgegenstände gelten hauptsächlich die Rechtmässigkeit der Datenbeschaffung und die Einhaltung von Treu und Glauben, die Zweckbindung und die Verhältnismässigkeit des Datenkatalogs, die Datensicherheitsmassnahmen sowie die Gewährleistung der Rechtsansprüche der Betroffenen. Die Kontrollgegenstände werden im Rahmen einzelner Prozesse des BV PLUS bei verschiedenen Ansprechpartnern untersucht. Als solche gelten das Kompetenzzentrum für Humanressourcen des Eidgenössischen Personalamtes (EPA), das Kompetenzzentrum SAP des Bundesamtes für Informatik und Telekommunikation (BIT) und der Personaldienst der Bundeskanzlei (BK). Letzterer soll beispielshalber für die gesamte Bundesverwaltung als Endbenutzer kontrolliert werden. Allfällige Empfehlungen an den Personaldienst der BK aufgrund der Kontrollresultate können unter Umständen für die Gesamtheit der Bundesverwaltung Geltung haben. Bei diesem Dienst werden hauptsächlich Identifikation und Authentifizierung, Passwort-Management, Bildschirmschoner und Schulung, beim Kompetenzzentrum SAP des BIT vor allem die Datensicherheitsmassnahmen kontrolliert werden. Gegenstand unserer Untersuchungen beim Kompetenzzentrum für Humanressourcen des EPA ist hauptsächlich der Datenkatalog.

Nach Beantwortung unserer Fragebögen sowie nach Durchführung der ersten Interviews haben wir die entsprechenden Sitzungsprotokolle erstellt und den Beteiligten zur Überprüfung und allfälligen Ergänzung unterbreitet. Die Antworten stehen zurzeit noch aus. Bei Bedarf werden weitere Interviews oder schriftliche Befragungen sowie Augenscheine folgen.

1.8 Handel und Wirtschaft

1.8.1 Revision des Aktienrechts; Umgang mit Handelsregistereinträgen

Das neue Aktienrecht ermöglicht eine vereinfachte Kommunikation zwischen der Gesellschaft und ihren Anteilseignern durch die Nutzung elektronischer Medien. Zudem wird in diesem Rahmen die Transparenz und Aktualität des Handelsregisters erhöht, indem verbindliche Fristen zur Eintragung von Ereignissen festgesetzt wurden. Wir vertreten allerdings die Meinung, dass darüber hinaus auch Fristen für die Sperrung des öffentlichen Zugangs zu Handelsregistereinträgen festgesetzt werden müssen, wenn diese im Geschäftsverkehr ihre Relevanz verloren haben. Insbesondere bei Löschungen (wie beispielsweise nach Konkursen) überwiegt nach einer gewissen Zeit das persönliche Interesse, ein vorurteilfreies Leben zu führen (Recht auf Vergessen). Daher kann es nach unserer Meinung nicht angehen, dass sämtliche Handelsregistereinträge «bis in alle Ewigkeit» öffentlich frei zugänglich sind.

Das revidierte Aktienrecht geht unter anderem vermehrt auf die Möglichkeiten der elektronischen Kommunikation ein und sieht erstmals den Einsatz von elektronischen Medien in der Kommunikation zwischen der Geschäftsleitung und den Aktionärinnen und Aktionären vor. Es regelt die Möglichkeiten einer multilokalen Generalversammlung (GV), bei denen die Bild- und Tonübertragung simultan an die verschiedenen Tagungsorte übertragen wird, die elektronische Einberufung der GV, die elektronische Vollmacht zur Stimmrechtsvertretung, die Verwendung elektronischer Mittel in der GV und eine vollständig elektronische GV, bei der auf eine herkömmliche Versammlung an einem Tagungsort ganz verzichtet werden kann. Wir geben hierbei zu bedenken, dass bei der konkreten Ausgestaltung der neuen Kommunikationsformen durch Unternehmen besonders datenschutzrechtlich relevante Aspekte beachtet werden müssen.

Im Zuge dieser Revision wurden auch mehrere Artikel im Hinblick auf die Fristen für die Veröffentlichung von Ereignissen im Handelsregister geändert. Wir vertreten die Meinung, dass darüber hinaus auch Fristen für die Entfernung von Handelsregistereinträgen vom allgemeinen öffentlichen Zugang definiert werden müssen. Da gewisse Veröffentlichungen im Handelsregister nach einer bestimmten Frist an Relevanz verlieren, sollten diese unseres Erachtens dann auch nicht mehr öffentlich zugänglich sein. Dies trifft vor allem auf Löschungen (sowohl von Vollmachten als auch von Firmen) zu, da diese mit der Zeit für den reibungslosen Verlauf des Geschäftsverkehrs an Relevanz verlieren. Zudem nimmt das persönliche Interesse einer von einer Löschung

betroffen Person mit der Zeit zu, ein vorurteilsfreies, also nicht übermässig von der Vergangenheit geprägtes Leben führen zu können (Recht auf Vergessen). Vor diesem Hintergrund kann es nach unserer Meinung nicht angehen, dass Daten «bis in alle Ewigkeit» öffentlich frei zugänglich sind (vgl. dazu auch Ziffer 1.8.2).

Wir haben daher vorgeschlagen, Fristen für die Sperrung des öffentlichen Zugangs als Norm in den «dreissigsten Titel: Das Handelsregister» des Obligationenrechts aufzunehmen. Da diese Änderung im laufenden Revisionsverfahren zeitlich nicht mehr möglich war, werden wir unseren Vorschlag im Gesetzgebungsverfahren erneut einbringen.

1.8.2 Die private Publikation von Handelsregisterdaten

Wer als Einzelunternehmung, als Personengesellschaft oder als juristische Person am Wirtschaftsleben teilnimmt, muss im Handelsregister eingetragen sein. Dabei sind die Vertretungsorgane mit vollem Namen anzugeben. Die Daten werden im Internet gesamthaft publiziert, von wo aus sie von einigen privaten Wirtschaftsauskunfteien integral übernommen werden. Diese reichern die Daten um andere Informationen an, strukturieren sie neu und veröffentlichen die Resultate ihrer Arbeit ebenfalls im Internet. Dies ist nicht nur dann problematisch, wenn die Daten nicht mehr aktuell sind. Die Wirtschaftsauskunfteien sollten auch in anderem Zusammenhang nicht über die staatliche Datenbearbeitung hinausgehen.

Die Websites der Wirtschaftsauskunfteien werden rege genutzt. Dieser Erfolg führt oft dazu, dass die Internetrecherche nach dem Namen natürlicher Personen an prominenter Stelle auf das Webangebot der Auskunfteien verweist. Viele Personen stören sich daran. Sie beanstanden entweder, es würde über Sachverhalte Auskunft gegeben, welche gar nicht mehr aktuell sind, oder sie stören sich aus prinzipiellen Gründen an der privaten Duplizierung von Handelsregisterdaten. In beiden Fällen verhält es sich so, dass gegenüber den privaten Wirtschaftsauskunfteien ein Löschungsrecht besteht. Verschiedene Wirtschaftsauskunfteien akzeptieren dies allerdings nicht.

Der Grossteil der bei uns eingegangenen Beanstandungen betraf eine bestimmte Wirtschaftsauskunftei. Wir sind daher mit einer Empfehlung an dieses Unternehmen gelangt, deren Hauptforderung darin bestand, das Löschungsrecht der betroffenen Personen künftig zu gewährleisten. Darüber hinaus stellten wir fest, dass die Datenbearbeitung auch in verschiedenen anderen Punkten geändert werden muss: In gewissen Konstellationen besteht im Hinblick auf die Datenaktualität eine Pflicht zur Datenlöschung auch ohne ausdrückliches Löschungsbegehren.

Die angegangene Wirtschaftsauskunftei hat unsere Empfehlung in allen Teilen zurückgewiesen. Wir haben die Angelegenheit daher dem Bundesverwaltungsgericht zur Überprüfung vorgelegt, welches seit der Revision der Bundesrechtspflege für Datenschutzklagen des EDÖB zuständig ist.

Mit seinem Urteil vom 26. Februar 2008 hat das Bundesverwaltungsgericht unsere Klage zwar abgewiesen, aber dennoch zahlreiche Fragen geklärt und damit für die betroffenen Personen Rechtssicherheit geschaffen. Es kam insgesamt zum Schluss, dass das öffentliche Weiterverbreitungsinteresse an Handelsregisterinformationen zeitlich unbeschränkt und unabhängig davon besteht, ob die Datenquelle öffentlichen oder privaten Ursprung ist, solange die Daten inhaltlich nicht verändert werden. Wir haben dies zur Kenntnis genommen. Dennoch sind wir der Meinung, dass Handelsregisterdaten, welchen keine rechtliche und tatsächliche Bedeutung mehr zukommt, auch nicht mehr im Internet öffentlich zugänglich sein müssen, und das persönliche Interesse der betroffenen Person in einem solchen Fall höher einzustufen ist als das öffentliche Weiterverbreitungsinteresse der Handelsregisterinformationen.

Aus diesem Grund werden wir uns mit der Thematik weiter auseinandersetzen, um gegebenenfalls auf dem Wege einer Gesetzesrevision die notwendigen Voraussetzungen für eine Sperrung von Handelsregisterinformationen, für die kein öffentliches Weiterverbreitungsinteresse mehr besteht, anzuregen. Von einem Weiterzug an das Bundesgericht sahen wir unter den gegebenen Umständen ab (vgl. dazu auch Ziffer 1.8.1).

1.8.3 Der gesetzeskonforme Umgang mit Bonitätsdaten

Bonitätsdaten sind all jene Personendaten, die über die Kreditwürdigkeit einer Person Auskunft geben. Sie werden von zahlreichen Akteuren bearbeitet. Dazu gehören vor allem Gläubiger, welche ihre Rechnungen nicht (oder zu spät) beglichen erhalten, die Inkassounternehmen, die mit der Einbringung der Forderungen beauftragt werden, und die Kreditauskunfteien, welche durch Zentraldatenbanken die Gefahr des Kreditausfalls zu verhindern suchen. Es sind in der Praxis bezüglich all dieser Datenbearbeitungsschritte rechtliche Unsicherheiten zu beobachten. Wir stehen mit Vertretern der Bonitätsdatendienstleister in einem konstruktiven Dialog, um die Rechtssicherheit zu verbessern.

Ein Grossteil der Bevölkerung ist sich des Vorhandenseins von Bonitätsdatenbanken gar nicht bewusst. Soweit die Datenbanken der Kreditauskunfteien öffentlich überhaupt thematisiert werden, nennt man sie gerne «Schuldnerdatenbanken», und als solche werden sie bisweilen auch skandalisiert. Daran ist zwar richtig, dass unrichtige

Bonitätsdaten einigen Schaden anrichten können; die Bonitätsdatenbanken erfüllen aber auch eine wichtige Funktion im Dienste der kreditgebenden Wirtschaft. Vor voreiligen Schlüssen ist also zu warnen. Zunächst gilt es das Problem als Datenbearbeitungskette mit mehreren datenschutzrechtlich eigenverantwortlichen Akteuren genau zu analysieren, wobei der Fokus auf die Schnittstellen dieser Akteure gelegt werden muss.

Eine erste Schnittstelle ist die Zusammenarbeit von Gläubigern und Inkassounternehmen. Beide Akteure müssen ihren Teil dazu beitragen, dass die Beanstandung von geltend gemachten Forderungen (Bestand oder Höhe) innert nützlicher Frist überprüft werden kann. Im Hinblick auf mögliche Fehlleistungen der Gläubiger – seien diese nun administrativer oder rechtlicher Art – kann die Klärung von Streitfällen nicht einfach den Betreibungsämtern und den Gerichten überlassen werden, da dies regelmässig zum Nachteil der betroffenen Personen geschieht. Die Gläubiger und die Inkassounternehmen müssen also sicherstellen, dass eine rasche Behandlung von Problemfällen möglich ist (Datenrichtigkeitskonzept), und es ist ausserdem zu regeln, wie mit Forderungen umgegangen wird, die sich in der «Schwebe» befinden (idealerweise vorübergehende Aussetzung der Inkassomassnahmen).

Eine weitere wichtige Schnittstelle besteht zwischen den Inkassobüros und Kreditauskunfteien. Hier herrscht teilweise die irrige Annahme vor, dass ein Datentransfer ohne jede Einschränkung möglich sei. Aus unserer Optik ist es unabdingbar, dass genau definiert wird, welche Falldaten weitergegeben werden dürfen und welche nicht (Verhältnismässigkeit der Datenbearbeitung). Der Dialog mit Partnern aus der Branche ist derzeit im Gange.

Letzteres gilt auch für all jene Fragen, die allein die Kreditauskunfteien betreffen. Hier gilt es namentlich zu klären, wie lange sich ein bonitätsrelevantes Negativereignis (z.B. Betreibung) auswirken darf, wann das so genannten Kredit-Scoring ein Persönlichkeitsprofil darstellt, und welche Pflichten den Kreditauskunfteien im Zusammenhang mit der (heute mangelhaft gewährleisteten) Transparenz der Datenbearbeitung entstehen (vgl. auch Ziffer 1.2.6).

1.9 Finanzen

1.9.1 Datenschutz im internationalen Zahlungsverkehr (SWIFT)

Durch den Bericht der «New York Times» vom 23. Juni 2006 wurde bekannt, dass die Society for Worldwide Interbank Financial Telecommunication (SWIFT) den USA zum Zweck der Terrorismusbekämpfung in begrenzten Umfang Zugang zu den im Operation Center in den USA befindlichen Daten gewährt hat. Die damit verbundenen Datenschutzprobleme konnten wir in Zusammenarbeit mit dem Bundesrat und den Schweizer Banken angehen, indem im Rahmen einer politischen Lösung mit den USA Sicherheitsgarantien vereinbart wurden und die Kundschaft von ihren Banken aktiv über die mögliche Weitergabe an die US-Behörden informiert wurde. Die SWIFT hat zudem angekündigt, in Zukunft nur noch die Transaktionsdaten in den USA zu bearbeiten, die den transatlantischen Zahlungsverkehr betreffen. Um diese Lösung technisch realisieren zu können, baut die SWIFT in der Schweiz ein drittes Operation Center auf.

Im Nachgang zu den Enthüllungen der «New York Times», wonach die US-Administration im Rahmen der Terrorismusbekämpfung Zugriff auf die Transaktionsdaten der SWIFT erhalten hat (vgl. unseren 14. Tätigkeitsbericht 2006/2007, Ziffer 1.8.1), wurden durch uns und die Schweizer Regierung Massnahmen zur Einhaltung des Datenschutzes im internationalen Zahlungsverkehr getroffen. Im Anschluss an die Analyse des Sachverhalts kamen wir zum Schluss, dass durch die Weitergabe der Transaktionsdaten durch die SWIFT das DSG in zweifacher Hinsicht verletzt wurde. Zum einen sind die in der Schweiz ansässigen Finanzinstitute ihrer Informationspflicht gegenüber ihren Kunden nicht nachgekommen, indem sie es unterlassen haben, sie über eine Datenweitergabe durch die SWIFT beziehungsweise über die Möglichkeit einer solchen Weitergabe zu informieren. Zum anderen erfolgte ein Datentransfer in die USA, wo kein angemessener Datenschutz gewährleistet ist. Beide Probleme wurden in Kooperation mit der Schweizer Regierung und den in der Schweiz ansässigen Finanzinstituten gelöst.

Im Hinblick auf die Informationspflicht der Banken haben wir den innovativen Weg einer «überwachten Selbstregulierung» der Banken beschritten, indem wir es den Banken überlassen haben, ihrer Informationspflicht in der Form nachzukommen, welche ihren Bedürfnissen am besten entspricht. Wir haben diesen Weg vorwiegend mit Blick auf das Vertrauen in den Finanzplatz Schweiz gewählt. In enger Zusammenarbeit mit der schweizerischen Bankiervereinigung erarbeiteten wir Informationsschreiben an

die Bankkunden, mittels welchen der Informationspflicht Genüge getan wurde. Diese Schreiben wurden von den Schweizer Banken bereits versandt. Im Vergleich zum europäischen Ausland, wo eine solche Information meist lediglich über einen entsprechenden Vermerk in den AGB stattfindet, haben wir hierdurch eine aktive Information der Schweizer Bankkunden in diesem Bereich erreicht. Gleichzeitig wurde durch die aktive und eigenständige Information der Kundschaft durch die Banken das Vertrauen in einen funktionierenden Datenschutz gestärkt.

Im Hinblick auf die Notwendigkeit einer politischen Lösung, welche sowohl die Anliegen der Terrorismusbekämpfung als auch die Datenschutzordnung der betroffenen Länder – so auch der Schweiz – respektiert, konnte eine zufrieden stellende Lösung ausgehandelt werden. Hierfür wurden mit den USA Sicherheitsgarantien beim Zugriff auf die Daten der SWIFT vereinbart. So kann die US-Administration von der SWIFT lediglich verlangen, innerhalb ihrer Datensammlung eine Suchabfrage zu starten, wenn Beweise vorliegen, dass eine Zielperson mit Terrorismus oder dessen Finanzierung in Verbindung steht. Die Ergebnisse der Suchabfrage werden im Anschluss nur dann der US-Administration übermittelt, wenn die Abfrage erfolgreich war. Damit erhält die US-Administration ausschliesslich zur Abklärung eines konkreten und bereits bestehenden Sachverhalts Zugang zu den betreffenden Daten. Zudem werden die Suchabfragen, einschliesslich der Beweise, welche zur Abfrage geführt haben, protokolliert. Weiterhin sieht die Vereinbarung vor, dass eine renommierte europäische Persönlichkeit ernannt wird, deren Aufgabe es ist, zu überprüfen, dass das Programm im Einklang mit den Zusicherungen zur Kontrolle des Schutzes der personenbezogenen Daten aus der EU durchgeführt wird. Damit gewährleistet die US-Administration im Bezug auf die SWIFT-Daten einen Datenschutz, welcher der Schweizer Rechtsordnung genügt.

Im Rahmen der Reorganisation des Geschäftsbetriebs und des in den letzen Jahren stark gestiegenen Transfervolumens hat sich die SWIFT entschieden, bis Ende 2009 neben den beiden Operation Center in Belgien und den USA ein drittes in der Schweiz aufzubauen und in diesem Zuge den Überweisungsverkehr in zwei Zonen (eine europäische und eine transatlantische) zu separieren. In diesem Rahmen würden innereuropäische Überweisungen von den beiden Operation Center in der Schweiz und in Belgien und transatlantische Überweisungen von den Operation Center in den USA und der Schweiz bearbeitet. Da die US-Administration lediglich auf die Daten, die im Operation Center in den USA bearbeitet werden, zugreifen kann, werden in Zukunft sämtliche innereuropäischen Überweisungen für die US-Administration nicht mehr direkt zugänglich sein.

1.9.2 Weitergabe von internationalen Zahlungsverkehrsdaten an ausländische Regierungen zum Zwecke der Durchsetzung von Sanktionsbestimmungen

Für Schweizer Kreditinstitute kann es im Rahmen ihrer internationalen Geschäftstätigkeit erforderlich sein, gegenüber Drittstaaten (insbesondere den USA) nachzuweisen, dass sie deren Sanktionsbestimmungen einhalten. Ansonsten kann ihnen der geschäftliche Zugang zu dem Staat unter Umständen erschwert werden. In diesem Rahmen zog ein Schweizer Kreditinstitut in Erwägung, im Rahmen des internationalen Zahlungsverkehrs, bei dem es als Transferbank fungierte, freiwillig Transferdaten an die USA zu übermitteln. Nach Abklärung des Sachverhalts und der rechtlichen Lage kamen wir zum Schluss, dass zum Nachweis der Einhaltung von Sanktionsbedingungen lediglich eine freiwillige Übermittlung von anonymisierten Transferdaten zulässig ist.

Wir haben für ein Schweizer Kreditinstitut abgeklärt, inwieweit es nach dem DSG zulässig ist, im Rahmen der Transfergeschäfte bei internationalen Überweisungen Daten an ausländische Behörden weiterzugeben. Im konkreten Fall war das Schweizer Kreditinstitut ein Zwischenglied in der Zahlungskette bei internationalen Zahlungsströmen und wollte gegenüber der US-Administration den Nachweis erbringen, dass es im Rahmen der Transfergeschäfte die US-Sanktionsbestimmungen gegen den Iran eingehalten hat.

Da beim Transfer von Überweisungen personenbezogene Daten bearbeitet werden, ist das DSG anwendbar. Eine Datenweitergabe ist daher immer nur dann möglich, wenn hierdurch die Persönlichkeit der betroffenen Person nicht widerrechtlich verletzt wird. Da für eine Übermittlung der Transaktionsdaten an die US-Behörden keine gesetzliche Grundlage besteht und kein überwiegendes öffentliches oder privates Interesse ersichtlich ist, wurde geprüft, inwieweit von einer implizit angenommenen Einwilligung ausgegangen werden kann.

Das Schweizer Kreditinstitut hat hierbei argumentiert, dass eine Person, welche einen Überweisungsauftrag in US-Dollar ausführen lässt, damit rechnen muss, dass die Datenbearbeitung in den USA durchgeführt wird. Innerhalb der Finanzwelt ist es allgemein bekannt, dass Devisentransaktionen – bis auf ganz wenige Ausnahmen – im Währungsland stattfinden und dass daher inländische mit ausländischen Banken Nostro-/ Vostrokontenbeziehungen unterhalten. Privatpersonen ist dies allerdings weitgehend unbekannt, und ein solches Wissen kann nach unserer Meinung nicht allgemein vorausgesetzt werden. Daher ist es Aufgabe der Bank des Auftraggebers

einer Finanztransaktion in Fremdwährungen (hier US-Dollar), ihre Kunden darüber zu informieren, dass ein Datentransfer zu einer Bank im Fremdwährungsland (hier USA) stattfinden kann. Im Rahmen des Transfergeschäfts kann allerdings die Transferbank durchaus davon ausgehen, dass die Bank des Auftraggebers ihren Kunden entsprechend informiert hat.

In den Fällen, in denen das Schweizer Kreditinstitut nun tatsächlich den Transfer über eine Bank oder Tochtergesellschaft in den USA abgewickelt hat und die US-Behörden basierend auf einer gesetzlichen Grundlage auf diese Daten zugreifen, steht dem aus datenschutzrechtlicher Sicht nichts entgegen, da für den Datentransfer ins Ausland zum Zwecke der Ausführung der Überweisung die Zustimmung des Kunden vorliegt. Hingegen würde eine nachträgliche freiwillige Datenübertragung an die US-Behörden gegen die Grundsätze der Datenbearbeitung (insbesondere das Zweckmässigkeitsprinzip) verstossen. Daher gelangen wir zum Schluss, dass eine freiwillige Datenübermittlung an die US-Behörden im vorliegenden Fall nicht zulässig ist. Kein Verstoss gegen das Datenschutzgesetz ist gegeben, wenn die US-Behörde die im Rahmen des Transaktionsprozesses in die USA übermittelten Transferdaten bei einer Filiale des Schweizer Kreditinstituts in den USA oder bei einer Partnerbank in den USA abfragt und hierzu gesetzlich legitimiert ist.

Darüber hinaus gaben wir zu bedenken, dass sich US-Sanktionen nicht gegen einzelne Personen, sondern im Normalfall gegen Staaten richten. Daher steht dem Schweizer Kreditinstitut die Möglichkeit offen, die zu übermittelnden Transaktionsdaten so zu anonymisieren, dass zwar noch ein Rückschluss auf Staat und eventuell Stadt von Sender und Empfänger, nicht aber auf den eigentlichen Sender oder Empfänger der Transaktion möglich ist. Auf diese Weise könnte das Schweizer Kreditinstitut gegenüber den ausländischen Behörden nachweisen, dass sie deren Sanktionsbestimmungen einhält, und gleichzeitig dem Datenschutz angemessen Rechnung tragen.

1.10 International

1.10.1 Internationale Zusammenarbeit

Die Globalisierung der Gesellschaft bringt Risiken für den Schutz der Rechte und Freiheiten mit sich, denen auf internationaler Ebene begegnet werden muss, namentlich um die Einführung einer universellen Datenschutzregelung zu erwirken. Der EDÖB wirkt denn auch aktiv an der internationalen Zusammenarbeit mit und beteiligt sich an den Arbeiten des Europarates, an der Europäischen Konferenz der Datenschutzbeauftragten, an den gemeinsamen Kontrollinstanzen Schengen und Eurodac, an der Internationalen Konferenz der Datenschutzbeauftragten und an der Frankophonen Vereinigung der Datenschutzbehörden.

Europarat

Wir waren an den Arbeiten des beratenden Ausschusses für das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung von personenbezogenen Daten (T-PD) und seines Büros beteiligt. Der beratende Ausschuss verabschiedete namentlich eine Stellungnahme zur Auslegung der Begriffe der automatischen Verarbeitung und des Inhabers der Datensammlung im Kontext der weltweiten Telekommunikationsnetze. Er erinnerte insbesondere daran, dass der Begriff der automatischen Verarbeitung im Sinne des Übereinkommens 108 so auszulegen ist, dass er auch die Datenerhebung im Hinblick auf eine automatische Verarbeitung umfasst. Was den Inhaber der Datensammlung oder den für die Verarbeitung Verantwortlichen anbelangt, so weist der Ausschuss darauf hin, dass sich häufig nur schwer bestimmen lässt, wer genau der Inhaber der Datensammlung ist, denn in der realen Wert der globalen Telekommunikationsnetze teilen sich mehrere Akteure die Verantwortung für die Datenbearbeitung. Der Ausschuss erinnert jedoch daran, dass der Inhaber der Datensammlung weiterhin gegenüber der von den Verarbeitungshandlungen betroffenen Person haftbar ist, selbst wenn das bedeutet, dass er in der Folge eine Regressklage gegen einen Zulieferer oder einen Mitverantwortlichen für die Verarbeitung anstrengen muss. Wenn daher mehrere Akteure jeweils einen Teil der Verarbeitung, gegebenenfalls in verschiedenen Ländern, durchführen, ist es an ihnen, die Verantwortlichkeit jedes Einzelnen unter Berücksichtigung der gesetzlichen Kriterien klar abzugrenzen. Der T-PD verabschiedete auch eine Stellungnahme zum Entwurf für einen Rahmenbeschluss des Europäischen Rates über den Schutz personenbezogener, im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeiteter Daten. Der

Ausschuss verweist auf die Geltung des Übereinkommens 108 auch für die polizeiliche und justizielle Zusammenarbeit in Strafsachen und betont, dass der Rahmenbeschluss die Anwendung des Übereinkommens nicht in Frage stellen kann und dass er vielmehr die im Übereinkommen definierten Grundprinzipien des Datenschutzes noch zusätzlich aufwerten sollte. Darüber hinaus spricht sich der Ausschuss für eine Anwendung des Beschlusses auf die Gesamtheit der einzelstaatlichen Datenverarbeitungen und nicht nur auf den grenzüberschreitenden Datenverkehr aus, um die polizeiliche und justizielle Zusammenarbeit zu erleichtern und einen wirksamen Schutz zu gewährleisten. Die Datenübermittlung in Drittstaaten muss den Anforderungen des Zusatzprotokolls entsprechen, und insbesondere sind bei Ausnahmen vom Grundsatz des angemessenen Schutzniveaus diese unter Berücksichtigung der Zweckbestimmung des Rahmenbeschlusses möglichst spezifisch zu definieren. Der T-PD verabschiedete auch eine Stellungnahme zur Vereinbarkeit der ADAMS-Anwendung (Anti Doping Administration and Management System) mit den Datenschutznormen des Europarates. Gemäss seinen Feststellungen wirft das von der Welt-Dopingagentur eingeführte Datenverarbeitungssystem mehrere Fragen zum Datenschutz auf, die namentlich mit der Information der betroffenen Personen, dem freien und aufgeklärten Einverständnis und der Rechtsgrundlage der Verarbeitung zusammenhängen. Schliesslich unternahm der T-PD auch erste Arbeiten betreffend die Profilierung, die zur Annahme von Richtlinien führen könnten. Er befasst sich auch weiter mit der Frage, ob es zweckmässig wäre, in einer noch zu erarbeitenden Rechtsurkunde das Grundrecht auf den Datenschutz zu verankern, und er bereitet eine Stellungnahme zur Auslegung der Befugnisse und der Rechtsstellung der Kontrollbehörden vor.

Europäische Konferenz der Datenschutzbeauftragten

Anlässlich der europäischen Konferenz der Datenschutzbeauftragten, die am 10. und 11. Mai 2007 in Larnaca (Zypern) stattfand, konnten die Datenschutzbeauftragten der Unterzeichnerstaaten des Übereinkommens 108 ihren Gedankenaustausch zu einigen der wichtigsten Themen für den Datenschutz (insbesondere die elektronische Patientenakte, Zertifizierung, polizeiliche und justizielle Zusammenarbeit, Jugendschutz) fortsetzen. Die Konferenz beschloss eine Verstärkung ihrer Kooperationsstruktur im Bereich Polizei und Justiz und setzte dafür eine Arbeitsgruppe mit einem Vorsitzenden und einem stellvertretenden Vorsitzenden und einem ständigen Sekretariat ein.

Die Konferenz verabschiedete eine Erklärung zum Entwurf für einen Rahmenbeschluss des europäischen Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden. Ziel dieses Vorschlags ist es, die Datenschutzvorschriften für die Datenverarbeitung

betreffend die 3. Säule zu harmonisieren und damit den Datenaustausch im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen zu erleichtern. Es geht darum, im Bereich der 3. Säule ein hohes Datenschutzniveau zu gewährleisten, das der Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr gleichwertig sein und die Anforderungen des Übereinkommens des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (SEV 108) und seines Zusatzprotokolls entsprechen sollte. Leider haben die Beratungen zu dem Text dieses Ziel verfehlt, da namentlich eine Mehrheit der Staaten den Geltungsbereich des Beschlusses auf den Informationsaustausch beschränken und die innerstaatliche Datenbearbeitung weiterhin dem jeweiligen nationalen Recht unterstellen möchte. Die Datenschutzbeauftragten äusserten daher erneut ihre Besorgnis angesichts dieser für das Datenschutzrecht nachteiligen Entwicklungen, und sie forderten die Staaten auf, sich für einen rechtlichen Rahmen einzusetzen, der ein hohes Datenschutzniveau gewährleistet (vgl. Anhang 4.18). Die Datenschutzbeauftragten verabschiedeten auch eine Stellungnahme betreffend den Verfügbarkeitsgrundsatz, in der sie die Prinzipien festlegen, welche für die Sicherstellung des Datenschutzes und die Wahrung der Rechte des Einzelnen bei der Bereitstellung von Daten zu Strafverfolgungszwecken einzuhalten sind (vgl. Anhang 4.19).

Arbeitsgruppe «Polizei und Justiz»

Der EDÖB und ein Vertreter der kantonalen Datenschutzbehörden beteiligen sich auch an der Arbeitsgruppe «Polizei und Justiz» der europäischen Konferenz. So können sie die gesetzgeberischen Entwicklungen im Zusammenhang mit dem Schengen-Besitzstand verfolgen und zum Ausbau des europäischen Datenschutzrechts im Bereich Polizei und Justiz beitragen oder an der Ausarbeitung gemeinsamer Aufsichtskonzepte mitwirken. Die Arbeitsgruppe verabschiedete insbesondere zusammen mit der gemäss Artikel 29 der europäischen Richtlinie 95/46/EG eingesetzten Gruppe eine gemeinsame Stellungnahme zum Rahmenbeschluss des Rates über die Verwendung von Passagierdaten zu Strafverfolgungszwecken. Die Datenschutzbeauftragten erinnern daran, dass sie den Kampf gegen den internationalen Terrorismus und das organisierte Verbrechen unterstützen. Dieser Kampf erfordert zwangsläufig die Erhebung und Bearbeitung von personenbezogenen Daten. Bei der Einrichtung eines europäischen PNR-Systems müssen indessen die sich daraus ergebenden Beschränkungen der Grundrechte ausreichend gerechtfertigt sein. Das Gleichgewicht zwischen der Garantie der Grundrechte und den für die Gewährleistung der öffentlichen Sicherheit unerlässlichen Einschränkungen muss gewahrt bleiben. Der Entwurf für einen

Rahmenvorschlag sieht die umfassende Datenerhebung bei sämtlichen in Europa eintreffenden oder ausreisenden Passagieren vor, unabhängig davon, ob es sich um unschuldige oder verdächtige Personen handelt. Diese Daten werden über einen Zeitraum von 13 Jahren aufbewahrt und sollen die Erstellung von Profilen ermöglichen. Dieser Vorschlag ist ein weiterer Baustein in der Errichtung einer Überwachungsgesellschaft unter dem Deckmantel der Terrorismusbekämpfung. Nach Auffassung der Datenschutzbeauftragten ist der Rahmenbeschlussentwurf unverhältnismässig und verletzt die Grundprinzipien des Datenschutzes nach Übereinkommen 108. So ist insbesondere die Notwendigkeit der Bearbeitung nicht ausreichend erwiesen; die Fluggesellschaften werden zur Bekanntgabe einer übermässigen Datenmenge verpflichtet; die Filterung der besonders schützenswerten Personendaten muss Aufgabe der für die Verarbeitung verantwortlichen Person sein; die Bereitstellung der Daten muss nach dem «Push»-System erfolgen; die Aufbewahrungsdauer der Daten ist zu verkürzen; die Datenschutzregelung, namentlich in Bezug auf die Rechte der betroffenen Personen und die Pflichten der für die Verarbeitung Verantwortlichen, muss überprüft werden.

Europäische Union

Seit der Annahme der bilateralen Abkommen Schengen / Dublin nehmen der EDÖB und ein Vertreter der kantonalen Datenschutzbehörden als Beobachter an den Arbeiten der Gemeinsamen Kontrollinstanz Schengen (GK) teil, welcher Vertreter der nationalen Datenschutzbehörden der Schengen-Staaten angehören. Die GK hat die Aufgabe, die technische Unterstützungsfunktion des zentralen Schengener Informationssystems (SIS) zu überwachen und die korrekte Umsetzung der Bestimmungen des Schengener Durchführungsabkommens zu überprüfen. Sie ist zuständig für Problemanalysen und Auslegungsfragen beim Betrieb des SIS. Sie gibt insbesondere Stellungnahmen und Berichte zur Auslegung des Schengener Durchführungsabkommens ab. Es handelt sich dabei um ein wichtiges Instrument zur Kontrolle der Einhaltung der Datenschutzbestimmungen im Rahmen der internationalen Zusammenarbeit im Bereich der Polizeitätigkeit und Strafverfolgung. Der EDÖB beteiligt sich zudem an den Arbeiten der Koordinationsgruppe Eurodac, welcher der Europäische Datenschutzbeauftragte und die nationalen Datenschutzbehörden angehören. Diese Gruppe hat namentlich die Aufgabe, gemeinsame Inspektionen des Eurodac-Systems durchzuführen, die Datenschutzprobleme im Rahmen des Systembetriebs zu untersuchen, Stellungnahmen zur Auslegung der Gesetzesbestimmungen zu erarbeiten und Empfehlungen abzugeben.

Internationale Konferenz der Datenschutzbeauftragten

Die 29. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre fand vom 25. bis 27. September 2007 in Montreal statt. Unter dem Thema «Horizonte des Datenschutzes: Terra Incognita» versammelten sich zu diesem Anlass rund 600 Teilnehmer aus der ganzen Welt. Die Datenschutzbeauftragten erhielten so die Gelegenheit zu einem Meinungsaustausch mit den Vertretern der Zivilgesellschaft (Regierungen, Verwaltung, Wirtschaft, Wissenschaft und Forschung, Konsumenten, internationale staatliche und nichtstaatliche Organisationen) über die gegenwärtigen Probleme des Datenschutzes, die namentlich den grenzüberschreitenden Datenverkehr, die Omnipräsenz der Informatik, die Politik der öffentlichen Sicherheit, den Schutz der Privatsphäre junger Menschen oder das Ineinandergreifen von Gesetz und Technologie betreffen. Aus diesem Gedankenaustausch konnten Lehren für das Verhalten der Datenschutzbehörden in den kommenden Jahren gezogen und Beiträge zur Verstärkung der internationalen Zusammenarbeit im Datenschutz entwickelt werden (http://www.conferencevieprivee2007.gc.ca). Die Konferenz bestätigte die Feststellung früherer Jahre, der zufolge die Überwachung eine Realität ist, die Technologien das Recht auf die Privatsphäre in Frage stellen, die allgegenwärtige Informatik und insbesondere die Bioinformatik den Menschen in ein Datenverarbeitungssystem verwandeln und die bisher von der Rechtsordnung angebotenen Lösungen angesichts der systematischen Beschattung der Privatpersonen nicht mehr genügen. Eine Neubestimmung der Zielvorstellungen unserer Gesellschaften im Bereich der Achtung der Privatsphäre und des Datenschutzes ist unerlässlich.

Die Datenschutzbeauftragten verabschiedeten im Rahmen ihrer geschlossenen Sitzung vier Resolutionen. Die erste Entschliessung gilt der Dringlichkeit, mit der weltweit gültige Normen für den Schutz der Passagierdaten aufgestellt werden sollten, welche die Regierungen für die Durchführung der Gesetze und die Gewährleistung der grenzübergreifenden Sicherheit verwenden. Diese Resolution greift eine Entschliessung auf, die wir anlässlich der 25. Internationalen Konferenz im September 2003 in Sydney vorgeschlagen hatten. Die zweite angenommene Resolution fordert die Ausarbeitung von Regeln im Zusammenhang mit dem Schutz der Privatsphäre im Bereich des Einsatzes und der Verwendung von Technologien. Mit diesen technischen und organisatorischen Spezifikationen sollen die rechtlichen Anforderungen umgesetzt werden. Diese Normen müssen in Zusammenarbeit mit den Datenschutzbehörden entwickelt werden. In einer dritten Entschliessung verlangen die Datenschutzbeauftragten eine Verstärkung der internationalen Zusammenarbeit. Eine vierte Resolution gilt schliesslich der Verbesserung bei der Organisation der internationalen Konferenz und namentlich der Entwicklung einer Website entsprechend dem Beschluss der 27. Konferenz von 2005 in Montreux.

Wir hatten auch die Gelegenheit, unseren Kollegen einen ersten Evaluationsbericht zur Umsetzung der Schlusserklärung der 27. Konferenz (Erklärung von Montreux) vorzulegen, mit der eine Verstärkung der universellen Geltung des Rechts auf Datenschutz und namentlich die Vorbereitung einer verbindlichen universellen Rechtsurkunde gefordert wurde (vgl. unseren 13. Tätigkeitsbericht, Ziffer 9.2.1 und Anhang 11.2). Diese Evaluation erfolgte auf der Grundlage eines Fragebogens, den wir an sämtliche an der Konferenz von Montreux teilnehmenden nationalen Datenschutzbehörden gerichtet hatten. Wie wir in diesem Bericht festhalten konnten, hat die Erklärung von Montreux im Jahr nach ihrer Annahme eine weite Verbreitung insbesondere über das Internet gefunden. Es ist allerdings schwierig, die Auswirkungen dieser Verbreitung abzuschätzen und namentlich zu beurteilen, wie weit die potenziellen Adressaten die Erklärung zur Kenntnis genommen haben und in ihre Tätigkeit einbeziehen. Obwohl die Erklärung zahlreichen nationalen und internationalen Akteuren zur Kenntnis gebracht wurde, hat es dennoch den Anschein, dass bisher nur wenige unter ihnen sie auch zum Bestandteil ihrer eigenen Vorgaben gemacht haben. Gezieltere Massnahmen haben eine gewisse Wirkung gezeigt. So haben mehrere Behörden die am Weltgipfel zur Informationsgesellschaft teilnehmenden Minister aufgefordert, die Annahme eines Hinweises auf den Datenschutz in den Akten der Gipfelkonferenz zu unterstützen. Dasselbe gilt für die Schlusserklärung des XI. Gipfels der Frankophonie, der im September 2006 in Bukarest stattfand.

Die Verwirklichung der Ziele der Erklärung ist ein dynamischer Prozess, der Zeit, Geduld und Ausdauer erfordern wird. Die Erklärung hat sich als positive und treibende Kraft für zahlreiche Initiativen ausgewirkt. Das Bewusstsein der universellen Geltung des Datenschutzes war noch nie so präsent wie heute, sie ist jedoch angesichts der inzwischen vorrangigen Ziele der Sicherheit und der Überwachung im Rahmen des Kampfes gegen den Terrorismus und das organisierte Verbrechen weiterhin äusserst gefährdet. Die Datenschutzbehörden werden ihrer Rolle in der heutigen Gesellschaft und der Bedeutung ihrer aktiven und koordinierten Präsenz bei der Verteidigung des Rechtes auf Datenschutz zunehmend gewahr. Die Zahl der europäischen und aussereuropäischen Staaten, namentlich der Länder der Frankophonie und der Iberoamerikanischen Konferenz, die eine verbindliche universelle Urkunde befürworten, nimmt laufend zu. Die Idee eines universellen Übereinkommens ist im Vormarsch. Ihre Verwirklichung wird jedoch nicht leicht sein und auf grosse Widerstände stossen. Mehrere ähnliche Initiativen gehen in die gleiche Richtung. Sie sollten koordiniert werden, damit sie sich gegenseitig ergänzen und das Hauptziel, das wir mit der Erklärung von Montreux anstreben, nämlich die Schaffung eines verbindlichen universellen Rahmens für den Datenschutz und die Achtung der Privatsphäre, nicht in Frage stellen. Die Datenschutzbeauftragten haben unseren Bericht einstimmig angenommen und uns beauftragt, auf der 30. Internationalen Konferenz im Oktober 2008 in Strassburg einen ergänzenden Bericht vorzulegen.

Frankophone Vereinigung der Datenschutzbehörden

Am 24. September 2007 fand in Montreal die erste Konferenz der Datenschutzbeauftragten der Frankophonie statt (http://www.cai.gouv.gc.ca/CCPDF), bei der auch wir vertreten waren. Die Konferenz befasste sich mit den Wechselwirkungen zwischen dem Schutz der Personendaten, der Demokratie und der Entwicklung. Sie bot die Gelegenheit zu einem Dialog zwischen Staaten mit einer bereits langjährigen Erfahrung im Bereich des Datenschutzes, die insbesondere über Datenschutzbehörden verfügen, und den Schwellenländern, die wie Burkina Faso gerade ein Gesetz verabschiedet haben, oder die kurz vor dem Beginn des Gesetzgebungsprozesses stehen. Ziel war auch die Schaffung eines Programms für die Zusammenarbeit und den Austausch zwischen den Datenschutzbehörden der französischsprachigen Länder im Hinblick auf eine gemeinsame Nutzung der konkreten Erfahrungen auf diesem Gebiet. Die Konferenz führte zur Gründung der Frankophonen Vereinigung der Datenschutzbehörden (Association francophone des autorités de protection des données). Sie steht unter der Leitung des Vorsitzenden der Kommission für Informationszugang von Quebec. Wir haben einen der beiden Sitze eines stellvertretenden Vorsitzenden inne. Die französische Datenschutz-Kontrollbehörde CNIL führt das Sekretariat. Die Vereinigung wird von der Internationalen Organisation der Frankophonie unterstützt, deren Ziele mit den ihren völlig übereinstimmen: Einsatz für den Frieden, die Demokratie und die Entwicklung des Rechts mittels Unterstützung des Rechtsstaats und der Menschenrechte. Die Vereinigung bemüht sich um die Stärkung der Leistungsfähigkeit ihrer Mitglieder bei der Förderung des Datenschutzes, den Informationsaustausch zwischen den Datenschutzbehörden, die Bildung von Zentren für Fachwissen und Erfahrungsaustausch, die Konsolidierung des Schutzes von Personendaten als Faktor in der Förderung des Rechtsstaates und der demokratischen Entwicklung. Sie möchte insbesondere den Schwellenländern bei der Einführung ihrer Gesetzgebung und ihrer Datenschutzbehörden helfen. Sie wird sich für die Annäherung der Gesetzgebungen einsetzen und so zur grenzübergreifenden Wirkung des Rechts, zur Verständlichkeit und Flexibilität in den Umsetzungsmethoden beitragen. Sie wird sich auch für die Anerkennung des universellen Rechts auf Datenschutz engagieren.

1.10.2 Internationale Arbeitsgruppe Datenschutz im Telekommunikationsbereich

Themen der 42. Sitzung der Arbeitsgruppe im Herbst 2007 in Berlin waren unter anderen der Datenschutz bei der Verbreitung digitaler Medieninhalte und beim digitalen Fernsehen sowie das E-Ticketing in öffentlichen Verkehrsmitteln.

Wir nahmen an der 42. Sitzung der «Berliner Gruppe» (International Working Group on Data Protection in Telecommunications, IWGDPT) vom 4.-5. September 2007 teil. Die Arbeitsgruppe ist bereits im Rahmen der Internationalen Konferenz der Datenschutzbeauftragten 1983 auf Initiative des Berliner Datenschutzbeauftragten gegründet worden und steht bis heute unter dessen Vorsitz.

Zum Thema Datenschutz bei der Verbreitung digitaler Medieninhalte wurde ein Arbeitspapier mit Empfehlungen verabschiedet: Interaktives, digitales Fernsehen eröffnet neue Möglichkeiten und Angebote für die Nutzer, gleichzeitig aber auch Gefahren für die Privatsphäre. Die Datenbearbeitungen werden meist von den Anbietern kontrolliert und sind für die Nutzer nur schwer durchschaubar. Beim Konsum der digitalen Inhalte können sehr sensible Informationen (insbesondere Persönlichkeitsprofile) über die Interessen und Vorlieben der Kunden entstehen. Daher fordert die Gruppe, dass auch im Zeitalter des digitalen Fernsehens eine anonyme Nutzung erhalten bleiben muss. Anonyme Zahlungswege sind mindestens als Option und ohne zusätzliche Kosten anzubieten. Wenn Personendaten bearbeitet werden, so müssen die Zuschauer vorgängig über den Umfang, den Zweck, den Ort und die Aufbewahrungsdauer informiert werden.

Ausserdem beschäftigte sich die Gruppe mit dem E-Ticketing in öffentlichen Verkehrsmitteln, das zunehmend Verbreitung findet. Meist werden personalisierte Chipkarten eingesetzt, die für die Nutzung bzw. Bezahlung der Transportleistung, aber auch verwandter Dienstleistungen wie etwa der Parkgebühren dienen. Es können so Informationen darüber entstehen, wer sich wann an einem bestimmten Ort aufgehalten hat (Bewegungsprofile). Die Arbeitsgruppe verlangt, dass die Datenschutzanforderungen bereits beim Entwurf von E-Ticketing-Systemen berücksichtigt werden. Ähnlich wie beim digitalen Fernsehen soll auch beim öffentlichen Verkehr eine anonyme Nutzung möglich bleiben (Barzahlung, Prepaid-Lösungen), und zwar ohne finanzielle Hürden. Bearbeiten die Transport- oder Verkehrsunternehmen Personendaten, haben sie die Datensparsamkeit zu respektieren und die Aufbewahrungsdauer auf das erforderliche Minimum zu beschränken. Gegenüber den Kunden ist volle Transparenz über sämtliche Datenbearbeitungen zu schaffen.

