16. Tätigkeitsbericht 2008/2009

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Tätigkeitsbericht 2008/2009
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 2008 und 31. März 2009 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. 410.016.d/f

Inhaltsverzeichnis

* Originaltext auf Französisch

* Originaltext auf Französisch

* Originaltext auf Französisch

* Originaltext auf Französisch

Vorwort

Ein erfolgreicher Datenschutz braucht Ausdauer und Pragmatismus

Facebook und andere Soziale Netzwerkseiten im Internet erfreuen sich zunehmender Beliebtheit und haben inzwischen weltweit mehrere hundert Millionen von Nutzerinnen und Nutzern. Vor allem die junge Generation findet es ausserordentlich cool, auf diesem Weg «Freunde» zu gewinnen, sich über gemeinsame Interessen auszutauschen und dabei auch sehr Persönliches preis zu geben. Interessant ist, dass zunehmend auch ältere Semester sich dieser Instrumente bedienen: Politiker realisieren, dass man auf diesem Weg gleichsam mit Schneeballeffekt fast gratis sehr viele Wählerinnen und Wähler erreichen kann. So dürfte der US-Präsident Barack Obama seine Wahl massgeblich der Einbindung der Sozialen Netzwerke in seine Kampagne zu verdanken haben. Auch in der Schweiz bedienen sich Politiker vermehrt dieses Instruments. So ist das Referendum gegen die biometrischen Pässe das erste erfolgreich eingereichte internetbasierte Referendum. Inzwischen ist klar, dass sehr viele Akteure – vom Arbeitgeber bis zu den Geheimdiensten – diese immer üppiger sprudelnde Informationsquelle für ihre Zwecke nutzen.

Im vergangenen Jahr waren wir intensiv mit den zahlreichen Aspekten dieses neuen Phänomens konfrontiert. Was bedeuten sie für den Datenschutz? Ob es uns passt oder nicht, die Verbreitung dieser Netzwerke ist nicht mehr aufzuhalten. Somit geht es für uns in erster Linie darum, die Entwicklung genau zu beobachten, um offensichtliche Fehlentwicklungen rechtzeitig erkennen und handeln zu können. Gleichzeitig haben wir uns darauf konzentriert, über unsere Website Verhaltensanweisungen zu propagieren, die einen gefahrlosen Umgang mit diesen neuen Möglichkeiten fördern. Für eine erfolgreiche Aufklärungsarbeit brauchen wir Augenmass und die Unterstützung anderer gesellschaftlicher Akteure. Ich denke da vor allem an die Schulen.

Ausdauer und Pragmatismus braucht es auch im heikelsten Bereich staatlicher Informationsbeschaffung und -bearbeitung: dem Staatsschutz. Seit Jahren fordern wir, dass das bestehende indirekte Auskunftsrecht in ein direktes überführt werden sollte und der Rechtsschutz der Bürgerinnen und Bürger verbessert werden müsse. Ziemlich genau 20 Jahre nach der Fichenaffäre kommt Bewegung in diese Sache. Ausgangspunkt waren die bekannt gewordenen Fichierungen von Basler Grossräten und Grossrätinnen kurdischer Herkunft. Im Gefolge der dadurch entstandenen Verunsicherung erreichte uns eine zehnfach höhere Zahl von Einsichtsgesuchen, und wir informierten in diesen Fällen die Gesuchsteller in Anwendung des Art. 18 Abs. 3 BWIS ausnahms-

weise, ob sie eingetragen waren oder nicht. Massgebend war für uns der Umstand, dass die Betroffenen befürchten mussten, dass sie wegen ihrer politischen Tätigkeit fichiert waren, was mit Art. 3 BWIS nicht vereinbar wäre. Bereits Anfangs Berichtsjahr machten wir in vier Fällen von dieser Ausnahmebestimmung Gebrauch. Dabei mussten wir uns zunehmend auch mit der Frage auseinander setzen, ob die vom DAP verfolgte Praxis mit den in Art. 3 BWIS statuierten Schranken vereinbar sei: Danach dürfen Informationen über politische Betätigungen und die Ausübung der Meinungs-, Koalitions- und Versammlungsfreiheit nicht bearbeitet werden. Diese Fälle zeigten einmal mehr die Mängel des derzeitigen indirekten Auskunftsrechts, das eine effektive Überprüfung der Einträge nicht zulässt.

Im Lichte dieser Fälle reichte Nationalrätin Susanne Leutenegger Oberholzer einen Vorstoss ein, der verlangt, dass auch im Bereich des Staatschutzes grundsätzlich ein direktes Einsichtsrecht gelten soll, wenn dem keine Staatschutzinteressen entgegenstehen. Der Bundesrat akzeptierte inzwischen ihren Vorschlag. Die derzeit hängige BWIS-Revision greift noch ein weiteres unserer langjährigen Ceterum censeo auf: Nachdem der Nationalrat zunächst wegen der fragwürdigen Verschärfung des Gesetzes auf diese Revision gar nicht erst eintreten wollte, ist nach dem Rückweisungsentscheid des Ständerates klar, dass der Bundesrat vor allem auch den Rechtschutz verbessern muss.

Der Bundesrat akzeptierte in der ersten Hälfte des letzten Jahres die Empfehlungen der Schengen-Evaluation und fasste entsprechende Beschlüsse zur Verbesserung der Unabhängigkeit des EDÖB und der Aufstockung der Ressourcen. Damit stand der Umsetzung des Abkommens nichts mehr im Wege. Inzwischen haben wir die uns obliegenden Kontroll- und Aufsichtsaufgaben aufgenommen. Letztes Jahr stand die Botschaft in Kiew auf dem Programm. Zusammen mit den Datenschutzbehörden der Schengen-Staaten wurde eine weitere Kontrolle durchgeführt. Dieses Jahr ist die Reihe am Fedpol und an weiteren Botschaften. Die notwendige Zusammenarbeit mit den Kantonen ist angelaufen und wird auf der Basis eines vom EDÖB initiierten Reglements an die Hand genommen.

Bei den eHealth-Projekten hat der Bundesrat das Realisierungstempo erhöht. Es ist nur noch eine Frage der Zeit, bis das elektronische Patientendossier Realität sein wird. Auf diesem Weg sind jedoch noch zahlreiche Probleme zu lösen, nicht zuletzt im Bereiche des Datenschutzes. Wir begleiten diese Projekte eng, da auf die Bürgerinnen und Bürger grosse Gefahren zukämen, wenn die Anliegen des Datenschutzes nicht gebührend berücksichtigt werden. Für uns ist klar, dass die Einführung des elektronischen Patientendossiers für die Betroffenen eine Verbesserung des Schutzes ihrer Krankenakte im Vergleich zum heutigen Papierdossier mit sich bringen muss.

Das Öffentlichkeitsgesetz steht nun im dritten Jahr. Die vom Gesetz nach drei Jahren vorzunehmende Evaluation, mit der wir das Institut de hautes études en administration publique IDHEAP beauftragt haben, liegt vor. Die Feststellungen sind für uns mehrheitlich nicht überraschend: Die Ressourcen für die Durchführung der Mediationen und die Erarbeitung der gesetzlich vorgesehenen Empfehlungen genügen nach wie vor nicht. Deshalb können die im Gesetz vorgegebenen Fristen nicht eingehalten und auch die übrigen uns übertragenen Aufgaben nicht korrekt erfüllt werden. Das hat unter anderem zur Folge, dass die Bekanntheit des Gesetzes ausserordentlich gering ist, was gemäss der Studie dazu führt, dass in der Schweiz im Vergleich zu anderen Staaten in Prozent der Bevölkerung mit Abstand am wenigsten Gesuche um Zugang zu amtlichen Dokumenten gestellt werden. In konzeptioneller Hinsicht wurde ein bedeutsamer Mangel ausgemacht: In Fällen, in denen die Verwaltung unseren Empfehlungen nicht folgt und der Gesuchsteller aus finanziellen Gründen den Fall nicht an das Bundesverwaltungsgericht weiterzieht, besteht vor allem in politisch heiklen Fällen keine Möglichkeit einer richterlichen Klärung. Die Studie empfiehlt deshalb, unsere Rechte zu stärken, indem uns wie im DSG das Recht gegeben wird, in wichtigen Fällen selbständig an das höchste Gericht zu gelangen. Wir sind gespannt, wie die Politik auf diese Empfehlungen reagieren wird. Diese Reaktion wird uns für unsere eigene Gewichtung der Aufgabe einen Anhaltspunkt geben, welche Priorität die Politik dem Öffentlichkeitsgesetz beimisst. Auch hier werden wir dran bleiben und uns mit Ausdauer und Pragmatismus für eine effiziente Umsetzung des Gesetzes bemühen.

Hanspeter Thür

Abkürzungsverzeichnis

AFAPDP	Association francophone des Autorités de protection des données personnelles
AFIS	Automatisiertes Fingerabdruck-Identifikationssystem
BAFU	Bundesamt für Umwelt
BAG	Bundesamt für Gesundheit
BAKOM	Bundesamt für Kommunikation
BFS	Bundesamt für Statistik
BGÖ	Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung
BIT	Bundesamt für Informatik und Telekommunikation
BJ	Bundesamt für Justiz
BPG	Bundespersonalgesetz
BPI	Bundesgesetz über die polizeilichen Informationssysteme des Bundes
BStatG	Bundesstatistikgesetz
BSV	Bundesamt für Sozialversicherungen
BVG	Bundesgesetz über die berufliche Alters-, Hinterlassenen- und Invalidenvorsorge
BVGer	Bundesverwaltungsgericht
BVV 3	Verordnung über die steuerliche Abzugsberechtigung für Beiträge an anerkannte Vorsorgeformen
BWIS	Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit
CODIS	Combined DNA Index System
DAP	Dienst für Analyse und Prävention (VBS)
DBG	Bundesgesetz über die direkte Bundessteuer
DEZA	Direktion für Entwicklung und Zusammenarbeit
DSG	Bundesgesetz über den Datenschutz

DSMS	Datenschutzmanagementsystem
EAV	Eidgenössische Alkoholverwaltung
EDA	Eidgenössisches Departement für auswärtige Angelegenheiten
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EPA	Eidgenössisches Personalamt
fedpol	Bundesamt für Polizei
GEWA	Datenverarbeitungssystem zur Bekämpfung der Geldwäscherei
GK	Gemeinsame Kontrollinstanz (Schengen)
GUMG	Bundesgesetz über genetische Untersuchungen beim Menschen
GwG	Geldwäschereigesetz
IPAS	Informatisiertes Personennachweis-, Aktennachweis- und Verwaltungssystem
ISA	Informationssystem Ausweisschriften
ISMS	Informationssicherheitsmanagementsystem
IWGDPT	International Working Group on Data Protection in Telecommunications
JANUS	Gemeinsames Informationssystem der kriminalpolizeilichen Zentralstellen des Bundes
KVG	Bundesgesetz über die Krankenversicherung
MEDAS	Medizinische Abklärungsstelle der Invalidenversicherung
RAD	Regionaler Ärztlicher Dienst
RTVG	Bundesgesetz über Radio und Fernsehen
RVOG	Regierungs- und Verwaltungsorganisationsgesetz vom 21. März 1997
SAS	Schweizerische Akkreditierungstelle
SBF	Staatssekretariat für Bildung und Forschung
SchKG	Bundesgesetz über Schuldbetreibung und Konkurs
SECO	Staatssekretariat für Wirtschaft SECO

Sedex	Secure data exchange
SGV	Schweizerische Gesellschaft der Vertrauens- und Versicherungsärzte
SIS	Schengener Information System
SKH	Schweizerischen Korps für humanitäre Hilfe
UBI	Unabhängige Beschwerdeinstanz für Radio und Fernsehen
UID	Unternehmens-Identifikationsnummer
ULD	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
UVG	Unfallversicherungsgesetz
VAD	Vertrauensärztlicher Dienst
VBGÖ	Verordnung vom 24. Mai 2006 über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsverordnung)
VBS	Departement für Verteidigung, Bevölkerungsschutz und Sport
VDSG	Verordnung zum Bundesgesetz über den Datenschutz
VDSZ	Verordnung über die Datenschutzzertifizierungen
VSABV	Verordnung über die Ausnahmen von der Schweigepflicht in der beruflichen Vorsorge und über die Auskunftspflicht der AHV/IV-Organe
VSMS	Verband Schweizer Markt- und Sozialforscher
VVG	Bundesgesetz über den Versicherungsvertrag
VwVG	Bundesgesetz über das Verwaltungsverfahren
Weko	Wettbewerbskommission

1. Datenschutz

1.1 Grundrechte

1.1.1 Produkt- und Systemzertifizierung im Datenschutzbereich

Wir haben den Auftrag erhalten, baldmöglichst die Richtlinien zur Festlegung der spezifischen Kriterien herauszugeben, die ein Produkt im Rahmen einer Zertifizierung erfüllen muss. Diese Aufgabe erweist sich jedoch als äusserst schwierig, da eine auf den Datenschutz ausgedehnte ISO-Zertifizierung 15408 ihrem Wesen nach komplex, im Verhältnis zu unserer gesetzgeberischen Situation teilweise phasenverschoben und vor allem schwer zu bewerkstelligen ist.

Was die Informationstechnologiedienste (IT-Dienste) anbelangt, würde sich die ISO-Norm 20000 von Vornherein recht gut eignen, doch wollte der Gesetzgeber diesen Bereich offenbar nicht einbeziehen. Schliesslich gibt es zwar den Kriterienkatalog EuroPriSe, der aber eine ziemlich gewagte Vermischung von Produkten und Dienstleistungen enthält und mehr einer Liste von Fragen zu Produkten oder Dienstleistungen und ihren Nutzern gleicht. Zudem ist EuroPriSe dem schweizerischen Recht nicht wirklich angemessen.