Die publizierten Papiere der Gruppe finden sich unter www.iwgdpt.org

2 Öffentlichkeitsprinzip

2.1 Erste Erfahrungen mit dem Öffentlichkeitsprinzip

Das Öffentlichkeitsprinzip etabliert sich in der Bundesverwaltung. Im letzten Jahr gewährten die Bundesämter bei zwei Dritteln der Gesuche einen vollständigen oder zumindest teilweisen Zugang zu den gewünschten Dokumenten. Bei den Schlichtungsverfahren konnte in fast allen Fällen ein für den Antragsteller günstigeres Resultat erreicht werden. Die Möglichkeiten des Öffentlichkeitsgesetzes werden insbesondere von Journalisten rege benutzt.

Seit dem 1. Juli 2006 haben Bürgerinnen und Bürger ein Recht auf Zugang zu amtlichen Dokumenten der Bundesverwaltung, der Parlamentsdienste und von Organisationen und Personen des öffentlichen oder privaten Rechts, die dem Öffentlichkeitsgesetz unterstehen. Gewährt eine dieser Stellen nur einen eingeschränkten oder gar keinen Zugang zu einem Dokument, so kann der Gesuchsteller bei uns einen Schlichtungsantrag einreichen. Die erste Bilanz eines ganzen Kalenderjahres zeigt nun ein durchweg positives Bild. Die Bevölkerung nutzt die Möglichkeiten des Öffentlichkeitsgesetzes zunehmend und erhält in den meisten Fällen auch Zugang zu den gewünschten Dokumenten.

Zugangsgesuche bei den Bundesämtern und Departementen

Die Stellen, die dem Öffentlichkeitsgesetz unterliegen, müssen uns jedes Jahr die Anzahl der eingereichten Zugangsgesuche und deren Beurteilung melden. So sollen im Jahr 2007 bei den Bundesbehörden 249 Zugangsgesuche eingereicht worden sein (s. Statistik unter Ziffer 3.5). In 147 Fällen gewährten die Behörden einen vollständigen und bei 20 Gesuchen einen teilweisen Zugang. 82 Zugangsgesuche wurden vollständig abgelehnt.

Folgende Aussagen lassen sich dazu machen:

- Bei zwei Dritteln aller eingereichten Zugangsgesuche wurde ein vollständiger oder teilweiser Zugang gewährt. Von einem teilweisen Zugang wird gesprochen, wenn beim fraglichen Dokument einzelne Textpassagen eingeschwärzt und/oder Personennamen anonymisiert werden. Bei einem knappen Drittel aller eingereichten Gesuche wurde der Zugang vollständig verweigert.

- Die grosse Zahl der Verweigerungen und die relativ geringe Zahl der teilweise gewährten Zugänge lassen erneut den Schluss zu, dass die Bundesbehörden (zu?) wenig von der Möglichkeit des teilweisen Zugangs Gebrauch machen. Offenbar wird der Zugang eher vollständig verweigert, als dass geprüft wird, ob ein teilweiser Zugang gewährt werden könnte. Das Öffentlichkeitsgesetz sieht diese Möglichkeit ausdrücklich vor und die Verwaltungseinheiten sollten im Rahmen der Anwendung des Verhältnismässigkeitsprinzips vermehrt dafür sorgen, dass ein Gesuchsteller wenn nicht vollständig, dann zumindest teilweise Einsicht in das gewünschte amtliche Dokument erhält.

- Bei zahlreichen Verwaltungseinheiten sind gemäss eigenen Angaben im Jahre 2007 überhaupt keine Zugangsgesuche eingegangen, andere wiederum meldeten über 30 Zugangsgesuche. Eine mögliche Erklärung für diese grossen Unterschiede ist, dass gewisse Ämter aufgrund der bearbeiteten Themen und Sachgebiete stärker im Fokus der Öffentlichkeit stehen und daher naturgemäss mehr Zugangsgesuche erhalten. In diesem Zusammenhang muss aber auch die Frage aufgeworfen werden, ob in allen Verwaltungseinheiten die eingehenden Zugangsgesuche erstens überhaupt als solche erkannt und zweitens auch systematisch erfasst werden. Aufgrund von Rückmeldungen der Ämter konnten wir zudem feststellen, dass Abgrenzungsschwierigkeiten zwischen einem Zugangsgesuch nach Öffentlichkeitsgesetz und einer allgemeinen Auskunftsanfrage bestehen. Das Öffentlichkeitsgesetz äussert sich zu dieser Frage nicht klar. Grundsätzlich tendieren wir zur Aussage, dass eine korrekte und systematische Erfassung aller Zugangsgesuche zu einer um einiges höheren Anzahl von gemeldeten Gesuchen führen würde.

- Keine verlässlichen Angaben lassen sich über die im Rahmen der Zugangsgewährung erhobenen Gebühren und über den bei den Ämtern und Departementen verursachten Zeitaufwand machen. Die uns gegenüber gemachten Angaben sind zu wenig aussagekräftig. Immerhin lassen sich folgenden Tendenzen feststellen: In den allermeisten Fällen wird für die Gewährung des Zugangs keine Gebühr verlangt. In Bezug auf den durch das Öffentlichkeitsgesetz verursachten zeitlichen Aufwand zeigt sich bei verschiedenen Ämtern und Departementen ein widersprüchliches Bild (sofern uns der Aufwand überhaupt gemeldet worden ist): Von geringem bis zu sehr hohem Aufwand findet sich alles. Im Hinblick auf die vom Öffentlichkeitsgesetz verlangte Evaluation ist es notwendig, dass diese Informationen künftig systematischer und exakter erhoben werden.

Schlichtungsanträge

Wird dem Gesuchsteller der Zugang teilweise bzw. ganz verweigert oder erhält er innerhalb der gesetzlich vorgesehen Frist von der Behörde überhaupt keine Antwort, so kann er bei uns einen Schlichtungsantrag einreichen. Während in den ersten sechs Monaten seit Inkrafttreten des Öffentlichkeitsgesetz (1. Juli 2006) lediglich sechs Schlichtungsanträge bei uns eingereicht wurden, waren es im Berichtsjahr 2007 bereits 36 (s. Statistik unter Ziffer 3.5).

Wir konnten im Jahre 2007 26 Schlichtungsanträge abschliessen. In 7 Fällen kamen wir zum Schluss, dass das Öffentlichkeitsgesetz nicht zur Anwendung gelangt. In zwei Fällen konnte mit den Beteiligten eine Schlichtung erzielt werden und bei 14 Schlichtungsanträgen erliessen wir – da keine einvernehmliche Lösung erreicht wurde – Empfehlungen (in zwei Verfahren jeweils zweier Antragsteller). Die Empfehlungen finden sich im Anhang (4.6 – 4.17). In drei Fällen wurde der Zugang vom Amt nachträglich noch gewährt.

Diese Zahlen lassen folgende Schlüsse zu:

- In 102 Fällen wurde der Zugang vollständig verweigert (82) respektive nur teilweise gewährt (20). Dem stehen 36 bei uns eingereichte Schlichtungsanträge gegenüber. Somit wurde bei einem Drittel aller ganz oder teilweise abgelehnter Zugangsgesuche ein Schlichtungsantrag eingereicht.

- In 14 von 16 Fällen konnte im Schlichtungsverfahren jeweils eine für den Gesuchsteller günstigere Lösung erzielt werden (d.h. es wurde ein weiter gehender Zugang gewährt als ursprünglich vom Bundesamt zugestanden).

- Bis auf zwei wurden alle Empfehlungen von den Antragstellenden und den Bundesämtern akzeptiert; lediglich in zwei Fällen verlangte der Gesuchsteller von der Behörde den Erlass einer Verfügung (zurzeit ist uns nicht bekannt, ob eine Beschwerde beim Bundesverwaltungsgericht eingereicht worden).

- In drei Fällen konnten hängige Schlichtungsverfahren eingestellt werden, weil die Behörden auf ihren Entscheid zurückgekommen sind und den Zugang zu den gewünschten Dokumenten nachträglich doch noch gewährt haben. Gerade diese Fälle zeigen, dass die Einführung des Öffentlichkeitsprinzips in der

Bundesverwaltung dazu geführt hat, dass einzelne Dokumente im Zweifelsfall eher publiziert als zurückgehalten werden. Diese Entwicklung wird auch immer wieder in Gesprächen mit Ämtern und den Departementen bestätigt.

- Nach eineinhalb Jahren Öffentlichkeitsgesetz lässt sich sagen, dass das Schlichtungsverfahren von den Bürgern rege benutzt wird. Mit Blick auf die Erfolgsquote der Verfahren kann zumindest als erstes Zwischenfazit festgehalten werden, dass das vom Gesetzgeber mit der Schaffung einer verwaltungsinternen, unabhängigen Schlichtungsstelle verfolgte Ziel, kostspielige und lange Gerichtsverfahren zu vermeiden, erreicht wurde.

Abschliessend lässt sich noch Folgendes festhalten:

- Eines der grossen Probleme im verwaltungsinternen Zugangsverfahren ist der grosse Rückstau bei der Behandlung der Schlichtungsgesuche. Dies ist bedauerlich und steht im Widerspruch zur Idee des Öffentlichkeitsprinzips. Gerade im Rahmen der Durchführung des Schlichtungsverfahrens zeigt sich immer wieder, dass auch die Ämter die gesetzlichen Fristen für die Beurteilung eines Zugangsgesuchs nicht immer einhalten.

- Ein Zugangsgesuch und in der Folge einen Schlichtungsantrag kann jedermann stellen. Es muss weder im ersten noch im zweiten Fall ein Interesse dargelegt werden. Dies mag ein Grund für die relativ hohe Zahl der eingereichten Schlichtungsgesuche sein.

- Es zeigt sich, dass insbesondere Journalisten, Rechtsanwälte und Interessenvertreter die Vorteile des Öffentlichkeitsgesetzes zu nutzen wissen. So werden beispielsweise Zugangsgesuche und Schlichtungsanträge gerne von Interessenvertretern (wie im Fall der ETH-Studie zu den Transfettsäuren von einer Konsumentenorganisation) oder von Konkurrenzunternehmen respektive von deren Rechtsanwälten (z.B. die Empfehlungen zum Vertrag des BAG betreffend die Beschaffung eines Präpandemie-Impfstoffes oder die Empfehlung betreffend die Zulassung von Arzneimitteln) eingereicht. Die Berufsgruppe, die am meisten Schlichtungsanträge einreicht, sind jedoch die Journalisten (11).

- Als Ausnahmegründe für die Verweigerung oder Einschränkung des Zugangs wurden am häufigsten das Geschäfts- und Fabrikationsgeheimnis, die internationalen Beziehungen und die noch nicht gefällten politischen oder administrativen Entscheide genannt.

- Unserer Ansicht nach besteht eine gewisse Tendenz der Behörden, sich nicht nur im Rahmen der Gesuchsbeurteilung, sondern auch im Schlichtungsverfahren bloss auf eine Ausnahmebestimmung zu berufen, ansonsten ihren ablehnenden Entscheid aber nicht weiter begründen. Die Ämter scheinen darauf zu vertrauen, dass wir im Schlichtungsverfahren einen entsprechenden Entscheid fällen. Dieses Vorgehen ist für die Gesuchsteller unbefriedigend und stossend. Diese sollten zumindest nachvollziehen können, aus welchen Gründen sich eine Behörde auf eine Ausnahmebestimmung beruft. Zudem sei an dieser Stelle daran erinnert, dass der EDÖB gemäss Intention des Gesetzgebers nicht eine vorweggenommene Gerichtsinstanz ist, sondern in erster Linie die Funktion einer Schlichtungsstelle einzunehmen hat und in diesem Sinne eine für alle Beteiligten akzeptable Lösung herbeiführen soll.

3 Der EDÖB

3.1 WebDatareg: das neue Programm für die Anmeldung und Abfrage von Datensammlungen über Internet

Gemäss dem neuen Artikel 11a des revidierten DSG führt der EDÖB ein Register der Datensammlungen, das über Internet zugänglich ist. Mit Unterstützung der Bundeskanzlei haben wir zunächst ein dreisprachiges Programm für die Online-Verwaltung der von den Bundesorganen und Privatpersonen eingereichten Anmeldungen von Datensammlungen definiert und danach abgenommen. Für alle betroffenen Akteure wird dadurch die für die Erfassung, Nachführung und Suche aufgewendete Zeit deutlich verkürzt werden. Ende 2007 und Anfang 2008 boten wir mehrere Schulungskurse für die Bundesorgane an, damit diese ihre bestehenden Anmeldungen wenn nötig aktualisieren können, bevor das Register zum voraussichtlichen Termin im Sommer 2008 ins Internet gestellt wird. Die Unternehmen werden dann übrigens ebenfalls die Möglichkeit haben, ihre Datensammlungen über Internet anzumelden.

Nach der vom Parlament am 24. März 2006 verabschiedeten Revision des DSG sieht Artikel 11a Absatz 1 zum Register der Datensammlungen nunmehr Folgendes vor: «Der Beauftragte führt ein Register der Datensammlungen, das über Internet zugänglich ist. Jede Person kann das Register einsehen.» Mit Unterstützung der Bundeskanzlei erstellten wir zunächst das Pflichtenheft für ein neues webgestütztes Programm für die Verwaltung und Abfrage der in diesem Register enthaltenen Daten. Dieses durchwegs dreisprachige neue Programm beruht auf der neuen Microsoft.NET-Umgebung mit einer vollständig neu normalisierten relationalen Datenbank. Um die Sicherheit des Internetzugangs zu garantieren, wird eine Replikation der zu veröffentlichenden Daten durch einen exklusiven Synchronisationsservice ausgehend von den im internen Netzwerk des Bundes verwalteten Referenzdaten gewährleistet.

In einem ersten Schritt wurde die Administrator-Task bei uns generiert, damit wir die neuen Anmeldungen und natürlich alle bisherigen, aus dem früheren Register übernommenen Anmeldungen verwalten können. In einer zweiten Phase (Ende 2007/Anfang 2008) boten wir eine zweisprachige Schulung für rund hundert Personen aus den anmeldenden Bundesorganen an, damit diese ihre neuen Anmeldungen mit Hilfe des neuen Programms erfassen und notfalls die Daten ihrer früheren Anmeldungen ändern können. In einer dritten Etappe werden wir allen betroffenen Privatpersonen (Unternehmen) eine Kopie der vorhandenen Anmeldungen zusenden und sie ersuchen, die Richtigkeit der angemeldeten Daten zu überprüfen. Ausserdem werden die-

se Unternehmen über ein Programm für die Anmeldung über Internet analog zu dem Programm verfügen, das die Bundesorgane erhalten; die Anmeldungsdaten werden uns jedoch per E-Mail in Form von PDF-Dateien und XML übermittelt. Nach der Authentifizierung des Anmelders werden wir somit ohne weiteres in der Lage sein, die eingegangenen XML-Daten in das Register zu importieren, und bei diesem Vorgang werden wir die Übersetzung der Bezeichnung und des Zwecks der Datensammlung in die beiden anderen Landessprachen besorgen.

Alle diese Etappen dienen letztendlich dem Zweck, eine Such- und Abfrageanwendung für die angemeldeten und im Register enthaltenen Datensammlungen über Internet verfügbar zu machen. Die amtliche Veröffentlichung dieses Registers im Internet sollte Anfang Sommer 2008 erfolgen.

3.2 2. Europäischer Datenschutztag

Am 28. Januar 2008 führten wir in Zusammenarbeit mit Schweizer Radio DRS und Radio Suisse Romande den 2. Europäischen Datenschutztag durch. Die Zielsetzung des Europarats – die Sensibilisierung der Bevölkerung – erreichten wir mit zahlreichen Sendungen sowie einem umfassenden Beratungsangebot für die Hörerinnen und Hörer.

Die beiden Radiostationen DRS und RSR nahmen den 2. Europäischen Datenschutztag zum Anlass, in verschiedenen Sendungen alltägliche Themen des Persönlichkeitsschutzes aufzugreifen: von E-Health über RFID-Chips, Datenspuren im Internet und insbesondere Web 2.0 zur grundsätzlichen Frage, was an Daten über eine Person überhaupt vorhanden ist und wer was damit unternimmt. Auf DRS1 nahm der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte Hanspeter Thür an mehreren Diskussionen teil, während der stellvertretende Datenschutz- und Öffentlichkeitsbeauftragte Jean-Philippe Walter den EDÖB bei La 1ère und Couleur 3 vertrat.

Parallel zu diesen Sendungen beantworteten Expertinnen und Experten des EDÖB die Fragen des Publikums an einer Hotline bzw. in einem Internetforum. In diesen knapp 200 Anfragen zeigte sich ein breites Spektrum von Anliegen, die die Menschen bezüglich des Schutzes ihrer Privatsphäre beschäftigen: Antragsformulare für Mietwohnungen, Videoüberwachung durch den Nachbarn, Referenzauskünfte des Arbeitgebers, Zugang zum Personaldossier, Einsicht in die bzw. Herausgabe der Krankengeschichte, Gesundheitskarte oder die Risiken bei der Verwendung der Kreditkarte sind nur einige der Themen. Diese Kontakte mit Teilen der Bevölkerung bestätigten mindestens partiell auch die Ansicht des Europarats, dass es an Wissen über den Datenschutz, über alltägliche Gefahren im Umgang mit Personendaten und über die Rechte der betroffenen Personen mangelt. Das zu ändern wird auch in Zukunft eines unserer Ziele sein.

3.3 Publikationen des EDÖB – Neuerscheinungen

Auch in diesem Berichtsjahr haben wir das Informationsangebot auf unserer Website ausgebaut. Veröffentlicht wurden unter anderem Erläuterungen zu Sicherheitsvorkehrungen bei der Benutzung von drahtlosen Netzwerken, zu so genannten schwarzen Listen in der Hotellerie und im Gastgewerbe und natürlich zum revidierten Datenschutzgesetz.

Am 1. Januar 2008 ist das revidierte Bundesgesetz über den Datenschutz in Kraft getreten. Die wichtigsten Änderungen, die diese Revision mit sich bringt, werden unter Themen – Datenschutz – Sonstige Themen – Revision des Bundesgesetzes über den Datenschutz (DSG) erläutert.

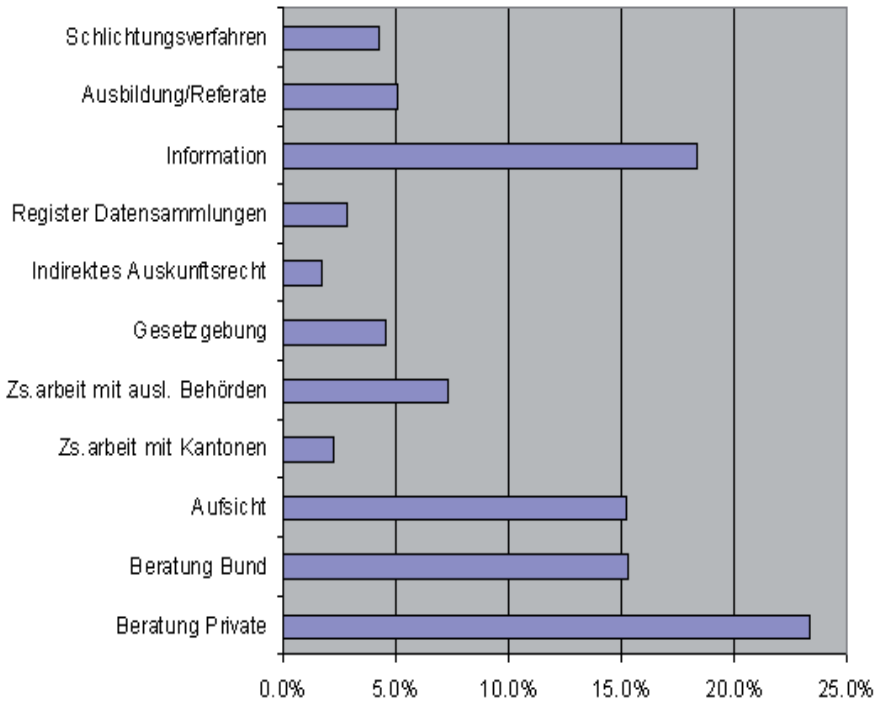
Wireless LAN – also drahtlose Netzwerke – erfahren eine immer weitere Verbreitung. Leider steigt das Bewusstsein der damit verbundenen Risiken für die Privatsphäre nicht im selben Ausmass. Wir haben unter Themen – Datenschutz – Internet – WLAN einige minimale Sicherheitshinweise veröffentlicht. Ausserdem haben wir in unserem Newsletter «datum» (Ausgabe 02/2007) diesem Thema einen Beitrag gewidmet.

Hotellerie und Gastgewerbe sind immer wieder mit Kundinnen und Kunden konfrontiert, die sich ungebührlich benehmen und der Zechprellerei, Sachbeschädigungen oder gar aggressiven Verhaltens anderen Gästen gegenüber schuldig machen. In diesem Zusammenhang wurde wiederholt die Frage an uns gerichtet, ob und unter welchen Bedingungen geschädigte Wirtinnen, Clubbetreiber und Hoteliers eine Datenbank einrichten können, um vor solchen Übeltätern zu warnen. Unter Themen – Datenschutz – Sonstige Themen – Schwarze Listen haben wir erläutert, worauf beim Anlegen solcher Warnlisten aus datenschutzrechtlicher Sicht besonders zu achten ist (siehe auch Anhang 4.1).

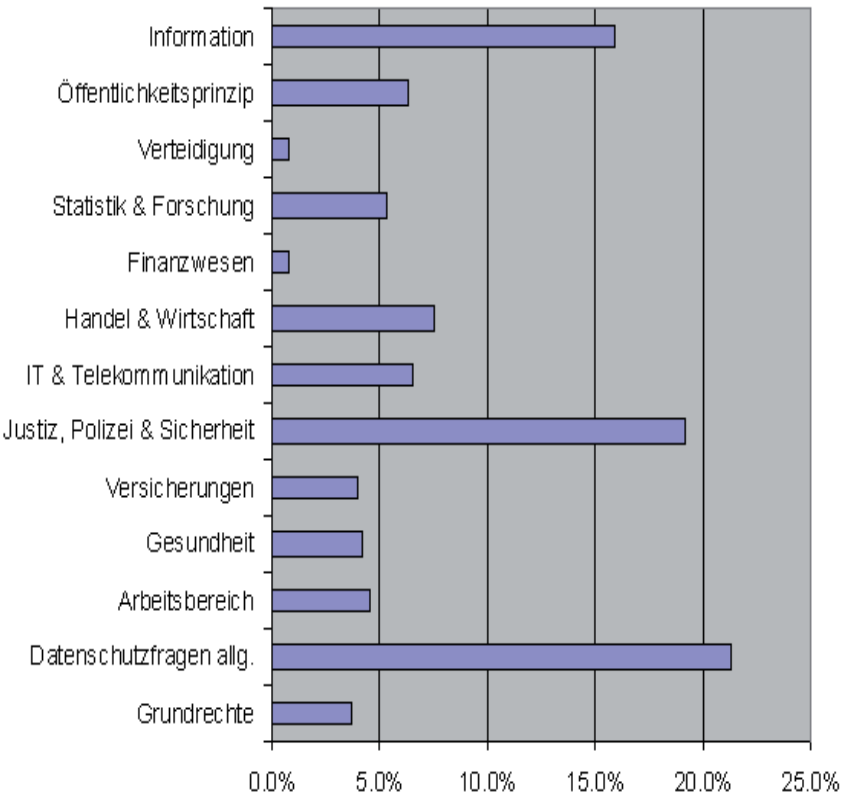
In unserem Newsletter «datum» (Ausgabe 02/2007) findet sich schliesslich noch ein Beitrag, der der Frage der Miniaturisierung von Überwachungsgeräten und dem so genannten Pervasive Computing, also der Durchdringung des Alltags mit Informationsverarbeitung, nachgeht («Vom Big Brother zum Little Brother»).

3.4 Statistik über die Tätigkeit des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten vom 1. April 2007 bis 31. März 2008

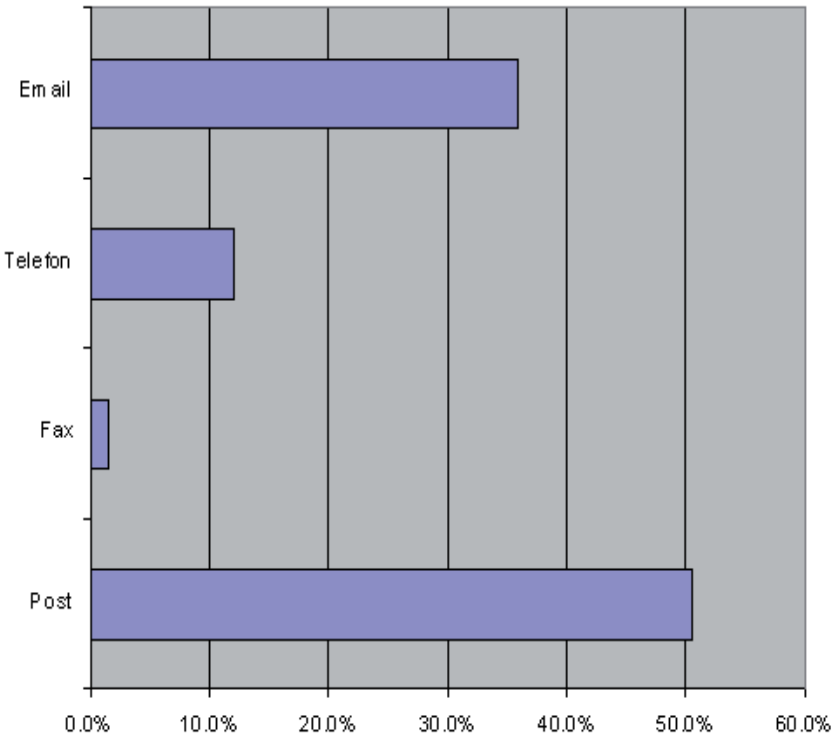
Aufwand nach Aufgabengebiet



Aufwand nach Sachgebiet



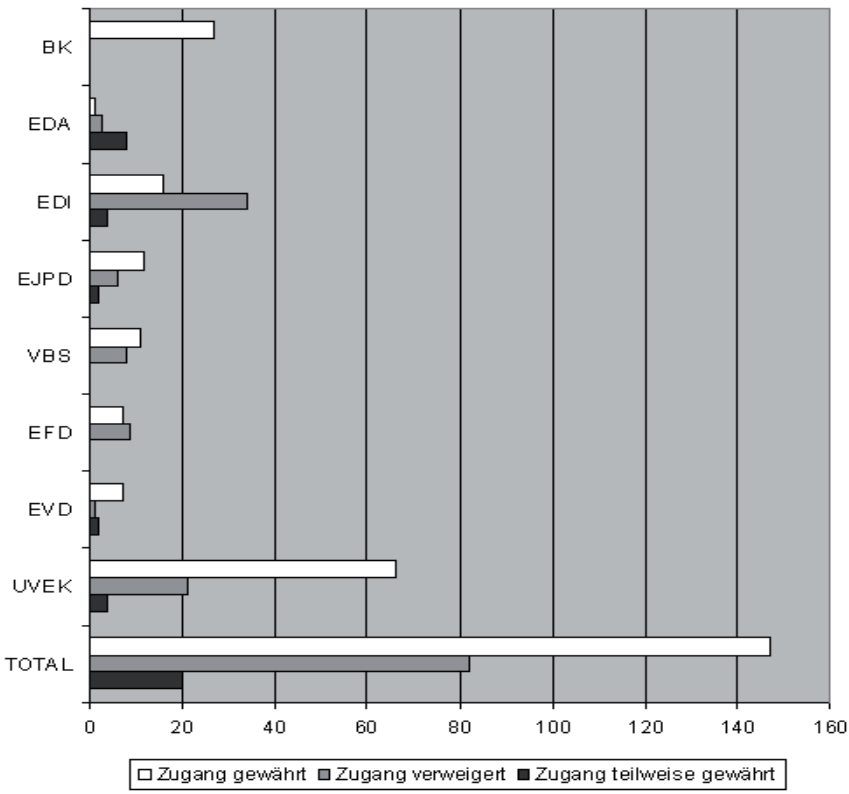
Herkunft der Anfragen



3.5 Statistik über die bei den Departementen eingereichten Zugangsgesuche nach Art. 6 des Öffentlichkeitsgesetzes (Zeitraum: 1. Januar 2007 bis 31. Dezember 2007)

Departement	Anzahl Gesuche	Zugang gewährt	Zugang verweigert	Zugang teilweise gewährt
BK (davon EDÖB)	27 (27)	27 (27)	0	0
EDA	12	1	3	8
EDI	54	16	34	4
EJPD	20	12	6	2
VBS	19	11	8	0
EFD	16	7	9	0
EVD	10	7	1	2
UVEK	91	66	21	4
TOTAL	**249**	**147**	**82**	**20**

Behandlung der Zugangsgesuche



Anzahl Schlichtungsgesuche nach Kategorien der Antragsteller im Jahr 2007

Kategorie Antragsteller	Anzahl
Privatpersonen (bzw. keine genaue Zuordnung möglich)	12
Medien/Journalisten	11
Interessenvertreter (Verbände, Organisationen, Vereine usw.)	5
Rechtsanwälte	6
Unternehmen	2
Total	36

3.6 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 1:	9 Personen
Einheit 2:	12 Personen
Einheit 3:	1 Person
Kanzlei:	3 Personen

4. Anhänge

4.1 Erläuterungen zum Thema «Schwarze Listen»

Hotellerie und Gastgewerbe sind immer wieder mit Kundinnen und Kunden konfrontiert, die sich ungebührlich benehmen und der Zechprellerei, Sachbeschädigungen oder gar aggressiven Verhaltens anderen Gästen gegenüber schuldig machen. In diesem Zusammenhang wurde wiederholt die Frage an den EDÖB gerichtet, ob und unter welchen Bedingungen geschädigte Wirtinnen, Clubbetreiber und Hoteliers eine Datenbank einrichten können, um vor solchen Übeltätern zu warnen.

Der Wunsch von Verantwortlichen von Gaststätten und verwandten Betrieben, wiederholt ausfällig gewordene Übeltäter endlich unschädlich zu machen und das eigene Gewerbe vor ihnen zu schützen, ist verständlich. Der Aufbau einer Datenbank durch Privatpersonen, wozu auch Wirte, Hoteliers etc. zählen, und der Zugriff einer ganzen Gruppe von Personen auf diese Daten sind jedoch aus datenschutzrechtlicher Sicht nicht unproblematisch.

Die gesetzlichen Vorgaben

Jeglicher Umgang mit Personendaten, also auch das Erfassen von Übeltätern und die Bekanntgabe ihrer Daten in einer Datenbank, stellt eine Datenbearbeitung nach dem Bundesgesetz über den Datenschutz (DSG) dar. Dieses Gesetz sieht nun vor, dass der Datenbearbeiter für seine Bearbeitung zunächst einen Rechtfertigungsgrund braucht. Als solcher zählen entweder die Einwilligung der betroffenen Person, ein überwiegendes privates oder öffentliches Interesse oder ein Gesetz. Für eine Schwarze Liste werden Übeltäter kaum ihre Einwilligung geben; auch existiert kein Gesetz, das die Betreiberinnen und Betreiber von Gaststätten verpflichtet, eine solche Datenbank zu führen. Hingegen kann das überwiegende private Interesse dieser Betreiber eine Bearbeitung von Personendaten rechtfertigen.

Weiter muss der Datenbearbeiter die allgemeinen Grundsätze des DSG einhalten. Das heisst, er muss

- die betroffenen Personen über den Zweck und die Bedingungen der Datenbearbeitung klar informieren (Grundsatz von Transparenz resp. Treu und Glauben);

und er darf

- nur die Personendaten bearbeiten, welche zur Erreichung des mit der Datenbearbeitung verfolgten Zwecks geeignet und notwendig sind (Verhältnismäs-

sigkeit) – es muss ein sinnvolles Verhältnis zwischen dem angestrebten Ziel und den verwendeten Mitteln bestehen

- die Daten nur zu dem Zweck bearbeiten, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist (Zweckmässigkeit)

Das Datenbearbeitungskonzept

Für ein klares und rechtlich einwandfreies Vorgehen empfiehlt sich die Erarbeitung eines Datenbearbeitungskonzepts, das allen Beteiligten als Regelwerk und den Erfassten als Schutz dienen soll.

Das Konzept umfasst folgende Punkte:

- Zweck: Der Zweck der Datenbearbeitung muss festgelegt werden. Im vorliegenden Fall geht es um die Erfassung der Personalien von Gästen, die sich in Gaststätten offensichtlich ungebührlich verhalten haben, um anderen Anbieterinnen und Anbietern ähnliche Schädigungen möglichst zu ersparen.

- Bedingungen der Erfassung von Personendaten in der Datenbank: Es muss festgehalten werden, dass die Erfassung nur zulässig ist, wenn für den angerichteten Schaden keinen Schadenersatz geleistet wurde oder wenn eine Schädigung nicht-materieller Natur, die auf ein offensichtlich ungebührliches Verhalten zurückging, verursacht wurde.

- Erfasste Personendaten: Ganz zentral ist die Definition, welche Personendaten genau in die Datenbank aufgenommen werden sollen. Im vorliegenden Fall scheint ausreichend, die Personalien der betroffenen Person und den Grund für ihre Erfassung (Art der Schädigung) zu speichern. Weiter braucht es für allfällige Rückfragen einen Identifikator der Person, die die Daten eingegeben hat.

- Information: Um Transparenz zu gewährleisten, müssen die Gäste über Zweck und Bedingungen der Beschaffung der Daten und ihrer Erfassung in der Datenbank klar informiert werden. Diese Informationen können zum Beispiel in die Allgemeinen Geschäftsbedingungen aufgenommen werden, die in der Gaststätte klar angeschlagen oder der Kundin oder dem Kunden bei einer allfälligen Anmeldung via Internet zur Kenntnis gebracht werden. Wenn die Reservation nicht via Internet erfolgt, können auf dem vor Ort auszufüllenden Formular entsprechende Informationen aufgeführt werden.

- Auskunfts- und Berichtigungsrecht. Der Inhaber einer Datensammlung muss gewährleisten, dass die betroffenen Personen ihr Auskunftsrecht geltend machen und die Daten allenfalls berichtigen lassen können. Dies bedeutet, dass die Gäste, deren Personalien tatsächlich in der Datenbank erfasst und somit anderen Anbieterinnen und Anbietern bekannt gegeben werden, informiert werden müssen, damit sie ihr Auskunfts- und Berichtigungsrecht wahrnehmen können.

- Zugang zur Datenbank: Eine solche Datenbank hat die Bedeutung einer Schwarzen Liste und darf auf keinen Fall öffentlich zugänglich sein. Der Zugriff auf die Datensammlung muss auf eine genau definierte Gruppe und konkrete Anfragen beschränkt werden. Es darf keine Einsicht in komplette Listen der erfassten Personen gewährt werden.

- Dauer der Aufbewahrung der Daten: Eine Aufbewahrungsdauer von zwei Jahren (bzw. die Vernichtung der Daten zwei Jahre nach dem letzten in der Datenbank erfassten Problem mit einer bestimmten Person) entspricht dem Grundsatz der Verhältnismässigkeit.

- Angemessener Schutz der Daten: Die Personendaten müssen durch angemessene organisatorische und technische Massnahmen gegen unbefugtes Bearbeiten geschützt werden.

Weitere Informationen zum Datenschutz finden Sie auf unserer Website www.derbeauftragte.ch.

- Zugang zur Datenbank: Eine solche Datenbank hat die Bedeutung einer Schwarzen Liste und darf auf keinen Fall öffentlich zugänglich sein. Der Zugriff auf die Datensammlung muss auf eine genau definierte Gruppe beschränkt werden und darf nur von Fall zu Fall möglich sein.

4.2 Erläuterungen zu «Voice over IP» und Datenschutz

Definition und Problematik

Die Internettelefonie (Voice over IP, VoIP) hat sich in letzter Zeit enorm entwickelt. Die Sprachübertragung erfolgt nicht mehr über die klassischen (separaten) Telefonnetze (PSTN, ISDN), sondern paketorientiert über das Internet. Es ergeben sich folgende wesentlichen Eigenschaften:

- Die Sprachübertragung erfolgt digital
- Die Kommunikation erfolgt über die üblichen Internetkanäle

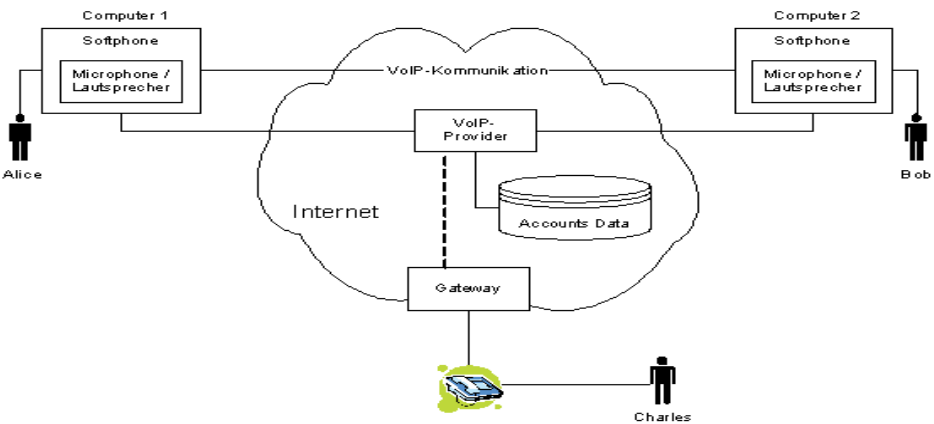
Diese beiden Eigenschaften erhöhen das Risiko einer unrechtmässigen Abhörung der Telefonate, denn es ist einfacher, an die übertragenen Daten zu kommen, und die digitalen Daten erleichtern eine automatisierte Auswertung.

Im Übrigen erleichtert es die digitale Form, die Sprach-Kommunikation zu kopieren, z.B. die elektronischen Spuren auf einem Server oder dem PC eines Benutzers.

Ziel

Das Ziel dieses Papiers ist es, die wesentlichen Datenschutzgefahren beim Einsatz von VoiP aufzuzeigen und Ratschläge sowohl an die Benutzer als auch an die Anbieter zur Verbesserung des Datenschutzes zu geben. Wir haben uns in diesem Zusammenhang wichtige verfügbare kostenlose Softphones angesehen.

Prinzipschema der Kommunikation:



Ratschläge des EDÖB

Aus der Beschäftigung mit den konkreten Softphone-Produkten haben wir erwartungsgemäss bezüglich Datenschutz Schwächen und Stärken festgestellt. Daraus können wir Ratschläge ableiten, die für die Anbieter allgemein gültig sind.

Auch die Benutzer selbst können für einen verbesserten Datenschutz sorgen: Unter den vielen vorhandenen Produkten sind bewusst diejenigen auszuwählen, welche die persönlichen Bedürfnisse am besten abdecken.

Ratschläge für die Benutzer

- **Lösung mit einer (wenn möglich offenen) Verschlüsselung wählen:** Wie allgemein bekannt, ist das Internet ein offenes Netz, bei dem a priori die Vertraulichkeit der Daten nicht gewährleistet ist. Das heisst, unverschlüsselte Gespräche könnten von Unbefugten mitgehört werden. Dies gilt insbesondere auch beim Einsatz von ungeschützten drahtlosen Netzwerken (WLAN). Da Telefongespräche sensible Personendaten enthalten können, ist der Einsatz einer Verschlüsselung sehr zu empfehlen. Der Einsatz von Verschlüsselungssystemen verlangt immer ein gewisses Vertrauen des Benutzers. Daher sind offene (d.h. verifizierbare) Lösungen den proprietären grundsätzlich vorzuziehen.

- **Regelmässige Software-Updates durchführen:** Im Laufe der Zeit werden in jeder Software Fehler und Sicherheitslücken entdeckt. Seriöse Anbieter korrigieren daher ihre Produkte regelmässig und stellen die Korrekturen zur Verfügung. Die Benutzer sollten sich daher unbedingt vergewissern, dass sie stets die neuste Version einer VoIP-Software einsetzen.

- **Vorhandene Datenschutzoptionen gemäss den eigenen Bedürfnissen aktivieren:** Die vorhandenen Datenschutzoptionen bringen nur dann einen Vorteil, wenn die Benutzer diese auch nach ihren Bedürfnissen einsetzen. Die Unterdrückung der Rufnummer (bzw. Identität) kann zum Beispiel je nach Anruf ein Vor- oder ein Nachteil für den Anrufer darstellen. Daher kann nicht pauschal gefordert werden, dass alle verfügbaren Datenschutzoptionen immer aktiviert sein sollen.

Ratschläge für die Anbieter

- **Verschlüsselung anbieten:** Die Vertraulichkeit der Gespräche kann nur mit einer Verschlüsselung der Datenströme erreicht werden. Daher hat der Anbieter unbedingt eine Verschlüsselungsmöglichkeit zu gewähren.

- **Offene Standards verwenden:** Um Transparenz und Vertrauen zu schaffen sind möglichst offene Standards zu verwenden. Dies gilt besonders für die Verschlüsselung. So können bei offenen Kommunikationsprotokollen auch Dritte Sicherheitsprodukte anbiete anbieten (z. B. Zfone).

- **Einfache Installation und Bedienung ermöglichen:** Ein Produkt wird erfahrungsgemäss nur dann von einer grossen Zahl von Benutzern eingesetzt, wenn es einfach und ohne besondere Kenntnisse und Erfahrung zu installieren, zu konfigurieren und zu bedienen ist.

- **Über die Datenschutz- und Datensicherheitsrisiken informieren:** Die Anbieter müssen die Benutzer umfassend über die beim Einsatz ihrer Produkte erfolgenden Datenbearbeitungen informieren (privacy policy). Dazu gehören auch allfällige Datenschutz- und Datensicherheitsrisiken. Nur so können sich die Benutzer adäquat schützen.

- **Die Datenbearbeitungen auf ein Minimum beschränken:** Im Sinne der Datensparsamkeit und Datenvermeidung sind nur diejenigen Daten zu bearbeiten, die für die Erbringung des Dienstes unbedingt notwendig sind.

- **Erkannte Fehler rasch korrigieren und automatische Updates anbieten:** Erkannte Fehler, die datenschutz-/datensicherheitsrelevant sind, sind sofort zu beheben. Den Anwendern ist auf rasche und gut ersichtliche Weise zu kommunizieren, dass neue Updates vorhanden sind.

- **Datenschutzoptionen einbauen und standardmässig aktivieren:** Der Benutzer sucht erfahrungsgemäss nicht aktiv nach allen möglichen Optionen. Daher sind die Datenschutz- und Datensicherheitsoptionen möglichst voreinzustellen. Der Benutzer sollte beispielsweise bei der Installation die Möglichkeit haben zu entscheiden, ob er im «elektronischen Telefonverzeichnis» vorkommen will oder nicht.

4.3 Empfehlung betreffend die Bearbeitung und Weitergabe von elektronischen Datenspuren durch die Firma X im Auftrag von Urheberrechtsinhabern

Bern, 09. Januar 2008

Empfehlung

gemäss

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

betreffend

die Bearbeitung und Weitergabe von elektronischen Datenspuren durch die Firma X im Auftrag von Urheberrechtsinhabern

I. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte stellt fest:

1. Die Firma X hat insbesondere in einer Besprechung und in einer Vorführung ihre Datenbearbeitung vorgestellt sowie in zwei Stellungnahmen den Eidgenössischen Datenschutz und Öffentlichkeitsbeauftragten (EDÖB) darüber informiert, dass sie im Auftragsverhältnis mit elektronischen Hilfsmitteln in der Schweiz Übermittlungsdaten (darunter Datum, IP-Adresse, Benutzername, etc.) von urheberrechtlich geschützten Werken aufzeichnet, welche auf peer-to-peer Netzwerken zum herunterladen (Download) angeboten werden (Aufzeichnungstätigkeit). Zudem gibt die Firma X diese aufgezeichneten Übermittlungsdaten im Anschluss an ihre Auftraggeber ins Ausland weiter.

2. Aufgrund der mit dem EDÖB abgehaltenen Sitzung und den beiden eingereichten Stellungnahmen kann die Aufzeichnungstätigkeit der Firma X wie folgt beschrieben werden:

   - Mittels der von ihr entwickelten Software (mit dem Namen «File Sharing Monitor» in der Version 1.8.1) sucht die Firma X automatisiert in verschiedenen peer-to-peer Netzwerken anhand eines speziell berechneten elektronischen Fingerabdrucks nach angebotenen (Upload) urheberrechtlich geschützten Werken, für welche sie von dem jeweiligen Urheberrechtsinhaber (oder deren Rechtsvertreter) einen Nachforschungsauftrag erhalten hat.

   - Sobald der von der Firma X entwickelte «File Sharing Monitor» anhand des elektronischen Fingerabdrucks ein urheberrechtlich geschütztes Werk findet, für welches die Firma X einen Nachforschungsauftrag hat, versucht dieser zu der Software des Anbieters des urheberrechtlich geschützten Werkes eine Verbindung aufzubauen, um das Werk herunterzuladen (Download).

   - Kann eine Verbindung zur Software des Anbieters des urheberrechtlich geschützten Werkes aufgebaut werden, so lädt der «File Sharing Monitor» dieses Werk automatisch ganz oder in Teilen herunter (Download) und zeichnet währenddessen einen Teil der zur Herstellung und Aufrechterhaltung der Internetverbindung zur Software des Anbieters ausgetauschten elektronischen Daten sowie weitere Daten (wie Uhrzeit und Datum) auf und speichert diese in einer Datenbank ab.

   - Im Anschluss daran übermittelt die Firma X die entsprechend aufgezeichneten und abgespeicherten Daten periodisch an den jeweiligen Urheberrechtsinhaber bzw. deren Rechtsvertreter.

3. Die von den Anbietern des jeweiligen urheberrechtlich geschützten Werkes übermittelten Verbindungsdaten sind zum Austausch des Werkes notwendig und werden von der von ihm verwendeten (Standard-)Software automatisch und ohne sein zutun übermittelt, da ansonsten technisch kein Datenaustausch stattfinden kann. Der Anbieter von urheberrechtlich geschützten Werken wird von der Firma X nicht darüber informiert, dass die von ihm übermittelten Verbindungsdaten aufgezeichnet und gespeichert werden.

4. Die von der Firma X aufgezeichneten Verbindungsdaten umfassen:

   - den Benutzernamen des Nutzers des peer-to-peer Netzwerkes

   - die IP-Adresse des verwendeten Internetanschlusses

- die GUID (spezielle Identifikationsnummer der vom Anbieter des urheberrechtlich geschützten Werkes verwendeten Software)
- das verwendete peer-to-peer Netzwerkprotokoll (Gnutella, eDonkey oder BitTorrent)
- den Namen und elektronischen Fingerabdruck (Hashcode) des urheberrechtlich geschützten Werkes
- das Datum und die Uhrzeit sowie den Zeitraum der Verbindung zwischen der Software der Firma X und der Software des Anbieters des jeweiligen urheberrechtlich geschützten Werkes.

Diese Daten werden sodann auf den Servern der Firma X in Steinhausen (ZG) gespeichert und nach Ländern und Anbietern von Internetanschlüssen sortiert. Die so erhobenen Daten werden anschliessend an die Urheberrechtsinhaber bzw. deren Rechtsvertreter ins Ausland weitergegeben und zur Identifikation des Inhabers des Internetanschlusses verwendet.

5. Zur Identifikation des Inhabers des Internetanschlusses reichen die Urheberrechtsinhaber bzw. ihre Rechtsvertreter bei den zuständigen Untersuchungsbehörden Strafklage gegen Unbekannt ein. Nachdem die zuständige Untersuchungsbehörde den Inhaber des Internetanschlusses identifiziert hat, verschaffen sich die Urheberrechtsinhaber bzw. deren Rechtsvertreter diese Identitätsdaten im Rahmen einer Akteneinsicht. Diese Daten werden dann in Abmahnverfahren verwendet, um gegenüber den betroffenen Personen Schadensersatzforderungen geltend zu machen und eine Unterlassungserklärung anzustreben. Tritt die betroffene Person nicht auf diese Forderungen ein, stellen die Inhaber der Urheberrechte bzw. deren Rechtsvertreter eine zivilrechtliche Durchsetzung ihrer Schadensersatzforderungen in Aussicht.

II. Erwägungen des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten:

1. Die von der Firma X durchgeführte Datenbearbeitung zielt darauf ab, den Urheberrechtsinhabern die Möglichkeit zu eröffnen, die hinter einem Austausch urheberrechtlich geschützter Daten stehenden Personen (Inhaber des Internetanschlusses bzw. Urheberrechtsverletzer) zu bestimmen. Da dies aufgrund der Verbindungsdaten (insbesondere der IP-Adresse) im Rahmen einer Strafanzeige in der Regel möglich ist, werden namentlich IP-Adressen als personenbezogene Daten angesehen (Art. 3 lit. a DSG; Basler Kommentar zum DSG, Urs Belser zu Art. 3 DSG, Rz. 6; Artikel 29 Datenschutzgruppe, Stellungnahme

04/2007 zum Begriff «personenbezogene Daten», http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_de.pdf). Da die IP-Adresse ein personenbezogenes Datum darstellt, sind alle mit ihr in Verbindung gebrachten Daten (wie in Rz. 4 aufgeführt) ebenfalls als personenbezogene Daten anzusehen. Zudem können in diesem Zusammenhang diese Daten als besonders schützenswertes Personendaten gemäss Art. 3 lit. c Ziff. 4 DSG angesehen werden, da sie im Rahmen eines Strafverfahrens zur Feststellung einer Straftat verwendet werden.

2. Unter «Bearbeiten» ist jeder Umgang mit Personendaten zu verstehen, dabei insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten (Art. 3 Bst. e DSG). Im vorliegenden Fall beschafft, verwendet und bewahrt die Firma X personenbezogene Daten auf und gibt die so erhobenen Personendaten an die Urheberrechtsinhaber bzw. deren Rechtsvertreter ins Ausland weiter. In einem zweiten Schritt verwenden die Urheberrechtsinhaber bzw. deren Rechtsvertreter die Verbindungsdaten, um über eine Strafanzeige den Inhaber des dazugehörigen Internetanschlusses zu identifizieren. Um die von der Firma X durchgeführte Datenbearbeitung beurteilen zu können, muss diese im Gesamtkontext und nicht isoliert betrachtet werden.

3. Die urheberrechtlich geschützten Werke sowie die zum Download benötigten Verbindungsdaten (IP-Adresse), für welche die Firma X einen Nachforschungsauftrag hat, werden auf peer-to-peer Plattformen von Teilnehmern an Tauschbörsen teilweise öffentlich zugänglich gemacht. Zudem ist die Firma X ohnehin ein Tauschpartner und erhält die zur Verbindung und dem dazugehörigen Download relevanten Daten vom Anbieter der jeweiligen Datei auf freiwilliger Basis. Diese der Firma X zugänglich gemachten Verbindungsdaten fallen daher nicht unter das Fernmeldegeheimnis. Für deren Bearbeitung (insbesondere Sammlung, Verarbeitung und Weitergabe der von der Firma X gesammelten personenbezogenen Daten) ist das Datenschutzgesetz (Art. 2 Abs. 1 lit. a DSG) anwendbar.

   Im Gegensatz zu den im vorliegenden Fall ausgetauschten und damit gegenüber dem Tauschpartner zugänglich gemachten Verbindungsdaten sind die zugehörigen Identitätsdaten (wie Name, Vorname, Adresse, etc., welche lediglich dem Anbieter des Internetanschlusses bekannt sind) grundsätzlich vom Fernmeldegeheimnis geschützt. Lediglich aufgrund einer gesetzlichen Grundlage kann das Fernmeldegeheimnis durchbrochen werden. Auf diese Weise können Untersuchungsbehörden gestützt auf Art. 5 des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (SR 780.1, BÜPF)

und Art. 14 Abs. 4 BÜPF aufgrund von Verbindungsdaten die dazugehörigen Identitätsdaten von den Anbietern von Fernmeldediensten herausverlangen. Obwohl das DSG auf ein Strafverfahren keine Anwendung findet (Art. 2 Abs. 2 lit. c DSG), sind die Untersuchungsbehörden dazu berechtigt, bei der Gewährung von Akteneinsichtsrechten gegenüber den Geschädigten mögliche entgegenstehende öffentliche und private Interessen zu berücksichtigen (vgl. z.B. Art. 108 des Entwurfs der Schweizerischen Prozessordnung StPO) und eine Interessensabwägung im Hinblick auf die Bekanntgabe der Daten durchzuführen. Zudem sind auch die Strafverfolgungsbehörden an das Amtsgeheimnis gebunden (Art. 320 StGB).

4. Die Voraussetzungen für eine Empfehlung im Sinne des DSG sind gegeben, da die Bearbeitungsmethoden grundsätzlich geeignet sind, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen (Art. 29 Abs. 1 lit. a DSG). Verstösst eine Datenbearbeitung zudem gegen die Vorschriften des Datenschutzes, kann der EDÖB gestützt auf Art. 29 Abs. 3 DSG empfehlen, die Datenbearbeitung zu ändern, einzustellen oder zu unterlassen.

5. Um die Konformität der Datenbearbeitung durch die Firma X mit dem DSG beurteilen zu können, muss diese im Hinblick auf die Voraussetzungen für eine rechtmässige Datenbearbeitung geprüft werden. Eine solche ist gegeben, wenn die Datenbearbeitung den Grundsätzen des Datenschutzes entspricht, welche namentlich sind: die Einhaltung des Rechtmässigkeitsprinzips (Art. 4 Abs. 1 DSG), des Zweckmässigkeitsprinzips (Art. 4 Abs. 3 DSG), des Transparenzprinzips (Art. 4 Abs. 2 DSG), des Verhältnismässigkeitsprinzips (Art. 4 Abs. 2 DSG) sowie die Grundsätze für eine Bekanntgabe der Daten ins Ausland (Art. 6 DSG). Falls diese nicht eingehalten werden und bei der Datenbearbeitung von einer Persönlichkeitsverletzung ausgegangen werden muss (Art. 12 DSG), ist darüber hinaus zu prüfen, ob Rechtfertigungsgründe (Art. 13 DSG) vorliegen, welche eine Datenbearbeitung dennoch ermöglichen. In diesem Rahmen kann die Firma X nach Art. 14 Abs. 2 DSG dieselben Rechtfertigungsgründe geltend machen, wie die Urheberrechtsinhaber.

Rechtmässigkeitsprinzip

6. Bis heute existiert in der Schweiz weder eine spezifische gesetzliche Grundlage, welche die systematische Erhebung von IP-Adressen in peer-to-peer Netzwerken erlaubt, noch ist eine solche Datenerhebung explizit verboten (vgl. StGB, BÜPF). Daher gelangt im vorliegenden Fall das DSG zur Anwendung. Im europäischen Ausland werden derzeit verschiedene gesetzliche Regelungen zur Bekämpfung der Film- und Musikpiraterie diskutiert.

Da die Datenbearbeitung ohne Wissen der betroffenen Personen automatisiert und proaktiv durchgeführt wird sowie der Inhaber der Datensammlung darüber hinaus in die Lage versetzt wird, mit den gesammelten Daten im Nachgang Strafuntersuchungen gegen eine von vorne herein unbestimmte Anzahl von Personen anzustossen, vertritt der EDÖB die Meinung, dass eine solche Untersuchung explizit gesetzlich geregelt werden muss. Dies gilt vor allem, da eine solche Datenbearbeitung eine grosse Reichweite hat und die Persönlichkeitsrechte einer Vielzahl betroffener Personen tangiert werden. Der gesetzliche Rahmen sollte darüber hinaus die Beweiskraft solcher über das Internet gesammelten Daten und ihre Zulässigkeit als Beweismittel regeln.

Zweckmässigkeitsprinzip

7. Gemäss dem Zweckmässigkeitsprinzip dürfen personenbezogene Daten nur zu dem Zweck verwendet werden – eine entsprechende gesetzliche Regelung vorbehalten – der bei deren Erhebung angegeben wurde oder aus den Umständen erkennbar ist.

8. Bei der Nutzung von peer-to-peer Netzwerken besteht der Zweck der Bekanntgabe und des Austausches von IP-Adressen im Austausch von Dateien zwischen den einzelnen Nutzern des peer-to-peer Netzwerkes. Die Verwendung dieser Daten durch die Firma X zum Zwecke der Feststellung von Urheberrechtsverletzungen stellt eine Entfremdung des ursprünglich angestrebten Zwecks dar. Aus den konkreten Umständen der Nutzung eines peer-to-peer Netzwerkes ist zudem auch nicht erkennbar, dass ein Tauschpartner systematisch Daten sammelt. Daher müsste nach datenschutzrechtlichen Gesichtspunkten die Firma X gegenüber den betroffenen Nutzern des peer-to-peer Netzwerkes den Zweck der von ihr durchgeführten Datenbearbeitung bekannt machen. Da die Firma X allerdings ihre Daten ohne Information und Wissen der betroffenen Personen erhebt, wird das Zweckmässigkeitsprinzip verletzt. In wieweit die Verletzung des Zweckmässigkeitsprinzips durch ein überwiegendes privates Interesse gerechtfertigt werden kann, wird nachfolgend geprüft (siehe Abschnitt: «Notwendigkeit eines Rechtfertigungsgrundes»).

Treu und Glauben sowie Transparenzprinzip

9. Datenbearbeitungen haben nach Treu und Glauben zu erfolgen (vgl. Art. 4 Abs. 2 DSG). Gegen den Grundsatz von Treu und Glauben verstösst z.B. derjenige, welcher heimlich Daten beschafft, ohne dabei gegen eine Rechtsnorm zu verstossen (BBl 1988 II 449). Aus diesem Prinzip ist die Anforderung abzuleiten, dass eine Datenbeschaffung für die betroffene Person transparent erfolgen muss. Dies bedeutet, dass eine Datenbeschaffung und jede weitere

Datenbearbeitung grundsätzlich für die betroffene Person erkennbar sein muss, der Betroffene also aus den Umständen heraus damit rechnen muss oder er entsprechend informiert bzw. aufgeklärt wird. Je einschneidender die Datenbearbeitung in Bezug auf die Persönlichkeitsrechte ist, desto höhere Anforderungen werden an die Transparenz gestellt (vgl. U. Maurer in Basler Kommentar, Datenschutzgesetz, Maurer/Vogt. Hrsg., 2006, Art. 4 Rz. 8). Nach den Regelungen des revidierten Datenschutzgesetzes (Art. 7a rev. DSG) wird sogar eine aktive Informationspflicht gefordert, wenn es sich um besonders schützenswerte Personendaten handelt und kein überwiegendes öffentliches oder privates Interesse dem entgegensteht (BBl 2003 I 2131).

10. Die von der Firma X durchgeführte Datensammlung erfolgt ohne jedes Wissen der betroffenen Personen (sei es der Inhaber des Internetanschlusses oder der eigentliche Urheberrechtsverletzer) und muss daher als heimliche Datenbeschaffung angesehen werden. Weder auf den Webseiten der Tauschbörsen, auf welchen man die File-Sharing-Software zur Teilnahme an einem peer-to-peer Netzwerk herunterladen kann, noch über die Kommunikationskanäle, über welche File-Sharing-Programme in der Regel verfügen, wird auf die Möglichkeit hingewiesen, dass die Verbindungsdaten aufgezeichnet werden könnten. Der Inhaber des Internetanschlusses erhält von der Datenaufzeichnung in keinem Fall Kenntnis, da er im Kommunikationsprozess zwischen dem Urheberrechtsverletzer und der Firma X nicht eingebunden ist. Zudem hat die Firma X denn auch eigens zur Sammlung von solchen Verbindungsdaten eine Software (File Sharing Monitor) entwickelt, welche dazu dient systematisch und ohne Kenntnis der Betroffenen Verbindungsdaten aufzuzeichnen. Alleine schon die Konzeption der Software, welche es erlaubt unerkannt Dateien herunterzuladen ohne dabei gleichzeitig andere Dateien zum Upload bereitzustellen ist darauf angelegt, heimlich Verbindungsdaten aufzuzeichnen. Heute gestatten übliche File-Sharing Programme eine Teilnahme an einem peer-to-peer Netzwerk nur dann einen Download, wenn gleichzeitig Dateien zum Upload zur Verfügung gestellt werden. Die Software der Firma X umgeht im peer-to-peer Netzwerk einen Upload, um am Tauschgeschehen teilzunehmen. Damit täuscht die von der Firma X verwendete Software vor, sie sei ein gewöhnlicher Teilnehmer eines peer-to-peer Netzwerkes, um so inkognito bzw. ohne Wissen der betroffenen Personen (Inhaber des Internetan-schlusses und/oder Urheberrechtsverletzer) Daten zu sammeln.

11. In wieweit die Verletzung des Transparenzprinzips durch ein überwiegendes privates Interesse gerechtfertigt werden kann, wird nachfolgend geprüft (siehe Abschnitt: «Notwendigkeit eines Rechtfertigungsgrundes»).

12. Weiterhin werden die von der Firma X gesammelten Daten vorwiegend mit dem Ziel gesammelt, um den Inhaber des jeweiligen Internetanschlusses zu identifizieren und anschliessend gegenüber diesem Zivilansprüche geltend zu machen. Da die Identifizierung der Inhaber eines Internetanschlusses ausschliesslich im Rahmen einer Strafanzeige möglich ist, da die Identitätsdaten grundsätzlich durch das Fernmeldegeheimnis geschützt sind, umgehen die Urheberrechtsinhaber mit der Einleitung eines Strafverfahrens als Mittel zum Zweck zur Feststellung der Identität des Inhabers des Internetanschlusses und zur Geltendmachung von Zivilansprüchen gegenüber diesen das Fernmeldegeheimnis. Ein solches Vorgehen ist als dem Prinzip von Treu und Glauben entgegengesetzt bzw. als rechtsmissbräuchlich anzusehen, da die Urheberrechtsinhaber das Rechtsinstitut der Akteneinsicht in einem Strafverfahren gegenüber einem Urheberrechtsverletzer dazu verwenden, sich für ein Zivilverfahren gegen einen gutgläubigen Inhaber eines Internetanschlusses durch die Umgehung des Telefongeheimnisses eine bessere Ausgangslage zu verschaffen. Es liegt in diesem Falle ein Institutionenmissbrauch vor (Heinrich Honsell, Basler Kommentar zum Zivilgesetzbuch, 2. Auflage, Helbing & Lichtenhahn Verlag, Basel, 2002, Art. 2, Rz. 51). Dies gilt umso mehr, als die Urheberrechtsinhaber bzw. ihre Rechtsvertreter meist nicht einmal das Ende der Strafuntersuchung abwarten, um ihre Zivilansprüche gegen den eigentlichen Urheberrechtsverletzer geltend zu machen. Vielmehr nehmen sie bereits während der laufenden Strafuntersuchung Akteneinsicht, um die Identität der gutgläubige Inhaber des Internetanschlusses zur Geltendmachung von zivilrechtlichen Forderungen festzustellen, obwohl diese keine Urheberrechtsverletzung begangen haben müssen.

13. Daher muss im Rahmen einer rein zivilrechtlichen Geltendmachung von Schadensersatzansprüchen im vorliegenden Fall ein überwiegendes privates Interesse der Urheberrechtsinhaber abgelehnt werden. Da ein solches Vorgehen darüber hinaus gegen den Grundsatz von Treu und Glauben verstösst, erübrigt sich eine Verhältnismässigkeitsprüfung für die Datenerhebung im Hinblick auf die Anstrengung eines Zivilverfahrens. Wenn eine Durchbrechung des Fernmeldegeheimnisses im Rahmen eines Zivilverfahrens ermöglicht werden soll, bedarf es nach Meinung des EDÖB hierzu einer gesetzlichen Grundlage, welche analog wie die BÜPF im Strafverfahren die Bedingungen für eine Durchbrechung des Fernmeldegeheimnisses regelt.

Verhältnismässigkeit der Datenbearbeitung zur Anstrengung eines Strafverfahrens

14. Nachfolgend wird die Verhältnismässigkeit ausschliesslich für die von der Firma X durchgeführte Datenbearbeitung im Rahmen der Anstrengung eines Strafverfahrens geprüft.

15. Damit eine Massnahme, welche in den Persönlichkeitsbereich einer privaten Person eingreift, als verhältnismässig eingestuft werden kann, muss diese im Hinblick auf den zu erreichenden Zweck geeignet und notwendig sein. Ausserdem muss der angestrebte Zweck in einem vernünftigen Verhältnis zum Eingriff in den Persönlichkeitsbereich der privaten Person stehen (Zumutbarkeit).

Geeignetheit

16. Um eine Urheberrechtsverletzung gemäss Art. 67 URG strafrechtlich ahnden zu können, ist es notwendig, den Verletzer des Urheberrechts festzustellen. Mit den von der Firma X unternommenen Massnahmen kann aufgrund der IP-Adresse inklusive Datum und Uhrzeit ihrer Verwendung der Inhaber des jeweiligen Internetanschlusses durch Untersuchungsbehörden mittels gesetzlich legitimierter Durchbrechung des Fernmeldegeheimnisses identifiziert werden (Art. 14 Abs. 4 BÜPF, vgl. auch hierzu Kritik von Bondallaz, a.a.O. Rz. 1803ff., 1834). Diese Massnahme ist geeignet, um den Täterkreis auf diejenigen Personen einzuschränken, welche den Internetanschluss benutzen und basierend hierauf weitere Massnahmen (wie z.B. Einvernahmen, Hausdurchsuchungen und/oder Beschlagnahmungen) zu ergreifen, um den tatsächlichen Urheberrechtsverletzer feststellen zu können. Daher ist die von der Firma X durchgeführte Datenbearbeitung geeignet, um eine Strafuntersuchung einzuleiten.

Erforderlichkeit

17. Die von der Firma X im Auftrag der Urheberrechtsinhaber ergriffenen Massnahmen zielen letztlich auf die Identifikation des Inhabers des Internetanschlusses ab. Für eine Anzeige bei den zuständigen Strafverfolgungsbehörden ist grundsätzlich ein erster Anhaltspunkt nötig, damit ein Strafverfahren gegen eine bestimmte Person eingeleiten werden kann. Daher kann es erforderlich sein, in diesem Rahmen eine Urheberrechtsverletzung festzustellen, da somit die Erfolgswahrscheinlichkeit der Überführung des Täters erheblich gesteigert wird.

Zumutbarkeit

18. Zur Feststellung einer Straftat, vertritt der EDÖB die Meinung, dass es einem Inhaber eines Internetanschlusses, über welchen eine Straftat begangen wurde, zuzumuten ist, einer Strafuntersuchung ausgesetzt zu werden, solange ihm hierdurch – bei Unschuldigkeit – keine ernsthaften Nachteile erwachsen. Solche können dem (unschuldigen) Inhaber eines Internetanschlusses bzw. weiteren Nutzer eines Internetanschlusses allerdings drohen, wenn dessen Identität im Rahmen des Akteneinsichtsrechts zu einem Zeitpunkt, in dem der Urheberrechtsverletzer noch nicht ermittelt wurde, den geschädigten Urheberrechtsinhabern bekannt gegeben wird. Der Tatsache, dass die Identitätsdaten hinter einer IP-Adresse grundsätzlich vom Fernmeldegeheimnis geschützt sind, ist im Rahmen des Auskunftsrechts der Geschädigten nach Meinung des EDÖB zwingend Rechnung zu tragen. Für die Urheberrechtsinhaber als Geschädigte ist es für die Wahrnehmung ihrer Mitwirkungs- und Kontrollrechte (vgl. Hauser/Schweri a.a.O, § 38 Rz. 5) nicht notwendig, die Identität des Inhabers des Internetanschlusses zu erhalten, welcher keine Urheberrechtsverletzung begangen hat. Ausserdem können Sie ihre zivilrechtlichen Ansprüchen gegenüber dem Urheberrechtsverletzer im Strafverfahren adhäsionsweise geltend machen. Hingegen ist dem überführten Urheberrechtsverletzer die Bekanntgabe seiner Identität gegenüber den geschädigten Urheberrechtsinhabern sehr wohl zuzumuten.

Notwendigkeit eines Rechtfertigungsgrundes

19. Die Aufzeichnung der Verbindungsdaten durch den «File Sharing Monitor» stellt aufgrund der oben genannten Gründe (Rz. 6-19) eine Persönlichkeitsverletzung gemäss Art. 12 Abs. 2 DSG dar, welche zur Anstrengung eines Strafverfahrens eines Rechtfertigungsgrundes nach Art. 13 Abs. 1 DSG bedarf. Art. 13 Abs. 1 DSG sieht als mögliche Rechtfertigungsgründe die Einwilligung des Verletzten, ein überwiegendes öffentliches oder privates Interesse oder das Gesetz vor. Bei der Datenbearbeitung der Personendaten durch die Firma X liegt keine Einwilligung der betroffenen Personen (weder des Inhabers der IP-Adresse noch des Urheberrechtsverletzers) vor, da die Datenerhebung ohne deren Wissen erfolgt. Während vom gutgläubigen Inhaber eines Internetanschlusses nie von einer Einwilligung ausgegangen werden kann, ist für den Urheberrechtsverletzer zu prüfen, ob er mit einer solchen Datenerhebung rechnen musste. Im vorliegenden Fall kann nicht von einer impliziten Einwilligung des Urheberrechtsverletzers ausgegangen werden, da die Daten lediglich zum Zwecke eines Datentransfers (urheberrechtlich geschütztes Werk

in elektronischer Form) zwischen zwei Computerprogrammen ausgetauscht und übertragen werden und der gewöhnliche Nutzer nicht davon ausgehen kann, dass der Tauschpartner von diesen Übertragungsdaten ohne weiteres Zutun Kenntnis erhält. So hat auch die Firma X eigens eine spezielle Software («File Sharing Monitor») entwickelt, um diese Daten überhaupt systematisch auszulesen und speichern zu können. Weiterhin ist ebenfalls keine gesetzliche Grundlage oder ein überwiegendes öffentliches Interesse für die von der Firma X durchgeführte Datenbearbeitung ersichtlich. Dennoch kann sich der Urheberrechtsverletzer im Gegensatz zum gutgläubigen Inhaber eines Internetanschlusses aufgrund der von ihm begangenen Straftat nicht auf seine Gutgläubigkeit berufen.

20. Damit ein überwiegendes privates Interesse angenommen werden kann, müssen gewisse Anforderungen erfüllt sein. Art. 13 Abs. 2 DSG enthält eine Aufzählung von sechs nicht abschliessenden Rechtfertigungsgründe, welche dem Richter einen gewissen Anhaltspunkt für die Interessenabwägung an die Hand geben sollen. So ist etwa «ein Beschaffen von Daten mit unrechtmässigen Mitteln nur selten, ein Beschaffen wider Treu und Glauben praktisch überhaupt nie zu rechtfertigen», während sich für eine blosse unrichtige Datenbearbeitung wohl eher ein Rechtfertigungsgrund finden lässt. Hierbei lassen sich die Rechtfertigungsgründe grundsätzlich in vier Gruppen einteilen ([direkte] wirtschaftliche Tätigkeiten, insbesondere Vertragsabschluss, wirtschaftlicher Wettbewerb, Kreditüberprüfung; Veröffentlichung in einem Medium; nicht personenbezogene Datenbearbeitung sowie Daten einer Person des öffentlichen Lebens bezüglich ihres Wirkens in der Öffentlichkeit). Ob ein Rechtfertigungsgrund gegeben ist, muss aufgrund der konkreten Umstände im Einzelfall anhand einer sorgfältigen Interessensabwägung entscheiden werden (Urteil der EDSK vom 21. November 1996, VPB 62.42B, E. V 1b). Als schützenswerte Interessen können hierbei alle «Interessen von allgemein anerkanntem Wert» angesehen werden (A. Bucher, natürliche Personen, S. 536 in Basler Kommentar zum DSG Corrado Rampini zu Art. 13 DSG Rz. 22).

21. Eine von der Firma X vorgenommene Datenbearbeitung und die anschliessende Einleitung eines Strafverfahrens (durch die Urheberrechtsinhaber bzw. deren Rechtsvertreter) zur Erlangung der sich hinter einer IP-Adresse verbergenden Identitätsdaten für die Anstrengung eines Zivilverfahrens verstossen gegen das Prinzip von Treu und Glauben. Eine solche Datenbearbeitung zur Geltendmachung von Zivilansprüchen kann daher nicht gerechtfertigt werden (vgl. Rz. 12).

22. Aus Art. 13 Abs. 2 DSG kann im vorliegenden Fall nur für Einleitung eines Strafverfahrens ein überwiegendes privates Interesse als Rechtfertigungsgrund entnommen werden, wobei allerdings eine Interessensabwägung entwickelt werden muss (vgl. Rz. 14ff.).

23. Bei der Verfolgung von strafrechtlich relevanten Verstössen gegen das Urheberrecht haben die Inhaber des Urheberrechts ein Interesse an der strafrechtlichen Ahndung solcher Verletzungen und im Nachgang an das Strafverfahren als Geschädigter ein Interesse an Entschädigungszahlungen, um den so entstandenen wirtschaftlichen Schaden (lucrum cessans) zu kompensieren. Diesen Interessen stehen die Persönlichkeitsrechte, insbesondere die informationelle Selbstbestimmung, der betroffenen Personen (Inhaber des Internetanschlusses und Urheberrechtsverletzer) gegenüber.

24. Eine Urheberrechtsverletzung gemäss Art. 67 URG ist nach Schweizer Recht ein Antragsdelikt. Damit eine Untersuchungsbehörde überhaupt ein Untersuchungsverfahren eröffnet, ist es notwendig, einen Anfangsverdacht einer Verletzung eines Urheberrechts festzustellen. Daher müssen gewisse Anhaltspunkte vorliegen, welche eine mutmassliche Urheberrechtsverletzung gemäss Art. 67 URG begründen. Sogar für eine heimliche Datenbearbeitung kann in diesem Rahmen ein ausreichender Rechtfertigungsgrund gegeben sein, wenn die Gefahr besteht, dass eine vorherige Anzeige aufgrund des Transparenzprinzips ein Strafverfahren verunmöglicht oder wesentlich erschwert, da der Urheberrechtsverletzer wichtige Beweismittel vernichten könnte bzw. diese gar nicht erst erhoben werden könnten.

25. Nach erfolgter Anzeige gegen Unbekannt ist es Sache der jeweiligen Strafverfolgungsbehörden, den tatsächlichen Sachverhalt zu ermitteln und den Täter ausfindig zu machen. Grundsätzlich stehen den Geschädigten im Rahmen eines Strafverfahrens Parteirechte, insbesondere Mitwirkungs- und Kontrollrechte zu (Hauser, Schweri, Schweizerisches Strafprozessrecht, 4. neu überarbeitete und ergänzte Auflage, Helbing & Lichtenhahn, Basel, Genf, München, 1999, §38, Rz. 5, 7). Hierbei beurteilt sich die Frage der Akteneinsicht nach den allgemeinen Verfahrensgrundsätzen wie sie auch in dem Entwurf zur Schweizerischen Strafprozessordnung (StPO, http://www.admin.ch/ch/d/ff/2007/6977.pdf) geregelt sind. Gemäss Art. 108 StPO darf die Einsichtnahme verweigert oder beschränkt werden, wenn ihr wesentliche öffentliche und private Interessen entgegenstehen oder wenn ein begründeter Verdacht besteht, dass eine Partei ihre Rechte missbraucht (BBl 2007 Nr. 42 S. 6977). In BGE 95 I 109 stellt das Bundesgericht fest, dass das Akteneinsichtsrecht (sowohl

in abgeschlossenen als auch in laufenden Verfahren) seine Grenzen an den öffentlichen Interessen des Staates oder den berechtigten Geheimhaltungsinteressen Privater findet. Aus diesem Grund kann es geboten sein, im Rahmen von laufenden Untersuchungen das Akteneinsichtsrecht zu verweigern. Im vorliegenden Fall wird das Akteneinsichtsrecht dazu gebraucht, gegenüber dem Inhaber eines Internetanschlusses ein Zivilverfahren zu einem Zeitpunkt anzustrengen, in welchem das Strafverfahren noch nicht abgeschlossen ist und der Urheberrechtsverletzer noch nicht feststeht. Zudem hat die geschädigte Partei ausschliesslich über das Akteneinsichtsrecht die Möglichkeit die sich hinter einer IP-Adresse verbergende Identität des Anschlussinhabers zu erlangen. In einem rein zivilrechtlichen Verfahren besteht eine solche Möglichkeit nicht, da die Identität hinter einer IP-Adresse vom Fernmeldegeheimnis geschützt ist. Wird die Identität des Inhabers eines Internetanschlusses dem Urheberrechtsinhaber bekannt, kann sich der Inhaber des Internetanschlusses mit Zivilforderungen konfrontiert sehen, obwohl er möglicherweise keine Urheberrechtsverletzung begangen hat. Der EDÖB vertritt die Meinung, dass eine solche Durchbrechung des Fernmeldegeheimnisses nur aufgrund einer gesetzlichen Grundlage möglich sein darf. Auf der anderen Seite entsteht dem Urheberrechtsinhaber kein nicht wieder gutzumachender Nachteil, wenn das Akteneinsichtsrecht erst nach erfolgreichem Abschluss der Strafuntersuchung gewährt wird und der Urheberrechtsverletzer gefunden wurde. Selbst eine adhäsionsweise Geltendmachung der Zivilansprüche im Rahmen des Strafverfahrens würde ausreichen, um die Zivilforderungen des Urheberrechtsinhabers angemessen zu berücksichtigen. Daher gebietet es das schützenswerte private Interesse des Anschlussinhabers, dass seine Identität nur dann bekannt gegeben wird, wenn ihm eine Urheberrechtsverletzung nachgewiesen werden konnte und er sich daher nicht auf seine Gutgläubigkeit berufen kann.

26. Dies gilt umso mehr als gemäss Art. 8 Abs. 1 der Konvention zum Schutze der Menschenrechte und Grundfreiheiten (SR 0.101, EMRK) jede Person das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz hat. Dieses Recht kann gemäss Art. 8 Abs. 2 EMRK von einer Behörde aufgrund einer gesetzlichen Grundlage (z.B. durch die BÜPF in Strafverfahren) eingeschränkt werden. Da sich allerdings Art. 8 Abs. 1 EMRK nicht nur an den Gesetzgeber, sondern auch an die anwendenden Behörden (hier die Strafverfolgungsbehörden) richtet (Stéphane Bondallaz, La protection des personnes et de leur données dans les télécommunications, Schulthess, Zürich, Basel, Genf, 2007, Rz. 334, S. 103), sind auch diese angehalten, die Per-

sönlichkeitsrechte im Rahmen des Akteneinsichtsrechts zu schützen. Daher sollte in jedem Fall verhindert werden, dass die Identität eines Inhabers des Internetzugangs (welche durch das Fernmeldegeheimnis geschützt ist und nur aufgrund einer gesetzlichen Grundlage durchbrochen werden kann) bekannt wird, solange diesem keine Schuld an der Urheberrechtsverletzung nachgewiesen werden kann.

27. In der derzeitigen Praxis kann aufgrund des von den Untersuchungsbehörden gewährten Akteneinsichtsrechts, die von der Firma X unternommene Datenbearbeitung nicht auf den Zweck der strafrechtlichen Verfolgung der Urheberrechtsverletzung nach Art. 67 URG beschränkt werden. Vielmehr werden über den Institutionsmissbrauch des Akteneinsichtsrechts diese von der Firma X erhobenen Daten unrechtmässig zur Anstrengung von Zivilverfahren gegen die jeweiligen gutgläubigen Inhaber des Internetanschlusses verwendet. Damit wird letztendlich im zivilrechtlichen Bereich das Fernmeldegeheimnis umgangen und die Urheberrechtsinhaber machen hiervon auch regen Gebrauch. Da hierdurch die Persönlichkeitsrechte einer unbeschränkten Anzahl gutgläubiger Inhaber von Internetanschlüssen verletzt werden, kann auch im vorliegenden Fall die Anstrengung eines Strafverfahrens nicht als ausreichender Rechtfertigungsgrund angesehen werden, solange nicht gewährleistet werden kann, dass die Identität gutgläubiger Inhaber von Internetanschlüssen im Strafverfahren geschützt werden.

Notwendigkeit einer gesetzlichen Grundlage und Schlussfolgerung

28. Faktisch ist der Umweg über die Einleitung eines Strafverfahrens, um so die Identität des Inhabers des Internetanschlusses zu erhalten, eine Umgehung des Fernmeldegeheimnisses im privatrechtlichen Bereich. Gemäss Art. 35 Abs. 1 BV ist der Gesetzgeber dazu angehalten, die Grundrechte, welche die Privatsphäre schützen auch im privatrechtlichen Bereich durchzusetzen (S. Bondallaz, a.a.O., Rz. 265). Eine Durchbrechung des Fernmeldegeheimnisses bedarf daher (wenn eine solche vom Gesetzgeber gewünscht wird) aus Sicht des EDÖB einer expliziten gesetzlichen Grundlage, welche regelt, wann, wie und unter welchen Bedingungen eine solche Durchbrechung möglich sein sollte. Das blosse Ausnutzen einer Gesetzeslücke kann hierfür nicht ausreichen.

29. Bereits in der parlamentarischen Diskussion zu Art. 51 URG im Hinblick auf die Durchsetzung der Auskunftspflicht von Nutzern urheberrechtlicher Werke gegenüber den Verwertungsgesellschaften präzisiert der Gesetzgeber in der Botschaft hierzu, dass die Erteilung von Auskünften zur Geltendmachung zivilrechtlicher Ansprüche nicht hoheitlich durchgesetzt werden kann, sondern

er verweist ausdrücklich auf den privatrechtlichen Klageweg (BBl 1989 III 561). Auch in der kürzlich geführten parlamentarischen Diskussion zur Umsetzung des WIPO-Abkommens wurde ein Ausbau der verwandten Schutzrechte diskutiert. Dieser wurde allerdings vom Gesetzgeber abgelehnt, da kein ersichtlicher Grund besteht von der 1992 vorgenommenen Interessensabwägung abzuweichen (BBl 2006 3404). Somit hat der Gesetzgeber bisher für eine Durchsetzung von zivilrechtlichen Urheberrechtsansprüchen mit hoheitlichen Mitteln noch keine gesetzliche Grundlage geschaffen.

30. Aus datenschutzrechtlicher Sicht könnte daher einzig die Sammlung von IP-Adressen inklusive Zeitstempel zum Zwecke der Strafverfolgung als ein überwiegendes privates Interesse angesehen werden (vgl. Rz. 19-24). Solange allerdings (sowohl in der Schweiz wie auch im Ausland) nicht gewährleistet ist, dass die Identität der Inhaber eines Internetanschlusses solange geschützt bleibt, bis diese der Urheberrechtsverletzung überführt werden konnten, ist die Datenbearbeitung durch die Firma X und die Urheberrechtsinhaber bzw. deren Rechtsvertreter in ihrer Gesamtheit dazu geeignet, die Persönlichkeit betroffener Personen (Inhaber von Internetanschlüssen, welche keine Urheberrechtsverletzung begangen haben) zu verletzen (vgl. Rz. 25-27).

31. Da nicht ausgeschlossen werden kann, dass die von der Firma X erhobenen Daten in der oben beschriebenen Form zur Identifikation eines Inhabers eines Internetanschlusses, welcher keine Urheberrechtsverletzung begangen hat, verwendet werden, ist die durchgeführte Datenbearbeitung insgesamt als unrechtmässig zu qualifizieren.

32. Zu prüfen ist auch, ob und in wie weit weniger schwerwiegende Möglichkeiten bestehen, um Urheberrechtsverletzungen zu bekämpfen. Hierbei ist vor allem an Massnahmen wie spezielle Filter zu denken, die von Anbietern von Internetzugängen genutzt werden können, um den Austausch spezifischer Dateien in P2P-Netzwerken auf der Basis einer Datenbank urheberrechtlich geschützter Werke zu unterbinden. Solche Technologien existieren bereits heute.

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

Die Firma X stellt die von ihr praktizierte Datenbearbeitung unverzüglich ein, solange keine ausreichende gesetzliche Grundlage für eine zivilrechtliche Nutzung der durch sie erhobenen Daten besteht.

Die Firma X teilt dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) innerhalb von 30 Tagen ab Erhalt dieser Empfehlung mit, ob sie die Empfehlung annimmt oder ablehnt. Wird diese Empfehlung nicht befolgt oder abgelehnt, so kann der EDÖB die Angelegenheit dem Bundesverwaltungsgericht zum Entscheid vorlegen (Art. 29 Abs. 4 DSG).

Bei Annahme der Empfehlung gilt der Fristablauf (30 Tage) gleichzeitig als Fristbeginn für die Umsetzung der genannten Massnahme.

Die vorliegende Empfehlung wird in Anwendung von Art. 30 Abs. 2 DSG in anonymisierter Form publiziert.

EIDGENÖSSISCHER DATENSCHUTZ- UND
ÖFFENTLICHKEITSBEAUFTRAGTER

Hanspeter Thür

4.4 Empfehlung betreffend Drogen- und Alkoholtests bei der SBB

Bern, 25. Mai 2007

Empfehlung

gemäss

Art. 27 des

Bundesgesetzes über den Datenschutz (DSG)

vom 19. Juni 1992

betreffend

Drogen- und Alkoholtests bei den Schweizerischen Bundesbahnen (SBB)

I. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) stellt fest:

1. Mitte März 2007 haben Berichte in den Medien für Aufsehen gesorgt, wonach die unter 40-jährigen Mitarbeiter der SBB mit Sicherheitsfunktionen – hauptsächlich Lokführer, Kondukteure, Rangier- und Gleisarbeiter – im Rahmen routinemässiger Gesundheitschecks auf Drogenkonsum untersucht werden. Der EDÖB hat sich daraufhin in den Medien dahingehend geäussert, dass bei Berufsgattungen mit hohem Sicherheitsaspekt, bspw. bei Lokführern, Drogentests durchaus denkbar seien. Nicht nachvollziehbar sei hingegen die Tatsache, dass die Tests auf illegale Drogen beschränkt werden. Alkohol könne, so der EDÖB, ein weitaus wichtigeres Sicherheitsproblem darstellen. Weiter sei

die Altersbeschränkung auf unter 40-jährigen nicht nachvollziehbar. Nicht hinzunehmen seien auch die Auswirkungen der Tests aufs Privatleben der betroffenen Personen, da dadurch ihr Freizeitverhalten kontrolliert wird. Der EDÖB teilte schliesslich mit, dass er die Rechtmässigkeit der Tests überprüfen lassen werde.

2. Der EDÖB ist nachträglich darauf aufmerksam gemacht worden, dass der Bundesrat bereits Anfang März 2007 einen Gesetzesentwurf verabschiedet hat, der Zwangstests für eine grosse Anzahl von Personen im öffentlichen Transportwesen vorsieht. Die Bestimmungen sind in einem Paket der Bahnreform 2 untergebracht und wurden unter dem Titel «Revision der Erlasse über den öffentlichen Verkehr» bereits dem Parlament zugeleitet. Danach sollen im Wesentlichen verdachtsfreie Atemalkoholproben sowie bei auffälligem Verhalten oder anderen Verdachtsmomenten Alkohol-, Medikamenten- und Drogentests durchgeführt werden können.

3. Mit Schreiben vom 12. März 2007 ist der EDÖB an die SBB mit dem Gesuch um Darstellung des genauen Sachverhalts gelangt.

4. In ihrer Stellungnahme vom 23. März 2007 haben die SBB im Wesentlichen die sicherheitsdienstlichen Aufgaben des Zugpersonals erläutert und eine Verordnung des UVEK als Grundlage für die medizinischen Erstuntersuchungen (VTE) angegeben. Für periodische Untersuchungen wird eine verordnungsausführende Richtlinie des Bundesamts für Verkehr (BAV) als Grundlage zitiert. Aus dem Schreiben ist weiter zu entnehmen, dass die Erstuntersuchung systematisch eine Untersuchung auf Drogenkonsum enthält, während es bei periodischen Untersuchungen eine Urin-Analyse zur Feststellung eines allfälligen Konsums von psychoaktiven Substanzen nur bei entsprechender Indikation gibt. Für das schon beschäftigte Zugspersonal hat das *Medical Service* entschieden, die Erstuntersuchung routinemässig grundsätzlich nur bei Personen unter 40 Jahren durchzuführen. Im Hinblick auf unregelmässigen oder punktuellen Cannabiskonsum verlangt das *Medical Service* gestützt auf die Departementsverordnung, sowohl im Rahmen von Erstuntersuchungen bei Bewerbern als auch bei periodischen Untersuchungen der Angestellten, eine Verzichtserklärung auf jeglichen Konsum und die Bereitschaft, sich unangemeldeten Urinuntersuchungen zu unterziehen.

5. Am 18. April 2007 hat eine Sitzung zwischen Vertretern der SBB und dem EDÖB stattgefunden. Dabei wurde seitens des EDÖB im Wesentlichen festgehalten, dass für die fraglichen Drogen- und Alkoholtests gegenwärtig keine genügende gesetzliche Grundlage besteht. Die SBB haben diesbezüglich auf

die VTE und die einschlägigen gesamtarbeitsvertraglichen Bestimmungen verwiesen. Die SBB haben beteuert, dass sie auf die fraglichen Tests aus Sicherheitsgründen nicht verzichten werden, da die Einwilligung der betroffenen Personen vorliegt. Die Sicherheitsrelevanz der in Frage kommenden Berufsgattungen wird seitens der SBB erläutert und ist auch für den EDÖB unbestritten. Weiter ist festgehalten worden, dass die Tests heute nur auf konkreten Verdacht vorgenommen werden. Verdachtsfreie Stichproben werden laut SBB nicht durchgeführt. Die SBB hat ausserdem die Kategorien von Stellen beschrieben, die mit Tests konfrontiert werden. Es sind dies im Wesentlichen die Angestellten mit fahrdienstlichen Funktionen wie die Zugabfertigung (Bremskontrolle, Abfahrbefehl, usw.) und das Unfallmanagement. Die betroffenen Arbeitnehmer werden laut SBB in schriftlicher Form über die Tests informiert. Weitere Fragen in Zusammenhang mit der konkreten Vorgehensweise der Tests sind anlässlich der Sitzung nicht beantwortet, und es wurde diesbezüglich auf ein künftiges Schreiben des *Medical Service* der SBB und des BAV verwiesen. Auf die Frage nach der unterschiedlichen Behandlung von unter und über 40-jährigen Angestellten haben die SBB dahingehend geantwortet, dass gemäss internationalen Studien und nach mehrjähriger Erfahrung des *Medical Service* das Problem des Drogenkonsums vor allem bei den unter 40-jährigen besteht. Deshalb haben die SBB auf entsprechende Tests bei über 40-jährigen Angestellten verzichtet.

6. In einem gemeinsamen Schreiben vom 20. April 2007 sind die Leitung des *Medical Service* als auch das BAV auf die Personengruppen mit sicherheitsrelevanten Aufgaben zurückgekommen und haben im Wesentlichen präzisiert, dass die Zugbegleiter in den fahrdienstlichen Aufgaben den Triebfahrzeugführenden gleichgestellt sind und bezüglich den medizinischen Untersuchungsanforderungen nur kleine Unterschiede bestehen.

7. Am 3. Mai 2007 ist das *Medical Service* auf die noch offenen Fragen in Zusammenhang mit dem Ablauf des Testverfahrens zurückgekommen und hat u. a. die Entstehung eines Verdachts auf Drogenkonsum beschrieben. Für die Details des Verfahrens wurde auf den Anhang 5 zur Richtlinie des BAV verwiesen. Es hat weiter festgehalten, dass letztes Jahr die SBB in einem Pilotversuch mit einer beschränkten Anzahl Personen Alkoholtests durchgeführt haben. Bezüglich Frequenz der Urin-Analysen wurde im Wesentlichen das Gleiche beteuert wie im Schreiben der SBB vom 23. März 2007.

8. Auf die Einzelheiten des Sachverhaltes und der Dokumentation wird, soweit erforderlich, noch in den Erwägungen eingegangen.

II. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte zieht in Erwägung

1. Natürliche oder juristische Personen, welche wie die SBB u. a. mit öffentlichen Aufgaben des Bundes betraut sind, gelten datenschutzrechtlich als Bundesorgane (Art. 3 lit. h Datenschutzgesetz, DSG, SR 235.1). Die Bestimmungen über das Dienstverhältnis des Bundespersonals finden übrigens auch auf das Personal der SBB Anwendung (Art. 15 des Bundesgesetzes über die Schweizerischen Bundesbahnen, SBBG, SR 742.31 und Art. 2 Abs. 1 lit. d des Bundespersonalgesetzes, BPG, SR 172.220.1). Verträge nach Obligationenrecht werden durch die SBB nur in begründeten Einzelfällen abgeschlossen (Art. 15 Abs. 3 SBBG), weshalb vorliegend von Bundespersonal und folglich – datenschutzrechtlich – von einem Bundesorgan auszugehen ist. Die vorliegende Empfehlung basiert auf Art. 27 DSG.

2. Die SBB bearbeiten Gesundheitsdaten ihrer Angestellten sowohl in Form detaillierter Fragebögen (diese sind nicht Gegenstand der vorliegenden Empfehlung) als auch aufgrund von Alkohol- und Drogentests. Gesundheitsdaten definieren sich als Informationen, die direkt oder indirekt Rückschlüsse über den physischen und psychischen Gesundheitszustand einer Person zulassen, Daten also, die im weitesten Sinn einen medizinischen Befund darstellen. Gemäss Art. 3 lit. c Ziff. 2 DSG gelten Daten über die Gesundheit als besonders schützenswerte Personendaten. Deren Bearbeitung bedarf eines speziellen Schutzes, der sich auch in der geeigneten Gesetzesgrundlage ausdrückt.

3. Die von den Alkohol- und Drogentests betroffenen Arbeitnehmerkategorien – Triebfahrzeugführende, Zugbegleiter, Rangierer – nehmen sicherheitsrelevante Funktionen wahr, weshalb diesbezüglich keine Einwände anzubringen sind und hier nicht speziell darauf eingegangen wird.

4. Bundesorgane dürfen gemäss Art. 17 Abs. 2 DSG besonders schützenswerte Personendaten sowie Persönlichkeitsprofile nur bearbeiten, wenn ein formelles Gesetz es ausdrücklich vorsieht oder wenn ausnahmsweise a) es für eine in einem formellen Gesetz klar umschriebene Aufgabe unentbehrlich ist, b) der Bundesrat es bewilligt, weil die Rechte der betroffenen Personen nicht gefährdet sind oder c) die betroffene Person im Einzelfall eingewilligt oder ihre Daten allgemein zugänglich gemacht hat.