Nach dem erfolgreichen Erlass der Richtlinien über die Mindestanforderungen, denen ein Datenschutzmanagementsystem (DSMS) genügen muss (vgl. «Richtlinien für die Zertifizierung von Organisationen» auf unserer Webseite www.derbeauftragte.ch, Themen – Datenschutz – Datenschutzzertifizierung), ist der EDÖB beauftragt, bis zum 1. Januar 2010 die Richtlinien zu den spezifischen Kriterien herauszugeben, die ein Produkt im Rahmen einer Zertifizierung erfüllen muss. Diese Aufgabe dürfte aus folgenden Gründen äusserst schwierig werden:

Der Bereich der Produkte und Systeme unterscheidet sich deutlich vom Gebiet der Organisation, wie die auf der Norm ISO/IEC 15408:2005 beruhende Zertifizierung «Drittpartei» beweist (Kriterien zur Evaluierung der IT-Sicherheit, auch bekannt unter der englischen Bezeichnung «Common Criteria for Information Technology Evaluations»). Diese Norm entspricht der Version 2.3 der gemeinsamen Kriterien, aus deren umfassender Überarbeitung im Jahre 2006 die derzeitige Version CC 3.1. hervorgegangen ist. Ausgehend von der Begleitnorm ISO/IEC 18045:2005 (Methodik zur Evaluierung der IT-Sicherheit, auch bekannt unter der englischen Bezeichnung «Common Methodology for Information Technology Evaluations» CEM) wird die Produktevaluierung zunächst von einer SAS-akkreditierten unabhängigen Prüfstelle durchgeführt. Der Eva-

luationsbericht wird sodann an die staatliche Produktzertifizierungsstelle (die es in der Schweiz noch nicht gibt) zur Beurteilung und gegebenenfalls zur Erteilung des Zertifikats weitergeleitet, dessen Anerkennung auf europäischer Ebene durch das Abkommen SOG-IS (Senior Officials Group for Information Security) und auf internationaler Ebene durch das Abkommen CCRA (Common Criteria Recognition Arrangement) garantiert ist. Abgesehen von dem festgestellten strukturellen Unterschied ist auch darauf hinzuweisen, dass die Zertifizierung ISO 15408-1/3 relativ komplex und damit eher aufwendig ist und sich auf die wesenseigene Sicherheit und nicht auf den Datenschutz bezieht, und dass sie viele ausserhalb des Bereichs Produkte/Systeme liegende Anforderungen umfasst. Die Erweiterung dieser Norm auf den Datenschutz erscheint uns daher äusserst schwer machbar.

Im Übrigen beziehen die IT-Produkte und -Systeme die IT-Dienste nicht fundamental mit ein, für welche die Norm ISO/IEC 20000:2005 (Information Technology – Service Management) als Referenz dienen könnte. Eine Ausweitung der Sicherheit auf den Datenschutz wäre hier leicht denkbar, wie wir das auch für die Erweiterung der Informationssicherheitsmanagmentsysteme (ISMS, ISO 27001) auf die DSMS getan haben (vgl. unseren 15. Tätigkeitsbericht 2007/2008, Ziff. 1.1.2). Es geht indessen weder aus dem DSG und der Verordnung über die Datenschutzzertifizierungen (VDSZ) noch aus den Erläuterungen dazu klar hervor, dass der Gesetzgeber die Dienste im Rahmen der Produkt- und Systemzertifzierung einbeziehen wollte. Die Herausgabe von Richtlinien für die IT-Dienste scheint uns daher verfrüht.

Schliesslich haben wir auch den vom Unabhängigen Landeszentrum für Datenschutz (ULD) Schleswig-Holstein erarbeiteten Anforderungskatalog geprüft, der heute als «EuroPriSe Criteria Catalogue V0.3» weitergeführt wird. Dieses Projekt für ein «europäisches Datenschutz-Gütesiegel» soll bescheinigen, dass die IT-Produkte oder -Dienste eine mit den europäischen Vorschriften und der Gesetzgebung der Pilotländer (Agencia de Protección de Datos de la Comunidad de Madrid und Commission Nationale Informatique et Libertés) konforme Verwendung erleichtern. Der vorgeschlagene Kriterienkatalog führt unseres Erachtens die IT-Dienste auf reichlich gewagte Weise ein, er stösst offenbar europaweit auf keine sehr breite Unterstützung und gleicht eher einer «Checklist» betreffend die Merkmale des Produkts oder des Dienstes und die Anforderungen an ihre Betreiber als einem Anforderungskatalog für zertifizierbare Produkte; ausserdem würde er eine ziemlich umfangreiche Anpassung an das schweizerische Recht notwendig machen. Wir werden daher unsere Nachforschungen in diesem weit gefassten Gebiet fortführen, um die erwarteten Richtlinien möglichst bald herausgeben zu können.

1.1.2 Inkrafttreten der Richtlinien für die Zertifizierung von Datenschutzmanagementsystemen

Am 1. September 2008 sind unsere Richtlinien über die Mindestanforderungen an ein Datenschutzmanagementsystem samt Anhang in Kraft getreten. Sie lehnen sich stark an die internationalen Standardnormen ISO 27001 und ISO 27002 an, wobei das Schwergewicht von der Informationssicherheit auf den Datenschutz verlagert wurde.

Wie wir in unserem 15. Tätigkeitsbericht 2007/2008 (Ziff. 1.1.1) festgehalten haben, sieht die Verordnung über die Datenschutzzertifizierungen (VDSZ) vor, dass der EDÖB Richtlinien über die Mindestanforderungen an das Datenschutzmanagementsystem zu erlassen habe. Diese Richtlinien über die Zertifizierung von Organisationen und Verfahren (nachfolgend: DSMS-Richtlinien) haben wir nun ausgearbeitet. Sie sind am 1. September 2008 in Kraft getreten (siehe auf unserer Webseite www.derbeauftragte.ch, Themen – Datenschutz – Datenschutzzertifizierung).

Unsere DSMS-Richtlinien lehnen sich stark an die internationalen Normen und Standards an, insbesondere an ISO 27001:2005 (betreffend das Informationssicherheitsmanagementsystem), aber auch an ISO 9001:2000 (betreffend das Managementsystem), wie dies in der VDSZ vorgesehen ist. Bei der Erstellung unserer Richtlinien haben wir vor allem die in den vorgenannten ISO-Normen enthaltenen Anforderungen an Managementsysteme übernommen. Gleichzeitig haben wir sichergestellt, dass das Schwergewicht auf die Datenschutzaspekte gelegt wurde. So ist anstelle des in ISO 27001:2005 enthaltenen Begriffs «Informationssicherheit» der Begriff «Datenschutz» einzusetzen. Auch wurde allgemein die Risikoanalyse gemäss ISO ergänzt durch die Einführung einer (Nicht-)Konformitätsanalyse. Als Ziele und Massnahmen führen die Richtlinien die allgemeinen Grundsätze nach DSG auf. Diese Ziele und Massnahmen haben wir im «Leitfaden für das Datenschutz-Management» im Anhang zu den Richtlinien konkretisiert. Der Leitfaden beschreibt für jeden Datenschutzgrundsatz jeweils das Ziel sowie die entsprechende Massnahme und anschliessende Umsetzung (eine ausführlichere Beschreibung findet sich in unserem 15. Tätigkeitsbericht 2007/2008, Ziff. 1.1.2).

Nachdem unsere DSMS-Richtlinien in Kraft getreten sind, steht es nun privaten Unternehmen frei, sich bei der Schweizerischen Akkreditierungsstelle (SAS) zu akkreditieren, um sodann Datenschutzzertifizierungen vornehmen zu können.

1.1.3 Volkszählung 2010

Im Rahmen der Vorbereitungsarbeiten für die eidgenössische Volkszählung 2010 haben wir mit dem Bundesamt für Statistik zusammengearbeitet und zu den Änderungsentwürfen zur Verordnung über die eidgenössische Volkszählung und zur Verordnung über die Durchführung von statistischen Erhebungen des Bundes Stellung genommen.

Im Jahre 2010 wird die eidgenössische Volkszählung erstmals in der Schweiz hauptsächlich auf der Grundlage von Informationen aus den Verwaltungsregistern sowie teilweise von Umfrageerhebungen bei einer Stichprobenauswahl von Haushalten durchgeführt. Anlässlich der Vorbereitungsarbeiten für diese Volkszählung haben wir mit dem Bundesamt für Statistik zusammengearbeitet und im Rahmen der Vernehmlassungsverfahren zum Entwurf zur Abänderung der Verordnung über die eidgenössische Volkszählung und zum Verordnungsentwurf über die Durchführung von statistischen Erhebungen des Bundes Stellung genommen. Bei dieser Gelegenheit hoben wir insbesondere die Notwendigkeit hervor, einerseits ein minimales Sicherheitsniveau für die elektronische Übertragung von Personendaten, die nicht über die Plattform Sedex erfolgt, festzulegen und andererseits die Bedingungen für eine Anonymisierung der Personendaten im Rahmen der eidgenössischen Volkszählung 2010 zu präzisieren.

1.1.4 Identifikationsnummer für Unternehmen

Nach einer ersten Projektversion zur Einführung einer Rechtsgrundlage für die neue Unternehmens-Identifikationsnummer (UID) in einer Verordnung und im Anschluss an unsere Kritik erklärte sich das Bundesamt für Statistik bereit, ein neues Gesetz auszuarbeiten. Die Verwendung der UID im Sektor Business to Business ist indessen unseres Erachtens weiterhin problematisch.

Das Bundesamt für Statistik (BFS) plant die Einführung einer Unternehmens-Identifikationsnummer (UID). Ziel dieses Projekts ist ein erleichterter Informationsaustausch innerhalb der Verwaltung (Government to Government, G2G), zwischen den Unternehmen und der Verwaltung (Business to Government, B2G) sowie zwischen den verschiedenen Unternehmen (Business to Business, B2B).

In einer ersten Projektversion sah das BFS die Einführung der Rechtsgrundlage in der Verordnung über das Betriebs- und Unternehmensregister vor. Im Anschluss an unsere Kritik zu diesem Thema (vgl. unseren 15. Tätigkeitsbericht 2007/2008, Ziff. 1.1.6)

hat das BFS anerkannt, dass eine Gesetzesgrundlage im formellen Sinn notwendig ist, und uns einen Gesetzesentwurf über die Unternehmens-Identifikationsnummer und das Unternehmens-Identifikationsregister vorgelegt (UID-Gesetz).

In verschiedenen Punkten, die insbesondere die Sicherheit der Daten und ihre Bekanntgabe an Dritte betreffen, konnten wir Kompromisslösungen finden. Eine Divergenz besteht jedoch weiterhin bezüglich dem Einsatz der UID zwischen verschiedenen Unternehmen (Sektor B2B): Es zeigt sich nämlich, dass diese Verwendung die Möglichkeiten für eine Überwachung und Persönlichkeitsverletzung stark erhöht. Diese Risiken, wie etwa die Profilierung, wurden weder analysiert noch wenigstens in der vorgelegten Dokumentation hervorgehoben. Wir sind der Meinung, dass die Benutzung der UID für B2B-Anwendungen verboten oder zumindest eingeschränkt werden sollte.

1.1.5 Neues Abkommen zwischen der Schweiz und den USA über die Übermittlung von Flugpassagierdaten

Zwischen der Schweiz und den USA wurde ein neues Abkommen betreffend die Übermittlung von Passagierdaten an die US-Behörden durch Fluggesellschaften abgeschlossen. In unserer Stellungnahme bemängelten wir, dass das neue Abkommen keine eigene Datenschutzklausel mehr enthält, sondern lediglich auf amerikanisches Recht verweist.

Die Schweiz und die USA haben die Übermittlung von Personendaten der Passagiere an die US-Behörden durch Fluggesellschaften 2005 in einem Abkommen geregelt (vgl. unseren 13. Tätigkeitsbericht 2005/2006, Ziff. 1.1.2). Dieses ist 2008 abgelaufen. Daher wurde nun ein neues Abkommen abgeschlossen.

Im neuen Abkommen wird festgehalten, dass die zu liefernden Personendaten datenschutzrechtlich der amerikanischen «System of Records Notice (SORN) for the Automated Targeting System (ATS)» unterstehen. Nebst diesem Verweis findet sich im Abkommen selbst – anders als im vorherigen – keine eigene Datenschutzbestimmung mehr. Aus diesem Grund hielten wir in unserer Stellungnahme zum Abkommensentwurf fest, dass es für die Übermittlung der Personendaten eine gesetzliche Grundlage, wie beispielsweise das bisherige Abkommen, brauche. Darin müsste auch die Bearbeitung inkl. das Beschaffen der Personendaten, die Zugriffe, die Aufbewahrung und Löschung der Personendaten, das Auskunftsrecht usw. geregelt werden. Mit dem vorgesehenen Hinweis auf die SORN werde auf amerikanisches Recht (einer «Notice») verwiesen, das nun auch dann Anwendung finden solle, wenn Personendaten von der Schweiz in die USA übermittelt würden. Die SORN könne jedoch einseitig von

den USA abgeändert werden, ohne dass die Schweiz darauf Einfluss nehmen könne. Änderungen würden der Schweiz lediglich mitgeteilt. Aufgrund dessen erachteten wir die SORN als keine genügende gesetzliche Grundlage im Sinne des DSG. Daran ändert auch die Tatsache nichts, dass die USA im Abkommen versichern, dass die Personendaten den gleichen Datenschutz geniessen wie im 2007 zwischen den USA und der EU abgeschlossenen Abkommen über die Übermittlung von Flugpassagierdaten. Dort wurden zudem die datenschutzrechtlichen Garantien noch mehr gelockert, wie dies die Artikel 29 Datenschutzgruppe der EU in einer Stellungnahme festgehalten hat. Zudem wäre es begrüssenswert gewesen, wenn die Schweiz mit den USA ein analoges Abkommen, ohne einseitigen Verweis auf amerikanisches Recht, hätte abschliessen können.

1.1.6 Abschluss eines Safe-Harbor-Abkommens Schweiz-USA

Die Vereinigten Staaten verfügen über kein angemessenes Datenschutzniveau, so dass für den Transfer von Personendaten zu einer Unternehmung in den USA spezielle Garantien vereinbart werden müssen. Gemeinsam mit dem Staatssekretariat für Wirtschaft (SECO) haben wir mit den USA ein Regelwerk ausgearbeitet, welches für die darunter zertifizierten Unternehmen ein ausreichendes Datenschutzniveau gewährleistet. Auf diese Weise wird der Datentransfer zwischen Schweizer und zertifizierten U.S. Unternehmen erheblich erleichtert.

Da die Gesetzgebung der USA aus Sicht der Schweiz keinen angemessenen Datenschutz gewährleistet, mussten Unternehmen in der Schweiz mit ihren Partnern in den USA bisher einen Vertrag abschliessen, der einen ausreichenden Datenschutz garantiert, und ihn uns zur Prüfung vorlegen. Erst danach dürfen Personendaten an das Unternehmen in den USA übermittelt werden. Das bestehende Safe Harbor Agreement zwischen der EU und den USA wird vom EDÖB als Vereinbarung erachtet, welche einen ausreichenden Schutz gewährleistet. Deshalb haben uns die USA angefragt, ob die Schweiz dem Safe Harbor Agreement beitreten wolle. Zusammen mit dem SECO hat der EDÖB im Rahmen des «Kooperationsforums Schweiz-USA für Handel und Investitionen» mit dem U.S.-Department of Commerce nun das «U.S.-Swiss Safe Harbor Framework» als neues Instrument geschaffen, welches den Datentransfer zwischen der Schweiz und den USA für Unternehmen vereinfacht.

Künftig können sich U.S. Unternehmen beim Handelsministerium der USA unter diesem Abkommen zertifizieren. Damit verpflichten sie sich, die darin festgehaltenen Datenschutzgrundsätze einzuhalten. Für zertifizierte Unternehmen gewährleistet dies in

den USA einen angemessenen Datenschutz. Damit kann ein freier Datenverkehr zwischen Schweizer und U.S. Unternehmen stattfinden. Die Europäische Gemeinschaft verfügt seit dem Jahr 2000 über ein vergleichbares Regime.

Für Unternehmen in der Schweiz hat dieses Regime den Vorteil, dass sie mit zertifizierten U.S. Unternehmen weder einen Vertrag aushandeln noch den EDÖB über den Datentransfer informieren müssen. Die Rechte der betroffenen Personen werden gleichfalls gestärkt. So sieht das «U.S.-Swiss Safe Harbor Framework» spezielle Konfliktlösungsgremien im Fall von Datenschutzrechtsverletzungen vor. Daneben kann in den USA die Federal Trade Commission bei schwerwiegenden und wiederholten Datenschutzverletzungen Massnahmen gegen zertifizierte Unternehmen ergreifen. Das Department of Commerce (www.export.gov/safeharbor) führt auf seiner Webseite eine Liste dieser Unternehmen.

Mit dem «U.S.-Swiss Safe Harbor Framework» haben das SECO und der EDÖB mit den USA eine Grundlage geschaffen, welche auf der einen Seite den Datentransfer zwischen den beiden Ländern erleichtert und auf der anderen Seite die Datenschutzrechte der betroffenen Personen stärkt.

1.2 Datenschutzfragen allgemein

1.2.1 Datenschutzkonforme Videoüberwachung dank Chiffrierung

Die Videoüberwachung entwickelt sich ständig weiter. Dank der verschiedenen Methoden zur Bildverschlüsselung und der Aufteilung der Chiffrierschlüssel lassen sich datenschutzkonforme Technologien einsetzen und mögliche Missbräuche vermeiden. Vereinbarungen zwischen Entwicklern und Herstellern gestatten eine bessere Verbreitung dieser Technologien.

In unserem letzten Tätigkeitsbericht hatten wir eine Anwendung für eine datenschutzfreundliche Videoüberwachung vorgestellt (vgl. 15. Tätigkeitsbericht 2007/2008, Ziff. 1.2.3). Die Technologien, welche die Methode der Chiffrierung (verschlüsselte Bilder) verwenden, werden laufend weiterentwickelt.

Zusätzlich zur Chiffriermethode haben die Entwickler nun die Möglichkeit einer Aufteilung des Dechiffrierschlüssels in zwei physisch getrennte Teile geschaffen. Diese Eigenschaft kann das Vier-Augen-Prinzip gewährleisten: Die beiden Teile des Schlüssels werden an zwei verschiedene Personen übermittelt, was mögliche Missbräuche erheblich einschränkt. Dieses Feature wird von den Endbenutzern sehr geschätzt. Ausserdem haben die Entwickler eine Vereinbarung mit der multinationalen Herstellerfirma einer Verwaltungssoftware für Videoüberwachungssysteme (ähnlich dem webbasierten Videoüberwachungssystem, vgl. dazu Ziff. 1.2.2) abgeschlossen. So ist es in Zukunft möglich, diesen Kameratyp in ein Standard-Managementprodukt zu integrieren. Dank solcher Vereinbarungen haben die Entwickler die Möglichkeit einer besseren Verbreitung ihrer Kameras.

Wir befürworten die Entwicklung und Verbreitung von datenschutzfreundlichen Technologien und Produkten.

1.2.2 Netzwerkbasiertes Videoüberwachungssystem

Dank der technischen Fortschritte der letzten Jahre haben sich die Videoüberwachungssysteme namhaft weiter entwickelt. Vom einfachen Modell mit einer Kamera und einem Bildschirm ist man zu komplexeren Systemen übergegangen, bestehend aus mehreren an verschiedenen Standorten angebrachten und von mehreren Nutzern überwachten Kameras. Während die Entwicklung der Technik zu einer Ausbreitung der Videoüberwachungssysteme geführt hat, sind auch neue Produkte auf dem Markt erschienen, die einen besseren Datenschutz sicherstellen können.

Noch vor einiger Zeit beschränkten sich die Videoüberwachungssysteme auf einfache Kameras und Betriebspersonal, das die Bilder in Echtzeit verfolgte. Die Entwicklung der Technik in den letzten Jahren, insbesondere die Verbreitung von Internet und Digitalkameras, ermöglicht nunmehr die Ausarbeitung komplexerer Systeme. Während diese Entwicklung einerseits eine Ausbreitung der Videoüberwachung auslöste, sind andererseits heute auch datenschutzfreundliche Technologien erhältlich.

Die modernen Videoüberwachungssysteme verfügen so über mehrere hundert Kameras, die auf die ganze Welt verteilt sind. Dank der Verbreitung über Internet gelangen die Bilder zu zahlreichen Nutzern in mehreren Überwachungszentralen. Die Nutzer können unterschiedliche Aufgaben, Verantwortungsbereiche und Rechte haben. Die Videoüberwachungssysteme müssen die Verwaltung aller dieser Variablen ermöglichen. Die Bilder werden nicht mehr direkt übermittelt, sondern in einer zentralen Datenbank zusammengeführt, auf welche die Nutzer zugreifen können. Der Schutz dieser Datenbank – sowie ihres Host-Servers – spielt eine grundlegende Rolle.

Im Rahmen unserer Aufsichtstätigkeiten haben wir die Entwicklung der Technik verfolgt und insbesondere ein netzbasiertes Videoüberwachungssystem mit folgenden Eigenschaften untersucht:

- Die Übertragung der Bilder zwischen den Kameras und dem Server sowie zwischen dem Server und den Nutzern wird chiffriert. Dies verhindert unbefugte Zugriffe und gestattet die Benutzung des Internets als Kommunikationsmittel ohne das Risiko einer Persönlichkeitsverletzung.
- Obwohl eine robuste Chiffrierung die Ideallösung wäre, gewährleistet schon eine Codierung der Bilder in der Datenbank ein minimales Sicherheitsniveau, insbesondere wenn der physische und logische Zugriff auf den Server ebenfalls geschützt sind.

- Für sehr sensible Zugriffe, beispielsweise auf den Server, ist die Wahl eines doppelten Schlüssels (Vier-Augen-Prinzip) möglich.
- Es kann definiert werden, welche Kameraeigenschaften (zum Beispiel Zoom, Drehung, Aktivierung des Mikrofons usw.) welchen Nutzern zur Verfügung stehen. Zudem lassen sich die Rechte der verschiedenen Nutzer definieren (zum Beispiel die Bilder zu sehen, die Bilder zu exportieren, einen Alarm auszulösen, usw.).
- Eine Protokollierung der Zugriffe gibt Aufschluss darüber, wer (welcher Nutzer) was getan hat (beispielsweise Bilder ansehen) und wann.
- Die Möglichkeit, verschiedene Kameramodelle zu integrieren, erlaubt eine grosse Flexibilität und gegebenenfalls eine Auswechslung der Kameras.

Wir sind der Ansicht, dass ein solches Produkt die legitimen Interessen der Videoüberwachung mit denen des Datenschutzes in Einklang bringt, insbesondere wenn die gewählten Kameras eine an der Basis robuste Chiffrierung ermöglichen (vgl. dazu Ziff. 1.2.1).

1.2.3 Leitfaden zu biometrischen Erkennungssystemen

Wir haben einen Leitfaden für Entwickler und Betreiber von Systemen der biometrischen Erkennung ausgearbeitet. Er ist in drei Abschnitte unterteilt: Der erste enthält terminologische Präzisierungen. Der zweite listet die für die Planung und die Nutzung solcher Systeme geltenden Leitsätze auf. Im letzten Teil wird erörtert, welche Aspekte bei der Beurteilung von biometrischen Erkennungssystemen zu berücksichtigen sind, und welchen datenschutzrechtlichen Anforderungen solche Systeme genügen sollten.

Auf Grund von zahlreichen Fragen im Bereich der Biometrie, und insbesondere im Anschluss an unsere Empfehlung für eine Dezentralisierung der biometrischen Daten im Sportzentrum KSS (vgl. dazu Ziff. 1.2.4), haben wir einen Leitfaden zu biometrischen Erkennungssystemen erstellt. Dieses Dokument ist in drei Abschnitte unterteilt. Der Einführungsteil ist insbesondere der Terminologie gewidmet, deren Kenntnis für ein gutes Verständnis der komplexen Materie notwendig ist. Der zweite Abschnitt zählt die bei der Planung und Nutzung solcher Systeme geltenden Leitsätze auf und erläutert sie. Der dritte und letzte Teil besteht in einem Leitfaden, der eine Liste von Fragen umfasst, die sich im Rahmen der Beurteilung solcher Systeme stellen; dann folgen die Anforderungen, die solche Systemen unter dem Gesichtspunkt des Datenschutzes zu erfüllen haben.

Terminologisch ist zwischen den biometrischen Aufnahmeprozessen, also der Aufzeichnung einer persönlichen biometrischen Referenz, und den biometrischen Verfahren zur Überprüfung einer angeblichen Identität und Identifizierung einer Person aufgrund einer vorhandenen biometrischen Angabe zu unterscheiden. Auf der Grundlage verschiedener biometrischer (physiologischer oder verhaltenstypischer) Merkmale werden Rohdaten erstellt, aus denen abgeleitete Daten oder biometrische Profile gewonnen werden. Letztere ermöglichen die Feststellung einer Identität oder die Identifizierung der betroffenen Person aufgrund des biometrischen Vergleichs zwischen dem Referenz- und dem Testprofil. Da jeder biometrische Vergleich probabilistischer Art ist, sind die Rate der falschen Übereinstimmungen (wenn eine Person als eine andere identifiziert wird) und die Rate der falschen Zurückweisungen (wenn die registrierte Person nicht erkannt wird), und damit die Zuverlässigkeit des Systems von der gewählten Akzeptanzschwelle abhängig.

Die im zweiten Teil des Leitfadens erwähnten Prinzipien – die Rechtmässigkeit, die Verhältnismässigkeit, die Zweckbindung und die Transparenz der biometrischen Bearbeitungen, die Richtigkeit (oder die Qualität) und die Sicherheit der biometrischen Daten, sowie die Rechte der betroffenen Personen – haben ihre Grundlage im DSG.

Mit Bezug auf den Evaluationsleitfaden gilt die erste Serie von Fragen der Zweckbindung des Erkennungssystems, der Art des Erkennungsverfahrens (Überprüfung oder Identifikation) und den Modalitäten der Speicherung der biometrischen Daten. Die zweite Fragenserie betrifft die Mittel der biometrischen Erkennung – die verwendeten Modalitäten (biometrische und/oder traditionelle Verfahren), die Spuren, die Art (Rohdaten oder abgeleitete Daten) und den Sensibilitätsgrad der gewählten biometrischen Merkmale. Die dritte Serie geht auf die Aspekte der Datensicherheit und der Zuverlässigkeit des Systems ein; dabei werden die Systemarchitektur, die Sicherheitsmassnahmen und die Funktionsweise der Aufnahme- und Erkennungsverfahren, einschliesslich ihrer Konfiguration und ihrer technischen Leistungsfähigkeit, analysiert. In der vierten und letzten Fragenserie schliesslich werden die Rechte der betroffenen Personen und die Voraussetzungen für die Pflicht zur Anmeldung der erstellten biometrischen Datensammlungen zusammengefasst.

1.2.4 Biometrische Zugangssysteme beim Sportzentrum KSS: weitere Entwicklung

Nachdem sich das Sportzentrum KSS geweigert hat, eine unserer Empfehlungen zu befolgen, haben wir den Fall dem Bundesverwaltungsgericht zur Entscheidung unterbreitet.

Nach Erhalt unserer Empfehlungen (vgl. unseren 15. Tätigkeitsbericht 2007/2008, Ziff. 1.2.5) liess uns das Sportzentrum KSS in Schaffhausen wissen, dass es sich weigere, die Empfehlung betreffend die dezentralisierte Speicherung der biometrischen Daten umzusetzen.

Werden Personendaten in einer zentralisierten Datenbank gespeichert, verlieren die betroffenen Personen die Kontrolle über die Verwendung ihrer Daten. Nun sieht der Verhältnismässigkeitsgrundsatz aber vor, dass jegliche Bearbeitung von Personendaten mit Hilfe von Mitteln erfolgen muss, die zur Erreichung des verfolgten Zwecks geeignet sind und die in Anbetracht der Zweckbestimmung nicht übermässig erscheinen. Im vorliegenden Fall sind wir der Auffassung, dass die Speicherung der biometrischen Daten in einer zentralisierten Datenbank angesichts der Zweckbindung der Bearbeitung einen unverhältnismässigen Eingriff in die Rechte der betroffenen Personen darstellt.

Die Dezentralisierung der biometrischen Daten kann mittels unterschiedlicher Technologien erzielt werden. Es gibt verschiedene Arten von Datenträgern, die es den betroffenen Personen ermöglichen, die Verwendung ihrer Personendaten teilweise oder vollständig zu kontrollieren. Im Fall KSS haben wir die Umsetzung einer Zwischenlösung empfohlen (biometrischer Vergleich auf der Karte – «match on card»), die eine Teilkontrolle bietet. Mit dieser Art Datenträger lassen sich die biometrischen Daten auf einer persönlichen Karte speichern und das Vergleichsverfahren kann auf der Karte erfolgen.

Angesichts der Weigerung des KSS, unsere Empfehlung zu befolgen, haben wir den Fall dem Bundesverwaltungsgericht unterbreitet. Wir erwarten derzeit noch seinen Entscheid.