5. Die heutigen gesetzlichen Grundlagen, auf welche sich die SBB für die Vornahme der fraglichen Drogen- und Alkoholtests stützen, befinden sich einerseits in der Eisenbahnverordnung (EBV, SR 742.141.1), andererseits in der auf Letzterer basierenden departementalen Verordnung über die Zulassung zum

Führen von Triebfahrzeugen der Eisenbahnen (VTE, SR 742.141.142.1) und in den entsprechenden Ausführungsrichtlinien der SBB (Z 162.1) sowie in Art. 129 und 130 des Gesamtarbeitsvertrags (GAV), welcher die SBB gemäss Art. 38 des Bundespersonalgesetzes (BPG, SR 172.220.1) abgeschlossen haben. Gesetzliche Grundlagen im formellen Sinne, d. h. in Form eines von der Bundesversammlung erlassenen, referendumspflichtigen Gesetzes, welches sowohl den Zweck als auch den Umfang der Datenbearbeitung, die dabei verwendeten Mittel und die zur Bearbeitung befugten Behörden hinreichend bestimmt, bestehen keine bzw. es wurden dem EDÖB seitens der SBB keine angegeben. Das Erfordernis der Rechtssetzungsstufe auf formeller Ebene ist somit nicht erfüllt. Es ist festzuhalten, dass weder departementale Verordnungen noch die entsprechenden Ausführungsrichtlinien die vom DSG vorausgesetzte nötige Rechtssetzungsstufe für Datenbearbeitungen aufweisen.

6. Es geht folglich darum abzuklären, ob in einem formellen Gesetz eine klar umschriebene Aufgabe der SBB die Vornahme von Alkohol- und Drogentests voraussetzt. Damit gemäss der Ausnahmebestimmung von Art. 17 Abs. 2 lit. a DSG vom Erfordernis der formellgesetzlichen Grundlage abgewichen werden kann, müssen die Bedingungen der Unentbehrlichkeit für die Aufgabenerfüllung wie auch der klaren Aufgabenbeschreibung in einem formellen Gesetz erfüllt sein. Mit dem Erfordernis der klaren Umschreibung wird verlangt, dass die Aufgabe, für welche die Personendaten bearbeitet werden müssen, ausdrücklich in einem formellen Gesetz erwähnt und somit in ihrem Umfang klar erkennbar ist. Das Eisenbahngesetz (EBG, SR 742.101), worauf sich die von den zuständigen Stellen als gesetzliche Grundlagen angegebene EBV und die VTE stützen, enthält keinen ausdrücklichen Hinweis auf die Unentbehrlichkeit von Alkohol- und Drogentests für die Aufgabenerfüllung. Diese erste Voraussetzung von Art. 17 Abs. 2 lit. a DSG ist also nicht erfüllt. Dessen ungeachtet findet diese Ausnahmebestimmung auch aus folgenden Gründen keine Anwendung: Da es sich bei Art. 17 Abs. 2 lit. a DSG explizit um eine Ausnahmebestimmung vom Grundsatz handelt, wonach eine Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen immer eine formellgesetzliche Grundlage benötigt, kann sich diese Bestimmung konsequenterweise nur auf Aufgabenerfüllungen beziehen, die normalerweise keine Bearbeitung derartiger Daten benötigen. Damit wird auch klargestellt, dass es sich nur um Datenbearbeitungen in Einzelfällen handeln darf. Eine Datenbearbeitung verliert ihren Charakter der Ausnahme, sobald diese eine gewisse Regelmässigkeit oder Dauerhaftigkeit enthält. In solchen Fällen wäre eine Berufung auf die Ausnahmebestimmung weder mit Art. 17 Abs. 2 lit. a

DSG noch mit dem Legalitätsprinzip nach Art. 5 BV vereinbar (vgl. Y. Jöhri/M. Studer in Basler Kommentar zum Datenschutzgesetz, Helbing/Lichtenhahn Hrsg., Art. 17 N 47). Da es sich im vorliegenden Fall um eine regelmässige Bearbeitung von besonders schützenswerten Gesundheitsdaten seitens der SBB handelt, können sich Letztere auf die Ausnahme von Art. 17 Abs. 2 lit. a DSG nicht berufen. Die obigen Ausführungen gelten ebenfalls für die anderen Ausnahmebestimmungen nach Art. 17 Abs. 2 lit. b und c DSG, weshalb auf diese nicht näher eingegangen wird.

7. Im Rahmen der Revision der Erlasse über den öffentlichen Verkehr (insb. Bundesgesetz über die Bahnreform 2), beabsichtigt der Gesetzgeber, Vorschriften zur Dienstfähigkeit einzuführen (Art. 80 – 85 Bahnreform 2). Dabei werden der Begriff der Dienstunfähigkeit sowie die Feststellungsmethoden beschrieben. Zur Feststellung der Dienstunfähigkeit werden einerseits nicht invasive, verdachtsfreie Atem-Alkoholtests (Art. 82 Abs. 1), andererseits – bei Vorliegen eines Verdachts auf bzw. Anzeichen von Dienstunfähigkeit – invasive Tests (darunter Urintests und Blutproben) vorgesehen (vgl. Art. 82 Abs. 2). In den Ausführungsbestimmungen soll der Bundesrat festlegen, bei welcher Alkohol- und Drogenkonzentration Dienstunfähigkeit angenommen werden soll. Obwohl heute eine formell- und materiell-gesetzliche Grundlage fehlt, gehen wir mit Blick auf die Bahnreform 2 davon aus, dass die Tests unter Berücksichtigung der Gefahrenlage der SBB vertretbar sind. Wir sind jedoch der Auffassung, dass sich die SBB in ihrer heutigen Praxis an den einschlägigen Bestimmungen in der Revision des Bundesgesetzes über die Bahnreform 2 zu orientieren haben.

8. Die heutige Praxis der Alkohol- und Drogentests bei den SBB lässt sich wie folgt umschreiben: Als erstes wird bei jedem Neuangestellten mit sicherheitsdienstlichen Aufgaben eine medizinische Erstuntersuchung vorgenommen (Art. 23 VTE). Die – verdachtsfreie – Urin-Analyse zur Feststellung eines allfälligen Konsums von psychoaktiven Substanzen (Drogen oder Medikamente) sind Bestandteil der Erstuntersuchung (vgl. § 4.2.2 der Richtlinie des BAV vom 1. Januar 2006 zur medizinischen Tauglichkeitsuntersuchung). Gemäss Art. 53 VTE finden in regelmässigen Zeitabständen weitere medizinische Untersuchungen statt. Dabei können bei entsprechender Indikation ebenfalls Urin-Analysen durchgeführt werden (vgl. § 4.2.3 Richtlinie BAV). Alkoholtests werden weder in der VTE noch in der Richtlinie BAV speziell geregelt. Sie werden aber im Anhang 5 zur Richtlinie BAV beschrieben. Chronischer Alkoholmissbrauch bzw. Alkoholabhängigkeit – analog zum Drogenkonsum bzw. zur Drogenabhängigkeit sowie zu anderen Suchtformen – stellt ebenfalls

einen Ablehnungsgrund für Bewerber sowie einen Ausschlussgrund für die Weiterbeschäftigung dar (§ 4.3 Richtlinie BAV). Im Anhang 5 zur Richtlinie BAV werden die Untersuchungen auf Suchtkrankheiten – Alkohol- und Drogenmissbrauch – beschrieben, wobei der Cannabis-Konsum gegenüber den anderen Drogen hervorgehoben wird. Bezüglich eines unregelmässigen oder punktuellen Cannabis-Konsum halten das Medical Service und das BAV in ihrem Schreiben vom 20. April 2007 zudem fest, dass unangemeldete Urinanalysen jederzeit möglich sind. Anlässlich der Sitzung vom 18. April 2007 haben die SBB aber bestätigt, dass Drogentests nur bei Vorliegen eines konkreten Verdachts bzw. einer Indikation durchgeführt werden. Nach Angaben der SBB wurden bis dato keine Alkoholtests vorgenommen.

9. Bei der Gegenüberstellung der Drogentest-Praxis der SBB (vgl. insb. Schreiben vom Medical Service und vom BAV vom 20. April 2007) mit den heutigen und zukünftigen gesetzlichen Grundlagen (insb. VTE und ihre Anhänge sowie Art. 82 ff Bahnreform 2) fällt auf, dass unangekündigte Urinanalysen zur Aufdeckung eines unregelmässigen oder punktuellen Cannabis-Konsums jederzeit möglich sind, wogegen gemäss Art. 53 VTE (und gemäss Art. 82 Abs. 2 Bahnreform 2) invasive Urinanalysen zur Aufdeckung von Drogenkonsum nur bei entsprechender Indikation durchgeführt werden dürfen. Im Hinblick auf unregelmässigen oder punktuellen Cannabis-Konsum verlangt das Medical Service gerade gestützt auf die VTE, sei es bei Bewerbern oder bei periodischen Untersuchungen, eine Verzichtserklärung auf jeglichen Konsum und die Bereitschaft, sich unangemeldeten Urinuntersuchungen zu unterziehen. Wenn unter dem Begriff «unangemeldete Urinanalysen» verdachtsfreie Tests zu verstehen sind, verstösst die heutige Praxis gegen die VTE und gegen die einschlägigen Bestimmungen der Bahnreform 2. Ausserdem stellen Tests, welche den Cannabis-Konsum während der Freizeit betreffen, welcher keinen Einfluss auf die Verkehrssicherheit hat, einen unverhältnismässigen Eingriff in die Privatsphäre der Angestellten dar (Art. 4 Abs. 2 DSG). Der Arbeitgeber ist nicht berechtigt, durch Aufstellung von Verhaltensregeln für die Freizeit und durch entsprechende Kontroll-Tests samt Resultaten in übermässiger Art und Weise in die Privatsphäre der Angestellten einzugreifen. Wie bereits unterstrichen, wird die Bahnreform 2 nicht invasive Atem-Alkoholtests verdachtsfrei (Art. 82 Abs. 1), invasive Drogentests jedoch nur noch bei entsprechender Indikation (Art. 82 Abs. 2 und 3) vorsehen.

10. Alkoholtests sind gegenwärtig – verdachtsfrei – in der Erstuntersuchung vorgesehen (vgl. Anhang 5 Richtlinie BAV), in den periodischen Untersuchungen werden sie nicht detailliert angesprochen, wobei anzunehmen ist, dass sie bei Indikation einmal monatlich vorgenommen werden (Nachweis der einmonatigen Alkoholabstinenz zum Wiedererlangen der Fahrtauglichkeit nach Alkoholproblem, § B, Anhang 5 zur Richtlinie BAV). Nach der Bahnreform 2 werden Alkoholtests sowohl verdachtsfrei in der Erstuntersuchung als auch später nach Indikation vorgenommen.

11. Der Vergleich zwischen Drogen- und Alkoholtests in den heute geltenden gesetzlichen Grundlagen zeigt auf, dass in der Erstuntersuchung sämtliche sicherheitsgefährdende Substanzen verdachtsfrei untersucht werden können, währenddem in späteren Untersuchungen nur der Cannabis-Konsum verdachtsfrei untersucht werden kann. Alkohol- und andere Drogentests setzen hingegen immer eine entsprechende Indikation voraus. Wie schon gesehen, wird es in der Bahnreform 2 diese Unterschiede nicht mehr geben.

12. In Zusammenhang mit der Erstuntersuchung für das schon beschäftigte Zugspersonal haben das *Medical Service* und das BAV sowie die SBB in ihren Schreiben festgehalten, dass gestützt auf unbestrittene medizinische Erhebungen resp. Untersuchungsergebnisse und nach Absprache mit der Fachstelle Medizin des BAV Drogentests routinemässig grundsätzlich nur bei Personen unter 40 Jahren durchgeführt werden. Wenn aber die Sicherheit bei den SBB eine zentrale Rolle spielt, ist es nicht nachvollziehbar, warum die Tests nur bei unter 40-jährigen, nicht aber bei über 40-jährigen Angestellten vorgenommen werden. Die Drogen- und Alkoholtests würden u. E. an Glaubhaftigkeit gewinnen, wenn sämtliche Angestellte, welche eine sicherheitsrelevante Aufgabe innehaben, unabhängig ihres Alters den Tests unterzogen würden. Mit Sicherheitsproblemen werden nämlich auch über 40-jährige Mitarbeiter konfrontiert und mit Drogen-, vor allem aber mit Alkoholproblemen ebenfalls. Es ist nicht einzusehen, warum der Arbeitgeber seine Überwachungspflichten gegenüber älteren Mitarbeitern einzig gestützt auf statistische Erfahrungswerte betreffend Drogen- (aber nicht Alkohol-) konsum anders wahrnehmen sollte als bei jüngeren Angestellten. Mit anderen Worten ist ein Drogen- und Alkoholkonsum bei älteren Mitarbeitern nicht a priori auszuschliessen. Da die Sicherheit im vorliegenden Fall ein gegenüber dem Persönlichkeitsschutz des Angestellten überwiegendes Interesse darstellt, ist die durch die fragliche Ungleichbehandlung entstehende Sicherheitslücke nicht zu rechtfertigen.

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

1. Die SBB haben sich bei der Feststellung der Dienstunfähigkeit, namentlich bei der Durchführung von Alkohol- und Drogentests, an den einschlägigen Bestimmungen der Bahnreform 2 (Art. 82 ff) zu orientieren.
2. Daten zum Drogenkonsum der Angestellten während der Freizeit, welcher die Verkehrssicherheit der SBB nicht mehr tangiert, dürfen nicht bearbeitet werden.
3. Es sind Grenzwerte für Drogen- und Alkoholtests zu definieren, welche sich an den Sicherheitsanforderungen der Verkehrssicherheit orientieren. Werden diese Grenzwerte unterschritten, sollen keine Daten bearbeitet werden.
4. Die SBB teilen dem Eidg. Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) innerhalb von 30 Tagen ab Erhalt dieser Empfehlung mit, ob sie die Empfehlung annehmen oder ablehnen. Wird diese Empfehlung nicht befolgt oder abgelehnt, so kann der EDÖB die Angelegenheit dem Eidgenössischen Departement für Umwelt, Verkehr, Energie und Kommunikation (UVEK) zum Entscheid vorlegen (Art. 29 Abs. 4 DSG).
5. Bei Annahme der Empfehlung gilt der Fristablauf (30 Tage) gleichzeitig als Fristbeginn für die Umsetzung der genannten Massnahmen.

EIDGENÖSSISCHER DATENSCHUTZ- UND
ÖFFENTLICHKEITSBEAUFTRAGTER

Hanspeter Thür

4.5 Empfehlung betreffend die Bearbeitung von Handelsregisterdaten durch die X.-AG

Bern, 2. Mai 2007

Empfehlung

gemäss

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

betreffend

die Bearbeitung von Handelsregisterdaten durch die X.-AG

I. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte stellt fest:

Die X.-AG publiziert im Internet Handelsregisterdaten sowohl von Unternehmen, die aktuell am Wirtschaftsleben teilnehmen, wie auch von jenen, die aus diesem Kreislauf zwischenzeitlich ausgeschieden sind. Die Daten werden ohne Einwilligung der betroffenen Personen publiziert.

Diese Datenbearbeitung wurde uns gegenüber seitens betroffener Personen wiederholt kritisiert. Beanstandet wurde namentlich, dass die X.-AG Personendaten auch dann nicht löscht, wenn sich die betroffene Person ausdrücklich gegen deren Publikation im Internet ausgesprochen hatte. Bei der Prüfung der Rechtslage hat sich gezeigt, dass dies nicht das einzige Datenschutzproblem ist.

Der seit dem Jahr 2005 bestehende Kontakt zwischen unserer Behörde und der X.-AG hat bislang nicht zur Folge gehabt, dass die unsererseits angemeldeten Bedenken umfassend ausgeräumt worden sind.

Nach einer ausführlichen schriftlichen Erörterung der Rechtslage unsererseits (Schreiben vom 27. März 2007) hält die X.-AG im Wesentlichen an ihrem Standpunkt fest.

II. Erwägungen des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten:

Auf der Basis unserer Erörterung der Rechtslage vom 27. März 2007 wiederholen wir die Hinweise für eine datenschutzkonforme Bearbeitung von Handelsregisterdaten durch die X.-AG im Rahmen einer Empfehlung im Sinne von Artikel 29 DSG.

Die Voraussetzungen für eine Empfehlung im Sinne dieser Bestimmung sind gegeben. Die Bearbeitungsmethoden sind geeignet, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen (Art. 29 Abs. 1 lit. a DSG).

1. Handelsregisterdaten als Personendaten

Der Begriff der Handelsregisterdaten umfasst sämtliche Informationen in den Registern der kantonalen Handelsregisterämter. Der Begriff umfasst ausserdem die Daten von Publikationsorganen, die ausschliesslich Registerdaten enthalten, wie das Schweizerische Handelsamtsblatt (SHAB) und der zentrale Firmenindex (Zefix).

Personendaten sind alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen (Art. 3 lit. a DSG).

Handelsregisterdaten stellen damit Personendaten dar: Die im Handelsregister publizierten Informationen beziehen sich stets auf natürliche Personen (z.B. bei einer Einzelfirma) und je nach Rechtsform des eingetragenen Sachverhaltes gleichzeitig auch auf eine juristische Person.

2. Die Bearbeitung von Handelsregisterdaten durch Privatpersonen als Vorgang im Geltungsbereich des Datenschutzgesetzes

Das Datenschutzgesetz ist auf öffentliche Register des Privatrechtsverkehrs nicht anwendbar (Art. 2 Abs. 2 lit. d DSG). Allerdings hatte der Gesetzgeber bei der Schaffung dieser Bestimmung einzig die Datenbearbeitung durch die zuständigen staatlichen Organe im Auge (vgl. BBl 1988 II 413, 444); auf die Bearbeitung von Handelsregisterdaten durch Privatpersonen ist das Datenschutzgesetz uneingeschränkt anwendbar.

3. Die Bearbeitung von Handelsregisterdaten durch Privatpersonen als möglicherweise persönlichkeitsverletzender Vorgang

Gemäss Art. 12 Abs. 3 DSG besteht eine gesetzliche Vermutung, nach welcher die Bearbeitung von Personendaten keine Persönlichkeitsverletzung darstellt, wenn diese durch die betroffene Person allgemein zugänglich gemacht worden sind. Nachdem Handelsregisterdaten öffentlich sind, ist zu prüfen, ob auf der Grundlage dieser Bestimmung die Möglichkeit der Persönlichkeitsverletzung allgemein ausgeschlossen ist.

Vorausgesetzt wäre dafür, dass die Datenpublikation aus freien Stücken geschieht. Genauer ist ein Willensakt vonnöten, der sich exakt auf die Publikation der Daten bezieht und auf irgendeinen anderen Vorgang (vgl. die Beispiele in Basler Kommentar zum DSG, 2. Aufl. 2006, Rn. 16 zu Art. 12 DSG).

Bei Handelsregisterdaten handelt es sich grundsätzlich nicht um allgemein zugänglich gemachte Personendaten: Soweit nämlich eine Eintragungspflicht in das Handelsregister besteht, ist weder die Datenpublikation selbst verhandelbar, noch deren Inhalt (vgl. Art. 10 Abs. 1 HRegV und Art. 20 Abs. 1 HRegV). Lediglich bei Unternehmen, die sich trotz Fehlens einer Eintragungspflicht in das Handelsregister eintragen lassen (vgl. etwa Art. 119 Abs. 2 lit. a HRegV; SR 211.411), geht die Datenpublikation auf einen Willensakt zurück, der den Anforderungen von Art. 12 Abs. 3 DSG entspricht.

Nachdem Handelsregisterdaten nicht im Sinne des Datenschutzgesetzes «allgemein zugänglich gemacht» sind, gilt der in Art. 12 Abs. 1 DSG festgelegte Grundsatz: Wer Personendaten bearbeitet, darf die Persönlichkeit der betroffenen Personen nicht widerrechtlich verletzen.

4. Die Bearbeitung von Handelsregisterdaten durch Privatpersonen als möglicherweise widerrechtlicher Vorgang

Die Bearbeitung von Handelsregisterdaten durch Privatpersonen ist nicht gesamthaft durch einen besonderen Rechtfertigungsgrund im Sinne von Art. 13 Abs. 2 DSG gedeckt. Immerhin werden einige Bearbeitungsschritte in diesem Zusammenhang durch den Rechtfertigungsgrund des Art. 13 Abs. 2 lit. b DSG erfasst. Aus den Gesetzesmaterialien zu dieser Bestimmung wird deutlich, dass die Beschaffung von Handelsregisterdaten erlaubt sein soll, falls zwischen dem Datenbearbeiter und der betroffenen Person ein Wettbewerbsverhältnis besteht und ausserdem die Daten nur *intern* verwendet werden (vgl. BBl 1988 II 413, 461).

Der Gesetzgeber wollte also die systematische Weitergabe von Handelsregisterdaten durch Privatpersonen nicht in allgemeiner Form erlauben. Damit ist die persönlichkeitsverletzende Bearbeitung von Handelsregisterdaten durch Privatpersonen stets widerrechtlich, soweit sie denn nicht durch einen der allgemeinen Rechtfertigungsgründe im Sinne von Art. 13 Abs. 1 DSG gedeckt ist.

Im Hinblick auf die im konkreten Fall zu leistende Widerrechtlichkeitsprüfung (vgl. unten 8.) ist an dieser Stelle darauf hinzuweisen, dass gemäss der Botschaft zum Datenschutzgesetz zwar die im Handelsregister eingetragenen juristischen Personen «in gewissem Sinne [als] ‚öffentliche' Personen» anzusehen sind, nicht aber die natürlichen Personen, die in ihrer Eigenschaft als Organe juristischer Personen eingetragen sind (vgl. BBl 1988 II 414, 461). Diese gesetzgeberische Wertung gilt es auch vorliegend zu berücksichtigen.

5. Zur Bedeutung des Handelsregisterrechts für die private Bearbeitung von Handelsregisterdaten

Werden Daten durch verschiedene Akteure bearbeitet, erlangt das datenschutzrechtliche Gebot der Zweckbindung bei der Datenbearbeitung besondere Bedeutung (Art. 4 Abs. 3 DSG). Dies gilt ohne Weiteres auch im vorliegenden Fall, obwohl sich lediglich die Bearbeitung von Handelsregisterdaten durch *Privatpersonen* nach dem Datenschutzgesetz bemisst und nicht bereits die Datenerhebung durch den Staat. Vielmehr kommt man nicht umhin, den Zweck der staatlichen Datenerhebung (Handelsregisterzweck) zu berücksichtigen, um die Zulässigkeit der Weitergabe von Handelsregisterdaten durch Privatpersonen zu beurteilen (vgl. unten 6.).

6. Registerrechtliche Vorgaben für die private Weitergabe von Handelsregisterdaten durch den Zweck des Handelsregisters

Der Zweck des Handelsregisters ist nicht mittels ausdrücklicher Gesetzesbestimmung definiert. Gemäss einschlägiger Rechtsquellen (Rechtsprechung und Lehre; Art. 1 Abs. 2 und 3 ZGB) hat das Handelsregister mehr als bloss einen einzigen Zweck. Diese Zweckpluralität ist vorliegend von Bedeutung, als insbesondere auch die *Publizität* des Handelsregisters nicht dessen alleiniger Zweck ist: Die Öffentlichkeit des Registers ist vielmehr im Gesamtzusammenhang der damit angestrebten Rechtswirkungen zu sehen, die sich unter dem Stichwort des öffentlichen Glaubens zusammenfassen lassen.

Die private Publikation von Handelsregisterdaten steht mit dem öffentlichen Glauben des Handelsregisters in keinem Zusammenhang. Streng genommen liegt sie damit gesamthaft ausserhalb der Zwecksbestimmung, die für die Datenerhebung Gültigkeit hatte. Dennoch ist die private Verbreitung der Handelsregisterdaten nicht *per se* ein

Verstoss gegen das Zweckbindungsgebot: Auch wenn kein staatlicher Auftrag zur Maximierung der Publizität besteht, kann die private Weiterverbreitung der Handelsregisterdaten wirtschaftlich gewinnbringend sein.

Dennoch sind der Weitergabe von Handelsregisterdaten durch Privatpersonen Schranken gesetzt: Soweit Daten publiziert werden, die im Handelsregister nicht mehr auffindbar sind, stellt dies einen persönlichkeitsverletzenden Vorgang dar. Eine solche Ausdehnung des staatlichen Informationsangebots ist durch den Zweck nicht mehr gedeckt, der bei der Datenerhebung Gültigkeit hatte (Verstoss gegen Art. 4 Abs. 3 DSG).

Dieses gesetzeswidrige Zweckänderung bei der Datenbearbeitung präsentiert sich überdies gleichzeitig als Verstoss gegen das datenschutzrechtliche Verhältnismässigkeitsprinzip (Art. 4 Abs. 2 DSG). Die Frage der Zweckbindung und des zulässigen Umfangs der Datenbearbeitung sind im vorliegenden Fall untrennbar miteinander verbunden.

Ein Datenschutzverstoss ist damit erst dem Grundsatz nach umschrieben; allein mit Blick auf den Zweck des Handelsregisters lässt sich die Zulässigkeit der Datenbearbeitung nicht ermessen. Es ergeben sich aber für die Weitergabe von Handelsregisterdaten im Rahmen von Online-Publikationen aus dem Handelsregisterrecht konkretere Vorgaben (vgl. im Anschluss 7.)

7. Registerrechtliche Vorgaben für die private Datenweitergabe im Rahmen von Online-Publikationen

Die datenschutzrechtliche Problemlage durch die Übersteigerung des staatlichen Informationsangebots durch Privatpersonen steht in einem engen Zusammenhang mit den Möglichkeiten der *elektronischen* Datenbearbeitung: Nachdem es technisch möglich ist, die im Rahmen der Online-Publikation des SHAB (<www.shab.ch>) verfügbaren Daten laufend und gesamthaft zu speichern, können auf privater Basis ohne Weiteres Informationen zusammen getragen werden, die dem Umfang nach über die aktuellen Handelsregistereinträge hinaus gehen.

Da mit Blick auf den Zweck des Handelsregisters nur die aktuell im Handelsregister eingetragenen Informationen publik sein müssen, hat der Gesetzgeber die Regel aufgestellt, dass die Handelregisterdaten auf <www.shab.ch> nur während eines begrenzten Zeitraums zur Verfügung stehen (Vgl. Art. 11 Abs. 2 der VO über das Schweizerische Handelsamtsblatt; SR 221.415).

Diese staatliche Selbstbeschränkung vermittelt namentlich den betroffenen natürlichen Personen Schutz: Ausserhalb von <www.shab.ch> bleibt eine schweizweite, selektive Suche – bezogen auf natürliche Personen – im staatlichen Informationsangebot ohne Resultat.

Obwohl der Staat bei der Bearbeitung von Handelsregisterdaten dem Datenschutzgesetz nicht unterstellt ist, schützt das beschriebene Vorgehen die Datenschutzinteressen der betroffenen Personen: Der Staat stellt sicher, dass die wirtschaftliche Entflechtung natürlicher Personen von einem Unternehmen nach einer bestimmten Zeit auch auf der Ebene der Handelsregisterdaten durchschlägt.

Was die Bearbeitung von Handelsregisterdaten im Rahmen von Online-Publikationen von Privatpersonen betrifft, muss der beschriebene Schutz ebenfalls gewährleistet werden. Die Bestimmung in Art. 11 Abs. 2 der SHAB-Verordnung stellt insofern auch für Privatpersonen eine zwingende Vorgabe für die zulässige Maximaldauer der Datenspeicherung dar. Wird diese Vorgabe nicht erfüllt, ist vom Vorliegen eines Datenschutzverstosses auszugehen (Art. 4 Abs. 2 und 3 DSG; vgl. dazu oben 6.).

8. Prüfung des Verstosses gegen datenschutzrechtliche Bearbeitungsgrundsätze bei der Datenweitergabe durch die X.-AG

Die Datenbearbeitung durch die X.-AG ist in einigen Belangen nicht datenschutzkonform: Ein Verstoss gegen datenschutzrechtliche Bearbeitungsgrundsätze besteht dabei namentlich im Zusammenhang mit der Weitergabe der Personendaten von natürlichen Personen, insoweit diese natürlichen Personen in keiner Verbindung mehr zu einer im Handelsregister eingetragenen juristischen Person stehen bzw. wenn die juristische Person gar nicht mehr existiert (vgl. unten a).

Hingegen ist für die Weitergabe von Daten natürlicher Personen im Zusammenhang mit aktiven Firmen vom Vorliegen eines Rechtfertigungsgrundes auszugehen (vgl. unten a). Erlaubt ist grundsätzlich auch die Weitergabe der Daten juristischer Personen. Dies sowohl bei Unternehmen, die aus dem Wirtschaftskreislauf ausgeschieden sind, wie auch bei jenen, die daran aktuell teilnehmen (vgl. unten b).

a) Die Bearbeitung der Personendaten natürlicher Personen

Die Weitergabe der Personendaten natürlicher Personen, die in keiner Verbindung mehr zu einer im Handelsregister eingetragenen juristischen Person stehen, ist eine datenschutzwidrige Übersteigerung des staatlichen Informationsangebotes. Sobald die Verbindung auch unter <www.shab.ch> nicht mehr abrufbar ist, stellt die Internetpublikation dieser Daten durch Privatpersonen eine persönlichkeitsverletzende Datenbearbeitung dar (vgl. oben *5., 6. und 7.*).

Ein Rechtfertigungsgrund, welcher die persönlichkeitsverletzende Datenweitergabe erlauben würde, ist nicht ersichtlich. Denn einerseits ist die Datenweitergabe nicht durch einen besonderen Rechtfertigungsgrundes gedeckt (vgl. oben *4.*), andererseits liegt auch kein allgemeiner Rechtfertigungsgrund vor: Innerhalb der Rechtfertigungsgründe in Art. 13 Abs. 1 DSG vermöchte einzig eine Einwilligung der betroffenen Personen die Datenweitergabe zu rechtfertigen, die aber durch die X.-AG nicht eingeholt wird (Massengeschäft).

Ein überwiegendes Interesse an der Datenpublikation besteht hinsichtlich vergangener Wirtschaftsbindungen nicht: Wäre es für ein störungsfreies Wirtschaftsgeschehen erforderlich, dass sämtliche vergangenen Verbindungen zwischen natürlichen und juristischen Personen umfassend bekannt sind, hätte sich der Staat im Rahmen SHAB-Verordnung keine Beschränkung der Speicherdauer auferlegt.

Vor dem Hintergrund dieser gesetzgeberischen Wertung ist festzustellen, dass das Publikumsinteresse an der wirtschaftlichen Vergangenheit einer natürlichen Person weniger schwer wiegt, als das Interesse dieser Person, mit einem Unternehmen nicht in Verbindung gebracht zu werden. Diese können in verschiedener Hinsicht ein Interesse daran haben, dass die Loslösung von einer juristischen Person nicht unterschlagen wird. Namentlich im Zusammenhang mit den (gesellschaftlich stigmatisierenden) Firmenkonkursen ist darauf hinzuweisen, dass ein «Recht auf Vergessen» auch bezogen auf die wirtschaftliche Biographie einer Person besteht.

Anders verhält es sich im Zusammenhang mit Unternehmen, die aktiv am Wirtschaftsleben. In diesem Zusammenhang entsteht durch die Datenbearbeitung der X.-AG eine datenschutzrelevante Übersteigerung des staatlichen Informationsangebots lediglich insofern, als dass auf der Internetplattform der X.-AG eine schweizweite, personenbezogene Suche zur Verfügung steht, welche auch den Zeitraum betrifft, der über <www.shab.ch> nicht mehr abgefragt werden kann. Insofern ist zwar auch in diesem Zusammenhang eine persönlichkeitsverletzende Datenbearbeitung festzustellen (vgl. oben *5., 6. und 7.*), jedoch ist in diesem Zusammenhang ein überwiegendes Interesse des Publikums vorstellbar (überwiegendes privates Interesse im Sinne von Art. 13 Abs. 1 DSG).

Allerdings ist das Privatheitsinteresse der natürlichen Personen deswegen nicht belanglos. Immerhin ergibt sich aus den Materialien des Datenschutzgesetzes, dass die Bearbeitung der Daten natürlicher Personen im Zusammenhang mit Handelsregistereinträgen nur mit Zurückhaltung erfolgen soll (vgl. oben 4.). Dies hat namentlich zur Folge, dass die betroffene Person die Möglichkeit haben muss, durch die Intervention bei der X.-AG ihre Daten löschen zu lassen (vgl. dazu im Anschluss 9.)

b) Die Bearbeitung der Personendaten juristischer Personen

Auch die Publikation von Personendaten juristischer Personen ist eine persönlichkeitsverletzende Datenbearbeitung, soweit das staatliche Informationsangebot übersteigert wird (vgl. oben *5., 6. und 7.*).

Dies ist im Rahmen der Datenbearbeitung der X.-AG insofern der Fall, als auch Angaben über erloschene juristische Personen publiziert werden. Wir gehen in diesem Zusammenhang allerdings davon aus, dass im Zusammenhang mit diesen Daten kein schützenswertes Privatheitsinteresse besteht.

Insoweit auf der Internetplattform der X.-AG Informationen über *aktive* Firmen publiziert werden, die auf obsolet gewordenen Handelsregistereinträgen beruhen (z.B. Angabe über die zwischenzeitlich geänderte Kapitaleinlage), handelt es sich zwar ebenfalls um eine persönlichkeitsverletzende Datenbearbeitung (vgl. oben *5., 6. und 7.*), wir gehen aber davon aus, dass die diesbezügliche Datenweitergabe durch ein überwiegendes privates Interesse gedeckt ist: Das Publikum hat durchaus ein Interesse an der Kenntnis, wie sich ein Unternehmen bezüglich bestimmter handelsregisterrelevanter Sachverhalte entwickelt hat. Eine Ausnahme ist nur zu machen, wenn sich die zuständigen Organe einer juristischen Person gegen die Datenweitergabe auf der Internetplattform der X.-AG ausdrücklich aussprechen (vgl. im Anschluss 9.)

9. Datenschutzverletzung durch die Bearbeitung von Handelsregisterdaten gegen den Willen der betroffenen Person

Gemäss Art. 12 Abs. 2 lit. b DSG stellt die Bearbeitung von Personendaten gegen den ausdrücklichen Willen der betroffenen Person stets eine Persönlichkeitsverletzung dar, die nur erlaubt wäre, wenn die Datenbearbeitung durch einen Rechtfertigungsgrund gedeckt ist.

Dabei kann für die Widerrechtlichkeitsprüfung nicht integral auf das bereits Gesagte verwiesen werden, da sich im Kontext von Art. 12 Abs. 2 lit. b DSG die Persönlichkeitsverletzung nicht primär aus dem Handelsregisterrecht herleitet, sondern aus dem Datenschutzgesetz selbst. Immerhin gilt aber für die Widerrechtlichkeitsprüfung auch in *diesem* Zusammenhang die Feststellung, dass ein besonderer Rechtfertigungsgrund im Sinne von Art. 13 Abs. 2 DSG fehlt (vgl. oben *4.*). Zu prüfen ist damit einzig, ob ein privates Interesse im Sinne von Art. 13 Abs. 1 DSG vorliegt, welches das ausdrückliche Verbot der Datenbearbeitung überwiegen würde.

Dies ist nicht der Fall. Die private Duplizierung der Handelsregisterdaten auf der Internetplattform der X.-AG dient primär den wirtschaftlichen Interessen dieses Unternehmens, und erst in zweiter Linie den Informationsbedürfnissen des Publikums. Gegen

die solcherart motivierte Datenpublikation ist das datenschutzrechtlich fundamentale Interesse der Betroffenen an informationeller Selbstbestimmung abzuwägen: Der Sinn von Art. 12 Abs. 2 lit. b DSG liegt exakt darin, dass die von einer Datenbearbeitung betroffenen Personen dieses Recht aktiv durchsetzen können.

Das Recht der betroffenen Person auf informationelle Selbstbestimmung wiegt deutlich schwerer. Denn zum einen sind wirtschaftliche Interessen kaum je höher zu gewichten als das Interesse an der Verfügungsgewalt über die eigenen Daten. Zum anderen ist die private Duplizierung von Handelsregisterdaten zwar wie gezeigt sinnvoll (vgl. oben *6.*), aber deswegen nicht unabdingbar.

Im Ergebnis ist festzuhalten, dass die X.-AG auf ausdrückliches Begehren der betroffenen (natürlichen oder juristischen) Person hin, keine Daten mehr über diese bearbeiten darf; namentlich dürfen die Daten nicht mehr auf der Internetplattform der X.-AG publiziert werden.

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

1. Die Löschung von Personendaten ohne ausdrückliches Begehren der betroffenen Person

- Wenn zwischen einer natürlichen und einer juristischen Person keine Verbindung mehr besteht, dürfen die Personendaten der betroffenen natürlichen Personen auf der Internetplattform der X.-AG maximal so lange publiziert werden, wie die Daten auch unter <www.shab.ch> abrufbar sind (drei Jahre, bzw. ein Jahr im Fall von Firmenkonkursen).

- Die beschriebene Massname ist eine Daueraufgabe. Sie muss aber überdies für das aktuelle Informationsangebot der X.-AG rückwirkend umgesetzt werden. Für die entsprechenden Arbeiten erachten wir einen Zeitraum von sechs Monaten als angemessen.

- Die X.-AG muss sämtliche Personendaten natürlicher Personen löschen, die sie bislang auf ihrem Internetauftritt im Zusammenhang mit juristischen Personen publiziert hat, die nicht mehr existieren. Auch für die Umsetzung dieser Massnahme erachten wir einen Zeitraum von sechs Monaten als angemessen.

2. Die Löschung von Personendaten bei ausdrücklichem Begehren der betroffenen Person

- Natürliche und juristische Personen haben einen Anspruch, die Bearbeitung ihrer Personendaten zu untersagen (Art. 12 Abs. 2 lit. b DSG). Die X.-AG muss künftig nach Erhalt einer entsprechenden Erklärung den Willen der betroffenen Personen umsetzen. Namentlich sind die Daten innert angemessener Frist von der Internet-Plattform der X.-AG zu entfernen.
- Als angemessene Frist erachten wir die Löschung der Daten innert dreier Arbeitstage ab Erhalt der Erklärung der betroffenen Person.

Die X.-AG teilt dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) innerhalb von 30 Tagen ab Erhalt dieser Empfehlung mit, ob sie die Empfehlung annimmt oder ablehnt. Wird diese Empfehlung nicht befolgt oder abgelehnt, so kann der EDÖB die Angelegenheit dem Bundesverwaltungsgericht zum Entscheid vorlegen (Art. 29 Abs. 4 DSG).

Bei Annahme der Empfehlung gilt der Fristablauf (30 Tage) gleichzeitig als Fristbeginn für die Umsetzung der genannten Massnahmen.

Die vorliegende Empfehlung wird in Anwendung von Art. 30 Abs. 2 DSG in anonymisierter Form publiziert.

EIDGENÖSSISCHER DATENSCHUTZ- UND
ÖFFENTLICHKEITSBEAUFTRAGTER

Hanspeter Thür

4.6 Empfehlung an das Bundesamt für Gesundheit: «Vertrag Präpandemieimpfstoff I»

Bern, 12. März 2007

Empfehlung

gemäss

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

zum Schlichtungsantrag von

X
(Antragsteller)

gegen

Bundesamt für Gesundheit (BAG), Bern

I. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte stellt fest:

1. Mit einer Pressemitteilung informierte das BAG am 18. Oktober 2006 darüber, dass der Bundesrat den Kauf von acht Millionen Dosen eines Präpandemie-Impfstoffes beschlossen hat. Demnach unterzeichnete das BAG einen entsprechenden Vertrag mit dem Pharmaunternehmen GlaxoSmithKline (GSK). Gleichzeitig wurde mit dem Unternehmen eine Reservationsübereinkunft für Pandemie-Impfstoffe vereinbart. Gemäss Pressemitteilung des BAG betragen die Kosten für die Präpandemie- und Pandemie-Impfstoffe 180 Millionen Franken.

2. Der Antragsteller reichte am 27. Oktober 2006 beim Eidg. Departement des Innern (EDI) ein schriftliches Zugangsgesuch ein. Darin ersuchte der Antragsteller u.a. um Zugang zum Vertrag und zur Reservationsübereinkunft inklusiv allfälliger Anhänge. Das Gesuch wurde zuständigkeitshalber an das BAG überwiesen.

3. Das BAG teilte dem Antragsteller am 29. November 2006 mit, dass «der Vertrag und die darin ebenfalls enthaltene Reservationsübereinkunft dem Geschäfts- und Fabrikationsgeheimnis (untersteht), da er vertrauliche Geschäfts- und Fabrikationsdaten unserer Vertragspartnerin enthält». In der Folge lehnte das BAG den Zugang gestützt auf Art. 7 Abs. 1 Bst. g des Bundesgesetzes über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsgesetz, BGÖ; SR 152.3) ab.

4. Der Antragsteller reichte mit Schreiben vom 6. Dezember 2006 beim Eidg. Datenschutz- und Öffentlichkeitsbeauftragten (der Beauftragte) einen Schlichtungsantrag nach Art. 13 BGÖ ein (eingegangen am 7. Dezember 2006). Der Antragsteller führte an, dass sich «eine vollständige Verweigerung der Herausgabe nicht mit dem Verhältnismässigkeitsprinzip in Einklang bringen [lasse], weil mit Sicherheit nicht der gesamte Inhalt des GSK-Vertrags und allfälliger Anhänge (bzw. der GSK-Verträge) Geschäfts- und Fabrikationsgeheimnisse betrifft.»

5. Am 8. Dezember 2006 forderte der Beauftragte das BAG auf, ihm die für die Bearbeitung des Schlichtungsantrags notwendigen Dokumente zu übermitteln. Die gewünschten Dokumente trafen am 13. Dezember 2006 beim Beauftragten ein.

6. Am 9. Februar 2007 lud der Beauftragte GSK als in der Sache Betroffene zu einer Stellungnahme ein (s. unten Ziffer II B. 8). In ihrer Antwort vom 20. Februar 2007 vertrat GSK die Ansicht, dass der Vertrag als Gesamtdokument zu betrachten sei und weitestgehend Geschäfts- und Fabrikationsgeheimnisse enthalte. Die wenigen, unbedenklichen Bestimmungen, die zugänglich ge-

macht werden könnten, hätten für sich keine eigene Aussagekraft. Aus diesen Gründen vertrat GSK die Ansicht, dass von einem teilweisen Zugänglichmachen des Vertrages abgesehen und der Zugang vollumfänglich verweigert werden sollte.

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 BAG 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. Geschäfts- und Fabrikationsgeheimnis Art. 7 Art. 1 Bst. g BGÖ

1. Das BAG lehnte den Zugang des Antragstellers mit der Begründung ab, dass der Vertrag vertrauliche Geschäfts- und Fabrikationsdaten von GSK enthalte. Der Antragsteller wendete sich mit seinem Schlichtungsantrag dagegen, dass das BAG aufgrund der Ausnahmebestimmung über das Geschäfts- und Fabrikationsgeheimnis den Zugang *vollumfänglich* verweigerte. Der Beauftragte prüft daher zuerst die Frage, ob der Vertrag tatsächlich vollständig respektive teilweise Geschäfts- oder Fabrikationsgeheimnisse enthält.

2. Art. 7 BGÖ enthält eine abschliessende Liste mit Ausnahmefällen, bei deren Vorliegen der Zugang zum amtlichen Dokument eingeschränkt, aufgeschoben oder verweigert werden kann. Dabei handelt es sich um eine Aufzählung privater oder öffentlicher Interessen, die gemäss dem Willen des Gesetzgebers dem Grundsatz der Transparenz vorgehen und eine Geheimhaltung bestimmter Dokumente rechtfertigen. Gemäss Art. 7 Abs. 1 Bst. g BGÖ muss kein oder nur ein beschränkter Zugang gewährt werden, wenn durch eine vollumfängliche Gewährung Berufs-, Geschäfts- oder Fabrikationsgeheimnisse offenbart werden können.

3. Die Einführung des Öffentlichkeitsprinzips hat nicht zur Folge, dass Bundesbehörden nun Berufs-, Geschäfts- und Fabrikationsgeheimnisse von Privaten, von denen sie Kenntnis haben, an interessierte Dritte ausserhalb der Verwaltung bekannt geben müssen. Vielmehr ist die Verwaltung gemäss Öffentlichkeitsgesetz gehalten, diese Geheimnisse zu schützen. Eine Definition der Begriffe des Geschäfts- oder Fabrikationsgeheimnisses finden sich weder in der Botschaft noch im Öffentlichkeitsgesetz oder einem anderen Bundesgesetz. Die Botschaft führt dazu lediglich aus, dass das Zugänglichmachen bestimmter Informationen nicht zu einer Wettbewerbsverzerrung zwischen Marktteilnehmern führen darf[1].

4. Das Bundesamt für Justiz, das für die Umsetzung des Öffentlichkeitsgesetzes verantwortlich zeichnete, umschrieb Geschäfts- oder Fabrikationsgeheimnisse als «Informationen, die sich auf eine Tätigkeit beziehen, die unter *Wettbewerb oder wettbewerbsähnlichen Bedingungen* stattfindet und denen *Geheimnischarakter* zukommt (d.h. es geht um Tatsachen, die weder offenkundig noch allgemein zugänglich sind). Es muss ein *legitimes Geheimhaltungsinteresse* bestehen und der Geheimhaltungswille der privaten Drittperson muss zumindest aus den Umständen ersichtlich sein.»[2]

[1] BBl 2003 2012
[2] Bundesamt für Justiz: «Umsetzung des Öffentlichkeitsprinzips in der Bundesverwaltung: Häufig gestellte Fragen» vom 29.06.2006

Entscheidend für die Beurteilung, ob eine Ausnahme nach Art. 7 BGÖ vorliegt, ist darüber hinaus die Tatsache, dass das öffentliche oder private Interesse (hier an der Wahrung des Geschäfts- und Fabrikationsgeheimnisses) durch einen Zugang mit «*einer gewissen Wahrscheinlichkeit*»[3] beeinträchtigt würde. In diesem Fall überwiegt das Interesse an der Geheimhaltung und das Transparenzprinzip muss zurücktreten.

5. Der Beauftragte darf in seiner Empfehlung keine vertraulichen oder geheimen Informationen und Details aus dem fraglichen Dokument bekannt gegeben. In Bezug auf den hier zu beurteilenden Vertrag kann lediglich festgehalten werden, dass es sich dabei um einen 62 Seiten umfassenden Vertrag mit 8 Anhängen handelt. Der Vertrag enthält u.a. detaillierte Ausführungen zur Zusammensetzung des Impfstoffes, zu Preisen, Lieferbedingungen und Garantieleistungen.

   GSK steht in Bezug auf die Herstellung von Präpandemie- und Pandemie-Impfstoffen *im Wettbewerb mit anderen Marktteilnehmern*. Unbestritten ist ebenso die Tatsache, dass sämtliche Informationen zur Zusammensetzung, Wirkungsweise usw. des Impfstoffes unter das Fabrikationsgeheimnis fallen. Angesichts der Risiken, die mit einer Pandemie für die Menschen verbunden sind, ist es nach Auffassung des Beauftragten angebracht, bestimmte Informationen als Geschäftsgeheimnisse einzustufen, beispielsweise die Bezeichnung der Produktionsorte einzelner Bestandteile des Impfstoffes respektive Angaben über deren Auslieferung ab den verschiedenen GSK-Unternehmen.