1.2.5 Datenbearbeitungen durch Markt- und Sozialforschungsinstitute

Im Bemühen, die Grundsätze des DSG einzuhalten und sich so von weniger seriösen Firmen abzuheben, die im Bereich der Direktvermarktung tätig sind, ist der Verband Schweizer Markt- und Sozialforscher (VSMS) an uns gelangt, um uns verschiedene Datenschutzfragen zu unterbreiten und sich zu vergewissern, dass seine Methoden wie auch seine Dokumentation wirklich im Einklang mit der schweizerischen Gesetzgebung stehen. Wir haben die gestellten Fragen beantwortet und der Branche verschiedene Verbesserungen vorgeschlagen. Der Verband ist unseren Anmerkungen gefolgt und hat seine Reglemente und internen Weisungen angepasst.

Der Verband Schweizer Markt- und Sozialforscher (VSMS) vertritt die Interessen seiner Branche im Namen seiner Einzel- und Kollektivmitglieder, zu denen insbesondere die wichtigsten im Bereich der Sozial- und Marktforschung tätigen Institute gehören. Ebenfalls in dem Verband vertreten sind die Forscher von Instituten, die im Bereich Markt-, Meinungs- und Sozialforschung spezialisiert sind, die unabhängigen Werbeberater oder Marketingleiter in Unternehmen oder Organisationen, die eine mit Marktforschung verbundene Tätigkeit verfolgen, sowie Dozenten und Studenten der Sozialwissenschaften.

Markt- und Sozialforschung ermöglicht die Erhebung von verschiedenen Informationen über das wirtschaftliche, kulturelle und politische Leben eines Landes oder einer Region. Im Rahmen einer Marktforschung oder einer Meinungsumfrage werden Personen aus der Bevölkerung aufgefordert, ihre ganz persönliche Ansicht zu zahlreichen Themen zu äussern. Dies geschieht freiwillig. Über die Auswertung dieser Informationen können unter anderem eine Momentaufnahme der politischen Meinungen in der demokratischen Schweiz erstellt, der Stand der gesellschaftlichen und kulturellen Entwicklung ermittelt oder auch Produkte und Dienstleistungen bewertet und optimiert werden; so soll es möglich werden, die Funktionsweise der Gesellschaft besser zu verstehen und zu begreifen, wie die Bevölkerung oder ihre verschiedenen Teilgruppen denken und handeln. Die Unternehmen bedienen sich der Marktforschung, um das Konsum- und Kaufverhalten zu analysieren und damit den Bedürfnissen und Wünschen der Verbraucher besser gerecht zu werden. Unternehmen, Organisationen und andere Vereinigungen, aber auch politische Entscheidungsträger, Parteien und Verwaltungen stützen sich auf die im Rahmen dieser Erhebungen gewonnenen Daten, um wichtige Entscheidungen zu treffen.

Die Markt- und Sozialforschungsinstitute, die sich auf das kollektive Markenzeichen berufen, bieten die Gewähr, dass keine Erhebung zu offen eingestandenen oder verborgenen Verkaufs-, Werbe- oder Bestellzwecken durchgeführt wird. Ebenso garantieren die Richtlinien des VSMS, dass die Daten nur in anonymisierter Form ihren Auftraggebern oder Dritten bekannt gegeben werden, sodass sich die Identität der betroffenen Personen nicht aus ihren Antworten ableiten lässt. Personen, die sich zur Teilnahme an einer Umfrage bereit erklären, gehen davon aus, dass ihre Daten vom Forschungsinstitut ausgewertet und spätestens vor der Übermittlung der Untersuchungsergebnisse an Dritte anonymisiert werden.

In diesem Rahmen hat uns der VSMS ein Problem unterbreitet, mit dem er derzeit konfrontiert ist: Die Auftraggeber des VSMS möchten neuerdings zum Zweck der Qualitätskontrolle Interviews oder Gruppendiskussionen anhören und Dokumente oder Informationen erhalten, die eine Identifikation der Befragten ermöglichen würden. Dazu halten wir fest, dass eine Bekanntgabe (nicht anonymisierter) Personendaten an Dritte zum Zweck der Qualitätskontrolle eine Zweckänderung darstellt und für die betroffene Person klar erkennbar und durch einen Rechtfertigungsgrund (grundsätzlich die Einwilligung) legitimiert sein muss.

Wir haben dem VSMS eine Anpassung seiner internen Regelungen und Verträge im Einklang mit der Datenschutzgesetzgebung empfohlen. Der Verband hat unsere Bemerkungen befolgt und die notwendigen Änderungen vorgenommen.

1.2.6 Datenaustausch zwischen Pensionskasse und Steuerverwaltung

Wir haben ein Gutachten erstellt, in welchem die Frage zu klären war, ob eine Pensionskasse datenschutzrechtliche Bestimmungen verletzt, wenn sie in Erfüllung einer gesetzlichen Meldepflicht jährlich Renten- und Leistungsbescheinigungen an die Steuerverwaltung bekannt gibt. Wir kommen zum Schluss, dass sowohl steuerrechtlich als auch versicherungsrechtlich eine gesetzliche Grundlage für eine Bescheinigungspflicht vorliegt. Weder Art. 86a Abs. 1 lit. e BVG noch Art. 19 Abs. 4 DSG sind im Falle von gesetzlichen Meldepflichten anwendbar.

Die Steuerverwaltung des Kantons Bern verlangte gestützt auf Art. 172 Abs. 1 lit. b des bernischen Steuergesetzes (StG) die jährliche Einreichung von Renten- und Leistungsbescheinigungen. Mit der Einführung des neuen Lohnausweises wurde ein Formular eingeführt, das neu als Lohn- und Rentebescheinigung bezeichnet wird. Mit dieser Neuregelung verlangt nun die kantonale Veranlagungsbehörde die jährliche Meldung.

Die Rechtsvertreterin der Pensionskasse erblickte darin einen Konflikt zwischen Art. 172 Abs. 1 lit. b des StG und Art. 129 Abs. 1 lit. b des Bundesgesetzes über die direkte Bundessteuer (DBG) einerseits sowie Art. 17 und 19 DSG und Art. 86a Abs. 1 lit. e des Bundesgesetzes über die berufliche Vorsorge (BVG) andererseits.

Wir haben ein Gutachten erstellt mit dem Ziel, die Frage zu beantworten, ob die Pensionskasse mit der gesetzlich festgelegten jährlichen Meldung an die Steuerbehörde datenschutzrechtliche Bestimmungen verletzt.

Zunächst war zu prüfen, ob nach Art. 17 Abs. 1 DSG für die Beschaffung der Daten eine gesetzliche Grundlage vorhanden ist, aufgrund welcher die Steuerbehörde die Rentendaten verlangen kann. Es wurde festgestellt, dass für die Einreichung von Renten- und Leistungsbescheinigungen eine gesetzliche Grundlage für die Meldepflicht sowohl in Art. 172 Abs. 1 lit. b StG als auch in Art. 129 Abs. 1 lit. b des DBG vorhanden ist. Neben den Steuergesetzen findet sich auch in der Gesetzgebung über die berufliche Vorsorge, Art. 81 Abs. 3 BVG und Art. 8 der Verordnung über die steuerliche Abzugsberechtigung für Beiträge an anerkannte Vorsorgeformen (BVV 3), eine gesetzliche Bescheinigungspflicht gegenüber den Steuerbehörden. Da die Bescheinigungspflicht ausdrücklich in den Steuergesetzen geregelt ist, verletzt die Datenbekanntgabe Art. 19 Abs. 1 DSG nicht.

Danach war zu prüfen, ob Art. 19 Abs. 4 DSG eine Einschränkung der zulässigen Datenweitergabe erlaubt. Da die spezialgesetzliche Regelung im BVG Vorrang hat, war zu klären, ob die Pensionskasse die Datenweitergabe gestützt auf die datenschutzrechtliche Bestimmung nach Art. 86a Abs. 1 lit. e BVG einschränken oder verweigern dürfte. Wie die Auslegung ergab, ist Art. 86a Abs. 1 lit. e BVG infolge der Einführung der Datenschutzgesetzgebung des Bundes entstanden. Dabei wurden datenschutzrechtliche Bestimmungen des BVG an das DSG angepasst. Bis zum Gesetz über die Anpassung und Harmonisierung der gesetzlichen Grundlagen für die Bearbeitung von Personendaten in den Sozialversicherungen vom 23. Juni 2001 waren die Datenbekanntgabe und die Ausnahmen von der Schweigepflicht in der Verordnung des Bundesrates vom 7. Dezember 1987 geregelt gewesen.

Aus Gründen der Rechtsicherheit und der Vereinheitlichung wurden verschiedene Änderungen in den Sozialversicherungsgesetzen eingefügt. Im Bereich des BVG wurden die Anpassungen mit der Einfügung des Art. 86a ff. vollzogen. Art. 86a Abs. 1 lit. e BVG bezieht sich auf die Datenbekanntgabe und entspricht sinngemäss dem bisherigen Art. 1 Abs. 1 der Verordnung über die Ausnahmen von der Schweigepflicht in der beruflichen Vorsorge und über die Auskunftspflicht der AHV/IV-Organe (VSABV), welcher die Auskunftspflicht regelte. Diese Bestimmung unterschied zwischen einer

Datenbekanntgabe im Einzelfall auf schriftliches und begründetes Gesuch hin, Fällen, in denen Daten ohne weiteres auf Anfrage hin bekannt gegeben werden, sowie Fällen, in denen es keine Zustimmung für die Datenbekanntgabe braucht. Wenn die Pensionskasse gestützt auf Art. 86a Abs. 1 lit. e BVG ihre Datenbekanntgabe einschränken oder verweigern könnte, wäre eine Berufung auf den Rechtfertigungsgrund «besondere schützenswerte Privatinteressen» möglich. Nach bundesgerichtlicher Rechtsprechung müssen sich solche überwiegende private Interessen jedoch in der Person des Versicherten selbst, dem Arbeitgeber oder anderer beteiligter Personen manifestieren. In erster Linie sind dies Daten, welche die Gesundheit oder berufliche Verhältnisse oder Geschäftsgeheimnisse betreffen. Daher kommt Art. 86a Abs. 1 lit. e BVG unserer Schlussfolgerung nach nur dann zur Anwendung, wenn eine Behörde ein Auskunftsbegehren an eine Personalfürsorgestiftung im Rahmen der Amtshilfe stellt. Bei Rentenbescheinigungen, die aufgrund einer gesetzlich festgelegten Meldepflicht einzureichen sind, muss die Veranlagungsbehörde kein Auskunftsbegehren stellen. Die Pensionskasse hat keine Auskunftspflicht, sondern unterliegt einer speziellen Bescheinigungspflicht, wonach sie der Veranlagungsbehörde die Bescheinigungen unaufgefordert zuzusenden hat.

Wir kamen zum Ergebnis, dass die Veranlagungsbehörde weder Art. 17 noch Art. 19 DSG verletzt, da sie aufgrund von Art. 172 Abs. 1 lit. b StG, Art. 129 Abs. 1 DBG sowie Art. 81 Abs. 3 BVG und Art. 8 BVV3 rechtmässig Steuerdaten beschafft.

Auch unterliegt die Pensionskasse gemäss Art. 172 Abs. 1 lit. b StG und Art. 129 Abs. 1 lit. b DBG keiner Auskunftspflicht, sondern einer Meldepflicht, weshalb in diesem Zusammenhang weder Art. 86a Abs. 1 lit. e BVG noch Art. 19 Abs. 4 DSG zur Anwendung kommen. Die Pensionskasse verletzt daher die Schweigepflicht bei der Bekanntgabe der Rentenbescheinigungen nicht.

1.2.7 Weitergabe von Personendaten durch Bundesbehörden an Dritte

Eine Bundesbehörde darf auf Anfrage Personendaten an Dritte bekannt geben, wenn dafür eine Rechtsgrundlage besteht. Ohne Rechtsgrundlage kann die Behörde auf Anfrage auch Name, Vorname und Geburtsdatum einer Person bekannt geben, wobei sie je nach Zusammenhang oder Person allfälligen Schutzbedürfnissen Rechnung zu tragen hat.

Bundesbehörden haben uns angefragt, ob sie Personendaten auch ohne Einwilligung der betroffenen Person Dritten bekannt geben dürfen.

Nach Art. 19 Abs. 1 DSG dürfen Bundesorgane Personendaten bekannt geben, wenn dafür eine Rechtsgrundlage im Sinne von Art. 17 DSG besteht oder – namentlich – wenn die betroffene Person im Einzelfall eingewilligt hat der Empfänger glaubhaft macht, dass die betroffene Person die Einwilligung verweigert oder Bekanntgabe sperrt, um die Durchsetzung von Rechtsansprüchen oder die Wahrnehmung anderer schutzwürdiger Interessen zu verwehren (beispielsweise um der Zahlung von Schulden zu entgehen). Dabei muss der betroffenen Person vorher wenn möglich Gelegenheit zur Stellungnahme gegeben werden. Wir haben mitgeteilt, dass es sich bei der erwähnten gesetzlichen Vorschrift um eine Kann-Vorschrift handelt, weshalb das Bundesorgan nicht zur Bekanntgabe verpflichtet ist. Die betroffene Person ist vorher grundsätzlich anzuhören.

Ein Bundesorgan kann zudem nach Art. 19 Abs. 2 DSG Name, Adresse und Geburtsdatum einer Person auch dann bekannt geben, wenn die Voraussetzungen nach Art. 19 Abs. 1 DSG nicht vorhanden sind. Demzufolge können diese Daten ohne Einwilligung und ohne Anhörung bekannt gegeben werden. Auch diese Vorschrift ist eine Kann-Vorschrift, welche das Bundesorgan nicht zur Auskunft verpflichtet.

Je nach Zusammenhang oder Person kann aber auch die Bekanntgabe von Name, Adresse oder Geburtsdatum zu einer Verletzung der Persönlichkeits- und Grundrechte führen. Deshalb müssen Bundesorgane bei der Datenbekanntgabe nach Art. 19 Abs. 2 DSG allfälligen Schutzbedürfnissen Rechnung tragen.

1.2.8 Publikation von Fahndungs- und Vermisstmeldungen auf privaten Webseiten

Die Publikation von polizeilichen Fahndungsmeldungen im Internet rechtfertigt sich durch das öffentliche Interesse an der raschen Ergreifung der Person sowie der Verhinderung von Delikten. Nach einer gewissen Zeit – spätestens nach der Verhaftung bzw. dem Auffinden der gesuchten Person – entfällt jedoch diese Rechtfertigung und die entsprechenden Personendaten sind vom Netz zu nehmen.

Von dritter Seite sind wir auf eine Webseite aufmerksam gemacht worden, die unter anderem polizeiliche Fahndungsmeldungen, Berichte über Delikte und Vermisstmeldungen publiziert. Dabei werden Personendaten von Verdächtigen, von Tätern und auch von Opfern veröffentlicht. Die Texte sind teilweise mehrere Jahre alt.

Das Publizieren von Personendaten im Internet stellt eine Datenbearbeitung im Sinne des Bundesgesetzes über den Datenschutz dar, wofür eine private Person einen Rechtfertigungsgrund benötigt. Die Rechtfertigung kann durch Einwilligung der betroffenen Person, durch ein überwiegendes privates oder öffentliches Interesse oder durch eine gesetzliche Grundlage erfolgen.

Die Publikation einer polizeilichen Fahndungsmeldung im Internet rechtfertigt sich durch ein überwiegendes öffentliches Interesse (Ergreifung der Person, Verhinderung weiterer Delikte etc.). Zudem bestehen auf kantonaler Ebene gesetzliche Grundlagen, welche eine solche öffentliche Ausschreibung grundsätzlich legitimieren. Diese Publikationen liegen nämlich im Kompetenzbereich der kantonalen Datenschutzaufsichtsbehörden.

Das öffentliche Interesse an einer solchen Publikation erlischt allerdings spätestens dann, wenn die gesuchte Person aufgefunden wurde. So war denn auch für die meisten der auf der betreffenden Webseite publizierten Dokumente keine Rechtfertigung mehr ersichtlich, es sei denn, die betroffenen Personen hätten eingewilligt, wovon aber nicht auszugehen ist.

Von der Veröffentlichung betroffene Personen können vom Betreiber der Webseite verlangen, dass ihre Daten gesperrt werden. Diese Forderung lässt sich auch zivilrechtlich durchsetzen. Die Betroffenen können darüber hinaus Schadenersatz für eine erfolgte Persönlichkeitsverletzung verlangen.

Wir haben den Betreiber der Internetseite gebeten, diejenigen Personendaten, für die kein Rechtfertigungsgrund (mehr) vorliegt, umgehend unzugänglich zu machen.

1.2.9 Weitergabe von Unterschriftenbögen durch die Unabhängige Beschwerdeinstanz

Die unabhängige Beschwerdeinstanz für Radio und Fernsehen (UBI) leitet bei einer Popularbeschwerde die Unterschriftenliste unaufgefordert an den Programmverantwortlichen weiter. Obwohl wir festgestellt haben, dass im konkret unterbreiteten Fall das DSG nicht gilt, spielen datenschutzrechtliche Fragen durchaus eine Rolle. Wir haben der UBI mitgeteilt, dass für die unaufgeforderte Bekanntgabe der Unterschriftenliste eine gesetzliche Grundlage fehlt. Weiter haben wir darauf hingewiesen, dass es Aufgabe des Gesetzgebers wäre, beispielsweise im Rahmen einer allfälligen Revision das Bundesgesetz über Radio und Fernsehen entsprechend anzupassen.

Eine Person hat bei der unabhängigen Beschwerdeinstanz für Radio oder Fernsehen (UBI) eine Popularbeschwerde eingereicht. Eine solche muss u.a. zusammen mit einer Liste mit der Unterschrift von zwanzig Personen eingereicht werden. Die UBI hat Beschwerde und Liste an den Programmverantwortlichen weitergeleitet.

Zu prüfen war, ob diese Weitergabe der Unterschriftenliste das Datenschutzgesetz verletzt hat. Wir haben die UBI, die bereits das Bundesamt für Justiz (BJ) um eine Kurzanalyse in dieser Frage gebeten hatte, zu einer Stellungnahme eingeladen. Das BJ verneinte die Anwendung des Datenschutzgesetzes im konkreten Fall, weil es sich einerseits um ein hängiges und andererseits um kein erstinstanzliches Verfahren handle. Diese Auffassung teilten auch wir. Gleichzeitig bedeutet das aber nicht, dass datenschutzrechtliche Fragen keine Rolle spielen.

Wie unsere Abklärungen ergeben haben, leitet die UBI praxisgemäss die Unterschriftenliste zusammen mit der Kopie der Beschwerde an die Programmverantwortlichen weiter. Damit gibt sie Personendaten bekannt. Als Bundesorgan darf die UBI dies nur tun, wenn eine gesetzliche Grundlage vorhanden ist, es sei denn, gesetzliche Ausnahmebestimmungen wären anwendbar. Im Bundesgesetz über Radio und Fernsehen (RTVG) gibt es keine gesetzliche Grundlage für die Weiterleitung der Unterschriftenliste. Wir haben der UBI mitgeteilt, dass die gegenwärtige Praxis der unaufgeforderten Weitergabe der Unterschriftenliste nicht dem Datenschutz entspricht. Es wäre Aufgabe des Gesetzgebers, das RTVG beispielsweise im Rahmen einer allfälligen Revision diesbezüglich anzupassen.

Ergänzend führten wir aus, dass wir für die aufgeforderte Bekanntgabe der Personendaten im Rahmen des Akteneinsichtsrechts eine gesetzliche Grundlage sehen. In der Frage, ob das Akteneinsichtsrecht nach Art. 27 Abs. 1 lit. b des Bundesgesetzes über das Verwaltungsverfahren (VwVG) zu verweigern ist oder nicht, wäre im Einzelfall vor der Bekanntgabe eine Interessenabwägung vorzunehmen. Die Überprüfung der Frage, ob und unter welchen Umständen das Akteneinsichtsrecht zu verweigern ist, obliegt jedoch den Gerichten.

1.2.10 Bearbeitungsregelement: Kontrollverfahren

Bearbeitungsreglemente sind gemäss den Vorgaben zu erstellen und nachzuführen. Darin sind unter anderem auch die Kontrollverfahren aufzuführen. Angaben dazu fehlen jedoch in den meisten Reglementen. Audits sollten aber insbesondere bei sensitiven Systemen regelmässig durchgeführt werden.

Leider müssen wir nach wie vor feststellen, dass Bearbeitungsreglemente in vielen Fällen nicht entsprechend den Vorgaben geführt werden. In einigen Fällen fanden wir heraus, dass die Reglemente anfangs recht gut waren, in der Folge aber nicht mehr nachgeführt wurden. Häufig konnten wir aufgrund des Bearbeitungsreglements auch feststellen, dass namentlich während des Betriebs der Datensammlungen keine internen oder externen Kontrollen durchgeführt wurden. Dies ist bedauerlich, weil gerade in der Betriebsphase wichtige Erkenntnisse gewonnen werden können, um das System u. a. auch im Bereich des Datenschutzes zu optimieren. Regelmässige Überprüfungen oder Audits sind daher sehr wichtig, weil sie dem Inhaber der Datensammlung wichtige neue Erkenntnisse bringen, aufgrund derer er entsprechende Entscheidungen fällen kann. Das Bearbeitungsreglement soll für Transparenz sorgen. Erst aufgrund transparenter Informationen ist es möglich, die Systeme entsprechend zu steuern.

Eine Auflistung der Anforderungen an ein Bearbeitungsreglement ist auf unserer Webseite zu finden: www.derbeauftragte.ch, Dokumentation – Datenschutz – Leitfäden – Technische und organisatorische Massnahmen, rechte Spalte unter «Weitere Informationen».

1.3 Internet und Telekommunikation

1.3.1 Internet-Tauschbörsen: Klage beim Bundesverwaltungsgericht

Wir haben unsere Empfehlung an ein im Bereich der Bekämpfung von Urheberrechtsverletzungen in Internet-Tauschbörsen (Peer-to-Peer-Netzwerke) tätiges Unternehmen dem Bundesverwaltungsgericht (BVGer) zum Entscheid vorgelegt (vgl. unseren 15. Tätigkeitsbericht 2007/2008, Ziff. 1.3.1). Nach zwei Schriftwechseln erwarten wir nun den Entscheid des BVGer.

1.3.2 Jugendschutz im Internet

Minderjährige können ohne die Zustimmung ihrer gesetzlichen Vertreter keine Datenschutzerklärung abgeben. Dies kann die Betreiber von Internetseiten vor Probleme stellen, insbesondere, wenn sich Jugendliche auf einer Webseite (beispielsweise für ein Gewinnspiel) registrieren. Von einer impliziten Einwilligung der Eltern im Rahmen der Internetbenutzung auszugehen, kann problematisch sein. Wir schlagen den Betreibern daher vor, von den gesetzlichen Vertretern eine Einwilligung einzuholen.

Für Betreiber von Webseiten ist es kaum möglich, in der virtuellen Welt die Identität ihrer Besucher zu überprüfen. Vor allem im Bereich Jugendschutz kann dies zu erheblichen Problemen führen. Insbesondere den Betreibern von Webseiten für Kinder und Jugendliche, die eine Registrierung vorsehen, stellt sich die Frage, wie die Zustimmung der gesetzlichen Vertreter eingeholt werden kann. Im Rahmen einer Beratung haben wir uns also mit der Frage beschäftigt, unter welchen Umständen eine rechtsgültige Zustimmung in die Datenbearbeitung minderjähriger Personen im Alter zwischen 12 und 16 Jahren zustande kommen kann.

Gemäss dem Bundesgesetz über den Datenschutz müssen betroffene Personen, soweit es für die Bearbeitung ihrer Personendaten notwendig ist, in eine solche einwilligen. Ein Webseitenbetreiber kann die Registrierung seiner Besucher vorsehen, damit diese beispielsweise einem sozialen Netzwerk beitreten oder an einem Gewinnspiel teilnehmen können. Für die Bearbeitung der Personendaten benötigt er jedoch eine Einwilligung (solange er sich nicht auf eine gesetzliche Grundlage oder ein überwiegendes privates oder öffentliches Interesse berufen kann). In der Regel ist dies unproblematisch, da sich Personen auf eigenen Namen registrieren und somit (bei

ausreichender vorgängiger Information) zumindest von einer impliziten Zustimmung ausgegangen werden kann. Richtet sich allerdings eine Webseite an minderjährige Personen, stellt sich die Frage, ob und inwieweit diese eine rechtsgültige Einwilligungserklärung abgeben können.

Eine Zustimmung kann grundsätzlich nur zustande kommen, wenn die zustimmende Person handlungsfähig, das heisst mündig und urteilsfähig ist. Nach dem Schweizerischen Zivilgesetzbuch ist dies bei einer natürlichen Person erst mit vollendetem 18. Lebensjahr der Fall. Davor benötigt sie für Verpflichtungsgeschäfte (also alle Rechtshandlungen, welche eine Belastung oder einen Verzicht auf Rechte beinhalten) die Zustimmung ihres gesetzlichen Vertreters. Dabei spielt der Schutz des Unmündigen eine zentrale Rolle. Der gesetzliche Vertreter kann aber eine generelle Zustimmung für eine ganze Reihe von Verpflichtungsgeschäften erteilen, sofern diese überblickbar und in ihren potentiellen Auswirkungen berechenbar bleiben. Er muss also nicht in jedes einzelne Rechtsgeschäft einwilligen, das sein Mündel abschliesst.

Es ist fraglich, ob eine durch die gesetzlichen Vertreter erteilte Erlaubnis zur Internetnutzung als Rahmen ausreicht, um damit eine implizierte rechtsgültige Einwilligung zur Bearbeitung derjenigen personenbezogenen Daten anzunehmen, welche die Minderjährigen im Internet freiwillig offenbaren. Für die Altersklasse zwischen 12 und 16 Jahren ist dies aus unserer Sicht zu verneinen. Da der Datenschutz die Wahrung der Persönlichkeitsrechte zum Ziel hat, können nach Ansicht des EDÖB die Befugnisse urteilsfähiger Unmündiger im Umgang mit den ihnen zur freien Verfügung stehenden Vermögenswerten (Taschengeld) nicht angewendet werden. Wenn sich Minderjährige auf einer Webseite registrieren und dabei eine Datenschutzerklärung abgeben, ist unserer Meinung nach die Zustimmung der gesetzlichen Vertreter erforderlich.

Werden Eltern unverhofft vom Betreiber einer Webplattform brieflich aufgefordert, ihre Zustimmung für die Nutzung der Plattform abzugeben, kann dies zu Irritationen führen. Daher raten wir zu folgendem Vorgehen:

Betreiber einer Webplattform sollten nach vorgängiger Information in einem ersten Schritt grundsätzlich nur die Adresse des Minderjährigen erfragen, aufgrund welcher sie dann die Eltern anschreiben können. Dabei sollten die Jugendlichen bestätigen, dass sie die Eltern um Zustimmung gefragt haben. Der Betreiber seinerseits müsste die minderjährigen User darauf aufmerksam machen, dass die Eltern in den nächsten Tagen diese Zustimmung per Post schriftlich zu bestätigen haben. Dies soll beim Minderjährigen bewirken, dass er bereits vor oder während seiner Eingabe seine Eltern um ihre Zustimmung bittet. Somit sind diese informiert und werden nicht von der Post überrascht. Stimmen die Eltern zu, darf die Nutzung freigeschaltet werden. Stimmen sie nicht innerhalb nützlicher Frist zu, sind sämtliche eingegebenen Daten zu löschen.

1.3.3 Ärztebewertungsseiten im Internet

Im Anschluss an zahlreiche Beschwerden über die Webseite für die Bewertung von Ärzten www.okdoc.ch haben wir den Sachverhalt abgeklärt und die Datenschutzanforderungen im Rahmen der anonymen Online-Bewertung von Praktikern des Gesundheitswesens genauer ausgeführt.

Die Online-Schaltung einer Webseite zur Bewertung von Ärzten www.okdoc.ch im Mai 2008 hat von Seiten der Praktiker aus dem Gesundheitswesen zahlreiche Beschwerden ausgelöst. Daraufhin haben wir gemäss Art. 29 DSG den Sachverhalt bei der für diese Bewertungsseite verantwortlichen Firma Bonus AG abgeklärt und ihr im Juni 2008 unsere Empfehlungen vorgelegt. Sie bezogen sich insbesondere auf die notwendige Einwilligung der betroffenen Ärzte und auf deren Möglichkeit, sich nicht nur den Bewertungen, sondern auch der Erwähnung der Personalien (Name, Fachgebiet und Adresse) zu widersetzen. Nach einer Besprechung mit dem Verantwortlichen hat Bonus.ch die Bewertungsseite in eine Empfehlungsseite umgewandelt.