   GSK hat an der Wahrung ihrer Fabrikations- und Geschäftsgeheimnisse ein *legitimes Interesse*. Nach Einsichtnahme in das fragliche Dokument ist der Beauftragte zur Überzeugung gelangt, dass das Zugänglichmachen einzelner Textpassagen oder des ganzen Vertragsdokuments nicht nur mit einer gewissen Wahrscheinlichkeit, sondern mit Bestimmtheit zu einer Offenbarung bestimmter Fabrikations- oder Geschäftsgeheimnisse führen würde und für GSK mit Nachteilen im Wettbewerb im In- und Ausland verbunden wäre.

   Nach Ansicht des Beauftragten ist es daher grundsätzlich richtig, dass der Zugang zu weiten Teilen des Vertragstextes, d.h. zu den Ziffern 2-19 sowie sämtlichen Anhängen, aufgrund des Vorliegens des Ausnahmefalls von Art. 7 Abs. 1 Bst. g BGÖ nicht gewährt wird.

[3] BBl 2003 2006f.

6. Der Antragsteller beanstandet nicht die Tatsache, dass es sich vorliegend um einen Ausnahmefall von Art. 7 Abs. 1 Bst. g BGÖ handelt. Vielmehr macht er geltend, dass das BAG nach dem *Verhältnismässigkeitsprinzip* einen teilweisen Zugang zum Dokument hätte gewähren sollen.

   Das BAG hat entschieden, den Zugang *vollumfänglich* zu verweigern, da der Vertrag «vertrauliche Geschäfts- und Fabrikationsdaten unserer Vertragspartnerin enthält». Im Folgenden gilt es zu prüfen, ob diese Haltung vom Öffentlichkeitsgesetz abgedeckt ist.

7. Das Öffentlichkeitsgesetz besagt nicht, dass der Zugang zu einem Dokument vollumfänglich verweigert werden muss, nur weil das Dokument ein (oder mehrere) Fabrikations- oder Geschäftsgeheimnis(se) enthält. Vielmehr bietet Art. 7 BGÖ neben der vollumfänglichen Verweigerung auch die *Möglichkeit der Beschränkung des Zugangs* im Umfang des tatsächlich gegebenen Geschäfts- oder Fabrikationsgeheimnisses (Art. 7 Abs. 1 BGÖ). In Anwendung des Verhältnismässigkeitsgebots gilt es somit stets zu prüfen, ob allenfalls ein teilweiser Zugang gewährt werden kann, indem die sensiblen Teilbereiche des Dokuments abgedeckt, entfernt oder verschlüsselt werden können.

   Nach Ansicht des Beauftragten enthalten weite Teile des Vertrages Geschäfts- und Fabrikationsgeheimnisse (s. o. Ziffer II B. 5). Seiner Einschätzung nach gilt dies indes nicht für die Seiten 1-9, welche das Inhaltsverzeichnis, die Präambel und die Ziffer 1 des Vertrages (Definitionen und Interpretationen) beinhalten. Diese Vertragsteile enthalten nicht vollumfänglich respektive nicht überwiegend Geschäfts- und Fabrikationsgeheimnisse. Sie können somit grundsätzlich zugänglich gemacht werden. Der Beauftragte teilte seine Einschätzung GSK mit und räumte ihr als in der Sache Betroffene die Gelegenheit zur Stellungnahme ein.

8. GSK hielt in ihrer Stellungnahme fest, dass sie es den Vertrag als Gesamtdokument versteht, das weitestgehend Geschäfts- und Fabrikationsgeheimnisse beinhaltet. Das «Zugänglichmachen der wenigen, aus unserer Sicht unbedenklichen Bestimmungen hat keine eigene Aussagekraft.» Aus diesem Grund vertrat GSK die Ansicht, dass der Zugang zum gesamten Dokument verweigert werden sollte. Darüber hinaus hielt GSK fest, dass auch in der Präambel und den Definitionen «kommerziell wichtige Geschäfts- und Fabrikationsgeheimnisse» enthalten seien, und bezeichnete jene Textstellen, die aus diesem Grund nicht zugänglich gemacht werden sollten.

9. Wie bereits in Ziffer II B. 5 erwähnt, darf der Beauftragte in einer Empfehlung die als geheim bezeichneten Textpassagen nicht aufführen. Der Beauftragte erachtet das Geheimhaltungsinteresse von GSK an den von ihr bezeichneten Stellen betreffend die Seiten 1-9 des Vertrages als legitim. Diese Vertragsbestandteile (ebenso wie die Ziffern 2-19 sowie die Anhänge) fallen damit unter die Ausnahmebestimmung von Art. 7 Abs. 1 Bst. g BGÖ und müssen nicht zugänglich gemacht werden.[4] Im Weiteren gilt es nun zu prüfen, ob in Bezug auf die Seiten 1-9 ein teilweiser Zugang gewährt werden kann.

   Werden die nicht zugänglichen Passagen abgedeckt, so bleibt etwa die Hälfte des Textes der Seiten 1-9 offen. Nach Ansicht des Beauftragten kann nicht die Rede davon sein, dass die zugänglichen Informationen in Bezug auf diesen Vertragsbestandteil keinen Sinn mehr ergeben und daher der Zugang gänzlich verweigert werden kann. Das Öffentlichkeitsgesetz verlangt im Übrigen nicht, dass die offenen (d.h. nicht abgedeckten) Passagen in Beziehung zu den abgedeckten Teilen eines Dokuments gesetzt werden müssen, um deren Zugänglichkeit zu beurteilen. Nach Ansicht des Beauftragten ist daher ein beschränkter Zugang zu den Seiten 1-9 zu gewähren.

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

1. Das Bundesamt für Gesundheit gewährt dem Antragsteller einen teilweisen Zugang zum Vertrag mit GlaxoSmithKline zu Table of Contents (Seite 2 und 3), Preamble (Seite 4) und die Ziffer 1 «Definitions and Interpretation» (Seite 4-9). Der Zugang wird entsprechend den im Anhang zu dieser Empfehlung aufgeführten Textpassagen zur Preamble und den Definitions beschränkt.

   Zu den Ziffern 2-19 und zu den Anhängen A-H ist kein Zugang zu gewähren.

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

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

[4] Diese vertraulichen Passagen aus den Seiten 1-9 werden im Anhang zu dieser Empfehlung aufgeführt, sind aus dem erwähnten Grund jedoch nur für das BAG und GSK zugänglich.

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

4. Als von der Empfehlung Betroffene kann GlaxoSmithKline innerhalb von 10 Tagen nach Erhalt dieser Empfehlung beim Bundesamt für Gesundheit den Erlass einer Verfügung nach Artikel 5 des Verwaltungsverfahrensgesetzes verlangen, wenn sie mit der Empfehlung nicht einverstanden ist (Art. 15 Abs. 1 BGÖ).

5. Gegen die Verfügung kann beim Bundesverwaltungsgericht Beschwerde geführt werden (Art. 16 BGÖ).

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

7. Die Empfehlung wird eröffnet:

   - X
   - Bundesamt für Gesundheit (inklusiv Anhang)
     3003 Bern
   - GlaxoSmithKline AG (inklusiv Anhang)
     Talstrasse 3 – 5
     3053 Münchenbuchsee

Hanspeter Thür

4.7 Empfehlung an das Bundesamt für Verkehr: «Dienstpläne von Eisenbahnunternehmen»

Bern, den 1. Juni 2007

Empfehlung

gemäss

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

zum Schlichtungsantrag von

X

gegen

Bundesamt für Verkehr (BAV), Bern

I. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte stellt fest:

1. Das Bundesamt für Verkehr (BAV) ist das Aufsichtsorgan des Bundes über die Eisenbahnen. Es ist damit auch für die Überprüfung der Einhaltung des Bundesgesetzes vom 8. Oktober 1971 über die Arbeit in Unternehmen des öffentlichen Verkehrs (Arbeitszeitgesetz AZG, SR 822.21) zuständig. Im Zuge der Untersuchungen zum Zugsunglück in Dürrenast BE vom Mai 2006 hatte das BAV von der BLS AG die Dienstpläne und Diensteinteilungen der am Unfall beteiligten Personen einverlangt. Gegenüber dem Antragsteller (Journalist) bestätigte das BAV, dass gegen die BLS ein Strafverfahren eingeleitet worden sei.

2. Das BAV teilte dem Antragsteller auch mit, dass es gestützt auf Art. 20 des Arbeitszeitgesetzes von zwei Eisenbahnunternehmen (Unternehmen A und Unternehmen B) Dienstpläne und Diensteinteilungen einverlangt hatte (dabei wurden total vier Diensteinheiten überprüft). Gemäss dieser Bestimmung sind das Unternehmen und die Arbeitnehmer «verpflichtet, den Aufsichtsorganen die erforderlichen Auskünfte über den Vollzug des Gesetzes und dessen Verordnung zu erteilen sowie die Dienstpläne und Diensteinteilungen zur Verfügung zu halten.» Bei Widerhandlungen gegen die gesetzlichen Arbeits- und Ruhezeiten kann die Aufsichtsbehörde Strafanzeige einreichen.

3. Gestützt auf die eingereichten Unterlagen erstellte das BAV für jede überprüfte Diensteinheit einen Auswertungsbericht. In diesen Berichten werden u.a. die Ergebnisse der Analyse der Dienstpläne und -einteilungen, allfällige Verstösse gegen das Arbeitszeitgesetz, eine Risikobewertung sowie die vom BAV vorgeschlagenen Verbesserungsmassnahmen festgehalten.

4. Nach einer gewissen Zeit erkundigte sich der Antragsteller über den Stand der Angelegenheit, worauf ihm das BAV lediglich mitteilte, dass die Untersuchungen zwar abgeschlossen seien, über die Resultate jedoch nicht informiert würde. In der Folge reicht der Antragsteller am 10. November 2006 beim BAV ein schriftliches Zugangsgesuch ein und verlangte Zugang zu den Dienstplänen und -einteilungen der zwei Eisenbahnunternehmen.

5. Das BAV teilte dem Antragsteller am 23. November 2006 mit, dass gestützt auf Art. 7 Abs. 2 des Bundesgesetzes über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsgesetz, BGÖ; SR 152.3) «zu den erhaltenen Informationen und deren Auswertung kein Zugang gewährt werden (kann), denn dadurch würde die Privatsphäre der betroffenen Personen beeinträchtigt.» Deswegen müssten die amtlichen Dokumente gemäss Art. 9 BGÖ «vor Weitergabe soweit anonymi-

siert werden, dass keine Rückschlüsse auf natürliche oder juristische Personen erfolgen können.» Weiter führte das BAV aus, «da es sich bei Dienstplänen und Diensteinteilungen naturgemäss um Unterlagen mit sehr vielen Personendaten handelt, würden sie durch eine Anonymisierung sinnlos werden.»

6. Der Antragsteller reichte mit Schreiben vom 30. November 2006 beim Eidg. Datenschutz- und Öffentlichkeitsbeauftragten (der Beauftragte) einen Schlichtungsantrag nach Art. 13 BGÖ ein (eingegangen am 6. Dezember 2006). Der Antragsteller führte an, dass das BAV ihm den Zugang zu besagten amtlichen Dokumenten verweigert hatte.

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[1]. 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.

[1] Botschaft zum Öffentlichkeitsgesetz, BBl 2003 2023

3. Das Schlichtungsverfahren kann auf schriftlichem Weg oder konferenziell (mit einzelnen oder allen Beteiligten) unter Leitung des Beauftragten stattfinden. Die Festlegung des Verfahrens im Detail obliegt alleine dem Beauftragten[2].

   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. Sachlicher Geltungsbereich

1. Wie aus den Medien zu entnehmen war, hat das BAV im Zuge der Untersuchungen im Zusammenhang mit dem Unfall in Dürrenast ein Strafverfahren gegen die BLS eingeleitet. Das Öffentlichkeitsgesetz sieht einen Vorbehalt zugunsten von Verfahrensgesetzen vor (Art. 3 BGÖ). Der Zugang zu Dokumenten, die Teil eines hängigen oder abgeschlossenen Verfahrens sind, beurteilt sich damit einzig nach dem jeweiligen Verfahrensrecht. Dies gilt auch für Strafverfahren (Art. 3 Abs. 1 Bst. a Ziff. 2 BGÖ).

   Alle Dokumente, die in Zusammenhang mit dem Unfall in Dürrenast stehen und sich im Besitz des BAV befinden, fallen nicht in den sachlichen Geltungsbereich des Öffentlichkeitsgesetzes (Art. 3 Abs. 1 Bst. a Ziff. 2 BGÖ). *Gestützt auf das Öffentlichkeitsgesetz besteht kein Anspruch auf Zugang zu diesen Dokumenten*[3].

2. Aus den Unterlagen, die das BAV dem Beauftragten zur Verfügung gestellt hat, geht hervor, dass gegen eines der zwei untersuchten Eisenbahnunternehmen (Unternehmen A), bei dem lediglich eine Diensteinheit überprüft wurde, ein Strafverfahren eingeleitet worden ist.

   Folglich besteht gemäss Öffentlichkeitsgesetz kein Anspruch auf Zugang zu den Dokumenten betreffend das Eisenbahnunternehmen A.

[2] BBl 2003 2024

[3] S. dazu auch Schlussbericht der Unfalluntersuchungsstelle Bahnen und Schiffe über den «Aufprall eines Dienstzuges auf eine stehende Wagengruppe, 17. Mai 2006, in Dürrenast/Thun» http://www.uus.admin.ch/imperia/md/content/uus/schlussberichte/4020506.pdf)

C. Zugang zu Dokumenten mit Personendaten Dritter

1. Im Folgenden gilt es, die Frage des Zugangs zu den Dokumenten betreffend das Eisenbahnunternehmen B zu beurteilen. Es handelt sich dabei um die vom BAV einverlangten Dienstpläne und -einteilungen sowie die von BAV erstellten Auswertungsberichte. Das BAV lehnt den Zugang zu den gewünschten Dokumenten vollumfänglich ab und begründete dies mit dem Schutz der Privatsphäre der in den Dokumenten erwähnten Personen (Art. 7 Abs. 2 und Art. 9 BGÖ).

2. Die kurze Erfahrung seit Inkrafttreten des Öffentlichkeitsgesetzes zeigt, dass Bundesorgane in der überwiegenden Mehrheit der Gesuche den Zugang entweder vollumfänglich gewähren oder vollständig ablehnen. Sie lassen dabei ausser Acht, dass das Öffentlichkeitsgesetz einen teilweisen Zugang zu einzelnen Inhalten des Dokuments vorsieht respektive vorschreibt («einschränken» gemäss Art. 7). Dies gilt explizit auch für amtliche Dokumente, die Personendaten Dritter enthalten. Kann ein Dokument nicht entsprechend den Vorgaben von Art. 9 BGÖ anonymisiert werden, so darf eine Behörde nicht von vornherein davon ausgehen, dass der Zugang stets verweigert werden muss. Sie muss vielmehr die notwendigen Schritte unternehmen, um der gesuchstellenden Person einen (vollumfänglichen oder eingeschränkten) Zugang zum Dokument zu ermöglichen. Die Behörde ist nach Öffentlichkeitsgesetz gehalten, die Drittperson in das Gesuchverfahren einzubeziehen ist, wenn sie die Gewährung des Zugangs in Betracht zieht (Art. 11 BGÖ).

   Bundesstellen sollten nach Einschätzung des Beauftragten vermehrt von der Möglichkeit der Anhörung der betroffenen Drittperson Gebrauch machen. Denn es ist durchaus denkbar, dass diese keine Einwände gegen die Gewährung des Zugangs zum fraglichen Dokument erhebt.

3. Die zu beurteilenden amtlichen Dokumente (Dienstpläne und -einteilungen sowie Auswertungsberichte) enthalten Personendaten (einerseits Angaben zum Unternehmen, anderseits Angaben zu den Arbeitnehmern) sowie Angaben, die auch Rückschlüsse auf Personen ermöglichen (Dienststelle, Orte, Funktionsbezeichnungen etc.). Zu Recht verweist das BAV darauf, dass amtliche Dokumente, welche Personendaten enthalten, aus Gründen des Persönlichkeitsschutzes nach Möglichkeit vor der Einsichtnahme zu anonymisieren sind (Art. 9 BGÖ). Der Beauftragte kann allerdings dem BAV nicht folgen, wenn es festhält, dass Dienstpläne und -einteilungen «durch eine Anonymisierung sinnlos werden.»

Es kann nicht die Aufgabe eines Bundesamtes sein, darüber zu urteilen, ob die Informationen, zu denen der Gesuchsteller Zugang beantragt, für ihn sinnvoll sind oder nicht. Ebenso wenig muss das Bundesamt in Betracht ziehen, welche Schlüsse und Wertungen der Gesuchsteller aus den zugänglichen Informationen ziehen könnte. Gemäss Öffentlichkeitsgesetz muss sich das Bundesamt in erster Linie darauf beschränken, die Voraussetzungen für die Gewährung des Zugangs zu erfüllen. Dass auch anonymisierte Dokumente einen (sinnvollen oder sinnentleerten) informativen Inhalt aufweisen, zeigt der zu beurteilenden Fall. Aus anonymisierten Dienstplänen und -einteilungen lassen sich eine Vielzahl von Informationen entnehmen, wie beispielsweise Arbeits- und Ruhezeiten. Es versteht sich von selbst, dass die *Namen der Angestellten sowie alle weiteren Angaben, welche die Angestellten identifizieren könnten*, vor der Gewährung des Zugangs abgedeckt werden müssen.

Die blosse Tatsache, dass in den einzelnen Dokumenten zahlreiche Personendaten abzudecken sind, rechtfertigt keine vollumfängliche Ablehnung des Gesuchs. Dies zeigt sich schon daran, dass zum einen der Gesetzgeber auch die besonders aufwändige Bearbeitung geregelt hat (Art. 10 Abs. 4 BGÖ in Verbindung mit Art. 10 der Verordnung über das Öffentlichkeitsprinzip der Verwaltung, Öffentlichkeitsverordnung, VBGÖ; SR 152.31) und zum andern für arbeitsintensive Gesuche eine Gebühr verlangt werden kann (s. unten Bst. D).

4. Das Eisenbahnunternehmen B ist eine juristische Person. Juristische Personen besitzen grundsätzliche die gleichen Rechte und Pflichten wie natürliche Personen. Sie haben Anspruch auf Schutz vor Missbrauch ihrer Personendaten und können sich auf das Datenschutzrecht berufen (Art. 2 des Bundesgesetzes über den Datenschutz, DSG, SR 235.1). Es stellt sich daher die Frage, ob auch das Eisenbahnunternehmen B aus Gründen des Persönlichkeitsschutzes ein Recht darauf hat, *anonym* zu bleiben.

   Gemäss Art. 7 Abs. 2 BGÖ können im Rahmen der Zugangsgewährung in Ausnahmefällen auch Personendaten eines Dritten bekannt gegeben, wenn an deren Bekanntgabe *ein überwiegendes öffentliches Interesse* besteht. Art. 6 Abs. 2 VBGÖ enthält eine nicht abschliessende Auflistung von Fällen, in denen das öffentliche Interesse am Zugang das Interesse der Drittperson am Schutz ihrer Privatsphäre überwiegt. Zur Feststellung des überwiegenden öffentlichen Interesses muss eine Interessenabwägung zwischen dem Schutz der Privatsphäre des Dritten und dem öffentlichem Interesse am Zugang zum fraglichen Dokument vorgenommen werden (Art. 6 Abs. 1 VBGÖ).

Entscheidend für die Beurteilung der Frage, welches Interesse eine Privatperson an der Geheimhaltung ihres Namens resp. ihrer Firma hat, sind u.a. ihre Funktion oder Stellung, die Umstände der Informationsbeschaffung sowie die Art der betroffenen Daten[4].

- Bei einem konzessionierten Eisenbahnunternehmen handelt es sich um eine juristische Person, die mit der Erfüllung einer öffentlichen Aufgabe betraut ist. Sie muss sich daher weitergehende Beeinträchtigungen ihrer Privatsphäre als eine «einfache» juristische oder natürliche Person ohne Bezug zur Öffentlichkeit oder zur Verwaltung gefallen lassen.

- Das Unternehmen war gemäss Art. 20 AZG verpflichtet, dem BAV die fraglichen Informationen zu übermitteln[5].

- Bei der Art der betroffenen Daten handelt es sich um die Firma des Eisenbahnunternehmens und die von ihr zu verantwortenden Verstösse gegen das Arbeitszeitgesetz. Diese Informationen stehen in einem direkten Zusammenhang mit der Erfüllung der öffentlichen Aufgabe.

Entscheidend für die Gewichtung des öffentlichen Interesses am Zugang zu den Dokumenten sind u.a. der Schutz der öffentlichen Sicherheit, die Beziehung zwischen dem Eisenbahnunternehmen und der Verwaltung, das Gewicht der fraglichen Materie sowie das Vorliegen eines besonderen Informationsinteresses.

- Das Arbeitszeitgesetz bezweckt «in erster Linie die Gewährleistung der Sicherheit für die Benutzer der öffentlichen Verkehrsmittel»[6]. Dies geschieht u.a. durch Vorgaben in Bezug auf die Arbeits- und Ruhezeit (Art. 3ff. AZG). Zur Wahrung der Verkehrs- und Betriebssicherheit (sowie zum Schutz der Arbeitnehmer) wurde dem BAV eine Aufsichtstätigkeit übertragen. Der Gesetzgeber stellt damit einen direkten Zusammenhang zwischen der Arbeitszeit der Angestellten von konzessionierten Eisenbahngesellschaften und der Sicherheit der Fahrgäste her.

- Das Eisenbahnunternehmen hat vom Bund eine Konzession erhalten. Aufgrund der besonderen Natur der Beziehung zwischen der Drittperson und dem Bund besteht bereits ein grösseres Interesse an der Transparenz.

[4] zu den massgeblichen Kriterien der Interessenabwägung s. Brunner «Öffentlichkeit der Verwaltung und informationelle Selbstbestimmung: Von Kollisionen und Verkehrsregeln», Ziff. IV 3; in «Selbstbestimmung und Recht», Festgabe für Rainer J. Schweizer, Schulthess 2003

[5] Aus dieser Tatsache lässt sich nach der hier vertretenen Ansicht nicht zwingend ableiten, dass der Zugang zu solchen Informationen restriktiver gehandhabt werden muss (anders Brunner).

[6] BBl 1971 I 442

- Dem öffentlichen Verkehr kommt in der Schweiz eine grosse Bedeutung zu. Eine grosse Anzahl von Bürgerinnen und Bürgern sind täglich auf den öffentlichen Verkehr angewiesen. Es ist daher nachvollziehbar, dass die Öffentlichkeit nach einem Zugsunglück ein besonderes Interesse an Informationen zur Sicherheit des Eisenbahnverkehrs in der Schweiz hat.

Die Sicherheit im Eisenbahnverkehr hat oberste Priorität. Der Beauftragte vertritt daher die Ansicht, dass Bürgerinnen und Bürger ein ebenso grundlegendes wie berechtigtes Interesse haben zu wissen, ob die vom Staat konzessionierten Transportunternehmen im Allgemeinen die gesetzlichen Vorgaben für den öffentlichen Verkehr einhalten und ob sie im Besonderen die Sicherheitsanforderungen beachten. Demgegenüber schätzt der Beauftragte das Interesse des betroffenen Eisenbahnunternehmens an der Wahrung seiner Privatsphäre als ungleich geringer ein, zumal die sie betreffenden Informationen in einem direkten Zusammenhang mit der Erfüllung einer öffentlichen Aufgabe stehen und keine gravierenden Verstösse gegen das Arbeitszeitgesetz festgestellt worden sind. Die Bekanntgabe des Namens stellt nach Meinung des Beauftragten daher nur einen geringen Eingriff in die Privatsphäre dar.

Aufgrund der vorangehenden Ausführungen gelangt der Beauftragte zur Überzeugung, dass vorliegend das öffentliche Interesse am Zugang zu den Dokumenten (d.h. die Sicherheit im Bahnverkehr) das private Interesse an der Geheimhaltung des Namens überwiegt.

Dieser Bekanntgabe von Personendaten steht auch das Datenschutzgesetz nicht entgegen, denn der Gesetzgeber hat für diese Ausnahmefälle eine Koordinationsnorm im Datenschutzgesetz geschaffen[7]. Gemäss Art. 19 Abs. 1*bis* DSG können Personendaten bekannt gegeben werden, wenn (a.) die betreffenden Personendaten im Zusammenhang mit der Erfüllung öffentlicher Aufgaben stehen; und (b.) an deren Bekanntgabe ein überwiegendes öffentliches Interesse besteht. Beide Voraussetzungen sind vorliegend gegeben.

5. Zusammenfassend kommt der Beauftragte in Bezug auf den Zugang zu den Dokumenten, die das Eisenbahnunternehmen B betreffen, zum folgenden Schluss:

   - Dienstpläne und -einteilungen, die das Eisenbahnunternehmen B dem BAV im Rahmen seiner Auskunftspflicht nach Art. 20 AZG zugestellt hat, sowie Kontroll- und Auswertungsberichte, die das BAV im Rahmen seiner Aufsichtstätigkeit nach Art. 18 AZG erstellt hat, sind nach Öffentlichkeitsgesetz grundsätzlich zugänglich.

[7] BBl 2003 2033

- Die Namen der Angestellten sowie alle weiteren Angaben, welche die Angestellten identifizieren könnten (wie Dienststelle, Arbeitsorte, Funktionsbezeichnungen), müssen vor Gewährung des Zugangs abgedeckt werden.
- Der Name des Eisenbahnunternehmens B muss gestützt auf Art. 7 Abs. 2 BGÖ nicht abgedeckt werden.

D. Gebühren

Der Zugang zu amtlichen Dokumenten ist in der Regel gebührenpflichtig (Art. 17 BGÖ sowie Art. 14ff. VBGÖ). Dieser Grundsatz gilt auch, wenn vorgängig ein Schlichtungsverfahren durchgeführt worden ist.

Da im vorliegenden Fall zahlreiche Dokumente zu anonymisieren sind, informiert das BAV den Antragsteller, wenn die Kosten für die Gewährung des Zugangs voraussichtlich 100 Franken übersteigen, und teilt ihm die zu erwartende Höhe der Gebühr mit. Möchte der Antragsteller am Zugangsgesuch festhalten, so muss er das Gesuch innert 10 Tagen bestätigen, ansonsten gilt es als zurückgezogen (Art. 16 Abs. 2 BGÖ).

E. Schlussbemerkung

162 1. Grundsätzlich gilt es festzuhalten, dass dem Transparenzprinzip gerade bei Aufsichts- und Kontrolltätigkeiten der Ämter über Private, denen eine öffentliche Aufgabe zur Erfüllung übertragen worden ist, eine besondere Bedeutung zukommt. Durch Zugang zu Auswertungs- und Inspektionsberichten können die Bürgerinnen und Bürger einerseits die Verwaltung und von ihr beauftragte Dritte kontrollieren. Andererseits kann dadurch das Vertrauen in Behörden und Organisationen, denen öffentliche Aufgaben übertragen wurden, verbessert werden. Sowohl Kontrolle als auch Vertrauensbildung sind *zentrale Ziele* des Öffentlichkeitsgesetzes[8]. Es ist daher zu fordern, dass Bundesbehörden in Zukunft vermehrt Massnahmen ergreifen, damit Kontrollberichte, Inspektionsberichte und Auswertungen – auf Gesuch hin oder öffentlich – zugänglich gemacht werden können. Dieser Forderung sollten die Ämter bereits bei Erstellung eines Berichts Rechnung tragen und entsprechende Vorkehrungen treffen.

[8] BBl 2003 1976

2. Wie bereits in früheren Schlichtungsverfahren festgestellt, herrscht zurzeit eine gewisse «Alles oder Nichts»-Mentalität. Die Bundesämter machen zu wenig von der Möglichkeit (und Verpflichtung!) Gebrauch, einen *teilweisen* Zugang zu amtlichen Dokumenten zu gewähren. Das Verhältnismässigkeitsprinzip verlangt, dass der Zugang nur so gering wie möglich eingeschränkt wird. So lange die nicht anonymisierten (Art. 9 BGÖ) und/oder nicht abgedeckten respektive entfernten Teile (Art. 7 BGÖ) eines Dokuments noch substanzielle und sinnvolle Informationen enthalten, muss ein teilweiser Zugang zum Dokument gewährt werden.

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

1. Das Bundesamt für Verkehr gewährt dem Antragsteller einen teilweisen Zugang zu den Dienstplänen und -einteilungen des Eisenbahnunternehmens B sowie den Auswertungsberichten des BAV betreffend das Eisenbahnunternehmen B. Dabei deckt es die Namen der Angestellten sowie diese identifizierende Angaben ab. Der Name des Eisenbahnunternehmens ist zugänglich zu machen.

2. Das Bundesamt für Verkehr erlässt eine Verfügung nach Art. 5 des Verwaltungsverfahrensgesetzes (SR 172.021), wenn es in Abweichung dieser Empfehlung dem Antragsteller den teilweisen Zugang nicht gewährt.

   Das Bundesamt für Verkehr 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 Bundesamt für Verkehr den Erlass einer Verfügung nach Artikel 5 des Verwaltungsverfahrensgesetzes verlangen, wenn er mit der Empfehlung nicht einverstanden ist (Art. 15 Abs. 1 BGÖ).

4. Als von der Empfehlung betroffene Drittperson kann das Eisenbahnunternehmen B innerhalb von 10 Tagen nach Erhalt dieser Empfehlung beim Bundesamt für Verkehr den Erlass einer Verfügung nach Artikel 5 des Verwaltungsverfahrensgesetzes verlangen, wenn es mit der Empfehlung nicht einverstanden ist (Art. 15 Abs. 1 BGÖ).

5. Gegen die Verfügung kann beim Bundesverwaltungsgericht Beschwerde geführt werden (Art. 16 BGÖ).

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

7. Die Empfehlung wird eröffnet:

   - X
   - Bundesamt für Verkehr (inklusive Anhang)
     3003 Bern
   - Eisenbahnunternehmen B, gemäss Anhang (inklusive Anhang)

Hanspeter Thür

4.8 Empfehlung an das Eidgenössiche Departement für auswärtige Angelegenheiten: «Protokoll Freizügigkeitsabkommen EU»

Bern, den 2. Juli 2007

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, Bern

I. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte stellt fest:

1. Der Antragsteller reichte am 1. Dezember 2006 beim Eidg. Departement für auswärtige Angelegenheiten EDA ein Gesuch um Zugang zum Protokoll der Sitzung vom 6. Juli 2006 des Gemischten Ausschusses[1] zum Abkommen zwischen der Schweizerischen Eidgenossenschaft einerseits und der Europäischen Gemeinschaft und ihren Mitgliedstaaten andererseits über die Freizügigkeit (Freizügigkeitsabkommen)[2].

2. Das EDA lehnte am 20. Dezember 2006 den Zugang zum Sitzungsprotokoll vollumfänglich ab, weil das gewünschte Dokument noch nicht fertig gestellt sei und damit kein amtliches Dokument im Sinne des Bundesgesetzes über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsgesetz, BGÖ; SR 152.3) vorliege. Zudem enthalte das Dokument Positionen über laufende und künftige Verhandlungen, welche in keinem Fall zugänglich seien.

3. Der Antragsteller reichte per Mail am 10. Januar 2007 beim Eidg. Datenschutz- und Öffentlichkeitsbeauftragten (der Beauftragte) einen Schlichtungsantrag nach Art. 13 BGÖ ein. Darin führte er an, dass das EDA ihm den Zugang zum besagten amtlichen Dokument (Protokoll des Gemischten Ausschusses) verweigert habe, «obwohl in der Zwischenzeit die EU Teile der Ergebnisse selbst publiziert hat» (Zitat Schlichtungsantrag).

   In einem dem Schlichtungsantrag beigefügten Schreiben hält der Antragsteller u.a. fest, dass er auch bei der Europäischen Kommission ein Zugangsgesuch eingereicht habe. Auf Anfrage teilte die Kommission dem Beauftragten mit, dass bei ihr keine Gesuche zum betreffenden Sitzungsprotokoll eingegangen sind.

[1] Zu den Aufgaben der Gemischten Ausschüsse s. Europabericht 2006 des Bundesrates, BBl 2006 6815, 6848, Ziffer 3.1.2.2 Institutionelle Aspekte
[2] SR 0.142.112.681; s. insbes. Art. 14 «Gemischter Ausschuss»

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[3]. 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 Detail obliegt alleine dem Beauftragten[4].

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

[3] BBl 2003 2023
[4] BBl 2003 2024

B. Sachlicher Geltungsbereich

1. Der Antragsteller verlangt vom EDA Zugang zum Protokoll. Die nachfolgenden Ausführungen beschränken sich daher auf dieses Dokument.

   Betreffend den Hinweis des Antragstellers, dass die EU als wesentliches Ergebnis des Gemischten Ausschusses vom 6. Juli 2006 den Beschluss Nr. 1/2006 publiziert hat (2006/652/EG), gilt es festzuhalten, dass dieser Beschluss auch von den zuständigen Schweizer Behörden publiziert wurde[5].

2. Das Öffentlichkeitsgesetz verleiht einer Person das Recht, amtliche Dokumente einzusehen und von den Behörden Auskünfte über den Inhalt amtlicher Dokumente zu erhalten (Art. 6 Abs. 1 BGÖ). Gemäss Art. 5 Abs. 3 Bst. b BGÖ gelten jedoch *nicht fertig gestellte* Dokumente nicht als amtliche Dokumente; diese Dokumente sind nach Öffentlichkeitsgesetz also *nicht* respektive erst *nach* deren Fertigstellu ng zugänglich.

   Beim zu beurteilenden Dokument handelt es sich um das Protokoll der letzten Sitzung des Gemischten Ausschusses zum Freizügigkeitsabkommen Schweiz – EG. Dieses Protokoll wird zurzeit von den Vertragsparteien überarbeitet, sodass es an der nächsten Sitzung des Gemischten Ausschusses (im Juli 2007) definitiv angenommen werden kann. Durch Einsichtnahme in das entsprechende Dossier beim Integrationsbüro[6] konnte sich der Beauftragte davon überzeugen, dass das Protokoll noch nicht definitiv fertig gestellt ist. Das EDA hat somit zu Recht keinen Zugang zum Protokoll gewährt. Spätestens nach Annahme des Protokolls durch den Gemischten Ausschuss (d.h. fertig gestelltes Dokument) *könnte* sich die Frage nach der Zugänglichkeit zu diesem Dokument erneut stellen. Bei ihrer Beurteilung muss auch geprüft werden, ob allenfalls eine Ausnahme vom Recht auf Zugang gegeben ist (s. nachfolgende Ziffer 4).

3. Das EDA führte sodann aus, dass das Protokoll Positionen *zu laufenden und künftigen Verhandlungen* beinhalte und daher in keinem Fall zugänglich sei (Art. 8 Abs. 4 BGÖ). Diese Aussage ist nach Ansicht des Beauftragten zu absolut. Das zu beurteilende Protokoll ist eine formelle Zusammenfassung der Gespräche und Ergebnisse der Sitzung vom 6. Juli 2006. Gemäss Geschäftsordnung des Gemischten Ausschusses (s. nachfolgende Ziffer 4) enthält das Protokoll «für jeden Tagespunkt die gefassten Beschlüsse, die verabschiede-

[5] s. Amtliche Sammlung des Bundesrechts vom 27. Dezember 2006, Seite 5851; AS 2006 5851
[6] Das Integrationsbüro koordiniert die Europapolitik des Bundes in Zusammenarbeit mit den zuständigen Fachstellen.

ten Erklärungen und die Schlussfolgerungen des Gemischten Ausschusses.» Für den Beauftragten stellt sich vorweg die Frage, inwiefern *Positionen*, *die in Verhandlungen bereits geäussert worden sind*, tatsächlich unter die Bestimmung von Art. 8 Abs. 4 BGÖ fallen können. Vielmehr besteht der Sinn dieser Bestimmung darin, Positionen so lange vor dem Zugang zu schützen, als sie *der anderen Verhandlungspartei* noch nicht kundgetan worden sind. Überdies muss in Anwendung des Verhältnismässigkeitsprinzips selbst dann, wenn das Protokoll solche Aussagen enthält, stets geprüft werden, ob jene Teile des Dokuments, die keine Rückschlüsse auf laufende oder künftige Verhandlungspositionen zulassen, zugänglich gemacht werden können.

Letztendlich kann die Frage offen gelassen werden, ob das Protokoll tatsächlich laufende oder künftige Verhandlungspositionen enthält, da sich der vorliegende Fall nach Ansicht des Beauftragten in erster Linie danach beurteilt, ob ein Ausnahmefall nach Art. 7 BGÖ gegeben ist.

4. Gestützt auf Art. 14 des Freizügigkeitsabkommens hat der Gemischte Ausschuss eine Geschäftsordnung erlassen und mit Beschluss Nr. 1/2003 vom 16. Juli 2003 angenommen. Weder die EU noch die Schweiz haben den Beschlusstext Nr. 1/2003 als Ganzes publiziert. Immerhin wird in der schweizerischen «Rechtssammlung zu den ‚sektoriellen Abkommen' (Bilaterale I+II), Ziffer 7 Personenverkehr»[7] der Titel des Beschlusses Nr 1/2003 aufgeführt, aus dem sich entnehmen lässt, dass der Gemischte Ausschuss die Geschäftsordnung angenommen hat.

   Die Geschäftsordnung enthält unter anderem folgenden Artikel zur Vertraulichkeit der Tätigkeit des Gemischten Ausschusses:

   Artikel 13 Vertraulichkeit

   Die Beratungen in den Sitzungen und die Dokumente des Gemischten Ausschusses sind vorbehaltlich der rechtlichen Pflichten der Vertragsparteien hinsichtlich der Veröffentlichung der Beschlüsse und Empfehlungen und des Zugangs zu den Dokumenten vertraulich. Der Vorsitzende kann die Vertraulichkeit aufheben, sofern keine Vertragspartei Einwände erhebt.

   Die Vertragsparteien können öffentliche Informationsveranstaltungen organisieren oder Vertreter der Öffentlichkeit auf andere Weise über die Ergebnisse der Sitzungen des Gemischten Ausschusses informieren.

[7] s. http://www.admin.ch/ch/d/eur/gemaus.html

Für den vorliegenden Fall bedeutet dies, dass das Protokoll als Dokument des Gemischten Ausschusses grundsätzlich vertraulich ist, soweit ein Vertragsstaat aufgrund seines innerstaatlichen Rechts nicht verpflichtet ist, den Zugang zu gewähren. Mit anderen Worten sieht die Geschäftsordnung des Gemischten Ausschuss ausdrücklich einen Vorbehalt zugunsten des Öffentlichkeitsprinzips, d.h. in der Schweiz des Öffentlichkeitsgesetzes, vor. Allerdings soll der Zugang erst gewährt werden, wenn sich keine andere Vertragpartei dagegen ausspricht.

Der Zugang zu einem Dokument kann nach Art. 7 Abs. 1 Bst. d BGÖ eingeschränkt, aufgeschoben oder verweigert werden, wenn durch seine Gewährung die aussenpolitischen Interessen oder die internationalen Beziehungen der Schweiz beeinträchtigt werden können. Die Botschaft des Bundesrates zum Öffentlichkeitsgesetz sieht ausdrücklich vor, dass Bundesstellen gehalten sein können, den Zugang zu amtlichen Dokumenten aufgrund «internationaler vertraglicher Verpflichtungen oder anerkannter Staatenpraxis (z.B. im Rahmen der Zusammenarbeit innerhalb internationaler Organisationen)»[8] zu beschränken. Darüber hinaus kann die einseitige Gewährung des Zugangs zu dem *von den Vertragsparteien als vertraulich bezeichneten, noch nicht fertig gestellten Protokoll* mit hoher Wahrscheinlichkeit die Zusammenarbeit im Gemischten Ausschuss belasten und so zu einer Beeinträchtigung der aussenpolitischen Interessen oder internationalen Beziehungen der Schweiz führen.

In Anbetracht der Möglichkeit der Aufhebung der Vertraulichkeit (Art. 13 des Geschäftsreglements des Gemischten Ausschusses) sowie angesichts der Tatsache, dass sowohl die EU wie auch die Schweiz für die Verwaltungstätigkeit ihrer Behörden das Öffentlichkeitsprinzip eingeführt haben, regt der Beauftragte an, dass die Schweizer Delegation anlässlich der nächsten Sitzung des Gemischten Ausschusses den *Antrag* stellt, *die Vertraulichkeit des Protokolls* der letzten Sitzung vollumfänglich oder in Teilen aufzuheben.

Gestützt auf die vorangegangenen Ausführungen kommt der Beauftragte zum Schluss, dass der Zugang zum Protokoll aufgrund von Art. 7 Abs. 1 Bst. d BGÖ (Beeinträchtigung der aussenpolitischen Interessen oder internationalen Beziehungen) in Verbindung mit Art. 5 Abs. 3 Bst. c BGÖ (nicht fertig gestelltes Dokument) bis zum Entscheid des Gemischten Ausschusses aufgeschoben werden soll.

[8] BBl 2003 2010

5. In einem dem Schlichtungsantrag beigefügten Schreiben hält der Antragsteller fest, dass er insbesondere an der Frage interessiert sei, «wer seitens der EG und der Schweiz an den Verhandlungen des Gemischten Ausschusses teilgenommen hat.»

   Eine Auflistung mit den *Namen beider Delegationen* soll im Anhang zum Protokoll aufgeführt werden. Eine Ablehnung des Zugangs mit dem Argument, dass dieses Dokument noch nicht fertig gestellt sei, wäre nach Ansicht des Beauftragten nicht statthaft, da davon ausgegangen werden muss, dass bereits vor der letzten Sitzung des Gemischten Ausschusses ein definitives Dokument mit allen Teilnehmenden erstellt worden ist.

   In Bezug auf die Bekanntgabe *der Namen der Schweizer Delegation* muss Folgendes hervorgehoben werden: Amtliche Dokumente, die Personendaten Dritter enthalten, sind vor der Einsichtnahme nach Möglichkeit zu anonymisieren (Art. 9 Abs. 1 BGÖ). Dabei gilt es zu beachten, dass es sich bei den Mitgliedern der Schweizer Delegation nicht um Personendaten von «privaten» Dritten handelt, sondern um Mitarbeitende von verschiedenen Schweizer Behörden, die in *ihrer amtlichen Funktion* an den Sitzungen des Gemischten Ausschusses teilnehmen. Dabei handelt es sich um Angestellte in einer höheren Führungsfunktion, die als offizielle Vertreter der Schweiz bei einer internationalen Verhandlung überdies eine besondere Verantwortung wahrnehmen. Diese Personen müssen eher eine Veröffentlichung ihrer Personendaten in Kauf nehmen als nachgeordnetes Behördenpersonal ohne Führungsverantwortung[9]. Überdies besteht unbestreitbar ein öffentliches Interesse an der Zusammensetzung einer Schweizer Delegation für internationale Verhandlungen.

   Das Transparenzprinzip geht in diesem konkreten Fall dem Anspruch auf Persönlichkeitsschutz so lange vor, als dass die Zugänglichmachung eines Dokuments für die Betroffenen mit hoher Wahrscheinlichkeit keine nachteiligen Folgen hat, was vorliegend nach Einschätzung des Beauftragten der Fall ist. Einer Bekanntgabe der Personendaten steht auch das Bundesgesetz über den Datenschutz (DSG, SR 235.1) nicht entgegen, wenn die betreffenden Personendaten im Zusammenhang mit der Erfüllung öffentlicher Aufgaben stehen und an ihrer Bekanntgabe ein überwiegendes öffentliches Interesse besteht (Art. 19 Abs. 1bis DSG).

[9] Erläuterungen zur Verordnung über das Öffentlichkeitsprinzip der Verwaltung, Art. 6 VBGÖ (Erläuterungen publiziert auf http://www.edoeb.admin.ch/org/00828/index.html?lang=de)

Aufgrund dieser Überlegungen hat der Beauftragte im Rahmen des Schlichtungsverfahrens den Vorschlag unterbreitet, die Namen der Mitglieder der Schweizer Delegation bekannt zu geben. Das Integrationsbüro teilte dem Beauftragten mit, dass das in der Sache federführende Bundesamt dies mit der Begründung ablehnte, dass nicht immer die gleichen Personen an den Sitzungen teilnehmen. Diese Begründung überzeugt nicht. Der Beauftragte hält an seiner Ansicht fest, dass die Namen und das jeweilige Bundesamt der Schweizer Delegation bekannt gegeben werden müssen.

Die EU-Delegation des Gemischten Ausschusses lehnte auf Anfrage des Beauftragten die Bekanntgabe der Namen ihrer Delegationsmitglieder ab. Der Beauftragte nimmt diese Entscheidung einer ausländischen Behörde zur Kenntnis.

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

1. Das Eidg. Departement für auswärtige Angelegenheiten schiebt den Zugang zum Protokoll der Sitzung vom 6. Juli 2006 des Gemischten Ausschusses bis zum Entscheid des Ausschusses über die Aufhebung der Vertraulichkeit des Protokolls auf.

2. Das Eidg. Departement für auswärtige Angelegenheiten gewährt dem Antragsteller umgehend Zugang zum Dokument, das die Mitglieder der Schweizer Delegation (Name, Funktion, Bundesbehörde) auflistet.

3. Das Eidg. Departement für auswärtige Angelegenheiten erlässt eine Verfügung nach Art. 5 des Verwaltungsverfahrensgesetzes, wenn es mit Ziffer 1 und/oder Ziffer 2 nicht einverstanden ist.

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

4. 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 Ziffer 1 und/oder Ziffer 2 nicht einverstanden ist (Art. 15 Abs. 1 BGÖ).

5. Gegen die Verfügung kann beim Bundesverwaltungsgericht Beschwerde geführt werden (Art. 16 BGÖ).

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

7. Die Empfehlung wird eröffnet:

   - X

   - Eidg. Departement für auswärtige Angelegenheiten
     3003 Bern

Hanspeter Thür

4.9 Empfehlung an das Bundesamt für Privatversicherungen: «Tarifkalkulationen»

Bern, den 13. Juli 2007

Empfehlung

gemäss

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

zum Schlichtungsantrag von

X
(Antragstellerin)

gegen

Bundesamt für Privatversicherungen (BPV), Bern

I. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte stellt fest:

1. Das Bundesamt für Privatversicherungen (BPV) erteilt als Aufsichtsbehörde Bewilligungen für Versicherungsunternehmen nach Art. 2 Abs. 1 Bst. a und b des Bundesgesetzes betreffend die Aufsicht über Versicherungsunternehmen (Versicherungsaufsichtsgesetz, VAG; SR 961.01). Dabei muss ein Versicherungsunternehmen u.a. im Bereich der Zusatzversicherung zur sozialen Krankenversicherung dem BPV die Tarifberechnungen zur Genehmigung unterbreiten (Art. 38 VAG i.V.m. Art. 4 Abs. 2 Bst. r VAG).

2. Die Antragstellerin wandte sich mit Schreiben vom 1. Dezember 2006 an das Bundesamt für Privatversicherungen (BPV) und informierte es darüber, dass ihr das Versicherungsunternehmen X für den Wechsel von der Kollektiv-Krankenversicherung in eine Einzel-Taggeldversicherung eine Offerte mit einer unverhältnismässig hohen Prämie unterbreitet habe. Die Antragstellerin verlangte vom Amt als Genehmigungsbehörde eine Stellungnahme.