Bei der Nachkontrolle der Umsetzung unserer Empfehlungen haben wir die Voraussetzungen festgelegt, welche die neue Empfehlungsseite erfüllen muss, um der Datenschutzgesetzgebung zu entsprechen:

- Die positiven Bewertungen und Kommentare können insofern aufbewahrt werden, als sie Praktiker des Gesundheitswesens betreffen, die sich nach Erhalt eines Informationsschreibens nicht gegen die fragliche Datenbearbeitung ausgesprochen haben (stillschweigendes Einverständnis).
- Die Reaktivierung der Empfehlungsmodalitäten für Ärzte, die sich einer Bewertung widersetzt haben, ist nur möglich, wenn sie sich nach Erhalt eines Informationsschreibens ausdrücklich damit einverstanden erklären, die Bewertung auf der neuen Webseite erscheinen zu lassen.
- Ebenso müssen die Personalien grundsätzlich von der Webseite entfernt werden, soweit die betroffenen Praktiker des Gesundheitswesens dies verlangt haben. Sie können nur fallweise wieder aufgenommen werden, wenn im Anschluss an die Zusendung des Informationsschreibens ein Arzt, der zuvor um Entfernung der ihn betreffenden Verkehrsdaten ersucht hatte, ausdrücklich deren Wiederaufnahme verlangt.

Bonus.ch hat diese Punkte unter dem Titel «Stillschweigendes Einverständnis und Widerspruchsrecht» in einem Abschnitt des an die Ärzte gerichteten Informationsschreibens aufgeführt. Der Versand des Informationsschreibens von Bonus.ch an alle Praktiker des Gesundheitswesens fällt in den Rahmen der Nachkontrolle der Umsetzung unserer Empfehlungen.

1.3.4 Persönlichkeitsschutz bei der Berichterstattung im Internet

Ob eine Berichterstattung im Internet die Persönlichkeitsrechte der Betroffenen verletzt, ist mit einer Verhältnismässigkeitsabwägung zwischen dem öffentlichen Interesse an dem Ereignis und dem schützenswerten Interesse an der Privatsphäre der Betroffenen zu beurteilen. Im Vordergrund der Berichterstattung sollte das Ereignis stehen und nicht der einzelne Teilnehmer, an dem kein öffentliches Interesse besteht. Wir erachten es in der Regel als widerrechtliche Persönlichkeitsverletzung, wenn Einzelne an den Pranger gestellt werden. Im vergangenen Jahr hatten wir mehrere solche Fälle zu beurteilen, weshalb wir Leitlinien zur Erleichterung der Verhältnismässigkeitsabwägung erarbeitet haben.

Immer häufiger werden auf Webseiten Berichte über Veranstaltungen veröffentlicht, die Teilnehmerinnen und Teilnehmer auf Photos zeigen. Dies reicht von der Berichterstattung über kleinere Veranstaltungen im Rahmen eines Vereins bis hin zu Grossveranstaltungen, über welche in Print- und Digitalmedien berichtet wird. Dabei stellt sich oft die Frage, inwieweit es zulässig ist, einzelne Personen erkennbar darzustellen, und ab welchem Zeitpunkt dies die Persönlichkeitsrechte verletzt. Dazu bedarf es einer Verhältnismässigkeitsabwägung zwischen dem öffentlichen Interesse an der Berichterstattung und den schützenswürdigen Interessen an der Privatsphäre der Betroffenen. Im vergangenen Jahr haben wir Leitlinien erarbeitet, welche eine solche Verhältnismässigkeitsabwägung erleichtern sollen.

Grundsätzlich müssen Teilnehmer und Besucher öffentlicher Veranstaltungen damit rechnen, in der einen oder anderen Weise in der Berichterstattung erwähnt bzw. fotographisch abgebildet zu werden, da solche Veranstaltungen im öffentlichen Interesse liegen. Allerdings ist nicht jegliche Art von Berichterstattung legitim. So sollten sich Texte und Bilder im Wesentlichen auf die im öffentlichen Interesse liegenden Aspekte (Veranstaltung selbst, besondere Vorkommnisse, etc.) beschränken und die Persönlichkeit der anwesenden Personen möglichst gut schonen. Darauf gilt es bei der Textredaktion und der Auswahl der Bilder zu achten. Relativ unproblematisch sind Berichte

über Personen des öffentlichen Lebens sowie solche, die im Wesentlichen den Charakter der Veranstaltung darstellen. Konzentrieren sich die Informationen hingegen auf einzelne Personen, die sich im Rahmen der Veranstaltung weder besonders exponiert noch einer solchen Berichterstattung zugestimmt haben, ist das in der Regel unzulässig. Werden zudem einzelne Personen oder Personengruppen (womöglich noch mit Namen) an den Pranger gestellt, so liegt meist eine unzulässige Persönlichkeitsverletzung vor.

Zahlreiche Veranstalter informieren die Teilnehmer auf ihren Webseiten darüber, dass solche Berichterstattungen möglich sind und personenbezogene Daten an Dritte weitergegeben werden. Wir haben festgestellt, dass sich einige Veranstalter, insbesondere im Rahmen des Sponsorings, sehr allgemein formulierte und weit reichende Nutzungsrechte der Personendaten der Teilnehmer einräumen lassen. Das erreichen sie mit entsprechenden und bei der Anmeldung obligatorischen Einwilligungsklauseln. Eine solche Vorgehensweise erachten wir als unzulässig; insgesamt ist die Tragweite der Datenbearbeitung in einem solchen Fall für den Betroffenen nicht mehr transparent, er daher auch nicht angemessen informiert. Zudem kann man nicht in jedem Fall die Einwilligung in solche Klauseln verlangen. Insbesondere ist dies im Rahmen des Marketings nicht möglich (vgl. dazu auch Ziff. 1.8.5).

In manchen Fällen werden allerdings auch einzelne Besucher einer Veranstaltung (oft ohne deren Wissen) porträtiert und ihre Personendaten im Internet veröffentlicht. Wenn kein überwiegendes öffentliches Interesse an der personenbezogenen Darstellung eines Betroffenen besteht, ist dies eine widerrechtliche Persönlichkeitsverletzung, da die Betroffenen nicht mit einer solchen Berichterstattung rechnen müssen. Die Datenbearbeitung ist für sie nicht erkennbar, und es kann nicht von einer impliziten Zustimmung ausgegangen werden. So wurden beispielsweise im Rahmen der Berichterstattung über das Sempacher Volksfest auf der Webseite www.indymedia.ch einzelne Teilnehmer, welche dem rechtsextremen Lager angehören sollen, von meist anonymen Autoren porträtiert und auf diese Weise an den Pranger gestellt.

Da die anonyme Berichterstattung in einigen Fällen eine freie Meinungsäusserung erst ermöglicht und damit einen wichtigen Bestandteil der Pressefreiheit darstellt, muss sie unserer Meinung nach grundsätzlich möglich bleiben. Journalisten und Berichterstatter sollten aber auf Persönlichkeitsverletzungen verzichten.

Ein weiteres Problem stellt das Hosting der Internetseiten im (nicht europäischen) Ausland dar, weil den betroffenen Personen kein effektiver Rechtsweg offen steht. Einmal mehr machen wir auf die Schwierigkeiten aufmerksam, einen effektiven Datenschutz in einem weltumspannenden Medium wie dem Internet durchzusetzen. Wir fordern daher allgemeine internationale Regelungen zur Verbesserung des Datenschutzes.

1.3.5 Auswertungstools für Webseiten

Im Auftrag der Bundesverwaltung und aufgrund verschiedener Bürgeranfragen haben wir die datenschutzrechtlichen Aspekte von Auswertungstools für Webseiten analysiert. Beim Einsatz von Auswertungstools zur Erstellung von Zugriffsstatistiken von Webseiten sind aus unserer Sicht verschiedene Voraussetzungen zu erfüllen. Insbesondere sind die Nutzer in einer Datenschutzerklärung darauf hinzuweisen, welche Daten über sie gesammelt und an wen sie weitergegeben werden (inklusive Angabe des Landes). Werden die Daten in ein Land weitergegeben, welches über kein angemessenes Datenschutzniveau verfügt, sind zusätzlich mit dem Anbieter des Auswertungstools Garantien zu vereinbaren, die ein ausreichendes Schutzniveau gewährleisten.

Im letzten Jahr sind immer mehr Webseitenbetreiber dazu übergegangen, ihre Webstatistiken nicht mehr selbst über entsprechende auf den Servern installierte Programme zu erstellen. Stattdessen lassen sie die Besuche auf ihren Webseiten durch Onlinetools (wie z.B. Google Analytics) auswerten. Da IP-Adressen als personenbezogene Daten betrachtet werden müssen, ist das Bundesgesetz über den Datenschutz (DSG) anwendbar. Um also solche Auswertungstools datenschutzrechtskonform einzusetzen, müssen Betreiber einer Webseite insbesondere die nachfolgend beschriebenen Punkte beachten.

Das Online-Auswertungstool wird mittels eines speziellen Bildelements sowie eines Skripts des Anbieters in der Webseite des Betreibers integriert. So erfasst der Anbieter des Auswertungstools die Zugriffe auf die Webseite, da beim Abruf des Bildelements die IP-Adresse der zugreifenden Nutzer von seinen Servern registriert wird. Es werden also die Randdaten des Internetnutzers, welche beim Besuch der Webseite anfallen, an den Anbieter des Auswertungstools weitergeleitet. Dieser Vorgang ist aus datenschutzrechtlicher Sicht als Datenbearbeitung durch Dritte zu qualifizieren. Eine solche ist gemäss Art. 10a DSG durch Vereinbarung möglich, wenn der Anbieter des Tools die Daten nur so bearbeitet, wie es der Betreiber der Webseite selbst tun dürfte, und keine gesetzliche oder vertragliche Geheimhaltungspflicht sie verbietet.

Aus diesem Grund muss der Betreiber einer Webseite den Anbieter des Auswertungstools vertraglich dazu verpflichten, die gelieferten Daten ausschliesslich zu den Auswertungszwecken des Betreibers (und nicht zu eigenen Zwecken) zu nutzen und die Datensicherheit zu gewährleisten. Zudem muss der Betreiber der Webseite aufgrund des Erkennbarkeitsprinzips die Nutzer im Rahmen einer Datenschutzerklärung auf die Verwendung eines solchen Tools sowie Art und Umfang der gesammelten Daten hinweisen.

Befinden sich die Server des Anbieters des Auswertungstools im Ausland, sind darüber hinaus die datenschutzrechtlichen Regelungen zum grenzüberschreitenden Datentransfer zu beachten. Personendaten dürfen nämlich nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, namentlich weil eine Gesetzgebung fehlt, die einen angemessenen Schutz garantiert (eine Auflistung der einzelnen Länder und ihres Datenschutzniveaus kann auf unserer Webseite www.derbeauftragte.ch unter Themen – Datenschutz – Übermittlung ins Ausland abgerufen werden). In diesem Fall darf ein solches Auswertungstool nur dann genutzt werden, wenn der Anbieter durch hinreichende Garantien einen angemessenen Schutz gewährleistet (Art. 6 Abs. 2 lit. a DSG). Dies erfolgt in der Praxis meist durch eine entsprechende schriftliche Bestätigung des Anbieters. Seit Januar 2009 steht beim Datentransfer in die USA zusätzlich das «U.S.-Swiss Safe Harbor Framework» als Instrument zur Gewährleistung eines ausreichenden Schutzniveaus zur Verfügung (siehe dazu Ziff. 1.1.6).

Solange der Betreiber einer Webseite diese Punkte beachtet, steht der Nutzung eines solchen Auswertungstools aus datenschutzrechtlicher Sicht nichts entgegen. Grundsätzlich sollten Betreiber einer Webseite allerdings evaluieren, inwieweit es für sie wünschenswert ist, Personendaten ihrer Webseitenbesucher ins Ausland zu übertragen. Ausländische Behörden könnten nämlich aufgrund ihrer nationalen Gesetzgebungen auf die sich in ihrem Land befindlichen Daten zugreifen.

1.3.6 Erläuterungen zu sozialen Netzwerken

Social Network Sites (SNS) liegen im Trend und die Zahl der Nutzerinnen und Nutzer steigt täglich an. Längst tauschen sie über soziale Netzwerke allerlei persönliche Informationen aus und erstellen so von sich selbst nicht selten ein Persönlichkeitsprofil, welches sie anderen Nutzern zur Verfügung stellen. Dabei werden oft die Risiken von sozialen Netzwerken übersehen. Wir haben diese Entwicklung zum Anlass genommen, diese Risiken näher unter die Lupe zu nehmen und Nutzern von SNS Tipps zum Umgang mit ihren Personendaten zu geben. Die Erläuterungen zu sozialen Netzwerken befinden sich im Anhang Ziff. 4.1.1 und können auf unserer Webseite www.derbeauftragte.ch, Themen – Datenschutz – Internet, abgerufen werden.

1.3.7 Erläuterungen zu Bewertungsplattformen im Internet

Bewertungen von verschiedenen Berufsgruppen im Internet (Ärzte, Professoren, Lehrer etc.) haben in letzter Zeit stark an Popularität gewonnen. Da eine online Bewertung die Persönlichkeit der bewerteten Person tangieren kann, haben wir uns entschlossen,

verschiedene Bewertungsseiten zu analysieren. Aus den gewonnenen Erkenntnissen haben wir Grundsätze für die Ausgestaltung und Nutzung von Bewertungswebseiten erarbeitet mit dem Ziel, den Benutzern, Entwicklern und Betroffenen solcher Seiten nützliche Ratschläge zu erteilen. Der Bericht befindet sich im Anhang Ziff. 4.1.2 und kann auf unserer Webseite www.derbeauftragte.ch, Themen – Datenschutz – Internet, abgerufen werden.