3. Mit dem Antwortschreiben vom 7. Dezember 2006 erläuterte das BPV der Antragstellerin u.a., dass das BPV im Genehmigungsverfahren «anhand der vorgelegten Tarife prüfe, ob sich die vorgesehenen Prämien in einem Rahmen halten, der einerseits die Solvenz des Versicherungsunternehmens und anderseits den Schutz der Versicherten vor Missbrauch gewährleistet.» Weiter führte das BPV aus, dass diese im Jahr 2005 vorgenommene Prüfung gezeigt habe, dass die beiden vorgängig erwähnten Bedingungen erfüllt gewesen seien, weshalb der vom Versicherungsunternehmen X vorgelegte Einzel-Taggeldtarif genehmigt worden sei.

4. Die Antragstellerin war mit der Stellungnahme des BPV nicht einverstanden und ersuchte mit Schreiben vom 10. Dezember 2006 um detaillierte Informationen zu den «versicherungstechnischen Grundlagen und (zur) Risikoberechnung». Zudem verlangte sie vom BPV die «notwendige Rechtsmittelbelehrung (…) um gegen diese Auswüchse juristisch vorzugehen.» Mit Schreiben vom 22. Dezember 2006 informierte das BPV der Antragstellerin darüber, dass es den «Wunsch nach Bekanntgabe der versicherungstechnischen Grundlagen» als Zugangsgesuch nach Art. 6 des Bundesgesetzes über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsgesetz BGÖ; SR 152.3) entgegengenommen habe und prüfen werde.

5. Am 31. Januar 2007 teilte das BPV der Antragstellerin mit, dass das Öffentlichkeitsgesetz nicht zur Anwendung gelange, weil die fraglichen Dokumente vor Inkrafttreten des Öffentlichkeitsgesetzes erstellt respektive empfangen wurden, und daher kein Zugang gewährt werde.

   Darüber hinaus vertrat das BPV die Ansicht, dass Tarifkalkulationen der Versicherer ein Geschäftsgeheimnis im Sinne von Art. 7 Abs. 1 Bst. g BGÖ seien und damit eine Ausnahme vom Öffentlichkeitsprinzips vorliege. Dies bedeute, «dass das Einsichtsrecht nach BGÖ entfällt.»

6. Mit Schreiben vom 3. Februar 2007 wandte sich die Antragstellerin an den Eidg. Datenschutz- und Öffentlichkeitsbeauftragten (der Beauftragte) und beantragte, dass das BPV angehalten werden solle, ihr Anfrage vom 10. Dezember 2006 zu beantworten. Der Beauftragte nahm das Schreiben der Antragstellerin als Schlichtungsgesuch entgegen.

   Die Prüfung des Beauftragten beschränkte sich auf die korrekte Anwendung des Öffentlichkeitsgesetzes. Demnach kann er in seiner Empfehlung eine Behörde dazu anhalten, Dokumente zugänglich zu machen, nicht aber, einen Brief zu beantworten. Zudem kann er sich aus Kompetenzgründen weder zur materiellen Fragen der Angemessenheit der Offerte des Versicherungsunternehmens noch zum Bewilligungsentscheid des BPV äussern.

7. Auf Anfrage überwies das BPV dem Beauftragten umgehend Kopien des Briefwechsels mit der Antragstellerin sowie von allen Dokumenten, die das Versicherungsunternehmen X im Rahmen des Genehmigungsverfahrens betreffend Tarife und Allgemeinen Versicherungsbedingungen dem BPV zugestellt hat oder von Letzterem in diesem Zusammenhang erstellt worden sind.

   Alle dem Beauftragten zur Verfügung gestellten Dokumente sind in einem Zeitraum von Mai 2005 und Juli 2005 erstellt worden.

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[1]. 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. Die Antragstellerin hat ein Zugangsgesuch nach Art. 6 BGÖ beim BPV eingereicht und eine ablehnende Antwort 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 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 Detail obliegt alleine dem Beauftragten[2].

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

B. Sachlicher Geltungsbereich

1. Die Antragstellerin stellte beim BPV den «Antrag», ihr «detailliert die versicherungstechnischen Grundlagen und Risikoberechnungen» mitzuteilen. Mit anderen Worten verlangte sie Zugang zu jenen Unterlagen des BPV, die es in Zusammenhang mit der Genehmigung von Tarifen und Allgemeinen Versicherungsbedingungen im Bereich der Krankenzusatzversicherung vom Versicherungsunternehmen X erhalten oder selbst erstellt hat.

   Mit Inkrafttreten des Öffentlichkeitsgesetzes auf 1. Juli 2006 muss jedes Bundesamt bei solchen Anfragen stets auch prüfen, ob damit um Zugang zu Dokumenten im Sinne von Art. 6 BGÖ ersucht wird. Zu Recht hat das BPV den «*Antrag*» *der Antragstellerin als Zugangsgesuch zu amtlichen Dokumenten behandelt.*

[1] BBl 2003 2023
[2] BBl 2003 2024

2. Die im Zusammenhang mit dem Genehmigungsverfahren der Tarifberechnungen stehenden und vom Beauftragten eingesehenen Dokumente datieren aus dem Zeitraum von Mai 2005 bis Juli 2005. Das BPV versicherte gegenüber dem Beauftragten, dass es seit dem 1. Juli 2006 keine diese Angelegenheit betreffenden Dokumente empfangen oder fertig erstellt habe.

3. Das Öffentlichkeitsgesetz findet nur auf amtliche Dokumente Anwendung, die nach seinem Inkrafttreten, d.h. ab 1. Juli 2006 von einer Behörde erstellt oder empfangen wurden (Art. 23 BGÖ). Dokumente, die vor diesem Datum erstellt oder empfangen worden sind, unterliegen somit nicht dem Öffentlichkeitsprinzip. Folglich besteht daher kein einklagbares Recht, diese Dokumente einzusehen und von den Behörden Auskünfte über ihren Inhalt zu erhalten[3]. Dies hindert eine gesuchstellende Person zwar nicht daran, ein Zugangsgesuch zu Dokumenten, die vor dem 1. Juli 2006 erstellt oder empfangen worden sind, einzureichen, denn die zuständige Behörde kann (*und soll nach Ansicht des Beauftragten wenn immer möglich*) auch in diesen Fällen den Zugang gewähren. Es gilt allerdings zu beachten, dass die Behörde von Gesetzes wegen nicht dazu verpflichtet ist. Vielmehr kann sie das Gesuch mit dem blossen Hinweis auf die Nichtanwendbarkeit des Öffentlichkeitsgesetzes ablehnen, ohne dass die gesuchstellende Person diese Zugangsverweigerung einklagen könnte.

4. Da das Öffentlichkeitsgesetz nicht zur Anwendung gelangt, kann auch die Frage offen gelassen werden, ob Tarifkalkulationen der Versicherer tatsächlich als Geschäftsgeheimnisse im Sinne von Art. 7 Abs. 1 Bst. cg BGÖ zu qualifizieren sind.

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

[3] Im ursprünglichen Entwurf des Bundesrates (BBl 2003 2047) findet sich diese Übergangsbestimmung noch nicht. Damit wären alle amtlichen Dokumente unabhängig vom Zeitpunkt ihrer Erstellung oder ihres Empfanges grundsätzlich öffentlich zugänglich gewesen. Die Zugangsbeschränkung auf nach dem 1. Juli 2006 erstellte Dokumente wurde erst in den parlamentarischen Beratungen beschlossen (s. dazu AB 2003 S 1142, AB 2004 N 1265)

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

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

   Gegen diese Verfügung kann die Antragstellerin beim Bundesverwaltungsgericht 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 der Antragstellerin anonymisiert.
4. Die Empfehlung wird eröffnet:

   - X
   - Bundesamt für Privatversicherungen
     3003 Bern

Jean-Philippe Walter

4.10 Empfehlung an das Bundesamt für Migration: «Kriterienliste Safe Countries»

Bern, 30. Juli 2007

Empfehlung

gemäss

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

zum Schlichtungsantrag von

X
(Antragstellerin)

gegen

Bundesamt für Migration (BFM), Bern

I. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte stellt fest:

1. Am 8. Dezember 2006 veröffentlichte das Bundesamt für Migration (BFM) eine Pressemitteilung, gemäss welcher der Bundesrat entschieden hat, Benin, Kroatien, Mali, Moldawien (ohne Transnistrien), Montenegro und die Ukraine neu als Safe Countries zu betrachten. Zudem habe der Bundesrat die Änderung der Kriterienliste zur Bezeichnung von Safe Countries gutgeheissen.

2. Die Antragstellerin reichte am 14. Dezember 2006 beim BFM ein Gesuch nach Art. 6 des Bundesgesetzes über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsgesetz, BGÖ; SR 152.3) um Zugang zu folgenden Dokumenten ein:

   - Geänderte Kriterienliste für die Beurteilung sicherer Herkunftsstaaten,
   - allfällige Gutachten, Beurteilungen, Stellungnahmen, welche im Rahmen der Änderung der Kriterienliste eingeholt wurden,
   - Lagebeurteilungen der sicheren Herkunftsstaaten, mit denen das Bundesamt seine Einschätzung begründet (Dokumente ab 1.07.2006),
   - Begründungen des Bundesamtes zuhanden des Bundesrates bezüglich der neu benannten «Safe Countries,»
   - Stellungnahme UNHCR und anderer Organisationen, die zum Entscheid angehört wurden, Benin, Kroatien, Mali, Moldawien (ohne Transnistrien), Montenegro und die Ukraine als zusätzliche «Safe Countries» zu bezeichnen,
   - weitere Dokumente, die zur Beurteilung der Sicherheit der «Safe Countries» geführt haben.

3. Das BFM gewährte am 18. Januar 2007 Zugang zur Liste der Kriterien der «Safe Countries» und verwies mit zwei Links auf öffentlich zugängliche Dokumente im Internet («Country Pages A - Z» des U.S. Departement of State sowie «Country Specific Asylum Policy OGNs» des brititschen Border and Immigration Agency). Den Zugang zu den übrigen Dokumenten verweigert das BFM, «car leur publication pourrait affaiblir la position de la Suisse lors de futures négociations et pourrait compromettre les intérêts de la Suisse en matière de politique extérieure et dans ses relations internationales (art. 7, al.1, let. D, LTrans).»

4. Mit Schreiben vom 8. Februar 2007 reichte die Antragstellerin beim Eidg. Datenschutz- und Öffentlichkeitsbeauftragten (der Beauftragte) einen Schlichtungsantrag ein. Sie machte dabei insbesondere geltend, dass das BFM seinen Entscheid nicht begründete. Es sei daher nicht nachvollziehbar, wie das BFM zu seiner Einschätzung gelange, dass «eine Veröffentlichung (…) die Schweizer Position bei zukünftigen aussenpolitischen Verhandlungen beeinträchtigen (würde)» und «die aussenpolitischen Beziehungen beeinträchtigen könnte.»

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[1]. 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. Die Antragstellerin hat ein Zugangsgesuch nach Art. 6 BGÖ beim BFM eingereicht und eine ablehnende Antwort 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 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 Detail obliegt alleine dem Beauftragten[2].

[1] BBl 2003 2023
[2] 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 Beurteilung der Angelegenheit eine Empfehlung abzugeben.

B. Sachlicher Geltungsbereich

1. Das BFM lehnte den Zugang zu den gewünschten Dokumenten ab und führte dazu lediglich aus, dass die Veröffentlichung dieser Dokumente die Position der Schweiz in künftigen Verhandlungen schwächen und die aussenpolitischen Interessen oder die internationalen Beziehungen der Schweiz beeinträchtigt werden könnten (Art. 7 Abs. 1 Bst. d BGÖ). Im Weiteren begründet das BFM seinen Entscheid nicht.

   Gemäss Botschaft zum Öffentlichkeitsgesetz sind negative Stellungnahmen kurz zu begründen[3]. Nach Ansicht des Beauftragten vermag die blosse Zitierung von Ausnahmebestimmungen (hier Art. 7 Abs. 1 Bst. d und Art. 8 Abs. 4 BGÖ) den Anforderungen an eine kurze Begründung nicht zu genügen. Es ist daher zu fordern, dass Bundesämter bei einer ablehnenden Stellungnahme nicht einfach den Wortlaut der Ausnahmebestimmung des Öffentlichkeitsgesetzes wiederholen, sondern den Entscheid in einer Weise *motivieren*, die es der antragstellenden Person erlaubt, den Verweigerungsentscheid des Bundesamtes *zumindest in Grundzügen nachvollziehen* zu können.

2. Bei den Unterlagen, die das BFM dem Beauftragten auf Anfrage zur Verfügung gestellt hat, handelt es sich um:

   - den Bundesratsantrag (inklusive 5 Anlagen),
   - das Übermittlungsblatt des BFM zum Bundesratsantrag (vom Direktor des BFM unterzeichnet, zuhanden des Departementschefs),
   - die Kriterienliste (datiert vom 12.12.06),
   - die Stellungnahmen des Eidg. Departements für auswärtige Angelegenheiten EDA und der Schweizerischen Asylrekurskommission ARK in der Ämterkonsultation «Safe Countries»,
   - die Stellungnahme des UNHCR.

   Im Folgenden gilt es hinsichtlich jedes einzelnen Dokuments zu prüfen, ob und in welchem Umfang der Zugang gemäss Öffentlichkeitsgesetz gewährt werden kann.

[3] BBl 2003 2023

3. Bundesratsantrag: Zur Wahrung des Kollegialitätsprinzips im Bundesrat sieht Art. 8 Abs. 1 BGÖ vor, dass kein Recht auf Zugang zu amtlichen Dokumenten des Mitberichtsverfahrens besteht. Der Ausschluss vom Öffentlichkeitsprinzip gilt auch, nachdem der Bundesrat den Entscheid gefällt hat[4]. Das Mitberichtsverfahren beginnt mit der Unterzeichnung des Antrags durch das federführende Departement (Art. 5 Abs. 1bis der Regierungs- und Verwaltungsorganisationsverordnung RVOV, SR 172.010.1).

   Der Beauftragte kommt zum Schluss, dass der vom Departementschef unterzeichnete Bundesratsantrag betreffend die Änderung der Kriterienliste von Safe Countries und die Bezeichnung von neuen Safe Countries nicht zugänglich ist.

4. Übermittlungsblatt des BFM zum Bundesratsantrag: Gemäss Botschaft zum Öffentlichkeitsgesetz sind jene Dokumente vom Zugang ausgenommen, die der Entscheidvorbereitung des Bundesrates dienen. Dazu gehören «Aufzeichnungen der Bundesratsmitglieder, ihrer persönlicher Berater und Beraterinnen und weiterer Mitarbeiter und Mitarbeiterinnen»[5]. Nach Ansicht des Beauftragten ist dabei die Tatsache, welcher Mitarbeiter dieses Übermittlungsblatt erstellt respektive unterzeichnet hat, weniger entscheidend, als vielmehr, ob das Übermittlungsblatt einen direkten Bezug zum Bundesratsantrag aufweist und damit den Entscheid des Bundesrates vorbereitet.

   Üblicherweise enthalten diese Übermittlungsblätter zuhanden des Departementschefs eine Zusammenfassung der wichtigsten Punkte des Bundesratsantrags und führen die Resultate der vorausgehenden Ämterkonsultation und allfällige Differenzen mit anderen Bundesstellen auf. Auch das hier zu beurteilende Dokument enthält diese Informationen und soll in erster Linie dem Departementschefs als Vorbereitungspapier dienen.

   Der Beauftragte ist der Meinung, dass solche Übermittlungsblätter, Begleitblätter etc. mit Informationen, die in einem *direkten, materiellen Zusammenhang* mit dem Bundesratsantrag stehen, grundsätzlich als Teil des Mitberichtsverfahrens betrachtet werden können und somit gestützt auf Art. 8 Abs. 1 BGÖ nicht zugänglich sind.

   Der Beauftragte kommt zum Schluss, dass das Übermittlungsblatt zum Bundesantrag im vorliegenden Fall nicht zugänglich ist.

[4] BBl 2003 2014
[5] BBl 2003 2014

5. Anlagen zum Bundesratsantrag: Der Bundesratsantrag enthält 5 Anlagen. Weder das Öffentlichkeitsgesetz noch die Botschaft sprechen sich klar darüber aus, ob diese Anlagen Teil des Bundesratsantrags sind. Der Beauftragte ist der Überzeugung, dass der Begriff «Bundesratsantrag» eng ausgelegt werden muss und daher nur der eigentliche Antrag, nicht aber dazugehörige Anlagen unter Art. 8 Abs. 1 BGÖ darunter fallen. Die Beurteilung des Zugangs zu Anlagen richtet sich somit nach dem Öffentlichkeitsgesetz.

Es handelt sich um folgende 5 Anlagen:

- Anlage 1: «Liste Safe Countries vom 1. Juli 2003»

  (*Die Gesuchstellerin beantragte keinen Zugang zu dieser Liste. In der Pressemitteilung des BFM vom 8. Dezember 2006 sind alle Safe Countries aufgeführt worden*.)

- Anlage 2: «Kriterien zur Beurteilung eines Staates im Hinblick auf dessen Bezeichnung als Safe Country vom 13. Juni 1996»

  Vor dem Inkrafttreten des Öffentlichkeitsgesetzes erstellte Dokumente fallen nicht in den Anwendungsbereich des Gesetzes. Ein Bundesamt trifft daher keine Pflicht, den Zugang zu diesen Dokumenten zu gewähren. Allerdings steht es der Behörde frei, dem Gesuch zu entsprechen. Angesichts der Tatsache, dass das BFM den Zugang zur aktuellen Kriterienliste (s. nachfolgend Anlage 3) gewährt, ist für den Beauftragten nicht ersichtlich, warum das Amt nicht auch den Zugang zu diesem Dokument gewährt hat.

  Da das Dokument vor Inkrafttreten des Öffentlichkeitsgesetzes erstellt worden ist, besteht kein Anspruch auf Zugang.

- Anlage 3: «Revidierte Kriterienliste: Kriterien zur Beurteilung eines Staates im Hinblick auf dessen Bezeichnung als «verfolgungssicher» im Sinne von Artikel 34 Absatz 1 AsylG»

  (Zugang durch das BFM am 18.01.2007 gewährt)

- Anlage 4: «Die geltenden und revidierten Safe Country-Beurteilungskriterien im Vergleich»

  Das Dokument enthält eine Synopse der beiden Versionen der Kriterienliste. Weder fallen die darin enthaltenen Informationen unter die Ausnahmen von Art. 7, noch stellen sie einen Anwendungsfall von Art. 8 BGÖ dar. Eine Beschränkung des Zugangs ist nicht gerechtfertigt.

  Der Beauftragte kommt zum Schluss, dass der Zugang zu diesem Dokument zu gewähren ist.

- Anlage 5: «Beurteilung der Eignung zur Bezeichnung als sichere Herkunftsstaaten von Benin, Kroatien, Mali, Moldawien (ohne Transnistrien), Montenegro und der Ukraine»

  Dieses Dokument enthält für jedes Land eine Beurteilung als Safe Country anhand der Kriterienliste (s. Anlage 3), einen Auszug aus der Asylstatistik das jeweilige Land betreffend, «wichtigste Vorbringen» der Asyl Suchenden und einen kurzen Abriss zur Asyl- und Wegweisungspraxis.

  Diese Informationen sind entweder bereits öffentlich zugänglich (wie die Asylstatistik) oder sie sind nicht als vertraulich zu qualifizieren. So ist nicht ersichtlich, weshalb die Vorbringen der Asyl Suchenden oder die Asylpraxis in der Art, wie sie in dem zu beurteilenden Dokument aufgeführt werden, nicht zugänglich gemacht werden können. Nach Einschätzung des Beauftragten handelt sich dabei um allgemeine Informationen, die weder die Beziehungen zu den betroffenen Staaten mit einer gewissen Wahrscheinlichkeit zu beeinträchtigen vermögen, noch sind diese Informationen geeignet, laufende Verhandlungspositionen (welche?) der Schweiz zu gefährden.

  Gleiches gilt grundsätzlich für die Einschätzung des BFM betreffend die Eignung als sichere Herkunftsstaaten: Der Beauftragte ist der Ansicht, dass für diese Einschätzungen überwiegend Informationen und Angaben aus allgemein zugänglichen Quellen (z.B. Zeitungsberichte, Rapporte NGOs, Internet) über das zu analysierende Land verwendet wurden. Eine Beschränkung des Zugangs regt der Beauftragte lediglich für jene Textpassagen an, in denen das BFM eine Wertung über aktuelle politische Begebenheiten des jeweiligen Landes abgibt (s. Anhang 1). Sie sind geeignet, die aussenpolitischen Beziehung im Sinne von Art. 7 Abs. 1 BGÖ zu beeinträchtigen.

  Der Beauftragte kommt zum Schluss, dass der Zugang zum Dokument teilweise gewährt werden muss.

6. In der Ämterkonsultation abgegebene Stellungnahmen: Die im Rahmen von Ämterkonsultationen abgegebenen Stellungnahmen sind nicht Bestandteil des Mitberichtsverfahrens und fallen daher unter das Öffentlichkeitsgesetz. Dabei ist zu beachten, dass ein Zugang zu diesen Stellungnahmen erst nach dem Entscheid des Bundesrates gewährt werden kann (Anwendungsfall von Art. 7 Abs. 1 Bst. a BGÖ) und dies auch nur soweit, als keine überwiegenden öffentlichen oder privaten Interessen gemäss Art. 7 dem Zugang entgegenstehen[6].

[6] BBl 2003 2015

Der Bundesrat kann *ausnahmsweise* beschliessen, dass aus diesen Gründen die Dokumente des Ämterkonsultationsverfahrens sogar nach seinem Entscheid *nicht* zugänglich sein sollen (Art. 8 Abs. 3 BGÖ). In der hier zu beurteilenden Angelegenheit sieht der Bundesratsbeschluss keinen entsprechenden Ausschluss vor. Daraus kann nur geschlossen werden, dass weder das federführende BFM (für das ganze Geschäft), noch ein anderes Bundesamt (d.h. EDA respektive ARK für ihre Stellungnahmen in der Ämterkonsultation) einen Antrag eingereicht haben, gemäss dem Dokumente aus dem Ämterkonsultationsverfahren als Ganzes oder in Teilen nach dem Entscheid des Bundesrates nicht zugänglich sein sollen (8 Abs. 3 BGÖ). Folglich unterliegen die im Rahmen der Ämterkonsultation abgegebenen Stellungnahmen grundsätzlich dem Öffentlichkeitsprinzip.

Der Zugang zur Stellungnahme der Asylrekurskommission ist nach Ansicht des Beauftragten vollumfänglich zu gewähren.

Der Zugang zur Stellungnahme des EDA ist nach Ansicht des Beauftragten teilweise zu gewähren. Eine Beschränkung regt der Beauftragte in jenen Fällen an, in denen die schweizerische Auslandvertretung eine Wertung über aktuelle politische Begebenheiten im jeweiligen Gastland abgibt (s. Anhang 2).

7. Briefwechsel mit dem UNHCR: Ein offener und ungeschränkter Austausch von Informationen mit internationalen Organisationen ist für schweizerische Amtsstellen unabdingbar. Dabei müssen sich beide Seiten darauf verlassen können, dass die Kontakte und die so ausgetauschten Informationen absolut vertraulich behandelt werden. Nach Ansicht des Beauftragten besteht die konkrete Befürchtung, dass schweizerische Behörden nicht mehr im gleichen Ausmass wie bis anhin von internationalen Organisationen oder anderen Staaten wichtige und vertrauliche Informationen erhalten würden, wenn die so erlangten Dokumente stets allgemein zugänglich gemacht werden müssten. Als Folge davon könnten negative Auswirkungen für die aussenpolitischen und internationalen Beziehungen der Schweiz nicht ausgeschlossen werden. Aus diesem Grund ist der *Beauftragte der Ansicht, dass das BFM den Zugang zur Antwort des UNHCR gestützt auf Art. 7 Abs. 1 d BGÖ verweigern kann.*

   Nichtsdestotrotz darf die Ausnahmebestimmung von Art. 7 Abs. 1 d BGÖ nicht dazu führen, dass ein Bundesamt den Zugang zu einem Dokument, das es von einer internationalen Organisation oder von einem anderen Staat erhalten hat, allein unter Bezugnahme auf seine Herkunft in jedem Fall unbesehen verweigert. Nach Ansicht des Beauftragten sollte das Amt insbesondere auch in jenen Fällen, in denen nicht mit Sicherheit ausgeschlossen werden kann, dass die von der Gegenseite erhaltenen Informationen teilweise oder vollum-

fänglich als vertraulich einzustufen sind, stets darum besorgt sein, dass das nun geltende Öffentlichkeitsprinzip angewandt werden kann. Dies bedeutet, dass das Bundesorgan die internationale Organisation oder den anderen Staat grundsätzlich anfragen sollte, ob sie respektive er Einwände gegen die Zugänglichmachung eines Dokuments haben.

Der Beauftragte erachtet es im vorliegenden Fall für angebracht, dass das Bundesamt einen allfälligen Zugang zur Stellungnahme des UNHCR in Absprache mit diesem gewährt respektive verweigert.

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

1. In Bezug auf die einzelnen Dokumente:

   1.1. Bundesratsantrag:
   Das Bundesamt für Migration gewährt keinen Zugang.

   1.2. Übermittlungsblatt zum Bundesratsantrag:
   Das Bundesamt für Migration gewährt keinen Zugang.

   1.3. Anlage 4 zum Bundesratsantrag «Die geltenden und revidierten Safe Country-Beurteilungskriterien im Vergleich»:
   Das Bundesamt für Migration gewährt vollumfänglichen Zugang.

   1.4. Anlage 5 zum Bundesratsantrag «Beurteilung der Eignung zur Bezeichnung als sichere Herkunftsstaaten von Benin, Kroatien, Mali, Moldawien (ohne Transnistrien), Montenegro und der Ukraine»
   Das Bundesamt für Migration gewährt einen teilweisen Zugang gemäss Anhang 1.

   1.5. Stellungnahme der Asylrekurskommission im Rahmen der Ämterkonsultation:
   Das Bundesamt für Migration gewährt vollumfänglichen Zugang.

   1.6. Stellungnahme des EDA im Rahmen der Ämterkonsultation:
   Das Bundesamt für Migration gewährt einen teilweisen Zugang gemäss Anhang 2.

   1.7. Stellungnahme des UNHCR:
   Das Bundesamt für Migration klärt beim UNHCR ab, ob dieses Einwände gegen die Zugänglichmachung seiner Stellungnahme vom 27. Oktober 2006 hat. Das Bundesamt gewährt den Zugang entsprechend der Antwort des UNHCR.

2. Das Bundesamt für Migration erlässt eine Verfügung nach Art. 5 des Verwaltungsverfahrensgesetzes, wenn es in Abweichung von Ziffer 1 den Zugang nicht gewähren will.

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

3. Die Antragstellerin kann innerhalb von 10 Tagen nach Erhalt dieser Empfehlung beim Bundesamt für Migration den Erlass einer Verfügung nach Artikel 5 des Verwaltungsverfahrensgesetzes verlangen (Art. 15 Abs. 1 BGÖ).

   Gegen diese Verfügung kann die Antragstellerin beim Bundesverwaltungsgericht Beschwerde führen (Art. 16 BGÖ).

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

5. Die Empfehlung wird eröffnet:

- X

- Bundesamt für Migration

  3003 Bern-Wabern

Hanspeter Thür

4.11 Empfehlung an die Eidgenössische Technische Hochschule: «Transfettsäuren»

Bern, den 18. September 2007

Empfehlung

gemäss

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

zum Schlichtungsantrag von

Antragsteller X
und
Antragstellerin Z

gegen

Eidgenössische Technische Hochschule ETHZ,
Zürich

I. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte stellt fest:

1. Am 6. Februar 2007 reichte der Antragsteller X (Medien) beim Bundesamt für Gesundheit (BAG) ein Gesuch um Zugang zu einer «Detailliste» ein, die in Zusammenhang mit der TransSwissPilot Studie der Eidgenössischen Technischen Hochschule Zürich (ETHZ) erstellt worden ist. Es handelt sich dabei um eine Auflistung von Lebensmittelprodukten (nachfolgend Produkteliste), die auf ihren Gehalt an «*trans*-Fettsäuren»(TFS) getestet wurden. Die Studie zeigt auf, dass in der Schweiz erhältliche Nahrungsmittel teilweise einen hohen Anteil an so genannten TFS enthalten.[1] Das BAG teilte X am 7. Februar 2007 per Mail mit, dass sich das BAG zwar an der Studie finanziell beteiligt hat, aber nicht über die einzelnen Resultate (im Sinne der Produkteliste) verfüge. Des Weiteren führte das BAG aus, dass es «an einer generellen Aussage interessiert [war] und (…) abklären (wollte), ob Handlungsbedarf besteht. Dieser Handlungsbedarf hat sich klar bestätigt.» Das BAG verwies in seinem Schreiben auf ein Webdokument mit den nächsten Schritten, um die «Situation zu verbessern.»

   Ebenfalls am 6. Februar 2007 reichte X bei der ETHZ ein entsprechendes Zugangsgesuch ein. Diese verweigerte dem Antragsteller am 9. Februar 2007 den Zugang und führte dazu aus, dass eine Veröffentlichung der Produkteliste konkret bedeute, «40 Produkte bekannt zu geben, bei denen erhöhte TFS registriert wurden. Es ist aber davon auszugehen, dass heute möglicherweise noch Hunderte von Produkten mit zu hohen TFS-Werten in den Regalen stehen. Die Sicherheit der Konsumentinnen und Konsumenten wäre somit trügerisch, weil die Auswahl der untersuchten Produkte gemäss Ziel der Pilotstudie nicht systematisch erfolgte. Somit würde das Geschäft A oder ein Produkt B, das – zufälligerweise – auf der «schwarzen Liste» steht, gemieden, das Geschäft Y, das möglicherweise noch höhere Werte in seinen Produkten aufweist, aber nicht in die Untersuchung einbezogen wurde, bliebe unbehelligt.»

2. Die Antragstellerin Z (Interessenvertretung) reichte am 8. März 2007 beim Bundesamt für Gesundheit BAG ein Gesuch um Zugang zur besagten Studie ein. Z wünschte «Einblick (…) in die detaillierten Ergebnisse» und beantragte Zugang zur «ungekürzten TransSwissPilot Studie». Das BAG antwortete am 22. März 2007, dass die ETHZ-Studie nicht im Auftrag des BAG durchgeführt worden sei und das BAG sich nur finanziell daran beteiligt hatte. Das Bundesamt verwies

[1] Internet-Dokument des BAG vom 30.01.2007 «Transfette: Bundesamt für Gesundheit diskutierte mit ETH-Experten und Lebensmittelindustrie konkrete Lösungswege»

auf eine von der ETHZ im Internet publizierte Zusammenfassung der Studie. Das BAG hielt überdies fest, dass es selber nicht im Besitz der Studie sei, sondern lediglich einer «unvollständigen Tabelle, welche einige der getesteten Produkte ohne nähere Angaben enthält.» Es handle sich dabei um ein nicht fertig gestelltes Dokument, welches gemäss Art. 3 Abs. 2 Bst. b des Bundesgesetzes über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsgesetz, BGÖ, SR 152.3) kein amtliches Dokument sei. Zudem müsse nach Ansicht des BAG der Zugang zu dieser Produkteliste aufgrund des Fabrikationsgeheimnisses gemäss Art. 7 Abs. 1 Bst. g BGÖ verweigert werden, da der Hersteller nicht verpflichtet sei, den TFS-Gehalt seiner Produkte offen zu legen. Der TFS-Gehalt bilde Teil der Rezeptur und unterliege daher dem Fabrikationsgeheimnis der Produktehersteller.

3. Der Antragsteller X reichte mit Mail vom 12. Februar 2007 und die Antragstellerin Z mit Schreiben vom 4. April 2007 (eingegangen am 5. April 2007) einen Schlichtungsantrag beim Eidg. Datenschutz- und Öffentlichkeitsbeauftragten (der Beauftragte) ein. Da sich die beiden Schlichtungsanträge auf die gleiche Studie beziehen, behandelt der EDÖB sie gemeinsam in einem Schlichtungsverfahren.

4. Im Rahmen des Schlichtungsverfahrens forderte der Beauftragte die ETHZ zu einer Stellungnahme auf. Die ETHZ führte für die Zugangsverweigerung in Bezug auf die vollständige Studie das Vorliegen eines Geschäftsgeheimnisses der ETHZ sowie in Bezug auf die Produkteliste das Fabrikationsgeheimnis der Produktehersteller an. Sie begründete dies folgendermassen:

Zum Geschäftsgeheimnis der ETHZ

Die ETHZ machte geltend, dass ein Geschäftsgeheimnis der ETHZ vorliege, da die Studie im Rahmen eines Projektes durchgeführt worden sei und die Resultate für eine Publikation in einer Fachzeitschrift verarbeitet werden müssten. Das Manuskript zur Publikation werde im Vorfeld zu einer internationalen Tagung (7th International Food Data Conference vom 21. – 24. Oktober 2007 in Sao Paulo) per Mitte Oktober 2007 eingereicht, und die Publikation erfolge voraussichtlich im Jahre 2008, wobei der genaue Zeitpunkt der Publikation nicht bekannt und auch nicht abschätzbar sei. Dabei sei eine detaillierte Identifikation der Produkte und der Hersteller nicht vorgesehen. Zumindest bis zum Zeitpunkt der Artikelpublikation könne und wolle die ETHZ die Resultate nicht zugänglich machen (und nach diesem Zeitpunkt liege ein Fabrikationsgeheimnis der Produktehersteller vor). Es sei international anerkannte Usanz,

dass Forschungsergebnisse vor ihrer Publikation von den Verantwortlichen unter Verschluss gehalten werden, da ansonsten Dritte über Art und Zeitpunkt der Publikation der Forschungsergebnisse bestimmen können. Den Forschern würde so die Herrschaft über die von ihnen erarbeiteten Daten und Erkenntnisse genommen. Zudem könne dadurch die Stellung im internationalen Wettbewerb untergraben werden, was ein Eingriff in die Wissenschaftsfreiheit von Art. 20 der Bundesverfassung sei.

Weiter führt die ETHZ mit Verweis auf die Botschaft zum Öffentlichkeitsgesetz aus, dass der Begriff des Geschäftsgeheimnisses weit zu verstehen sei und darunter auch laufende oder geplante Forschungsprojekte fallen.

Ausserdem sehe Art. 28 des Bundesgesetzes über die Forschung (FG; SR 420.1) vor, dass Forschungsergebnisse der Öffentlichkeit nur zugänglich seien, «soweit keine Interessen der Geheimhaltung (…) entgegenstehen.»

Zum Fabrikationsgeheimnis der Produktehersteller

Die ETHZ führte aus, dass ein Fabrikationsgeheimnis der Produktehersteller vorliege, weil die Studie die Zusammensetzung der Produkte untersuche. Gemäss Botschaft zum Öffentlichkeitsgesetz dürfe das Öffentlichkeitsprinzip nicht dazu führen, dass Fabrikationsgeheimnisse ausserhalb der Verwaltung stehenden Dritten offenbart werden. Durch die Veröffentlichung der Produkteliste würde in den wirtschaftlichen Wettbewerb eingegriffen. Zudem seien die Produkte willkürlich auswählt worden. Solange keine Deklarationspflicht für TFS bestehe, sei ein Hersteller auch nicht verpflichtet, den TFS-Gehalt offenzulegen. Somit unterliege der TFS-Gehalt einzelner Produkte dem Fabrikationsgeheimnis.

Um Schadenersatzforderungen von Seiten der Produzenten zu vermeiden, lehne die ETHZ eine Veröffentlichung der Produkteliste ab.

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.[2] 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. Die Antragstellenden haben ein Zugangsgesuch nach Art. 6 BGÖ beim BAG respektive bei der ETHZ eingereicht und ablehnende Antworten erhalten. Als Teilnehmende an einem vorangegangenen Gesuchsverfahren sind sie zur Einreichung eines Schlichtungsantrags berechtigt. Die Schlichtungsanträge wurden 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 Detail obliegt alleine dem Beauftragten.[3]

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

B. Sachlicher Geltungsbereich

1. Das Öffentlichkeitsgesetz findet Anwendung auf die *Dienststellen der Bundesverwaltung* (Art. 2 Abs. 1 Bst. a BGÖ). Die ETHZ als Verwaltungseinheit der *dezentralen* Bundesverwaltung fällt demnach in den Geltungsbereich des Öffentlichkeitsgesetzes.[4]

2. Die ETHZ verweigerte den Zugang zur Produkteliste mit der Begründung, die Studie samt der dazu gehörenden Dokumente und Resultate seien als Geschäftsgeheimnis zu betrachten, welches bis zur Veröffentlichung der Studie durch die Wissenschaftler Vorrang vor dem Öffentlichkeitsprinzip habe.

[2] BBl 2003 2023
[3] BBl 2003 2024
[4] BBl 2003 1986

Laufende oder geplante Forschungsprojekte können tatsächlich unter den Geheimnisbegriff der Ausnahmebestimmung von Art. 7 Abs. 1 Bst. g BGÖ fallen.[5] Der Beauftragte kann sich daher grundsätzlich der Haltung der ETHZ anschliessen, dass in Bezug auf Studien ein Geschäftsgeheimnis der ETHZ vorliegen *kann*. In Analogie zu Art. 9 Abs. 2 des Bundesgesetzes über das Urheberrecht und verwandte Schutzrechte (SR 231.1) muss der Wissenschaft und der Forschung tatsächlich bis zu einem bestimmten Grad das Recht zugestanden werden, selber darüber zu bestimmen, ob, wann und wie eine Studie erstmals veröffentlicht werden soll. Bis zu diesem Zeitpunkt muss das Öffentlichkeitsprinzip grundsätzlich hinter dem Geschäftsgeheimnis der Wissenschaftler zurücktreten. Hingegen muss eine Studie spätestens dann als veröffentlicht gelten, wenn der Wissenschaftler sie selber zugänglich macht oder einer Veröffentlichung zustimmt. Ab diesem Zeitpunkt kann er sich nicht mehr auf das Geschäftsgeheimnis berufen.

Das Öffentlichkeitsgesetz sieht für diese Fälle die Möglichkeit vor, dass der Zugang zu einem amtlichen Dokument aufgeschoben werden kann (Art. 7 Abs. 1 BGÖ).

3. Vorliegend hat die ETHZ nicht nur selber in allgemeiner Form im Internet[6] über die Studie berichtet (Text datiert von Ende Januar 2007), sondern die Verantwortlichen gaben auch in der Sendung MTW Menschen, Technik, Wissenschaft des Schweizer Fernsehens vom 4. Januar 2007 Einzelheiten der Studie bekannt.[7] Unter anderem wird im Beitrag auch ein Vergleich zwischen einer Produktgruppe mit einer grossen Menge an TFS und einer Produktgruppe mit einer geringen Menge gezeigt. Dabei sind die Produkte und die einzelnen Marken zweifelsfrei erkennbar. Es muss davon ausgegangen werden, dass das Forschungsteam die Produkte zusammengestellt hat.

4. Die Argumentation der ETHZ, dass die gesamte Studie bis zum Zeitpunkt der Publikation in der Fachzeitschrift Teil des Geschäftsgeheimnisses im Sinne des Öffentlichkeitsgesetzes sei und daher kein Zugang gewährt werden könne, erscheint dem Beauftragten aus folgenden Gründen nur beschränkt haltbar:

   - Durch die aktive Mitwirkung in einer Fernsehsendung haben die Forschenden einer Veröffentlichung der Studie in Teilen zugestimmt.

[5] so explizit BBl 2003 2012
[6] http://www.swissfir.ethz.ch/services/zutaten/tfs/index
[7] http://www.sf.tv/sf1/mtw/index.php?docid=20070104; Beitrag mit dem Titel: Transfettsäuren: Das Herzinfarktrisiko im Blätterteig

- Für den Vergleich zweier Produktgruppen haben die Forschenden einige Produkte hervorgehoben.
- Es ist davon auszugehen, dass weitere Teile der Studie an der internationalen Tagung veröffentlicht werden.

Der Beauftragte kommt daher zum Schluss, dass die ETHZ den Zugang zur TransSwissPilot Studie (exklusiv Produkteliste, siehe nachfolgende Ziffern) gestützt auf das Geschäftsgeheimnis von Art. 7 Abs. 1 Bst. g BGÖ bis nach der internationalen Tagung in Sao Paulo aufschieben kann. Danach muss der Antragstellerin Z der Zugang zur ungekürzten TransSwissPilot Studie gewährt werden.

5. In Bezug auf die Produkteliste mit den TFS-Gehalten in Lebensmitteln (Teildokument aus der Studie) macht die ETHZ geltend, ein Fabrikationsgeheimnis der Produktehersteller liege vor, «weil die Studie die Zusammensetzung der Produkte untersuchte».

   Gemäss Art. 7 Abs. 1 Bst. g BGÖ kann der Zugang zu amtlichen Dokumenten beschränkt werden, wenn dadurch ein Fabrikationsgeheimnis offenbart werden könnte. Ein Fabrikationsgeheimnis kann nur vorliegen, wenn die zu schützenden Informationen tatsächlich auch *Geheimnischarakter*[8] aufweisen. Wir gehen davon aus, dass Tests zur Feststellung des TFS-Gehalts von Lebensmitteln von jedem spezialisierten Labor durchgeführt werden können. Nach Ansicht des Beauftragten können daher die von der ETHZ in den getesteten Lebensmitteln festgestellten TFS-Gehalte nicht als Fabrikationsgeheimnisse der Produktehersteller bezeichnet werden.

   Es ist richtig, dass keine gesetzliche Deklarationspflicht für TGS-Gehalte in Lebensmitteln besteht. Diese Tatsache darf aber nicht mit einer Zugangsverweigerung gleichgesetzt werden. Die Gründe für eine Beschränkung des Zugangs sind abschliessend im Öffentlichkeitsgesetz abgeführt. Eine fehlende Deklarationspflicht fällt nicht darunter.

   Die ETHZ kann den Zugang zur Produkteliste nicht gestützt auf das Fabrikationsgeheimnisses der Produktehersteller von Art. 7 Abs. 1 Bst. g BGÖ verweigern.

[8] Bundesamt für Justiz: «Umsetzung des Öffentlichkeitsprinzips in der Bundesverwaltung: Häufig gestellte Fragen» vom 29.06.2006

6. Da nach Ansicht des Beauftragten weder ein Geschäftsgeheimnis der ETHZ noch ein Fabrikationsgeheimnis der Produktehersteller vorliegt, steht der von der ETHZ ins Feld geführte Art. 28 des Forschungsgesetzes der Zugänglichmachung der Produkteliste grundsätzlich nicht entgegen.

7. Im Folgenden gilt es zu prüfen, ob sich die Beschränkung des Zugangs zum gewünschten Dokument aufgrund anderer Bestimmungen des Öffentlichkeitsgesetzes rechtfertigt. Die Produkteliste enthält die Namen respektive Firmen der Produkthersteller. Es muss daher eine Beurteilung unter dem Aspekt des Zugangs *zu Dokumenten mit Personendaten Dritter* vorgenommen werden. Die im fraglichen Dokument aufgeführten Produzenten sind Personendaten im Sinne von Art. 3 Bst. a des Bundesgesetzes über den Datenschutz (DSG, SR 235.1). Es stellt sich daher die Frage, ob die Produkthersteller aus Gründen des Persönlichkeitsschutzes ein Recht darauf haben, *anonym* zu bleiben.

   Gemäss Art. 7 Abs. 2 BGÖ können im Rahmen der Zugangsgewährung ausnahmsweise auch Personendaten von Dritten bekannt gegeben, wenn an deren Bekanntgabe ein *überwiegendes öffentliches Interesse* besteht. Art. 6 Abs. 2 VBGÖ enthält eine nicht abschliessende Auflistung von Fällen, in denen das öffentliche Interesse am Zugang das Interesse der Drittperson am Schutz ihrer Privatsphäre überwiegt. Explizit wird dabei auch das Zugänglichmachen von amtlichen Dokumenten zum Schutz der öffentlichen Gesundheit aufgeführt (Art. 6 Abs. 2 Bst. b BGÖ). Zur Feststellung des überwiegenden öffentlichen Interesses muss eine Interessenabwägung zwischen dem Schutz der Privatsphäre des Dritten und dem öffentlichem Interesse am Zugang zum fraglichen Dokument vorgenommen werden (Art. 6 Abs. 1 VBGÖ).

8. Entscheidend für die Beurteilung der Frage, welches Interesse eine Privatperson an der *Geheimhaltung* ihres Namens respektive ihrer Firma hat, sind u.a. ihre Präsenz in der Öffentlichkeit, die Umstände der Informationsbeschaffung sowie die Art der betroffenen Daten.[9]

   Bei den betroffenen Daten handelt es sich nicht um besonders schützenswerte Personendaten im Sinne von Art. 3 Bst. c DSG. Die Produzenten treten auf dem Markt als Anbieter für die gestesteten Lebensmittel auf, welche für jedermann frei erwerbbar sind. Die ETHZ untersuchte für ihre Studie eine

[9] zu den massgeblichen Kriterien der Interessenabwägung s. Brunner «Öffentlichkeit der Verwaltung und informationelle Selbstbestimmung: Von Kollisionen und Verkehrsregeln», Ziff. IV 3; in «Selbstbestimmung und Recht», Festgabe für Rainer J. Schweizer, Schulthess 2003

grosse Anzahl von Lebensmitteln (120 Produkte) auf ihren TFS-Gehalt. Dabei wurden innerhalb der Lebensmittelgruppe mehrere Produkte getestet sowie eine ausgewogene Zahl verschiedener Produzenten berücksichtigt.

9. Bei der *Gewichtung des öffentlichen Interesses am Zugang* zum fraglichen Dokument kommt dem Schutz spezifischer öffentlicher Interessen eine besondere Bedeutung zu. Im vorliegenden Fall geht es nicht alleine um die Schaffung von Transparenz in Bezug auf die Verwaltungstätigkeit, sondern darüber hinaus um den *spezifischen Schutz der öffentlichen Gesundheit*. Die ETHZ hält in ihrer Internetpublikation zum Thema fest, dass bereits eine «geringere Aufnahme (an TFS) als gesundheitsbeeinträchtigend gilt» und dass selbst beim «Befolgen der Empfehlungen der Schweizer Lebensmittelpyramide eine gesundheitsbeeinträchtigende Zufuhr an TFS möglich» sei.[10] Aussagen gleichen Inhalts wurden im erwähnten TV-Beitrag gemacht.

10. Bei der *Interessenabwägung im vorliegenden Fall* gilt es auch zu berücksichtigen, welche Konsequenzen die Bekanntgabe der Produkteliste für die Produzenten hätte. Es ist möglich, dass das Zugänglichmachen (und eine spätere Veröffentlichung) der Produkteliste das Verhältnis der betroffenen Produzenten zu Mitkonkurrenten auf dem Markt beeinflussen könnte. Allerdings kann dabei die Tatsache nicht ausser Acht gelassen werden, dass derartige Vergleichs- und Qualitätstests von Lebensmitteln regelmässig auch von privater Seite (insbesondere von Konsumentenorganisationen, -zeitschriften, -sendungen in Radio oder Fernsehen) in Auftrag gegeben und publiziert werden. Der Auftraggeber dieser Tests wird dabei in aller Regel nicht mit Schadenersatzforderungen konfrontiert, sondern die Tests führen in den überwiegenden Fällen dazu, dass die Hersteller qualitative Verbesserungen an ihren Produkten vornehmen. Entscheidend scheint dem Beauftragten insbesondere, dass Produzenten, die ihre Produkte auf dem Markt anbieten, bis zu einem gewissen Grad hinnehmen müssen, dass Aussagen bezüglich der Qualität und der inhaltlichen Zusammensetzung ihrer Produkte gemacht werden.

    Diskussionen über die Auswirkungen von TFS auf die Gesundheit werden in der Wissenschaft und in den Medien seit einigen Jahren geführt. In der Wissenschaft scheint die Tatsache unbestritten, dass TFS gesundheitsbeeinträchtigend wirken. Generell wird der Volksgesundheit in unserer heutigen Gesellschaft ein immer grösserer Stellenwert eingeräumt. Vor diesem Hintergrund ist zu fordern, dass Konsumenten nicht nur in Teilen, sondern in vollem Umfang Zugang zu (abgeschlossenen und veröffentlichten) Studien betreffend

[10] http://www.swissfir.ethz.ch/services/zutaten/tfs/TransSwissPilot_Summary_Final_Web.pdf; S. 3

Gesundheitsrisiken haben sollten. Konsumenten sollten in Erfahrung bringen können, welche Produkte gesundheitsbeeinträchtigende Inhaltsstoffe enthalten. Zudem sei hier nochmals daran erinnert, dass das Öffentlichkeitsgesetz von der Bundesverwaltung Transparenz verlangt und dem Bürger Zugang zu amtlichen Dokumenten verschafft. Die ETHZ ist eine Bundesstelle (und als solche dem Öffentlichkeitsprinzip verpflichtet) und die TFS-Studie (samt den in diesem Zusammenhang erstellten schriftlichen Abhandlungen und Tabellen) sind zweifelsfrei als amtliche Dokumente im Sinne des Öffentlichkeitsgesetzes zu qualifizieren. Das zu beurteilende Dokument enthält eine Liste mit den TFS-Gehalten von Lebensmitteln. Diese Informationen können dazu beitragen, dass sich die interessierten Konsumenten bewusst mit ihrer Gesundheit auseinander setzen und gesundheitsbeeinträchtigende Lebensmittel meiden. Das Zugänglichmachen der Produkteliste mit den TFS-Gehalten dient dem Schutz der öffentlichen Gesundheit. Dieses öffentliche Interesse überwiegt jenes der Produzenten an einer Geheimhaltung ihrer Personendaten, da sie sich als Marktteilnehmer einer wissenschaftlichen und objektiven Kritik aussetzen lassen müssen und darüber hinaus die konkrete Beeinträchtigung ihrer Privatsphäre durch das Zugänglichmachen der Produkteliste als gering eingestuft wird.

11. *Aufgrund der vorangehenden Ausführungen gelangt der Beauftragte zur Überzeugung, dass vorliegend ein überwiegendes öffentliches Interesse am Zugang zur Produkteliste besteht und demnach der Zugang zur Produkteliste gewährt werden sollte.*

    Allerdings kann er dabei nicht ausser Acht lassen, dass das Öffentlichkeitsgesetz in den Fällen, in denen der Zugang zu Dokumenten mit Personendaten Dritter gewährt werden soll, explizit verlangt, dass die betroffenen Dritten über den geplanten Zugang informiert und um eine Stellungnahme gebeten werden (so genannte Anhörung gemäss Art. 11 BGÖ). Die ETHZ hat aufgrund ihrer Einschätzung der Sachlage darauf verzichtet.

    Aufgrund der komplexen Sachlage empfiehlt der Beauftragte Folgendes Vorgehen:

    - Vor der empfohlenen Zugänglichmachung der Liste muss jeder Produktehersteller von der ETHZ über die anstehende Zugänglichmachung der Produkteliste samt Produktehersteller informiert werden.
    - Die ETHZ gibt ihnen 10 Tage Gelegenheit zur Stellungnahme.
    - Danach gewährt die ETHZ umgehend Zugang zur Produkteliste und den Namen und Firmen der Produzenten.

- Spricht sich ein Produktehersteller fristgerecht gegenüber der ETHZ gegen die Bekanntgabe seines Namens respektiver seiner Firma aus, so kann er gleichzeitig innerhalb von 20 Tagen einen Schlichtungsantrag gemäss Art. 13 BGÖ stellen. Der Beauftragte wird in einem weiteren Schlichtungsverfahren auf neue Vorbringen des Betroffenen eingehen, soweit sie über die hier bereits vorgenommene Interessenabwägung hinausgehen.

12. Das BAG teilte den Antragstellenden jeweils mit, dass es lediglich den Auftrag zur Studie und Geld zur Finanzierung gegeben habe, aber nicht im Besitz der fertig gestellten Dokumente sei. Im Rahmen des Schlichtungsverfahrens stellte der Beauftragte fest, dass die von der ETHZ und dem BAG eingereichte Produktliste den *identischen Inhalt* aufweisen und das *gleiche Datum* tragen. Damit steht für den Beauftragten fest, dass das BAG entgegen seiner Aussage *im Besitz des definitiven Dokuments* war.

    Vorweg gilt es festzuhalten, dass die ETHZ als Urheberin des Dokuments für die Beurteilung des Zugangsgesuchs zuständig ist (Art. 10 Abs. 1 BGÖ). Zu Recht hat das BAG die Gesuchstellenden darauf hingewiesen. Losgelöst von dieser Frage sollte nach Ansicht des Beauftragten in Zukunft aber Folgendes beachtet werden: Zum einen sollte ein Amt die Gesuche von Amtes wegen an die zuständige Behörde weiterleiten.[11] Zum anderen ist zu fordern, dass ein Bundesamt im Zweifelsfall mit dem Ersteller eines Dokuments abklärt, ob es im Besitz eines fertig gestellten Dokuments im Sinne von Art. 5 BGÖ ist und die Gesuchsteller entsprechend korrekt informiert.

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

1. In Bezug auf folgende Dokumente:

    1.1. TransSwissPilot Studie:

    Die ETHZ schiebt den Zugang zur TransSwissPilot Studie (exklusiv Produkteliste, s. nachfolgende Ziffer 1.2) gestützt auf das Geschäftsgeheimnis von Art. 7 Abs. 1 Bst. g BGÖ bis nach der internationalen Tagung in Sao Paulo auf. Danach gewährt sie der Antragstellerin Z den Zugang zur ungekürzten TransSwissPilot Studie (exklusiv Produkteliste, s. nachfolgende Ziffer 1.2).

[11] so explizit BBl 2003 2019, letzter Abschnitt

1.2.Produkteliste:

Die ETHZ gewährt den Antragstellenden den Zugang zur Produkteliste. Vorgängig führt die ETHZ bei allen Produktherstellern eine Anhörung gemäss Art. 11 BGÖ durch. Danach gewährt die ETHZ den Zugang zur Produkteliste. Ist der Betroffene damit nicht einverstanden, kann er gemäss Art. 13 BGÖ ein Schlichtungsantrag beim Beauftragten einreichen.

2. Die ETHZ erlässt eine Verfügung nach Art. 5 des Verwaltungsverfahrensgesetzes, wenn sie in Abweichung von Ziffer 1 den Zugang nicht gewähren will.

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

3. Die Antragstellenden können innerhalb von 10 Tagen nach Erhalt dieser Empfehlung bei der ETHZ den Erlass einer Verfügung nach Artikel 5 des Verwaltungsverfahrensgesetzes verlangen (Art. 15 Abs. 1 BGÖ).

   Gegen diese Verfügung können die Antragstellenden beim Bundesverwaltungsgericht Beschwerde führen (Art. 16 BGÖ).

4. Diese Empfehlung wird veröffentlicht. Zum Schutz der Personendaten der am Schlichtungsverfahren Beteiligten werden die Namen der Antragstellenden anonymisiert (Art. 13 Abs. 3 VBGÖ).

5. Die Empfehlung wird eröffnet:

   - Antragsteller X
   - Antragstellerin Z
   - Eidg. Technische Hochschule Zürich
     Rämistr. 101
     8092 Zürich

Hanspeter Thür

4.12 Empfehlung an die PostFinance, Schweizerische Post: «PostFinance»

Bern, den 21. September 2007

Empfehlung

gemäss

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

zum Schlichtungsantrag von

X
(Antragsteller)

gegen

PostFinance,
Schweizerische Post, Bern

I. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte stellt fest:

1. Der Antragsteller stellte per Mail bei der PostFinance ein Gesuch um «Einsicht in ein amtliches Dokument (…), dass [sic!] in statistischer Art und Weise die Missbrauchsfälle aufzeigt, die mit der Postcard begangen worden sind.»

2. Die PostFinance teilte dem Antragsteller am 16. Februar 2007 ebenfalls per Mail mit, dass die Zahlen zu den Missbrauchsfällen vertraulich seien und nicht veröffentlicht würden. Ausserdem gelange das Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsgesetz, BGÖ; SR 152.3) in diesem Fall nicht zur Anwendung.

3. Der Antragsteller reichte am 16. Februar 2007 einen Schlichtungsantrag beim Eidg. Datenschutz- und Öffentlichkeitsbeauftragten (der Beauftragte) ein.

   Im Rahmen des Schlichtungsverfahrens forderte der Beauftragte die Schweizerische Post auf darzulegen, weshalb die PostFinance vorliegend nicht dem Öffentlichkeitsgesetz unterstellt sei.

   In ihrer Stellungnahme vom 23. August 2007 teilte die Post dem Beauftragten u.a. mit, dass «Die Schweizerische Post (…) eine selbständige Anstalt des öffentlichen Rechts mit Rechtspersönlichkeit (ist) und deshalb vom persönlichen Geltungsbereich des BGÖ erfasst (ist), soweit sie Erlasse oder erstinstanzlich Verfügungen im Sinn von Art. 5 VwVG erlässt.» Im vorliegenden Fall sei «die Post jedoch nicht vom persönlichen Geltungsbereich erfasst, da die Post im Bereich der Leistungen von PostFinance weder Erlasse noch erstinstanzlich Verfügungen im Sinne von Art. 5 VwVG erlassen kann.» Die Post sei nur in den folgenden vier Bereichen noch hoheitlich tätig resp. erlasse erstinstanzliche Verfügungen:

   - Bundespersonalrecht inkl. Gleichstellungsgesetz (Art. 34 BPG bzw. Ziffer 20 Anhang 6 GAV Post),
   - Beschaffungsrecht, sofern sie als Auftraggeberin gemäss Art. 2 BoeB qualifiziert werden können,
   - Platzierung von Kundenbriefkästen (Art. 18 PG),
   - Gewähren von Vorzugspreisen für die Beförderung von Zeitungen und Zeitschriften (Art. 18 PG).

Im Weiteren führte die Post aus, dass sie in sämtlichen anderen Geschäftsbereichen weder hoheitlich tätig sei noch Verfügungen erlassen könne, und daher unterstehe sie vorliegend auch nicht dem Öffentlichkeitsgesetz. Zudem vertrat sie die Ansicht, dass «Auf den Schlichtungsantrag (…) bereits mangels Anwendbarkeit des BGÖ nicht einzutreten (ist).»

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

1. Das Bundesgesetz über das Verwaltungsverfahren (VwVG, SR 172.021) findet keine Anwendung auf das Schlichtungsverfahren gemäss Art. 13 BGÖ. In Fällen, in denen nicht bereits von Beginn weg *zweifelsfrei* feststeht, dass das Öffentlichkeitsprinzip nicht zur Anwendung gelangt, tritt der Beauftragte daher 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).

2. Das Öffentlichkeitsgesetz gilt unter anderem auch für nicht der Bundesverwaltung angehörende Organisationen und Personen des öffentlichen oder privaten Rechts, *soweit sie Erlasse oder erstinstanzlich Verfügungen* im Sinn von Artikel 5 des Bundesgesetzes über das Verwaltungsverfahren (SR 172.021) erlassen (s. Art. 2 Abs. 1 Bst. b BGÖ).

   Die Schweizerische Post *kann* in diese Kategorie fallen, allerdings nur wenn sie Verfügungen erlässt. Wie von der Post in ihrer Stellungnahme vom 23. August 2007 dargelegt, *ist dies im Geschäftsbereich PostFinance nicht der Fall*. Der Beauftragte schliesst sich den Ausführungen der Schweizerischen Post in Bezug auf den persönlichen Geltungsbereich nach Art. 2 BGÖ vollumfänglich an.

   Das Öffentlichkeitsgesetz findet auf den vorliegenden Fall keine Anwendung.

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

1. Das Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsgesetz, BGÖ) findet keine Anwendung auf den Geschäftsbereich PostFinance der Schweizerischen Post. Es besteht daher kein Anspruch auf Zugang zu Unterlagen betreffend die Missbrauchsfälle bei der Postcard.

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

3. Die Empfehlung wird eröffnet:

   - X

   - Die Schweizerische Post
     Rechtsdienst
     Viktoriastrasse 21
     3030 Bern

Jean-Philippe Walter

4.13 Empfehlung der Swissmedic, Schweizerisches Heilmittelinstitut: «Zulassung Arzneimittel»

Bern, den 11. Oktober 2007

Empfehlung

gemäss

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

zum Schlichtungsantrag von

Antragstellerin A
und
Antragstellerin B

gegen

Swissmedic,
Schweizerisches Heilmittelinstitut, Bern

I. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte stellt fest:

1. Die Antragstellerin A (Pharmaunternehmen) sandte am 16. und 17. Januar 2007 vier E-Mails (Zugangsgesuche 1 - 4) an Swissmedic und wollte wissen, ob Zulassungsgesuche für Arzneimittel (Neuanmeldungen oder Generika) mit vier bestimmten Wirkstoffen bei Swissmedic eingereicht worden seien (s. Art. 11f. des Bundesgesetzes über Arzneimittel und Medizinprodukte, Heilmittelgesetz, HMG; SR 812.21). Sie wollte insbesondere wissen, ob Zulassungsgesuche für Neuanmeldungen oder Generika eines Medikaments mit dem Wirkstoff Oxycontin (Oxycodonhydrochlorid) eingereicht worden seien (Zugangsgesuch 1)[1].

2. Swissmedic teilte der Antragstellerin A am 8. Februar 2007 mit, dass Dokumente erst zugänglich gemacht werden könnten, wenn der politische oder administrative Entscheid, für den sie die Grundlage darstellen, getroffen sei (Art. 8 Abs. 2 des Bundesgesetzes über das Öffentlichkeitsprinzip der Verwaltung, Öffentlichkeitsgesetz, BGÖ; SR 152.3). Die Daten und Dokumente, zu denen Zugang verlangte werde, würden unter diese Bestimmung fallen. Swissmedic vertrat die Ansicht, dass der Antragstellerin A «allfällige Dossiers von Konkurrenten zum heutigen Zeitpunkt nicht zugänglich gemacht werden können.»

   Swissmedic behielt sich eine eventuelle Prüfung der Ausnahmebestimmungen gemäss Art. 7 BGÖ zu einem späteren Zeitpunkt ausdrücklich vor.

3. Die Antragstellerin B (Pharmaunternehmen) verlangte am 19. Januar 2007 ebenfalls Zugang zu sämtlichen Dokumenten «betreffend ein Gesuch um Herstellung (Art. 5 ff. Heilmittelgesetz [SR 812.21, HMG]), Marktzulassung (Art. 9 ff. HMG), Ein- beziehungsweise Ausfuhr (Art. 18 ff. HMG) oder den Grosshandel (Art. 28 f. HMG) mit dem Wirkstoff Oxycodonhydrochlorid enthaltenen Arzneimittel, so dass für die Gesuchstellerin zumindest ersichtlich ist, wer die interessierenden Gesuche eingereicht hat, ob ein Muster eingereicht worden ist oder ob Swissmedic dazu aufgefordert hat, ein Muster einzureichen und welches allfällige Lieferanten oder Abnehmer des Arzneimittels sind.»

   Die Antragstellerin B wollte insbesondere mitgeteilt bekommen, ob eines von vier namentlich aufgeführten Unternehmen ein Zulassungsgesuch für Arzneimittel gemäss Heilmittelgesetz eingereicht hatte.

[1] Im Folgenden gilt es Zugangsgesuche nach Öffentlichkeitsgesetz und Zulassungsgesuche für Arzneimittel nach Heilmittelgesetz auseinander zu halten.

4. Am 8.Februar 2007 teilte Swissmedic der Antragstellerin B mit, dass der Zugang aufgrund von Art. 8 Abs. 2 BGÖ aufgeschoben werde. Auch hier führte Swissmedic aus, «dass allfällige Dossiers von Konkurrenten der Gesuchstellerin zum heutigen Zeitpunkt nicht zugänglich gemacht werden können.»

   Swissmedic behielt sich wiederum eine eventuelle Prüfung der Ausnahmetatbestände gemäss Art. 7 BGÖ zu einem späteren Zeitpunkt vor.

5. Am 21. Februar 2007 reichte der Rechtsanwalt C im Namen der Antragstellerinnen A und B einen Schlichtungsantrag beim Eidg. Datenschutz- und Öffentlichkeitsbeauftragten (der Beauftragte) ein. Die Antragstellerinnen vertraten die Auffassung, dass aufgrund der Gesetzessystematik nur der Bundesrat berechtigt sei, sich auf Art. 8 Abs. 2 BGÖ zu berufen. Zudem solle mit der Bestimmung nur der (physische) Zugang zu den Dokumenten ausgeschlossen werden, nicht aber das Erteilen von Auskünften über den Inhalt solcher Dokumente.

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

A In Bezug auf die Zugangsgesuche 1 - 4 der Antragstellerin A

1. Die Antragstellerin A möchte von Swissmedic wissen, ob Zulassungsgesuche für Arzneimittel mit bestimmten Wirkstoffen eingereicht worden sind. Die Antragstellerin verlangt keinen Zugang zu allfälligen Zulassungsgesuchen, sondern möchte gemäss Wortlaut der Mails lediglich wissen, ob Zulassungsgesuche eingereicht respektive Arzneimittel zur Registrierung angemeldet wurden.

   Zugangsgesuche nach Art. 6 BGÖ sind all jene Anfragen, die sich auf ein bzw. mehrere *Dokumente im Sinne des Öffentlichkeitsgesetzes* beziehen. Keine Zugangsgesuche nach Öffentlichkeitsgesetz sind namentlich Anfragen, bei denen bloss allgemeine Auskünfte verlangt werden[2].

   Nach Ansicht des Beauftragten handelt es bei allen vier Anfragen der Antragstellerin A nicht um Zugangsgesuche nach Öffentlichkeitsgesetz. Das Öffentlichkeitsgesetz gelangt daher nicht zur Anwendung.

B. In Bezug auf das Zugangsgesuch der Antragstellerin B

[2] s. Bundesamt für Justiz, Umsetzung des Öffentlichkeitsprinzips in der Bundesverwaltung: Häufig gestellte Fragen, Ziffer 6.1

B.1. 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[3]. 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. Die Antragstellerin B hat ein Zugangsgesuch nach Art. 6 BGÖ bei Swissmedic eingereicht und eine ablehnende Antwort erhalten. Als Teilnehmende an einem vorangegangenen Gesuchsverfahren ist sie zur Einreichung von Schlichtungsanträgen 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 Detail obliegt alleine dem Beauftragten.[4]

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

[3] BBl 2003 2023
[4] BBl 2003 2024

B.2. Sachlicher Geltungsbereich

1. Swissmedic ist eine Verwaltungseinheit der dezentralen Bundesverwaltung[5] und fällt unter den Geltungsbereich des Öffentlichkeitsgesetzes (Art. 2 Abs. 1 Bst. a BGÖ).

2. Die Antragstellerin B spezifiziert in ihrem Zugangsgesuch hinreichend jene amtlichen Dokumente, in die sie Einsicht nehmen möchte.

3. Im Unterschied zu Art. 7 BGÖ, bei dem die angefragte Behörde darüber entscheiden muss, ob ein öffentliches oder privates Interesse eine Zugangsbeschränkung rechtfertigt, hat der Gesetzgeber in Art. 8 BGÖ abschliessend «besondere Fälle» (so der Titel der Bestimmung) geregelt, bei denen der Zugang verweigert (Art. 8 Abs. 1, 3 und 4 BGÖ) respektive gewährt (Art. 8 Abs. 5 BGÖ) werden *muss*.

   Absatz 2 von Art. 8 BGÖ stellt dabei insoweit eine Besonderheit dar, als dass der Zugang nur *befristet* verweigert wird. Der Aufschub des Zugangs zu den entscheidrelevanten Dokumenten gilt allerdings nur bis zu jenem Zeitpunkt, an dem die Behörde den politischen oder administrativen Entscheid fällt. Nach dem Entscheid sind diese Dokumente hingegen grundsätzlich zugänglich.

4. Absatz 2 wurde erst im Rahmen der parlamentarischen Beratungen[6] eingefügt und erlaubt es der Verwaltung, Dokumente, welche die Grundlage für einen Entscheid bilden, befristet vom Zugang auszunehmen. Entgegen der Meinung der Antragstellerin B gilt der Absatz 2 für jede Behörde und nicht bloss für den Bundesrat. Der Gesetzgeber hat der freien Meinungsbildung der Behörden einen hohen Stellenwert eingeräumt. Sinn und Zweck dieser Bestimmung ist es, verwaltungsinterne Entscheidungsprozesse zu schützen, indem weder Einblick in Dokumente noch Auskünfte über deren Inhalt erteilt werden müssen. In diesem Zusammenhang sei auf Art. 6 Abs. 1 BGÖ verwiesen, der diese beiden Aspekte (Einsicht und Auskunft) ausdrücklich erwähnt. Die Antragstellerin B irrt somit mit ihrer Annahme, dass sich Art. 8 Abs. 2 BGÖ nur auf die Einsichtnahme in Dokumente, nicht aber auf die Erteilung von Auskünften aus diesen Dokumenten bezieht.

[5] BBl 2003 1986
[6] AB 2004 N 1258ff.

Offen lässt die Bestimmung allerdings, welche Anforderungen ein Dokument erfüllen muss, damit es als *Grundlage* für einen Entscheid bezeichnet werden kann. Das Bundesamt für Justiz hat im Rahmen der Umsetzungsarbeiten für das Öffentlichkeitsgesetz ausgeführt[7], dass sich das Dokument unmittelbar auf den zu treffenden Entscheid beziehen und für diesen von wesentlicher Bedeutung sein muss. Der Beauftragte schliesst sich dieser Meinung an und fordert, dass erstens diese Dokumente in einem direkten Zusammenhang zum Entscheid stehen müssen und zweitens der Entscheid ohne die besagten Dokumente nicht in der gleichen Weise getroffen werden könnte.

Das Heilmittelgesetz (Art. 11f. HMG) hält fest, welche Dokumente im Rahmen eines Zulassungsgesuchs für eine Neuanmeldung oder ein Generikum eines Arzneimittels bei Swissmedic eingereicht werden müssen. Diese Angaben und Unterlagen sind zentral und unabdingbar für den Zulassungsentscheid von Swissmedic.

Nach Ansicht des Beauftragten fallen alle Angaben und Unterlagen des Zulassungsverfahrens nach Heilmittelgesetz unter die Kategorie der entscheidrelevanten Dokumente von Art. 8 Abs. 2 BGÖ. Swissmedic kann daher den Zugang zu diesen Dokumenten bis zum Zulassungsentscheid aufschieben.

5. Gemäss Art. 67 Abs. 1 HMG muss Swissmedic Zulassungsentscheide veröffentlichen. Swissmedic kommt dieser Verpflichtung nach und veröffentlicht diese Entscheide im monatlich erscheinenden Swiss Medic Journal, dem offiziellen Publikationsorgan des Schweizerischen Heilmittelinstituts.

   Nachdem Swissmedic den Entscheid getroffen hat, fällt die Berechtigung für den Aufschub weg und der Zugang zu den amtlichen Dokumenten muss grundsätzlich gewährt werden. Im Rahmen einer neuerlichen Beurteilung des Zugangsgesuchs muss Swissmedic nun prüfen, ob ein vollumfänglicher Zugang gewährt werden kann oder ob sich allenfalls eine Beschränkung des Zugangs aufgrund der Artikel 7, 8 oder 9 BGÖ rechtfertigt.

6. Es ist Praxis von Swissmedic, auf Anfragen auch dann keine Auskunft zu erteilen, wenn kein Zulassungsverfahren für ein Arzneimittel hängig ist. Swissmedic begründet dieses Vorgehen damit, dass bereits die Auskunft, keine Zulassungsgesuche seien für einen bestimmten Wirkstoff eingereicht worden, den Wettbewerb zwischen den Markteilnehmern beeinflussen und für den Konsumenten negative Auswirkungen haben könne.

[7] Bundesamt für Justiz, Leitfaden Gesuchbeurteilung, Ziffer 4.1, S. 10

Diese Argumentation ist bis zu einem gewissen Grad zuzustimmen. Es kann tatsächlich sein, dass derartige Anfragen nur getätigt werden, um in Erfahrung zu bringen, ob Konkurrenten ein Zulassungsgesuch für einen Wirkstoff eingereicht haben, den auch der Anfragende selber auf dem Mark anbietet (wie vorliegend die Antragstellerin A). Es kann auch nicht ausgeschlossen werden, dass derartige Informationen den Marktauftritt eines Konkurrenten zu beeinflussen vermögen.

Allerdings darf nicht ausser Acht gelassen werden, dass in jenem Fall, in dem kein Zulassungsgesuch eingereicht worden ist, Swissmedic auch nicht im Besitz von amtlichen Dokumenten im Sinne des Öffentlichkeitsgesetzes ist. *Es ist daher unzulässig, wenn sich Swissmedic in diesen Fällen auf Art. 8 Abs. 2 BGÖ beruft und den Anfragenden im Glauben lässt, dass amtliche Dokumente nach einem administrativen Entscheid zugänglich gemacht werden. Der Beauftragte regt an, dass Swissmedic ihre Praxis in diesem Punkt überdenkt.*

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

1. Das Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsgesetz, BGÖ) findet keine Anwendung auf die 4 Anfragen der Antragstellerin A, da es sich dabei nicht um Zugangsgesuche nach Art. 6 BGÖ handelt.

2. Swissmedic schiebt den Zugang der Antragstellerin B gestützt auf Art. 8 Abs. 2 BGÖ bis zum administrativen Entscheid auf. Nach diesem Entscheid gewährt Swissmedic im Rahmen des Öffentlichkeitsgesetzes Zugang zu den Dokumenten des Zulassungsverfahrens für das gewünschte Arzneimittel.

3. Swissmedic erlässt eine Verfügung nach Art. 5 des Verwaltungsverfahrensgesetzes, wenn sie mit der Empfehlung in Ziffer 2 nicht einverstanden ist.

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

4. Die Antragstellerinnen können innerhalb von 10 Tagen nach Erhalt dieser Empfehlung bei Swissmedic den Erlass einer Verfügung nach Artikel 5 des Verwaltungsverfahrensgesetzes verlangen, wenn sie mit der Empfehlung in Ziffer 1 und Ziffer 2 nicht einverstanden sind (Art. 15 Abs. 1 BGÖ).

   Gegen diese Verfügung können die Antragstellenden beim Bundesverwaltungsgericht Beschwerde führen (Art. 16 BGÖ).

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

6. Die Empfehlung wird eröffnet:

   - Den Antragstellerinnen A und B, vertreten durch Rechtsanwalt C

   - Swissmedic,
     Schweizerisches Heilmittelinstitut
     Hallerstrasse 7
     Postfach
     3000 Bern 9

Jean-Philippe Walter

4.14 Empfehlung zuhanden des Bundesamtes für Umwelt: «Verordnungsentwurf über den Schutz vor Erschütterungen»

Siehe Abschnitt 4.14 im französischen Teil des Berichtes

4.15 Empfehlung an das Bundesamt für Kommunikation: «Qualitätsreport Swisscom Fixnet AG»

Bern, den 21. Dezember 2007

Empfehlung

gemäss

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

zum Schlichtungsantrag von

Antragsteller X

gegen

Bundesamt für Kommunikation BAKOM

I. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte stellt fest:

1. Der Antragsteller reichte am 14. April 2007 beim Bundesamt für Kommunikation BAKOM ein Zugangsgesuch zum jährlichen Bericht der Swisscom Fixnet AG (Swissom) zur Dienstqualität der Grundversorgung (nachfolgend Qualitätsreport) ein (Art. 16 Fernmeldegesetz, SR 784.10, in Verbindung mit Art. 21 Verordnung über Fernmeldedienste, SR 784.101.1).

2. Das BAKOM teilte dem Antragsteller am 16. April 2007 mit, dass der Qualitätsreport nicht zugänglich sei, da er Geschäftsgeheimnisse im Sinne von Art. 7 Abs. 1 Bst. g des Bundesgesetzes über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsgesetz BGÖ; SR 152.3) enthalte. Weiter wies das BAKOM darauf hin, dass Swisscom Fixnet AG als Grundversorgungskonzessionärin die einzige Anbieterin von Fernmeldediensten sei, welche dem BAKOM gegenüber solche Qualitätsreporte einreichen müsse. Durch deren Veröffentlichung könnte der Wettbewerb zwischen den einzelnen Marktteilnehmerinnen verzerrt werden.

3. Der Antragsteller war mit dieser Antwort nicht zufrieden und reichte am 20. April 2007 beim Eidg. Datenschutz- und Öffentlichkeitsbeauftragten (Beauftragter) einen Schlichtungsantrag gemäss Art. 13 BGÖ ein. Für den Antragsteller war es «insbesondere nicht nachvollziehbar, weshalb es sich bei den in den TAV[1] spezifizierten Qualitätskriterien um Geschäftsgeheimnisse handeln soll - letztlich geht es ja darum überprüfen zu können, ob die Konzessionärin ihrer Pflicht nachkommt (Qualität der Grundversorgung gemäss FMG 17, FDV 21 und Konzession Abschnitt 5).»

4. In einem Schreiben vom 30. November 2007 begründete das BAKOM gegenüber dem Beauftragten diese Zugangsverweigerung ausführlicher und liess ihm den Qualitätsreport «Grundversorgung 2006» der Swisscom zukommen. Das BAKOM vertrat die Ansicht, dass «es sich bei den jeweiligen Messresultaten klarerweise um Geschäftsgeheimnisse handelt, deren Offenlegung allfälligen Konkurrenten einen Einblick in geschäftsinterne Daten der Swisscom gewähren würde.» Entsprechende Wettbewerbsvorteile für die Konkurrenten könnten daher nicht ausgeschlossen werden. Zudem führte das BAKOM aus,

[1] TAV = Technische und administrative Vorschriften zur Dienstqualität der Grundversorgung, SR 784.101.113 / 1.2; veröffentlicht auf http://www.bakom.admin.ch/org/grundlagen/00563/00564/index.html?lang=de

dass die Swisscom «mehrmals klarerweise die ablehnende Haltung gegenüber einer allfälligen Publikation der jeweiligen Qualtiätsreporte kundgetan hat.» Als Beleg legte das BAKOM ein entsprechendes Schreiben der Swisscom vom 23. Dezember 2005 bei.

Das BAKOM hielt in seiner Stellungnahme u.a. auch fest, dass die Swisscom die Zielvorgaben für das Jahr 2006 erreicht habe.

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.[2] 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 BAKOM eingereicht und ablehnende Antworten erhalten. Als Teilnehmer an einem vorangegangenen Gesuchsverfahren ist er zur Einreichung eines Schlichtungsantrags berechtigt. Die Schlichtungsanträge wurden 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 Detail obliegt alleine dem Beauftragten[3].

[2] BBl 2003 2023
[3] 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 Beurteilung der Angelegenheit eine Empfehlung abzugeben.

B. Sachlicher Geltungsbereich

1. Das BAKOM verweigerte den Zugang zum Qualitätsreport 2006 der Swisscom mit dem Argument, dass er Geschäftsgeheimnisse im Sinne von Art. 7 Abs. 1 Bst. g BGÖ enthalte, deren Offenlegung zu einer Verzerrung des Wettbewerbs zwischen Marktteilnehmern führen könnte.

2. Die Einführung des Öffentlichkeitsprinzips hat nicht zur Folge, dass Bundesbehörden Berufs-, Geschäfts- und Fabrikationsgeheimnisse von Privaten, von denen sie Kenntnis haben, an interessierte Dritte ausserhalb der Verwaltung bekannt geben müssen. Vielmehr ist die Verwaltung gemäss Öffentlichkeitsgesetz gehalten, diese Geheimnisse zu schützen. Das Öffentlichkeitsgesetz enthält keine Legaldefinition der von ihm verwendeten Geheimnisbegriffe. Die Botschaft führt dazu lediglich aus, dass das Zugänglichmachen bestimmter Informationen nicht zu einer Wettbewerbsverzerrung zwischen Marktteilnehmern führen darf.[4]

3. Für das Bundesamt für Justiz umfassen Geschäfts- oder Fabrikationsgeheimnisse «Informationen, die sich auf eine Tätigkeit beziehen, die *unter Wettbewerb oder wettbewerbsähnlichen Bedingungen* stattfindet und denen *Geheimnischarakter* zukommt (d.h. es geht um Tatsachen, die weder offenkundig noch allgemein zugänglich sind). Es muss ein *legitimes Geheimhaltungsinteresse* bestehen und der Geheimhaltungswille der privaten Drittperson muss zumindest aus den Umständen ersichtlich sein.»[5]

4. Als Grundversorgungskonzessionärin muss Swisscom die Dienste von Art. 16 FMG in Verbindung mit Art. 15 FDV anbieten. Die Grundversorgungskonzessionärin ist als einzige Anbieterin von Fernmeldediensten von Gesetzes wegen dazu verpflichtet, jährlich einen Qualitätsreport beim BAKOM einzureichen. Der Report beschreibt die Qualität der Dienste der Grundversorgung von Swisscom Fixnet für ein Kalenderjahr. Er führt die gesetzlichen Zielvorgaben auf und bestimmt anhand von so genannten «beobachteten Vorfällen» die konkreten Messresultate für die verschiedenen Grundversorgungsdienste, die

[4] BBl 2003 2012

[5] Bundesamt für Justiz: «Umsetzung des Öffentlichkeitsprinzips in der Bundesverwaltung: Häufig gestellte Fragen» vom 29.06.2006; zur bundesgerichtlichen Umschreibung des Begriffs s.a. BGE 98 IV 210

im Rahmen der Konzession erbracht werden müssen. Diese Qualitätsreporte stellen für das BAKOM in seiner Funktion als Aufsichtsbehörde ein wichtiges Instrument dar, um zu überprüfen, ob die Swisscom die gesetzlich vorgegeben Qualitätskriterien in der Erhebungsperiode erreicht hat.

5. Die Messresultate betreffend die Einhaltung der gesetzlichen Qualitätskriterien sind unternehmensinterne Informationen der Swisscom, die aus ihrer Tätigkeit als Anbieterin von Fernmeldediensten im *Wettbewerb* mit anderen Anbieterinnen stammen. Wie oben ausgeführt, ist als Grundversorgungskonzessionärin einzig die Swisscom gesetzlich verpflichtet, diese Qualitätsreporte dem BAKOM einzureichen. Die andern Fernmeldedienstanbieter trifft diese Pflicht nicht, selbst wenn sie die gleichen Fernmeldedienste wie die Swisscom anbieten.

   Die Messresultate lassen Rückschlüsse auf die Geschäftstätigkeit der Swisscom zu. Es ist daher nachvollziehbar, dass die andern Fernmeldedienstanbieter ein Interesse an diesen Messresultaten haben könnten. Zudem könnte ein Anbieter aufgrund der Messresultate der Swisscom sein eigenes Auftreten auf dem Markt anpassen (z.B. fiktive Vergleiche), ohne selber die eigenen Kennzahlen bekannt geben zu müssen, und auf diese Weise die Wettbewerbsverhältnisse gezielt beeinflussen.

   Nach Ansicht des Beauftragten besteht daher ein legitimes Interesse der Swisscom an der Geheimhaltung der Messresultate der Qualitätsreporte. Die Swisscom hat diesen Geheimhaltungswillen gegenüber dem BAKOM mehrmals auch schriftlich mitgeteilt. Der Beauftragte teilt zudem die Meinung des BAKOM, wonach die Offenlegung dieser Messresultate zu einer negativen Wettbewerbsbeeinflussung führen könnte.

6. In Zusammenhang mit der Aufsichtstätigkeit von Bundesbehörden über private Unternehmen können Geschäftsgeheimnissen eine spezielle Bedeutung zukommen. So muss ein Unternehmen, das aufgrund einer gesetzlichen Verpflichtung einer staatlichen Behörde Informationen mit Geheimnischarakter mitzuteilen hat, darauf Vertrauen können, dass diese Informationen keinem Konkurrenten zugänglich gemacht werden. Ansonsten kann nicht ausgeschlossen werden, dass der Behörde nicht mehr vollständige Informationen zukommen und sie in der Folge ihre Aufsichtstätigkeit nicht mehr entsprechend der gesetzlichen Zielsetzung vornehmen kann.

7. *Der Beauftragte kommt zum Schluss, dass das BAKOM die Messresultate des Qualitätsreports «Grundversorgung 2006» zu Recht als Geschäftsgeheimnisse im Sinne von Art. 7 Abs. 1 Bst. g BGÖ qualifiziert hat.*

8. Art. 7 BGÖ sieht neben der vollumfänglichen Verweigerung auch die *Möglichkeit der Beschränkung des Zugangs* im Umfang des tatsächlich gegebenen Geschäftsgeheimnisses (Art. 7 Abs. 1 BGÖ) vor. In Anwendung des Verhältnismässigkeitsprinzips gilt es stets zu prüfen, ob allenfalls ein teilweiser Zugang gewährt werden kann, indem die sensiblen Teilbereiche des Dokuments abgedeckt, entfernt oder verschlüsselt werden können.

   In seiner Stellungnahme zuhanden des Beauftragten vertrat das BAKOM die Ansicht, dass eine Abdeckung der Messresultate die Aussagekraft des Qualitätsreports stark vermindern würde, und daher auf eine Herausgabe des Dokuments verzichtet worden sei. Dieser Haltung kann sich der Beauftragte nicht vollends anschliessen.

   Das BAKOM hat im Rahmen des Schlichtungsverfahrens mitgeteilt, dass die Swisscom die gesetzlich Zielvorgaben für das Jahr 2006 erfüllt hat. Diese Zielvorgaben sind öffentlich zugänglich (Fernmeldegesetz, Verordnung über Fernmeldedienste sowie Technische und administrative Vorschriften zur Dienstqualität der Grundversorgung). Ein Qualitätsreport enthält eine klare Auflistung aller gesetzlichen Zielvorgaben. Verbunden mit der Information, dass die Swisscom als Grundversorgungskonzessionärin die Qualitätsanforderungen für das Jahr 2006 erfüllt hat, kann ein Qualitätsreport auch ohne konkrete Messresultate für einen Gesuchsteller von Interesse sein. In diesem Sinn ist zu fordern, dass ein Bundesamt in Anwendung des Verhältnismässigkeitsprinzips stets bestrebt ist, den Zugang soweit als möglich zu gewähren.[6]

9. *Der Beauftragte ist der Meinung, dass die einzelnen Messresultate des Qualitätsreports «Grundversorgung 2006» gestützt auf Art. 7 Abs. 1 Bst. g BGÖ abgedeckt und dem Gesuchsteller in Anwendung des Verhältnismässigkeitsprinzips eine Kopie des Qualitätsreports zugestellt werden muss.*

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

1. Das Bundesamt für Kommunikation gewährt den teilweisen Zugang zum Qualitätsreport «Grundversorgung 2006» der Swisscom. Es deckt die konkreten Messresultate der Swisscom ab.

2. Das Bundesamt für Kommunikation erlässt eine Verfügung nach Art. 5 des Verwaltungsverfahrensgesetzes, wenn es in Abweichung von Ziffer 1 den teilweisen Zugang nicht gewähren will.

[6] s. dazu auch Empfehlung vom 1. Juni 2007 (BAV); Titel II. Erwägungen, Bst. C, Ziffer 3

Das Bundesamt für Kommunikation 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 Bundesamt für Kommunikation den Erlass einer Verfügung nach Artikel 5 des Verwaltungsverfahrensgesetzes verlangen (Art. 15 Abs. 1 BGÖ).

   Gegen diese Verfügung kann der Antragsteller beim Bundesverwaltungsgericht Beschwerde führen (Art. 16 BGÖ).

4. In Analogie zu Art. 22a des Bundesgesetzes über das Verwaltungsverfahren (SR 172.021) stehen gesetzliche Fristen, die nach Tagen bestimmt sind, vom 18. Dezember bis 2. Januar still. Die Frist beginnt somit am 3. Januar 2008.

5. Diese Empfehlung wird veröffentlicht. Zum Schutz der Personendaten der am Schlichtungsverfahren Beteiligten werden die Namen der Antragsteller anonymisiert (Art. 13 Abs. 3 VBGÖ).

6. Die Empfehlung wird eröffnet:

   - X

   - Bundesamt für Kommunikation
     Zukunftstrasse 44
     Postfach
     2501 Biel

Jean-Philippe Walter

4.16 Empfehlung für das Bundesamt für Gesundheit: «Vertrag Präpandemieimpfstoff II»

Bern, den 1. Februar 2008

Empfehlung

gemäss

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

zum Schlichtungsantrag von

X
(Antragstellerin)

gegen

Bundesamt für Gesundheit (BAG), Bern

I. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte stellt fest:

1. Mit einer Pressemitteilung informierte das Bundesamt für Gesundheit (BAG) am 18. Oktober 2006 darüber, dass der Bundesrat den Kauf von acht Millionen Dosen eines Präpandemie-Impfstoffes beschlossen hat. Demnach unterzeichnete das BAG einen entsprechenden Vertrag mit dem Pharmaunternehmen GlaxoSmithKline (GSK). Gleichzeitig wurde mit dem Unternehmen eine Reservationsübereinkunft für Pandemie-Impfstoffe vereinbart. Gemäss Pressemitteilung des BAG betragen die Kosten für die Präpandemie- und Pandemie-Impfstoffe 180 Millionen Franken.

2. Der Eidg. Datenschutz- und Öffentlichkeitsbeauftragte (Beauftragter) hat bereits zu einem früheren Zeitpunkt ein Schlichtungsgesuch betreffend den Zugang zu ebendiesem Vertrag zwischen BAG und GSK durchgeführt und in dieser Sache am 12. März 2007 eine Empfehlung[1] erlassen.

3. Am 10. Mai 2007 reichte die Antragstellerin beim BAG ein Gesuch um Zugang zum Vertrag ein. Sie machte geltend, dass sie unter anderem Inhaberin oder exklusive Lizenznehmerin von «vier Patentfamilien» sei, «die für die sog. ‚reverse genetics'-Technologie von zentraler Bedeutung sind.» Mit dieser Technologie liessen sich gezielt neue Impfstoffstämme entwickeln, mit deren Hilfe sich wiederum Grippe-Impfstoffe herstellen liessen. Die Antragstellerin sei daher daran interessiert zu erfahren, ob sich im Vertrag «zwischen der Schweizerischen Eidgenossenschaft und GSK Bestimmungen finden, gemäss denen die Herstellung der Präpandemie- und Pandemie-Impfstoffe unter Einsatz von ‚reverse genetics'-Technologie erfolgt.» Zudem wolle sie wissen, ob GSK im Vertrag zusichere, über die erforderlichen Rechte zur Verwendung der in Frage stehenden Technologie zu verfügen.

4. Das BAG gewährte der Antragstellerin am 22. Mai 2007 einen beschränkten Zugang entsprechend der Empfehlung des Beauftragten vom 12. März 2007.

5. Die Antragstellerin war damit nicht einverstanden und reichte am 11. Juni 2007 bei Beauftragten ein Schlichtungsgesuch gemäss Art. 13 des Bundesgesetzes über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsgesetz BGÖ; SR 152.3) ein. Sie machte geltend, dass sie ein legitimes Interesse daran habe, den Inhalt der Bestimmung über die «reverse genetics»-Technologie zu ken-

[1] Empfehlung vom 12. März 2007: BAG / Vertrag Präpandemieimpfstoff; alle Empfehlungen des Beauftragten werden veröffentlicht auf www.edoeb.admin.ch, Dokumentation, Öffentlichkeitsprinzip, Empfehlungen

nen. Ausserdem führte sie u.a. aus, dass «Der Grundsatz der Verhältnismässigkeit (…) nicht eingehalten (ist) und der Sinn des BGÖ (…) unterlaufen (wird), wenn der Zugang zum überwiegenden Teil des Vertrages gesamthaft verweigert wird, obschon es zur Wahrung der allenfalls berechtigten Geschäftsgeheimnisse genügen würde, bloss gezielt die wirklich sensitiven Stellen (Worte bzw. Zahlen, allenfalls Sätze oder Abschnitte) abzudecken.» Die Antragstellerin erklärte, dass sie «ausdrücklich nichts dagegen einzuwenden (hat), wenn im notwendigen Umfang Bestimmungen abgedeckt werden, die sich auf wirkliche Geschäftsgeheimnisse (…) beziehen.»

Weiter führte sie aus, dass sie «vornehmlich an denjenigen Vertragsbestimmungen interessiert (ist), die sich

1. möglicherweise mit der ‚reverse genetics'-Technologie befassen sowie
2. in denen GSK zusichert, über die Rechte an dieser Technologie zu verfügen, die zur Herstellung der Grippe-Impfstoffe erforderlich sind.»

Die Antragstellerin beantragte «im Sinne eines Eventualstandpunkts» deshalb, «dass zumindest diese Teile des Vertrages offengelegt werden (…)».

6. Am 28. November 2007 lud der Beauftragte GSK als in der Sache Betroffene zu einer Stellungnahme ein. In ihrer Antwort vom 7. Dezember 2007 teilte GSK dem Beauftragten mit, dass «die Bestimmungen über die notwendigen Rechte sehr allgemein gehalten (sind), insbesondere wird die ‚reverse genetics'-Technologie explizit nicht erwähnt.» Aus diesem Grund sei GSK bereit, über die Empfehlung vom 12. März 2007 hinaus eine Textpassage aus dem Titel «Infringement of IP Rights» des Vertrags zugänglich zu machen. Im Übrigen erachtete GSK das Zugänglichmachen weiterer Vertragsbestandteile «als nicht sinnvoll».

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[2]. 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. Die Antragstellerin hat ein Zugangsgesuch nach Art. 6 BGÖ beim BAG eingereicht und lediglich einen teilweisen Zugang 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 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 Detail obliegt alleine dem Beauftragten[3].

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

B. Sachlicher Geltungsbereich

1. Die Antragstellerin ist der Ansicht, dass der ihr vom BAG gewährte, eingeschränkte Zugang den Grundsatz der Verhältnismässigkeit verletze. Da das BAG sich in seinem Entscheid an die Empfehlung des Beauftragten vom 12. März 2007 in der gleichen Angelegenheit hielt, bringt die Antragstellerin zum Ausdruck, dass auch der Beauftragte die Verhältnismässigkeit nicht richtig angewendet habe.

2. Der Beauftragte beurteilte den Vertrag zwischen dem BAG und GSK bereits für seine Empfehlung vom 12. März 2007. In Anwendung des Grundsatzes der Verhältnismässigkeit kam er dabei zum Schluss, dass seiner Ansicht nach die Seiten 1 – 9 des Vertrages teilweise zugänglich zu machen sind, während die übrigen Vertragsbestandteile unter das Geschäfts- und Fabrikationsgeheimnis fallen.

[2] BBl 2003 2023
[3] BBl 2003 2024

Der Beauftragte hält an seiner Einschätzung und damit auch seiner Empfehlung vom 12. März ausdrücklich fest.