1.3.8 Erläuterungen zum Digitalen Fernsehen, zu ITV und IPTV

Sowohl im Internet als auch über Breitbandverbindungen steigt das Angebot an digitalen Filmen stetig an. Während bei der traditionellen terrestrischen Ausstrahlung von Programmen ein anonymer Konsum von Fernsehsendungen und Filmen möglich war, steht beim Digitalen Fernsehen bzw. IPTV ein breitbandiger Rückkanal zur Verfügung, über welchen sich theoretisch die Konsumgewohnheiten der Fernsehzuschauer ermitteln lassen. Diese neuen Technologien sind insbesondere für die Werbung sehr interessant, die sich auf diese Art personalisieren lässt. Wir haben in unseren Erläuterungen zum Thema Digitales Fernsehen die Risiken und Gefahren analysiert und geben Anbietern und betroffenen Konsumenten Tipps zum Umgang mit dem digitalen Medium. Der vollständige Bericht befindet sich im Anhang Ziff. 4.1.3 und kann auf unserer Webseite www.derbeauftragte.ch, Themen – Datenschutz – Sonstige Themen, abgerufen werden.

1.3.9 Erläuterungen zu Pay as You Drive und dem Einsatz von Black Boxen in Motorfahrzeugen

Risikominimierung und Gefahrenverhütung sind wichtige Anliegen von KFZ-Versicherungen. Seit dem letzten Jahr bietet in der Schweiz eine Versicherung einen Vertrag speziell für Junglenker an. Mit dem Einbau einer Black-Box, welche Daten über die Fahrzeugbewegungen kurz vor und nach einem Unfall aufzeichnet, erhalten sie einen erheblichen Prämienrabatt von bis zu 30%. Theoretisch ist es denkbar, mit den heute zur Verfügung stehenden Technologien das gesamte Fahrverhalten von Strassenverkehrsteilnehmern aufzuzeichnen und damit auch zu überwachen. Aus diesem Grund haben wir das Thema Pay as You Drive aus datenschutzrechtlicher Sicht analysiert. Der ausführliche Bericht zu dem Thema befindet sich im Anhang Ziff. 4.1.4 und kann auf unserer Webseite www.derbeauftragte.ch, Themen – Datenschutz – Versicherungen, abgerufen werden.

1.4 Justiz/Polizei/Sicherheit

1.4.1 Umsetzung Schengen

Die Berichte über die Umsetzung von Schengen und unsere damit verbundenen Tätigkeiten befinden sich in Ziffer 1.9.

1.4.2 Inkrafttreten des Bundesgesetzes über die polizeilichen Informationssysteme des Bundes

Das Bundesgesetz über die polizeilichen Informationssysteme des Bundes vereint in einem Regelwerk die Rechtsgrundlagen für einen grossen Teil der auf Bundesebene geführten polizeilichen Datensammlungen. Sämtliche Auskunftsgesuche zu diesen Datensammlungen sind direkt an das Bundesamt für Polizei zu richten.

Das Bundesgesetz über die polizeilichen Informationssysteme des Bundes (BPI) ist am 5. Dezember 2008 in Kraft getreten. Dieses Gesetz gilt für die vom Bund geführten polizeilichen Datensammlungen. Ausnahmen sind die Datensammlungen GEWA der Meldestelle für Geldwäscherei, ISIS des Dienstes für Analyse und Prävention (seit dem 1. Januar 2009 dem Generalsekretariat des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport VBS angeschlossen), die auf den DNA-Profilen beruhenden Datensammlung, die Datensammlung AFIS mit den Abbildungen der Fingerabdrücke und die Datensammlung ISA betreffend die Ausweisschriften. Bezüglich GEWA bestimmt das Geldwäschereigesetz (GwG), dass das Auskunftsrecht für Einzelpersonen nach Art. 8 BPI geregelt wird.

Die neue Gesetzgebung sieht vor, dass Auskunftsgesuche zur Datensammlung JANUS, in der Daten über das organisierte Verbrechen oder den Betäubungsmittelhandel und den Menschenhandel enthalten sind, sowie zur Datensammlung GEWA, welche die Bekämpfung der Geldwäscherei betrifft, direkt an das Bundesamt für Polizei (fedpol) und nicht mehr an unser Sekretariat zu richten sind. Wir sind jedoch immer noch sehr aktiv in diesem Bereich, namentlich bei der Bearbeitung von Prüfungsgesuchen betreffend JANUS und GEWA und von Gesuchen, die den Aufschub der Auskunft aufheben sollen. Diese Forderung wird gestellt, wenn der betroffenen Person durch den Aufschub ein erheblicher und nicht wiedergutzumachender Schaden erwachsen würde. Für weitere Einzelheiten bezüglich der Bedingungen für Auskünfte zu den Datensammlungen JANUS und GEWA verweisen wir auf unseren 15. Tätigkeitsbericht 2007/2008, Ziff. 1.4.4.

1.4.3 Augenscheine beim Pilotbetrieb des Nationalen Polizeiindexes

Die durchgeführten Augenscheine und die uns vom Bundesamt für Polizei zur Verfügung gestellte Dokumentation erlaubten uns die Feststellung, dass der Pilotbetrieb des Nationalen Polizeiindexes die Anforderungen des Bundesgesetzes über den Datenschutz und der Verordnung über den Pilotbetrieb des Nationalen Polizeiindexes einhält.

In Zusammenarbeit mit dem Bundesamt für Polizei (fedpol) haben wir im Februar 2008 Augenscheine bei der für den Pilotbetrieb des Nationalen Polizeiindexes verantwortlichen Abteilung des fedpol, bei der Einsatzzentrale fedpol, dem Lage- und Nachrichtenzentrum des Grenzwachtkorps in Bern und beim Kommando der Kantonspolizei Bern durchgeführt. Letzterer erfolgte in Zusammenarbeit mit dem Datenschutzbeauftragten des Kantons Bern. Bei den Augenscheinen ging es hauptsächlich darum, die Einhaltung des Bundesgesetzes über den Datenschutz und der Verordnung über den Pilotbetrieb des Nationalen Polizeiindexes zu überprüfen. Im Rahmen dieser Augenscheine haben wir namentlich die bearbeiteten Daten, den Zugang zum Index und die Datensicherheit analysiert.

Bezüglich der Bearbeitung der Personendaten hat uns fedpol bestätigt, dass die Kategorien «AFIS DNA» und «INTERPOL» des informatisierten Personennachweis-, Aktennachweis- und Verwaltungssystems im Bundesamt für Polizei (Datensammlung IPAS) und das Informationssystem der Bundeskriminalpolizei (Datensammlung JANUS) im Rahmen des Pilotbetriebs dem Index angeschlossen seien. Wie die Augenscheine zeigten, hatten die Nutzer Zugriff auf die in der Verordnung über den Pilotbetrieb des Nationalen Polizeiindexes vorgesehenen Daten. Dies beinhaltet Angaben zur Identifizierung der Person, Datum und Grund des Eintrags, wenn eine Person erkennungsdienstlich behandelt worden ist, den Namen der Behörde, bei der um weitere Informationen über die Person ersucht werden kann, und des Informationssystems, aus welchem die Daten stammen.

Im Rahmen des Pilotbetriebs des Nationalen Polizeiindexes wurden rund 500 individuelle Zugriffsbewilligungen an Nutzer beim Bund (rund 300 Zugriffe) und bei den Kantonen (rund 200 Zugriffe) bewilligt. Diese Zahl scheint, in Anbetracht der Gesamt-Benutzerzahl des Nationalen Polizeiindexes (rund 5'000 für die Bundesverwaltung, die Kantone und die Gemeinden), angemessen.

Im Bereich der Datensicherheit ist der Zugriff auf den Index durch verschiedene Sicherheitsmassnahmen geschützt. Sämtliche Datenübertragungen werden chiffriert und alle Aktivitäten protokolliert.

Abschliessend konnten wir aufgrund der durchgeführten Augenscheine und der vorgelegten Dokumentation feststellen, dass der Pilotbetrieb des Nationalen Polizeiindexes den Anforderungen des Bundesgesetzes über den Datenschutz und der Verordnung über den Pilotbetrieb des Nationalen Polizeiindexes entspricht.

1.4.4 Auskunftsgesuche betreffend das Informationssystem ISIS

Die Anzahl der Auskunftsgesuche betreffend das Informationssystem ISIS ist 2008 rasant angestiegen. Zum ersten Mal konnten wir zudem einzelne Gesuchsteller angemessen über das Vorhandensein von Einträgen informieren. Es wäre wünschenswert, wenn betreffend ISIS, wie neu für JANUS und GEWA, ein direktes Auskunftsrecht eingeführt werden könnte.

Die Anzahl der so genannten indirekten Auskunftsgesuche für die Datenbank ISIS (innere Sicherheit) hat 2008 enorm zugenommen. So sind insgesamt 148 Auskunftsgesuche für ISIS bei uns eingetroffen, gegenüber 19 im Vorjahr. Dieser rasante Anstieg beruht hauptsächlich auf zwei Gründen.

So kam es zum ersten Mal vor, dass wir bei in ISIS eingetragenen Personen von der gesetzlichen Ausnahmeregelung Gebrauch machten und sie angemessen über ihre Einträge informierten. In der Tat sieht das entsprechende Gesetz vor, dass wir grundsätzlich nur eine nichtssagende und stets gleichlautende Mitteilung verschicken. Aufgrund dieser Mitteilung weiss die betroffene Person nicht, ob über sie Einträge in ISIS vorliegen oder nicht. Sie erhält nur die Gewissheit, dass der EDÖB das Gesuch überprüft und bei allfälligen Unrechtmässigkeiten gegenüber dem Amt eine Empfehlung zu deren Korrektur erlassen hat. Die erwähnte gesetzlich vorgesehene Ausnahme, die eine weitergehende Information erlaubt, ist sehr eng auszulegen und im Einzelfall zu überprüfen. In den genannten Fällen ging es unter anderem um mehrere Gesuchsteller, die gleichzeitig ihr Auskunftsrecht für ISIS geltend machten. Alle Gesuchsteller vermuteten aufgrund bestimmter vorgefallener Tatsachen, in der Datenbank eingetragen zu sein. Unsere Überprüfungen ergaben, dass die von den Gesuchstellern darlegten Tatsachen zu keinen Einträgen in ISIS geführt hatten. Allerdings waren einige der Betroffenen aus anderen Gründen eingetragen. Nach Prüfung der einzelnen Gesuche kamen wir zum Schluss, dass die Voraussetzungen der Ausnahmebestimmung im BWIS (erheblicher nicht wieder gut zu machender Schaden der gesuchstellenden Person und keine Gefährdung der inneren und äusseren Sicherheit) in allen Fällen erfüllt waren. Folglich informierten wir die Gesuchsteller angemessen. Sie machten diese Informationen teilweise publik und forderten weitere Personen auf, bei uns ebenfalls

ihr Auskunftsrecht für ISIS geltend zu machen. Diesbezüglich ist darauf hinzuweisen, dass wir natürlich jeweils im Einzelfall überprüfen müssen, ob die Voraussetzungen für eine Abweichung von der Standardantwort gegeben sind.

Einen weiteren Auslöser von vielen Auskunftsgesuchen in ISIS bildeten sodann die in den Medien veröffentlichten Fälle einzelner Grossratsmitglieder des Kantons Basel-Stadt. Wie dabei publik wurde, habe die Geschäftsprüfungskommission von Basel-Stadt festgestellt, dass Daten über einige Grossratsmitglieder kurdischen Ursprungs an den Dienst für Analyse und Prävention (DAP) im Bundesamt für Polizei geschickt worden seien.

Im Zusammenhang mit ISIS sind nun verschiedene Fälle vor dem Bundesverwaltungsgericht hängig. Für uns ist natürlich von Interesse zu sehen, wie das Gericht entscheiden wird.

Der für ISIS verantwortliche DAP ist seit dem 1. Januar 2009 nicht mehr dem Bundesamt für Polizei, sondern dem Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) angegliedert. Wir gehen davon aus, dass dies an der bisherigen guten Zusammenarbeit nichts ändern wird.

Wie in Ziff. 1.4.2 des vorliegenden Tätigkeitsberichts erwähnt, gilt für die Datenbanken JANUS und GEWA neu das direkte Auskunftsrecht. Es wäre begrüssenswert, wenn für ISIS so rasch wie möglich eine analoge Regelung vorgesehen würde. Wir haben uns seit jeher gegen das so genannte indirekte Auskunftsrecht ausgesprochen und halten ein direktes Auskunftsrecht für angebrachter.

1.4.5 Aufnahme biometrischer Daten in Reisedokumente

Mehrere Anfragen sind bei uns eingegangen im Zusammenhang mit dem Referendum gegen den Bundesbeschluss vom 13. Juni 2008 über die Genehmigung und die Umsetzung des Notenaustauschs zwischen der Schweiz und der Europäischen Gemeinschaft betreffend die Übernahme der Verordnung (EG) Nr. 2252/2004 über biometrische Pässe und Reisedokumente (Weiterentwicklung des Schengen-Besitzstands). Wir haben auf unsere Stellungnahme (vgl. unseren 15. Tätigkeitsbericht 2007/2008, Ziff. 1.1.3) verwiesen und dabei daran erinnert, dass einerseits die EG-Verordnung keine Aufbewahrung der biometrischen Daten über die für die Ausstellung der Dokumente notwendige Zeit hinaus vorsieht, und dass wir andererseits eine zentralisierte Aufbewahrung der biometrischen Daten in Datensammlungen für Ausweise nicht unterstützen.

1.4.6 Verwendung von DNA-Profilen im Strafverfahren und zur Identifizierung von unbekannten und vermissten Personen

Im Rahmen unserer Funktion als Datenschutzaufsichtsbehörde haben wir eine Sachverhaltsabklärung beim Bundesamt für Polizei fedpol durchgeführt. Bei den überprüften Datenbearbeitungen wurde der Datenschutz vollumfänglich eingehalten.

Im Rahmen der Sachverhaltsabklärung wurden die Koordinationsstelle DNA (Betreiberin der Datenbank CODIS), die AFIS DNA Services (Betreiber der Datenbank IPAS) sowie die Kommunikationsplattform «Message Handler» überprüft. Wir haben schwergewichtig Dokumente über die Datenbearbeitung, die einzelnen Prozesse sowie die entsprechenden Datenflüsse einverlangt und analysiert.

Anlässlich eines Augenscheins bei der Koordinationsstelle DNA im Institut für Rechtsmedizin an der Universität Zürich-Irchel und bei den AFIS DNA Services beim Bundesamt für Polizei (fedpol) haben wir uns die Datenbearbeitungen vorführen lassen.