3. Der Beauftragte ist von Gesetzes wegen dazu angehalten, bei jedem neu eingereichten Schlichtungsantrag eine für alle Beteiligten akzeptable Einigung anzustreben. In diesem Sinne zeigte sich der Beauftragte bereit, die Frage eines weitergehenden Zugangs zu prüfen. Als in der Sache Betroffene steht GSK gemäss Öffentlichkeitsgesetz ein Anhörungsrecht (Art. 11 BGÖ) zu. Aus diesem Grund forderte der Beauftragte GSK auf, sich dazu zu äussern, ob sie bereit sei, im vorliegenden Fall einen weitergehenden Zugang zu gewähren bzw. ob und allenfalls unter welchen Auflagen ein Zugang zu den von der Antragstellerin explizit bezeichneten Vertragsbestandteilen (s. oben Ziffer I.5.) gewährt werden könne.

   In ihrer Antwort zeigte sich GSK bereit, eine weitere Textpassage zugänglich zu machen. Es handelt sich dabei um einen sechszeiligen Abschnitt aus dem Titel «Infringement of IP Rights» des Vertrags. GSK war indes nicht Willens, weitere Vertragsteile für Dritte zu öffnen oder der Antragstellerin einen Zugang unter Auflagen zu gewähren.

   Weder das BAG noch GSK sind somit bereit, einen weitergehenden Zugang zu gewähren. Der Beauftragte stellt daher fest, dass eine Schlichtung nicht möglich ist.

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

1. Das Bundesamt für Gesundheit gewährt der Antragstellerin Zugang zu Ziffer 15.3.1. Securing Intellectual Property Rights, 1. Abschnitt des Vertrags zwischen dem BAG und GlaxoSmithKline.

2. Das Bundesamt für Gesundheit erlässt eine Verfügung nach Art. 5 des Verwaltungsverfahrensgesetzes, wenn es in Abweichung dieser Empfehlung der Antragstellerin den vorgängig bezeichneten Zugang nicht gewährt.

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

3. Die Antragstellerin kann innerhalb von 10 Tagen nach Erhalt dieser Empfehlung beim Bundesamt für Gesundheit den Erlass einer Verfügung nach Artikel 5 des Verwaltungsverfahrensgesetzes verlangen, wenn sie mit der Empfehlung nicht einverstanden ist (Art. 15 Abs. 1 BGÖ).

4. Als von der Empfehlung Betroffene kann GlaxoSmithKline innerhalb von 10 Tagen nach Erhalt dieser Empfehlung beim Bundesamt für Gesundheit den Erlass einer Verfügung nach Artikel 5 des Verwaltungsverfahrensgesetzes verlangen, wenn sie mit der Empfehlung nicht einverstanden ist (Art. 15 Abs. 1 BGÖ).

5. Gegen die Verfügung kann beim Bundesverwaltungsgericht Beschwerde geführt werden (Art. 16 BGÖ).

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

7. Die Empfehlung wird eröffnet:

   - X
   - Bundesamt für Gesundheit
     3003 Bern
   - GlaxoSmithKline AG
     Talstrasse 3 – 5
     3053 Münchenbuchsee

Jean-Philippe Walter

4.17 Empfehlung an das Bundesamt für Umwelt: «Adresslisten und Abgabedeklarationen von Deponien und Abfallexporteuren»

Bern, 13. März 2008

Empfehlung

gemäss

Art. 14 des

Bundesgesetzes über das

Öffentlichkeitsprinzip der Verwaltung

vom 17. Dezember 2004

zum Schlichtungsantrag von

X

(Antragstellerin)

gegen

Bundesamt für Umwelt, 3003 Bern

I. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte stellt fest:

1. Die Antragstellerin (Deponieunternehmen) bezog sich in ihrem Schreiben vom 11. April 2007 an das Bundesamt für Umwelt (BAFU) auf dessen Internetpublikation «Abgabeerhebung und Abgeltungen VASA» (Verordnung über die Abgabe zur Sanierung von Altlasten VASA; SR 814.681) und stellte ein Gesuch, «uns Einblick in die Liste der Abgabepflichtigen (enthaltend Name und Adresse des Abgabepflichtigen und Höhe der Abgabe) für die Jahre 2002 bis 2006 zu gewähren.» Mit Abgabepflichtigen sind die Inhaber von Deponien (für die Ablagerung von Abfällen im Inland) sowie die Exporteure (für die Ausfuhr von Abfällen zur Ablagerung im Ausland) gemeint. Sie müssen auf die Ablagerung respektive Ausfuhr von Abfällen eine Abgabe entrichten (Art. 1f. VASA).

2. Das BAFU teilte der Antragstellerin mit Schreiben vom 1. Mai 2007 mit, dass der Zugang zu den gewünschten Dokumenten nicht gewährt werden könne. Erstens finde das Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsgesetz BGÖ; SR 152.3) keine Anwendung auf die Dokumente der Jahre 2002 - 2005, da diese vor Inkrafttreten des Öffentlichkeitsgesetzes erstellt oder empfangen wurden. Zweitens könne für jene Dokumente, die unters Öffentlichkeitsgesetz fallen, aus Gründen des Datenschutzes kein Zugang gewährt werden.

3. Die Antragstellerin reichte am 21. Mai 2007 beim Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (Beauftragter) einen Schlichtungsantrag ein.

4. Mit Schreiben vom 10. Dezember 2007 teilte das BAFU dem Beauftragten u.a. mit, dass der Zugang verweigert worden sei, weil die Voraussetzungen von Art. 19 Abs. 1 des Bundesgesetzes über den Datenschutz (DSG, SR 235.1) für die Herausgabe der Daten der Abgabepflichtigen nicht gegeben sei. Darüber hinaus sei nicht ersichtlich, «inwieweit im vorliegenden Fall ein öffentliches Interesse an der Veröffentlichung der detaillierten Daten (…) besteht.» Das BAFU führt dazu zum einen aus, dass es jedes Jahr einen Bericht mit den Ergebnissen betreffend die Abgabeerhebungen und Abgeltungen nach der VASA veröffentliche. Zum anderen bestehe «kein öffentliches Interesse daran, mit der Veröffentlichung der Daten zu kontrollieren, ob die einzelnen Abgabepflichtigen dem BAFU tatsächlich richtige Angaben gemacht haben. Diese Kontrolle obliegt dem BAFU selber.» Demgegenüber seien «die Interessen der Betroffenen, ihre Personendaten nicht zu veröffentlichen, hoch zu gewichten.» Aus den gemeldeten Angaben könne «auf den Geschäftsgang

der einzelnen Unternehmung geschlossen werden (…)». Es bestehe «deshalb kein die privaten Interessen der betroffenen Unternehmen überwiegendes öffentliches Interesse an der Veröffentlichung der fraglichen Daten (…)».
Das BAFU legte seiner Stellungnahme je eine Adressliste der Deponien und der Exporteure sowie eine Kopie einer Abgabedeklaration bei.

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.[1] 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. Die Antragstellerin hat ein Zugangsgesuch nach Art. 6 BGÖ beim BAFU eingereicht und ablehnende Antworten 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 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 Detail obliegt alleine dem Beauftragten[2].

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

[1] BBl 2003 *2023*
[2] BBl 2003 2024

B. Sachlicher Geltungsbereich

1. Das Öffentlichkeitsgesetz ist nur auf amtliche Dokumente anwendbar, die nach seinem Inkrafttreten (1. Juli 2006) von einer Behörde erstellt oder empfangen wurden (Art. 23 BGÖ). Die Abgabepflichtigen (Inhaber von Deponien und Exporteure) müssen dem BAFU jeweils bis zum 28. Februar für die im vorangegangenen Kalenderjahr entstandenen Abgabeforderungen eine Abgabedeklaration einreichen (Art. 5 VASA). Die Abgabedeklarationen für das Jahr 2005 mussten bis zum 28. Februar 2006, d.h. vor Inkrafttreten des Öffentlichkeitsgesetzes, beim BAFU eingereicht werden. Sie fallen daher nicht in den Geltungsbereich des Öffentlichkeitsgesetzes.

   Die Antragstellerin kann sich für den Zugang zu den Abgabedeklarationen der Jahre 2002 – 2005 nicht auf das Öffentlichkeitsgesetz berufen. Mit anderen Worten ist das BAFU nicht verpflichtet, gestützt auf das Öffentlichkeitsgesetz den Zugang zu diesen Dokumenten zu gewähren.

2. Nach Inkrafttreten dieses Gesetzes wurden die Abgabedeklarationen des Jahres 2006 eingereicht. Diese Dokumente sind unter Vorbehalt eines Ausnahmegrundes nach Art. 7 BGÖ grundsätzlich zugänglich. Die Antragstellerin beantragte «Einblick in die Liste der Abgabepflichtigen (enthaltend Namen und Adresse des Abgabepflichtigen und Höhe der Abgabe)». Das BAFU liess dem Beauftragten im Dezember 2007 eine Adressliste der Deponien und der Exporteure (beide Listen datieren vom Januar 2007) sowie eine Kopie einer Abgabedeklaration zukommen.

   Das Zugangsgesuch richtete sich nicht auf ein einziges, sondern auf mehrere Dokumente. Diese sind jedoch als solche klar spezifiziert. Das BAFU unterschied in seiner Beurteilung nicht zwischen den einzelnen Dokumenten und gab eine für alle Dokumente geltende, ablehnende Stellungnahme ab. Nach Ansicht des Beauftragten muss für jedes einzelne Dokument (Adressliste der Deponien, Adressliste der Exporteure, Abgabedeklarationen) gesondert geprüft werden, ob und in welchem Umfang ein Zugang gewährt werden kann.

3. Gemeinsam ist allen zu beurteilenden Dokumenten, dass sie Personendaten im Sinne von Art. 3 Bst. a DSG enthalten. Amtliche Dokumente, welche Personendaten enthalten, sind nach Möglichkeit vor der Einsichtnahme zu anonymisieren (Art. 9 Abs. 1 BGÖ). Im vorliegenden Fall möchte die Antragstellerin explizit Zugang zu den personenbezogenen Angaben; eine Anonymisierung ist zwar möglich, aber explizit nicht erwünscht. Ob ihm trotzdem eine Einsichtnahme in die entsprechenden Dokumente gewährt werden kann, beurteilt sich nach den Vorschriften der Bekanntgabe von Personendaten durch Bundesorgane (Art. 9 Abs. 2 BGÖ i.V.m. Art. 19 DSG).

4. Das BAFU hielt in seiner Stellungnahme zuhanden des Beauftragten fest, dass die Bekanntgabe gestützt auf Art. 19 Abs. 1 DSG nicht möglich sei, indem es unter anderem ausführte, dass «Buchstabe c (…) ebenfalls keine Berechtigung (gibt), die Personendaten dem Gesuchsteller bekannt zu geben. Die entsprechenden Angaben sind höchstens in Einzelfällen (Geschäftsberichte) offen gelegt worden.»

5. In Bezug auf die Bekanntgabe der Adressliste der Deponien schliesst sich der Beauftragte der Einschätzung des BAFU nicht an. Eine stichprobenweise Überprüfung durch den Beauftragten hat ergeben, dass alle privaten wie öffentlich-rechtlichen Deponien im Telefonbuch aufgeführt sind und/oder über eine eigene Homepage im Internet verfügen. Mit anderen Worten haben die Betroffenen ihre Personendaten (wie Firma, Adressen) allgemein zugänglich gemacht. Gemäss Art. 19 Abs. 1 Bst. c DSG dürfen Bundesorgane diese Personendaten ohne weiteres bekannt geben, es sei denn, die betroffenen Personen haben eine Bekanntgabe im konkreten Einzelfall ausdrücklich untersagt.

   Das BAFU kann die Adressliste der Deponien gestützt auf Art. 19 Abs. 1 Bst. c DSG zugänglich machen.

6. Auch die Adressen aller gemäss VASA abgabepflichtigen Exporteure finden sich in allgemein zugänglichen Quellen wie Telefonbuch oder Internet. Allerdings geben die Exporteure (sowohl private Unternehmen wie auch öffentlich-rechtliche Verbände der Kehrichtverbrennungsanlagen) nicht in jedem Fall von sich aus bekannt, dass sie Abfälle ins Ausland exportieren. Laut BAFU habe sich bei den Vorarbeiten zur Gesetzgebung gezeigt, dass die Exporteure diese Tatsache nicht allgemein zugänglich machen wollten.

   Aus diesem Einwand kann nicht gefolgert werden, dass der Zugang zur Adressliste der abgabepflichtigen Exporteure gemäss VASA unbesehen verweigert werden muss. Das Öffentlichkeitsgesetz will die Transparenz fördern und den Zugang der Öffentlichkeit zur Information gewährleisten (Art. 1 BGÖ). Für die Behörden bedeutet dies, alle notwendigen Vorkehrungen und Schritte zu unternehmen, um den gewünschten Zugang so weit als möglich zu gewähren. Dies gilt auch in Bezug auf amtliche Dokumente, die Personendaten Dritter enthalten. Gemäss Botschaft zum Öffentlichkeitsgesetz muss eine Behörde die betroffenen Dritten anhören (Art. 11 BGÖ), soweit sie «nicht von vornherein der Ansicht (ist), dass eine vom Öffentlichkeitsgesetz vorgesehene Ausnahme oder spezialgesetzliche Geheimhaltungs- oder Datenschutzbestimmung anwendbar ist»[3].

[3] BBl 2003 *2017*

Nach Ansicht des Beauftragten kommt in Bezug auf den Zugang zur Adressliste der Exporteure weder eine Ausnahmebestimmung des Öffentlichkeitsgesetzes noch eine spezialgesetzliche Geheimhaltungs- oder Datenschutzbestimmung zur Anwendung. Angesichts der betroffenen Personendaten (Firma und Adresse) und des als gering zu wertenden Eingriffs in die Privatsphäre der Betroffenen gelangt der Beauftragte zur Einschätzung, dass der Zugang zur Adresseliste der Exporteure gewährt werden sollte. Um den Anspruch auf rechtliches Gehör zu gewährleisten, müssen die betroffenen Exporteure vorgängig noch konsultiert werden. Aus verfahrensökonomischen Gründen empfiehlt er folgendes Vorgehen:

- Das BAFU informiert die Betroffenen über den bisherigen Verlauf und die Empfehlung des Beauftragten, den Zugang zur Adressliste der Exporteure zu gewähren.
- Es gibt den Betroffenen 10 Tage Gelegenheit zur Stellungnahme im Sinne von Art. 11 BGÖ.
- Danach gewährt das BAFU der Antragstellerin umgehend Zugang zu einer Auflistung mit den Adressen jener Exporteure, die sich nicht gegen das Zugänglichmachen ihrer Daten ausgesprochen haben.
- Das BAFU stellt jenen Exporteuren, die sich in der Anhörung dagegen aussprechen, umgehend eine Verfügung aus. Erheben die Betroffenen innerhalb der Rechtsmittelfrist keine Beschwerde beim Bundesverwaltungsgericht, so gibt das BAFU der Antragstellerin auch diese Personendaten bekannt.

7. Jeder Abgabepflichtige muss gemäss VASA eine Abgabedeklaration, in der die Menge der abgelagerten Abfälle und die zu leistenden Abgabebeträge aufgeführt werden, ausfüllen und dem BAFU einreichen. Diese Zahlen lassen zweifelsfrei Rückschlüsse auf Geschäftstätigkeit, Auftragslage und -erledigung zu. Eine Bekanntgabe dieser Informationen könnte den Wettbewerb zwischen den Teilnehmern beeinflussen und Marktverzerrungen zur Folge haben. Nach Ansicht des Beauftragten handelt es sich dabei um Informationen, die unter den Begriff des Geschäftsgeheimnisses von Art. 7 Abs. 1 Bst. g BGÖ fallen. Der Zugang zu den Abgabedeklarationen muss daher nicht gewährt werden.

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

1. Das Öffentlichkeitsgesetz findet lediglich Anwendung auf amtliche Dokumente, die nach Inkrafttreten des Öffentlichkeitsgesetzes (1. Juli 2006) von der Behörde erstellt oder empfangen wurden. Somit besteht kein Anspruch auf die Abgabedeklarationen der Jahre 2002-2005.

2. Das BAFU gewährt gestützt auf Art. 19 Abs. 1 Bst. c DSG einen vollständigen Zugang zur Adressliste der Deponien.

3. Das BAFU gewährt den Zugang zur Adressliste der Exporteure. Vorgängig führt das BAFU bei den Exporteuren eine Anhörung gemäss Art. 11 BGÖ durch.

4. Der Zugang zu den Abgabedeklarationen muss gestützt auf Art. 7 Abs. 1 Bst. g BGÖ nicht gewährt werden.

5. Das BAFU erlässt eine Verfügung nach Art. 5 des Verwaltungsverfahrensgesetzes, wenn es in Abweichung von Ziffern 2 und 3 den Zugang nicht gewähren will.

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

6. Die Antragstellerin kann innerhalb von 10 Tagen nach Erhalt dieser Empfehlung beim BAFU den Erlass einer Verfügung nach Artikel 5 des Verwaltungsverfahrensgesetzes verlangen (Art. 15 Abs. 1 BGÖ), wenn sie mit der Empfehlung in den Ziffern 1 bis 4 nicht einverstanden ist.

   Gegen diese Verfügung kann die Antragstellerin beim Bundesverwaltungsgericht Beschwerde führen (Art. 16 BGÖ).

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

8. Die Empfehlung wird eröffnet:

   - X
   - Bundesamt für Umwelt
     3003 Bern

Jean-Philippe Walter

4.18 Declaration adopted by the European Data Protection Authorities in Cyprus on 11 May 2007

In the Council of the European Union a proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters is subject of debate.

Creating a harmonised and high level of data protection covering police and judicial activities in the Union is indeed a crucial element for respecting and safeguarding fundamental rights such as the right of protection of personal data when creating an area of freedom, security and justice.

The initiatives in the European Union to improve the fight against serious crime and terrorism have in common the willingness to achieve that within the Union national borders become increasingly less relevant when defining the conditions for exchanging data between competent authorities so that law-enforcement data may be made available by various means including providing direct access to national data bases.

These initiatives clearly demonstrate that the Union's obligation to help improving the fight against serious crime is not limited to setting conditions for the exchange of information between the Member States; the initiatives clearly also have an impact on data processing on a national level preceding any possible exchange. It is evident that any development in this area must be balanced with adequate and harmonised data protection rights and obligations in which mutual trust is a key element.

Throughout the European Union data protection legislation applicable to law enforcement activities differs in nature and substance and therefore certainly does not provide for a harmonised data protection approach of law-enforcement information, data subjects rights and effective independent supervision.

In view of the increasing use of availability of information as a concept for improving the fight against serious crime and the use of this concept both on a national level and between Member States, the lack of a harmonised and high level of data protection regime in the Union creates a situation in which the fundamental right of protection of personal data is not sufficiently guaranteed anymore.

Referring to its Position Paper on law enforcement and information exchange in the EU (April 2005) and recalling its declarations of Krakow (2005), Budapest (2006) and London (2006), all European Data Protection Authorities therefore call upon the Member States represented in the Council of the European Union and the European Parliament to explore every possibility for creating such a harmonised and high level of data protection throughout the European Union.

The European Data Protection Authorities are aware of the fundamental discussion in the Council on the scope of the proposed framework decision: should it apply only to data exchanged between Member States or should it apply to all processing activities by police and judicial authorities.

Reiterating the national impact of the Union's initiatives and the clear risk that limiting the scope to data that are exchanged or may be exchanged between Member States would make the field of application of the proposed framework decision particularly unsure and uncertain, the European Data Protection Authorities **stress that only a comprehensive scope covering all types of processing of personal data could provide individuals with the necessary protection**.

The European Data Protection Authorities **furthermore stress that also on other data protection principles the version of the draft framework decision as presented by the German Presidency on 13 March 2007 does not present a solid and high data protection regime** and has neither taken on board our European data protection Authorities' Opinion issued on 24 January 2006 nor the EP's opinion from May 18, 2006.

Whilst the draft decision has brought about some improvements in view of achieving a harmonised processing framework, it is as yet unsatisfactory as regards the safeguards provided to ensure citizens' right to privacy.

This is especially the case if account is taken of the already existing European data protection legislation, in particular, the legal framework created by those national lawmakers when transposing directive 95/46/EC, also made it applicable to the processing of personal data in the sector at issue. Furthermore, the European Data Protection Authorities reiterate that it is necessary to preserve the existing data protection safeguards at national level by adopting binding European instruments.

With a view to making a real improvement in the third pillar data protection, the Conference of European data protection Authorities underlines the following key principles to be dealt with in the future important legislation of the framework decision:

- Purpose limitation: necessity to define clearly the legitimate purposes allowing the processing of personal data in the framework of police and judicial cooperation in criminal matters without maintaining any general clause allowing for further processing «for any other purposes». The purpose limitation principle is a key principle in the EU directive and Convention 108.

- Data categories: the processing of special categories of data is prohibited unless specific conditions are met and specific guarantees are foreseeing in the national legislation (Art. 8 EU Directive, Art. 6 Convention 108). Furthermore, appropriate safeguards shall be provided for the processing of biometric and genetic data.

- Categories of data subject: It is a requirement of the principle of proportionality to reintroduce distinctions between the different categories of data subject concerned by the processing for police and law enforcement purposes.

- Regulation of data transfers to third countries: It is a requirement of the adequacy principle that common criteria and a procedure for the adoption of the measures necessary in order to assess the level of data protection in a third country or international body is defined before transferring the personal data and not leave it entirely to the discretion of Member States. Fixing an EU standard in such a procedure is a requirement for achieving harmonisation in Europe and the concept of adequacy findings corresponds to the provision in the Council of Europe Convention of 28 January 1981 for the protection of Individuals.

- Information of the data subject: Information of the data subject shall provide for complete provisions including the identity of the data controller, the possible recipients and the legal basis for processing. Any restrictions shall be precise and limited.

- Right of access: the regime of the right of access must be in line with the requirements of the European Human Rights Convention and the case law. In excluding in some cases the possibility to have an effective right of appeal, the current proposal is not in line with those requirements. Furthermore the supervisory authorities or appeal jurisdiction shall have the right to communicate information to the data subject in case of unjustified refusal. The exception to the right of access shall also be more limited.

- Notification and prior checking: notification and prior checking of processing to the supervisory authority should, where appropriate, constitute a precondition for processing. Prior checking shall be carried out by the national data supervisory authorities. The possibility of exemptions from publication of notification will have to be considered according to the nature of processing.

- Supervisory authorities: the concept of a JSA shall be understood as an independent supervisory authority. The framework decision shall provide for its composition, tasks and competences. It shall be endowed in particular with consultative, investigative and intervention powers.

The European Data Protection Authorities also recognise the importance of adopting the framework decision as soon as possible. However, the proposal presently under discussion will not provide for a sufficiently harmonised and high level of data protection. The fundamental character of the framework decision not only for safeguarding the rights of the citizens of the European Union but also for law enforcement, justifies a discussion that is not compromised by a strict timeframe.

The European Data Protection Authorities therefore call upon the Council to allow itself more time for the negotiations to develop a framework decision offering a high level of data protection.

The European Data Protection Authorities are, of course, willing to contribute further in the process of adopting such a framework decision and suggest to be heard by the Council working group to explain their positions.

4.19 Common position of the European Data Protection Authorities on the use of the concept of availability in law enforcement, Adopted on 11 May 2007

DECLARATION

The European Union initiated several initiatives to improve the effectiveness of law enforcement and combating terrorism in the European Union. In this context, the exchange of law enforcement information in accordance with the principle of availability is a key issue in the third pillar cooperation.

Monitoring these developments, the Conference of European Data Protection Authorities already called on the Members of the European Union and the Commission, the Council and the European Parliament to establish strong and harmonized data protection safeguards[1].

The various forms in which this concept of «availability» is used, explicitly or implicitly, in developing strategies and legal instruments to improve effectiveness in law enforcement, makes it also necessary to establish a comprehensive framework for assessing the use of this concept. By creating such a framework, guidance will be provided to assess every proposal that uses the existence of personal data as a chance to improve the effectiveness of law enforcement. Such a framework may thus contribute to a balanced assessment of the interrelation between public security and the fundamental right of protection of personal data.

The Conference has adopted the attached Common Position on the use of the availability principle in law enforcement. This Common Position includes a checklist for assessing any proposal using availability of personal data as its basis.

This paper and checklist are addressed specifically to all EU institutions as well as national parliaments as a constructive contribution to respect and strengthen the civil liberties of the citizens living in the EU when expanding the possibilities for the use of information by law enforcement authorities.

[1] Krakow Declaration, 25-26 April 2005,
Budapest Declaration, 24-25 April 2006.

Executive summary

In the context of combating terrorism and improving internal security, the European Union initiated several initiatives to improve the effectiveness of law enforcement in the European Union, using the concept of availability as guiding principle for the exchange of law enforcement in third pillar cooperation.

The various forms in which this concept of availability is used, explicitly or implicitly, in developing strategies and legal instruments to improve effectiveness in law enforcement, makes it necessary to establish a comprehensive framework for assessing the data protection aspects relating to the use of this concept. By creating such a framework, guidance will be provided to asses every proposal that uses the existence of personal data as a chance to improve the effectiveness of law enforcement. Such a framework may thus contribute to a balanced assessment of the interrelation between public security and the fundamental right to the protection of personal data as enshrined in the Charter of Fundamental Rights of the European Union.

The European Data Protection Authorities, stressing the need to create such a framework, have developed some conditions and guidelines for assessing the use of the availability concept in the following Common Position paper and checklist. This checklist can be used for assessing every proposal that uses the availability of personal data as stepping stone to improve law enforcement. The European Data Protection Authorities urge the Commission, Council and European Parliament to use this checklist when developing, assessing and adopting any proposal using availability of personal data as a stepping stone to improve law enforcement or the cooperation between law enforcement authorities.

Common position on the use of the concept of availability in law enforcement

1. Introduction

In the context of combating terrorism and improving internal security, the European Union initiated several initiatives to improve the effectiveness of law enforcement in the European Union.

Article 29 TEU aims at providing citizens with a high level of safety within an area of freedom, security and justice. This area of freedom, security and justice is gradually developing and leads to the abolishment of the borders between the Member States for law enforcement information. However, the enforcement powers of the Member States are still bound by these national borders.

Within this context, the exchange of law enforcement information using the concept of availability has become a key issue in third pillar cooperation:

- as an important instrument in realising a free flow of law enforcement information, not hampered by internal borders,

- by providing for safety for the citizen by means of facilitating the combat of trans-border crime,

- by respecting the protection of fundamental rights and freedoms of the citizen, in particular the rights to privacy and data protection.

These three objectives must be met in a balanced way. This is not obvious in view of the specific character of law enforcement and also in the light of the trend in police work to increasingly use personal data for proactive research. A guiding principle in law enforcement seems to be: when data are needed, they should be used. Or, even clearer: when data are available they can be used.

This subject clearly demonstrates the close interrelation between public security and the fundamental right to the protection of personal data as enshrined in the Charter of Fundamental Rights of the European Union.

An important element in that interrelation is mutual trust. Mutual trust (and mutual recognition) is an essential condition for exchange of law enforcement information. Governments and government authorities are only prepared to effectively share information with (authorities in) other Member States if it is assured that these other Member States use this information with respect of appropriate legal conditions, for reasons of data protection and security.

Already adopted EU legislation as well as recent initiatives are not limited to stimulating the exchange of personal data between law enforcement authorities of personal that is data already processed by those authorities. Some also focus on the use for law enforcement purposes of personal data that are processed by parties in the private and public sector or in European data bases. When there seems to be an indication that these might be needed for law enforcement purposes, these data are (proposed to be) made available to law enforcement authorities.

The various forms in which this concept of availability is used, explicitly or implicitly, in developing strategies and legal instruments to improve effectiveness in law enforcement, makes it necessary to establish a comprehensive framework for assessing the data protection aspects relating to the use of this concept. By creating such a framework, guidance will be provided to assess every proposal that uses the existence of personal data as a chance to improve the effectiveness of law enforcement.

The European Data Protection Authorities, stressing the need to create such a framework, have developed some conditions and guidelines for assessing the use of the availability concept. The European Data Protection Authorities urge the Commission, Council and European Parliament to use these when developing, assessing and adopting any proposal using availability of personal data as a stepping stone to improve law enforcement or the cooperation between law enforcement authorities.

2. Scope of the availability concept

The strategy of the European Union as defined in The Hague Programme on strengthening freedom, security and justice[2] aims that with effect from 1 January 2008, the exchange of law enforcement information should be governed by the principle of availability.

Following that strategy the Commission presented on 12 October 2005 its proposal for a Council Framework Decision on the exchange of information under the principle of availability[3]. This proposal lays down an obligation for the Member States to give access to or to provide certain types of information available to their authorities (see Recital 6).

The principle of availability as used in The Hague Programme and the proposed Framework Decision mean that, throughout the European Union, a law enforcement officer in one Member State who needs information in order to perform his duties should be able to obtain this from another Member State and that the law enforcement authority in the other Member State which holds this information will make it available for the

[2] OJ C 53,3.3.2005, p.1.
[3] COM (2005) 490.

stated purpose. The proposed Framework Decision limits the principle of availability by stating that the decision does not entail any obligation to collect and store information for the sole purpose of making it available (Article 2(1)).

Sharing available information such as personal data, is already foreseen in existing EU legislation and multilateral conventions. Recent proposals for improving the cooperation between law enforcement authorities also use the availability concept as guiding principle. However, in all these legal instruments and proposals, availability of personal data is presented in different forms and modalities leading to different consequences. These differences make it necessary to further explore the scope of this concept.

One of the first examples of sharing personal data as a specific aspect of effective cooperation between European law enforcement authorities is perhaps the Convention of 19 June 1990 implementing the Schengen Agreement of 14 June 1985[4]. Processing personal data of specific categories of persons and making those available - by using one central information system - for different authorities in the States that implemented the Schengen Convention is seen as a necessary compensatory measure for creating a high level of security in an area of free movement of persons.

Another step in improving cooperation between law enforcement authorities was marked by the Europol Convention[5] and Eurojust Decision[6]. Two European offices were established with, among other tasks, a specific task to facilitate the exchange of law enforcement information.

These forms of cooperation may be characterised as cooperation by expressing the intention to share information without a specific obligation to do so.

More recent examples of making personal data available for law enforcement authorities are the Framework Decision on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union[7] and the Treaty of Prüm of 27 May 2005. These two legal instruments introduce a new element in law enforcement cooperation: Member States are in principle obliged to make personal data available. The use of wordings as: «shall provide at the request» (Framework Decision) and «will allow access… and right to consult» (e.g. Article 3(1) Prüm Treaty) clearly indicate the obliging character of making data available.

The Prüm Treaty furthermore introduces an obligation to set up certain data files to facilitate the prevention and prosecution of crimes. Contracting Parties must for example guarantee the availability of reference indexes of fingerprints (Article 8).

[4] OJ L 239, 22.9.2000, p.19.
[5] OJ C 316, 27.11.95, p.1.
[6] OJ L 63, 6.3.2002, p.1.
[7] OJ L 386, 29.12.2006, p.89.

The existing more or less voluntary exchange of information is in these areas not only replaced by an obligation to provide information, but also by an obligation to create for certain categories of personal data an infrastructure enabling other law enforcement authorities to have access to available data.

Such an obligation to make information available is not necessarily limited to law enforcement authorities. For example, Recital 19 of Directive 2006/24/EV on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, specifically mentions that «*it is necessary to ensure that retained data are made available*». It is ensured on a European level that certain categories of data processed by private parties should be made available for law enforcement.

The concept of availability is also an important subject of the Communication from the Commission to the Council and the European Parliament of 24 November 2005 on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs[8]. Sharing available information by linking databases is a key item in future thinking in the European Union.

Other initiatives such as the new legal basis of the second generation Schengen Information System and the creation of the Visa Information System also contain aspects of the availability concept. Personal data processed for a specific purpose is made available for other purposes such as law enforcement.

In view of this variety of manifestations of the concept of availability as key factor for the improvement of effectiveness of law enforcement and their impact on the fundamental right of protection of personal data, the European Data Protection Authorities stress the need to contextualize the practice of the use of the availability concept in a comprehensive way. Any action of harmonising the processing of personal data, either by introducing obligations to retain personal data or by introducing an obligation to set up specific data files, and the introduction of an intention or obligation to make these personal data available for law enforcement authorities or for European or international institutions involved with law enforcement, should be seen as implementation of the concept of availability.

Using this scope, the European Data Protection Authorities have explored its implications in perspective of the applicable data protection legislation.

[8] COM(2005) 597.

3. Applicable law

In addition to the right to respect for private and family life guaranteed by Article 8 of the ECHR and reaffirmed by Article 7 of the Charter of Fundamental Rights of the European Union, the new fundamental right to data protection is enshrined in Article 8 of the Charter.

The ECHR allows interference with the right to privacy if necessary for the interests referred to in the second paragraph of Article 8 and when justified by those interests; such interference must take account of the principle of proportionality. Article 8 of the Charter of Fundamental Rights expands on this, stipulating that personal data must be processed fairly for specified purposes, and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. This legitimate basis has also to fulfill the conditions of proportionality.

The 1981 Council of Europe Convention for the Protection of Individuals to Automatic Processing of Personal Data (Convention 108) provides more specific principles for data protection also applicable in the Third Pillar. There is also a Recommendation (No. R(87) 15) with specific data protection provisions for the use of personal data in the police sector, which was adopted in 1987 by the Committee of Ministers to Member States regulating the use of personal data in the police sector.[9]

The Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data[10] provides for a harmonized data protection regime in the European Union. Although activities referred to in Titles V and VI of the Treaty on European Union fall outside the scope of this directive, Member States apply the general data protection principles to law enforcement activities.

The Regulation 45/2001 of the European Parliament and of the Council of 18 September 2000[11] provides rules on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. The principles of this Regulation are used by defining the data protection regime applicable to the processing of personal data in European data bases such as the Visa Information System and the second generation Schengen Information System.

The Europol Convention and Eurojust Decision contain specific data protection regime for these organizations based on the general data protection principles as defined in the Convention 108 and the Recommendation No. R(87) 15 referred to above.

[9] Recommendation No. R (87) 15, of 17 September 1987
[10] OJ L 281, 23.11.1995, p. 31.
[11] OJ L 8, 12.1.2001, p.1.

Concerning data processing by private parties, public parties and the European Institutions and in European data files, the applicable EU laws contain a fundamental principle on the lawfulness of the processing of personal data: data should be collected for explicit and legitimate purposes and not further processed in a way incompatible with those purposes. An exemption or restriction is only allowed when provided for by law and when this constitutes a necessary measure to safeguard national and public security or the prevention, investigation, detection and prosecution of criminal offences. The definition used in those legal instruments for processing of data includes the disclosure by transmission, dissemination or otherwise making available.

In those situations where applying the availability concept, data which are originally processed for purposes outside the law enforcement scope are used for law enforcement, the exemption to the fundamental rule of purpose limitation needs to fulfill all the conditions for the use of this exemption.

4. Implementing the availability concept

The success of effective law enforcement will be dependant on the information position of law enforcement authorities, the possibility to collect within the limits of the law information, the quality and use of these data and the capability to share these data with other law enforcement authorities. The different forms of law enforcement cooperation in the European Union as described in Chapter 2, cover all these aspects.

In respect of all the initiatives to exchange personal data between law enforcement authorities in the European Union and the exchange with third States and parties, the European Data Protection Authorities already declared that «G*iven the Union's obligation to respect human rights and fundamental freedoms, initiatives to improve law enforcement in the EU, such as the availability principle, should only be introduced on the basis of an adequate system of data protection arrangements guaranteeing a high and equivalent standard of data protection*.»[12]

In that respect, the European Data Protection Authorities welcome the draft Council Framework Decision on the protection of personal data processed in the framework of police- and judicial cooperation in criminal matters[13]. A harmonised and high level of data protection in the area of law enforcement as should be ensured by a Council Framework Decision is now considered a conditio sine qua non for law enforcement in the European Union.

[12] Krakow Declaration, 25-26 April 2005.
[13] COM (2005) 475.

However, it should be stressed that such a harmonised data protection framework does in itself not present a comprehensive tool for assessing the implementation of the availability concept in all varieties as described in Chapter 2. That framework only applies when personal data are already processed by law enforcement authorities. Furthermore, the discussions on that draft Framework Decision are still taking place in the Council.

Since the variety in the use of the availability concept results in the application of different legal instruments, a comprehensive framework for assessing the use of this concept should therefore cover all aspects of the use of the availability concept. Such a framework should be a separate instrument also to be used supplementary to existing legislation.

5. A comprehensive framework for assessing the use of the availability concept.

Law enforcement is dependant on information. In principle two sources of information are used: information already processed by law enforcement authorities and information that is processed by others. This distinction is somewhat artificial since data processed by law enforcement authorities may have been obtained from private or public authorities.

When personal data are processed by private or public authorities, the data protection principles as defined in Directive 95/46/EC will be guiding. When these data are processed either by European institutions or in European data files, the principles of Regulation 45/2001 and/or the applicable specific rules for these files will apply.

As already stated, the use of these data for law enforcement purposes will in general constitute an exemption to the fundamental rule of purpose limitation and is only allowed when provided for by law and when this constitutes a necessary measure to safeguard national and public security or the prevention, investigation, detection and prosecution of criminal offences.

In case data are already processed by law enforcement authorities the (draft) Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters will provide for a necessary legal data protection framework for the processing and exchange of information between law enforcement authorities. However, new initiatives for processing these data may be introduced, based on the concept of availability.

In assessing whether an exemption is needed and in compliance with the formal conditions or when assessing new initiatives for making law enforcement data available, it will be necessary to focus on the different conditions provided for by the applicable data protection rules.

The first condition relates to the obligation that any measure should be provided for by law. This law must comply with strict criteria such as being clear, simple and precise: they are to be transparent and readily understandable for everybody. According to the case-law of the Court of Justice, the principle of legal certainty requires that legislation must be clear and precise and its application foreseeable by individuals. Furthermore, legislation must always determine the grounds, purpose and the conditions for the processing, as well as install an adequate and effective system of independent supervision.

The second condition which needs to be complied with is that any measure should be necessary and proportionate. It is especially the assessment of this aspect that needs a comprehensive approach. Such an approach should include the following assessment steps:

A. Evaluation of already existing legal measures allowing the processing including the exchange of data.

Are these measures not sufficient or is their implementation and follow up not effective? When a legal measure is effectively used but does apparently not provide for a sufficient and effective element in the fight against crime, this might be an indication that another measure is needed. However, when the evaluation demonstrates that already existing possibilities are not used sufficiently, this may create considerable doubt whether a proposed new measure will be a justified.

In case this assessment indicates that the legal measure could be justified, the following conditions should be met:

B.Proportionality

Effective enforcement, but with a minimum interference with privacy. This means a proportionality-test with the following elements:

- The measure must be appropriate, which means its con tribution to law enforcement must be clearly demonstrated.
- A measure with less impact can not lead to the same result.

- A balance must exist: where an impact on data protection may be justi fied in order to fight terrorism and other serious crime (as referred to in Article 2(2) of the Framework Decision on the Euro pean Arrest Warrant), this does not mean that these data may be made available to fight minor mis demeanours.
- The legal instrument should be subject of compulsory evaluation.

The third condition relates to the categories of data to be processed and other specific conditions. Different types of data are involved: ranging from identification data (used for both identification of data subject and for contacting him) and general and specific descriptive data (e.g. intelligence) to types identified on the basis of their biometrics (e.g. fingerprint and DNA digital representation) and sensitive data (as referred to in Article 8 of Directive 95/46). Similarly, different types of data subjects are involved: suspects, non suspects, witnesses, convicted or acquitted persons. The following points should be taken into account:

A. Legislation must distinguish between these data and must provide for complementary safeguards in respect of processing data that are likely to present specific risks to the rights and freedoms of the data subject, in particular sensitive data by introducing a sliding scale of protective measures, in which the characteristics of the data determine special conditions and limitations for their use. It should include criteria for a clear distinction between personal data, differentiating categories of personal data and their availability for specific categories of crime. For example, persons acquitted from a charge or against whom no charges are pressed should clearly be distinguished from convicted persons. Data on non-suspects and witnesses should be clearly distinguished from data on suspects. Such a distinction could be linked with the distinction between different categories of persons in Article 4(3) of the Commission proposal for a draft Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

B. Specific measures to assess the quality of data must be introduced to guarantee the highest possible level of data quality before data are to be made available. In view of the impact of the use of data for law enforcement purposes sufficient technical and organisational measures and procedures must be in place to guarantee the quality of data. In case such guarantees can not be provided for, this must be indicated and the use of

those data must be limited to a specific law enforcement activity with additional safeguards. An obligation to inform the recipient of personal data of any change in those data must be compulsory.

C. The use of biometric data in law enforcement requires extra safeguards for their use. Especially the use of these data for identification purposes, sometimes using systems that process huge amounts of these data such as the new Schengen information System must be accompanied by procedures for the individual to have the result of the comparison rechecked.

D. Specific processing operations that are likely to present specific risks (e.g. fishing expeditions, data mining, specific surveillance techniques) require extra safeguards for the use of these data and the monitoring of the use of these operations.

E. It will be important to ensure with technical and organisational measures and procedures that the receivers of personal data are supplied with the necessary information to use the data for the purposes for which they were exchanged and to keep them up to date.

F. When an initiative or proposal makes a choice between processing of personal data on a central level or decentralised, this choice may not only be motivated by reasons of operability. Such a choice must also take into account the need to guarantee the highest possible level of data quality and data protection standards. When decentralised processing provides for the best safeguards, central processing should not be an option.

The fourth condition relates to the access to these data.

Routine access to personal data must be prohibited. Access should be limited to specific cases or a specific law enforcement task, and control of the use of this access must be sufficiently safeguarded. Recipient authorities must be clearly identified. When direct access to data is proposed, the use of index or hit-no-hit systems and sufficient access controls are required.

The fifth condition relates to control and supervision.

In addition to the standard competences of law enforcement authorities, judicial authorities and data protection authorities for controlling and supervising data processing activities that are likely to present specific risks to the rights and freedoms of the data subject should be accompanied by additional and tailor made measures of control and supervision of all operational activities including the use and mis-use of personal data. Specific provisions are needed preventing difficulties arising from the exchange of data between Member States. Since those data are available within several jurisdictions, it must be ensured that control and supervision have effect in all jurisdictions involved.

6. Conclusion

The European Data Protection Authorities recognize that information and personal data are essential for effective law enforcement. They would reiterate, however, that any measure in which the concept of availability is used ought to be proportionate, respecting the fundamental rights of the individual. This Common Position and the checklist are addressed specifically to the EU institutions as a constructive contribution to current initiatives. It presents the conditions that must be met to maintain a high level of data protection in the field of law enforcement. The European Data Protection Authorities are, of course, willing to contribute further to ensuring that the process of improving law enforcement is combined with respect to fundamental rights.

Checklist assessing any measure implementing the availability concept in law enforcement.

I. Law and evaluation

Any measure must be provided for by law.
This law must comply with strict criteria such as being precise and creating certainty and foreseeability.

Furthermore, legislation must always:

- Determine the grounds,
- Purpose and
- The conditions for the processing.
- Install an adequate and effective system of independent supervision.

II. Necessity and proportionality

The measure should constitute a necessary safeguard.

A. Evaluation of already existing legal measures allowing the proces sing including the exchange of data.

- Are these measures not sufficient?
  - When a legal measure is effectively used but does apparently not provide for a sufficient and effective element in the fight against crime, this might be an indication that another measure is needed.
- Is their implementation and follow up not effective?
  - When the evaluation demonstrates that already existing possibilities are not used sufficiently, this may create considerable doubt whether a proposed new measure will be a justified exemption to the rule of purpose limitation.
- In case this assessment indicates that the legal measure could be justified, the following conditions of proportionality should be met:

B. Proportionality

- The measure should be designed to achieve
  - Effective enforcement,
  - Minimum interference with privacy.
- This means a proportionality-test with the following elements:
  - The measure must be appropriate, which means its contribution to law enforcement must be clearly demonstrated.
  - It must not be excessive, which means that a measure with less impact cannot lead to the same result.
  - A balance must exist: where an impact on data protection may be justified in order to fight terrorism and other serious crime (as referred to in Article 2(2) of the Framework Decision on the European Arrest Warrant), this does not mean that these data may be made available to fight minor misdemeanours.
- The legal instrument should be subject of compulsory evaluation.

III. *Specific conditions*

Different types of data are involved: ranging from identification data (used for both identification of data subject and for contacting him) and general and specific descriptive data (e.g. intelligence) to types identified on the basis of biometrics (e.g. fingerprint and DNA digital representation) and sensitive data (as referred to in Article 8 of Directive 95/46). Similarly, different types of data subjects are involved: suspects, non suspects, witnesses, convicted or acquitted persons. The following points should be taken into account:

A. Legislation must:

- Distinguish between these data,
- Provide for specific and complementary safeguards in respect of processing data that are likely to present specific risks to the rights and freedoms of the data subject, in particular the use of sensitive data by introducing a sliding scale of protective measures, in which the characteristics of the data determine special conditions and limitations for their use.

- Include criteria for a clear distinction between personal data, differentiating categories of personal data and their availability for specific categories of crime. (For example, persons acquitted from a charge or against whom no charges are pressed should, for example clearly be distinguished from convicted persons. Data on non- suspects and witnesses should be clearly distinguished from data on suspects.)

B. Specific measures to assess the quality of data must be introduced to guarantee the highest possible level of data quality before data are to be made available. In view of the impact of the use of data for law enforcement purposes sufficient technical and organisational measures and procedures must be in place to guarantee the quality of data. In case such guarantees cannot be provided for, this must be indicated and the use of those data must be limited to a specific law enforcement activity with additional safeguards. An obligation to inform the recipient of personal data of any change in those data must be compulsory.

C. The use of biometric data in law enforcement requires extra safeguards. Especially the use of these data to identify persons, sometimes using systems that process huge amounts of these data should be accompanied by procedures for the individual to have the result of the comparison rechecked.

D. Specific processing operations that are likely to present specific risks (e.g. fishing expeditions, data mining, specific surveillance techniques) require extra safeguards for the use of these data and the monitoring of these operations.

E. It will be important to ensure, by technical and organisational measures and procedures, that the receivers of personal data are supplied with the necessary information to use the data for the purposes for which they were exchanged and to keep them up to date.

F. When an initiative or proposal makes a choice between processing of personal data on a central level or decentralised, this choice must not only be motivated by reasons of operability. Such a choice must also take into account the need to guarantee the highest possible level of data quality and data protection standards. When decentralised processing provides for better safeguards, central processing should not be an option

IV. Access by law enforcement authorities to personal data

- Routine access to personal data must be prohibited.
- Access must be limited to specific cases or a specific law enforcement task.
- Control of the use of this access must be sufficiently safeguarded.
- When direct access to data is proposed, the use of index or hit-no-hit systems and sufficient access controls are required.
- The recipient authorities must be clearly identified.

V. Control and supervision

- In addition to the standard competences of law enforcement authorities, judicial authorities and data protection authorities for controlling and supervising data processing, activities that are likely to present specific risks to the rights and freedoms of the data subject should be accompanied by additional and tailor made measures of control and supervision of all operational activities including the use and mis-use of personal data.
- Specific provisions are needed preventing difficulties arising from the exchange of data between Member States. Since those data are available within several jurisdictions, it must be ensured that control and supervision have effect in all jurisdictions involved.