Die Sachverhaltsabklärung hat folgendes ergeben:

Die Strafverfolgungsbehörden aller Stufen sehen sich mit modernen Kriminalitätsformen konfrontiert, die sich durch hohe Mobilität, vermehrte Spezialisierung, Teamwork und den Einsatz technischer Mittel auszeichnen. Bei der Verfolgung dieser Kriminalitätsformen sind u.a. die rasche und zweifelsfreie Identifizierung von Tätern bzw. Tätergruppen sowie die Erkennung von kriminellen Aktivitäten und von Tatzusammenhängen, welche Kantons- und Landesgrenzen überschreiten, von grosser Bedeutung. Dazu gehört die systematische Auswertung jeglicher, auch der biologischen Spuren, so zum Beispiel die Identifikation mittels DNA-Profilen.

Am 1. Januar 2005 ist das Bundesgesetz über die Verwendung von DNA-Profilen im Strafverfahren und zur Identifizierung von unbekannten und vermissten Personen in Kraft getreten. Das Gesetz regelt, unter welchen Voraussetzungen DNA-Profile in Strafverfahren verwendet und in einem Informationssystem des Bundes bearbeitet werden können. Das Gesetz regelt ausserdem die Identifizierung von unbekannten, vermissten oder toten Personen ausserhalb des Strafverfahrens mit Hilfe des Vergleichs von DNA-Profilen.

Das DNA-Profil ist die für jedes Individuum spezifische Kombination aus Buchstaben und Zahlen, die mit Hilfe molekularbiologischer Techniken aus den nicht-codierenden Abschnitten der Erbsubstanz DNA gewonnen wird und die eindeutige Identifizierung einer Person erlaubt.

Ausgelöst wird der Prozess für die Identifikation mittels eines DNA-Profils durch die Strafverfolgungs- (kantonale Polizei) oder Strafuntersuchungsbehörde. Sie ist es auch, welche die Vorabklärungen basierend auf Fingerabdrücken vor- und die Wangenschleimhautabstriche (WSA) abnimmt sowie die Tatortspuren sichert und den Auftrag zur Profilanalyse erteilt.

Zu Beginn des Bearbeitungsprozesses wird dem biologischen Material durch die Polizei eine Prozess-Kontroll-Nummer (PCN) zugeordnet. Diese eindeutige und einmalige Bezeichnung jedes einzelnen WSA und jeder einzelnen Spur erlaubt eine zweifelfreie Nachverfolgbarkeit von der Materialerfassung bis zur Datenlöschung respektive Vernichtung des Materials und die Pseudonymisierung des Ablaufs.

Das forensische DNA-Analyselabor empfängt das biologische Material per Post, Kurier oder direkt durch die Polizei. Der Empfang jeder einzelnen Spur und jedes einzelnen WSA wird überprüft und bestätigt. Die für die Spurenverarbeitung notwendigen Fallangaben stellt die Polizei dem Labor zur Verfügung. Es erstellt die DNA-Profile der WSA und der Tatortspuren und übermittelt die Profile an die Koordinationsstelle DNA. Das biologische Material wird spätestens nach 3 Monaten vernichtet.

Die Koordinationsstelle DNA am Institut für Rechtsmedizin Zürich betreibt im Auftrag des Bundes die DNA-Profildatenbank CODIS (Combined DNA Index System). Sie nimmt die DNA-Profile des Labors oder der Bundeskriminalpolizei (Interpol-Anfragen) entgegen, speichert sie in CODIS, führt den automatisierten Abgleich mit den bereits vorhandenen DNA-Profilen durch und wertet das Suchresultat aus.

Bei einer Übereinstimmung zwischen einem Personen-Profil und einer Spur von einem Tatort spricht man von einem «Hit». Ein solcher Hit trägt zur Klärung eines oder mehrerer Fälle bei, in belastendem oder in entlastendem Sinne. Das definitive Suchresultat in Form von Search- und Hit-PCN übergibt die Koordinationsstelle DNA den AFIS DNA Services beim fedpol.

Ende 2007 enthielt die Datenbank CODIS 92'912 Personenprofile und 17'346 Tatortspuren. Daraus erfolgten folgende Hits bzw. Treffer:

Person-Spur: 3'210 Hits

Person-Person (eineiige Zwillinge): 17 Hits

Spur-Spur: 4'809 Hits (diese Hits geben wertvollen Aufschluss über Tatzusammenhänge)

Die AFIS DNA Services erhalten das Suchresultat als PCN. Die Ergebnismeldung wird automatisch mit den entsprechenden Personen- und Falldaten in IPAS ergänzt. Die komplette Meldung wird zusammen mit dem Meldungsverteiler durch die AIFS DNA Services kontrolliert, nötigenfalls korrigiert und ergänzt. Anschliessend wird sie dem Meldungsverteiler entsprechend frei geschaltet.

Am Schluss des Abklärungsprozesses kann die Polizei die Meldung einsehen, ausdrucken oder direkt in ihre Rapporte übernehmen. Sie leitet die Informationen bei Bedarf an die betroffenen Justizbehörden weiter. Die Auslösung des Löschauftrages erfolgt durch die Polizei selbständig oder im Auftrag der zuständigen Justizorgane. Die Koordinationsstelle DNA führt die eintreffenden Löschaufträge in CODIS aus. Den sicheren Datentransfer garantiert eine eigens für diesen Zweck erstellte Kommunikationsplattform.

Die Datenbanken CODIS (DNA-Profil) und IPAS (Personen- und Fall-Daten) sind physisch und organisatorisch getrennt und können nur mittels oben erwähnter PCN bei einem Hit verknüpft werden. Die Koordinationsstelle DNA nimmt zusammen mit den AFIS DNA Services regelmässige Abgleiche zwischen den Datenbanken CODIS und IPAS vor.

Im Rahmen unserer Sachverhaltsabklärung haben wir festgestellt, dass bei den überprüften Bearbeitungen der Datenschutz vollumfänglich eingehalten wird.

1.4.7 Gesichtserkennungssysteme in Sportstadien

Wir wurden angefragt, zu zwei Teilaspekten des Projekts «Sicherheit im Sport» Stellung zu nehmen. Dabei handelte es sich vor um allem die Themen «Einsatz von Biometrie resp. von Gesichtserkennungsgeräten bei den Eingängen eines Stadions» und «Verknüpfung von Videoaufnahmen in den Stadien und Biometrie resp. Gesichtserkennung». Der Einsatz von Gesichtserkennungssystemen in Stadien ist datenschutzrechtlich zulässig, wenn bestimmte Voraussetzungen eingehalten werden.

Vertreter von Bund, Kantonen und Sportverbänden setzten sich zu einem «Runden Tisch zur Bekämpfung von Gewalt im und um den Sport» zusammen. In diesem Zusammenhang wurden wir von einer Arbeitsgruppe des runden Tischs angefragt, zu zwei Teilaspekten des Projekts «Sicherheit im Sport» Stellung zu nehmen. Dabei handelte es sich vor allem um die Themen «Einsatz von Biometrie resp. von Gesichtserkennungsgeräten bei den Eingängen eines Stadions» und «Verknüpfung von Videoaufnahmen in den Stadien und Biometrie resp. Gesichtserkennung». Wir wiesen darauf hin, dass das Bundesgesetz über den Datenschutz gilt, wenn Personendaten von privaten Personen (private Stadionbetreiber) oder Bundesorganen (Bundesamt für Polizei) bearbeitet werden. Dagegen finden die kantonalen Datenschutzgesetze Anwendung bei der Datenbearbeitung durch kantonale Organe (z.B. Kantonspolizei, Stadtpolizei). Für die datenschutzrechtliche Beurteilung ist in solchen Fällen der jeweilige kantonale (resp. städtische) Datenschutzbeauftragte zuständig. Folglich bezog sich unsere (nach-

folgende) Stellungnahme einzig auf die Datenbearbeitung durch private Personen und Bundesorgane. Generell gilt, dass die allgemeinen Datenschutzgrundsätze (Rechtmässigkeit, Verhältnismässigkeit, Zweckbindung, usw.) zu beachten sind. Sodann brauchen private Personen für die Bearbeitung von Personendaten einen Rechtfertigungsgrund, nämlich die Einwilligung der betroffenen Person, ein überwiegendes privates oder öffentliches Interesse oder ein Gesetz. Bundesorgane ihrerseits dürfen dann Personendaten bearbeiten, wenn dafür eine gesetzliche Grundlage besteht.

Zum Einsatz von Biometrie resp. von Gesichtserkennungsgeräten bei den Eingängen eines Stadions gab uns die Arbeitsgruppe für das Pilotprojekt Rahmenbedingungen an. Ziel des Projekts ist es, Gewalt zu verhindern, indem möglichst viele Personen mit Stadionverbot oder einer anderen Massnahme nach Art. 24a ff. des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit (BWIS; Rayonverbot, Ausreisebeschränkung, Meldeauflage, Polizeigewahrsam) erkannt und am Eintritt ins Stadion gehindert werden.

Bei den eingesetzten Gesichtserkennungsinstallationen handelt es sich um semi-mobile Geräte, die an verschiedenen Eingängen des Stadions aufgestellt werden, ohne dass die Zuschauer im Voraus wissen, an welchen. Dabei erfolgt die Gesichtskontrolle mehr oder weniger gleichzeitig mit der Personenkontrolle und für die betroffenen Personen erkennbar. Bei der Gesichtserkennung ist jeweils eine Fachperson anwesend.

Die Fotos, die in die Gesichtserkennungsinstallationen eingegeben werden, stammen einerseits aus der Datenbank des Bundesamtes für Polizei HOOGAN, andererseits aus den Stadionverbotslisten der Sportclubs und/oder Sportverbände. Die Daten bleiben immer nach Herkunft getrennt. Es werden insbesondere keine Daten aus HOOGAN in die Stadionverbotslisten kopiert; die Daten werden auf separaten chiffrierten USB-Sticks übergeben und in zwei gesonderte Galerien eingelesen.

Die vom Bundesamt für Polizei vorselektionierten Daten aus HOOGAN werden erst kurz vor der Sportveranstaltung eingelesen und kurz nach der Veranstaltung unter Beaufsichtigung des zuständigen Polizeivertreters wieder vernichtet. Es gelten also die gleichen Bedingungen wie bereits heute, mit dem Unterschied, dass die Daten nicht auf Papier, sondern auf einem chiffrierten USB-Stick geliefert werden. Das Bundesamt für Polizei wird das Bearbeitungsreglement HOOGAN sowie die HOOGAN-Richtlinie entsprechend anpassen.

Die eingelesenen Fotos werden mit den hereinkommenden Stadionbesuchern verglichen (facetracking). Ergibt sich kein Treffer, erfolgt auch keinerlei Speicherung der Bilder der hereinkommenden Personen. Was bei einem Treffer geschieht, kann noch konfiguriert werden, auf jeden Fall sollte aus Beweisgründen in diesen Fällen ein Ausdruck erfolgen. Im Pilotprojekt wird es auch keine eigene «Datenbank Biometrie» geben.

Unter diesen Voraussetzungen gaben wir folgende datenschutzrechtliche Beurteilung ab: Für die Weitergabe von Daten aus HOOGAN an die Organisatoren und Sicherheitsverantwortlichen sind gesetzliche Grundlagen gegeben (BWIS und die entsprechende Verordnung). Zudem dürfen die Daten gemäss den gesetzlichen Grundlagen in elektronischen Personenerkennungssystemen bearbeitet werden. Allerdings wären noch das Bearbeitungsreglement sowie die Richtlinie zu HOOGAN anzupassen, da dort eine Weitergabe auf Papier und nicht in elektronischer Form vorgesehen ist. Wichtig ist dabei weiterhin die Sicherstellung, dass erstens die herausgegebenen Daten protokolliert werden, und dass zweitens die Daten nach der Sportveranstaltung sicher gelöscht und nicht weiterverwendet werden. Wir halten fest, dass die Übergabe der Daten auf einem chiffrierten USB-Stick gegenüber einer Datenübergabe auf Papier aus datenschutzrechtlicher Sicht mindestens als gleichwertig einzustufen ist.

Für die Weitergabe von Daten aus den Stadionverbotslisten der Sportclubs oder Sportverbände an die Organisatoren und Sicherheitsverantwortlichen kann grundsätzlich das Vorliegen eines Rechtfertigungsgrundes (überwiegendes privates oder öffentliches Interesse) bejaht werden. Allerdings müssen auch hier die allgemeinen Datenschutzprinzipien eingehalten werden. Insbesondere dürfen die Personendaten nur dann bearbeitet werden, wenn sie rechtmässig erhoben wurden. Als Beispiel sei genannt, dass Fotos von Personen mit Stadionverboten nur dann bearbeitet werden dürfen, wenn die Fotos rechtmässig gemacht wurden. Dies ist dann der Fall, wenn die Bilder im Rahmen einer Videoüberwachung zu Sicherheitszwecken im Stadion gemacht wurden und das gespeicherte Bildmaterial sicherheitsrelevant ist (etwa im Falle von Ausschreitungen).

Auch bei der Gesichtserkennung bei der Personenkontrolle durch die privaten Stadionbetreiber resp. deren Sicherheitsverantwortliche lässt sich grundsätzlich das Vorliegen eines Rechtfertigungsgrundes (überwiegendes privates oder öffentliches Interesse) bejahen. Auch hier gelten die allgemeinen Datenschutzprinzipien. So dürfen nach dem Verhältnismässigkeitsprinzip nur diejenigen Daten bearbeitet werden, die für den verfolgten Zweck tatsächlich geeignet und notwendig sind. Weiter ist die Datensicherheit nach DSG zu gewährleisten. Aufgrund von BWIS muss zudem sichergestellt werden, dass die Daten aus HOOGAN nicht mit den anderen Daten vermischt und nach der Veranstaltung wieder gelöscht werden. Weiter wären die Zuschauer über die Gesichtserkennung zu informieren, mit Hinweisschildern und eventuell einer Mitteilung auf der Eintrittskarte. Aus Beweiszwecken ist der Ausdruck eines Treffers sicher zulässig. Wird der Fall der Kantonspolizei übergeben, richtet sich die Datenbearbeitung wie erwähnt nach kantonalem Recht.

Wir wiesen die Arbeitsgruppe darauf hin, dass nicht der EDÖB, sondern die jeweiligen Datenbearbeiter (Bundesamt für Polizei, Organisatoren gemäss BWIS usw.) für die Einhaltung der Datenschutzgesetzgebung verantwortlich bleiben. Schliesslich erlaubten wir uns die Bemerkung, dass für uns immer noch fraglich ist, ob angesichts der geplanten Datenbearbeitungen die effektive Trefferquote der Gesichtserkennungsanlage wirklich gross genug und damit die Zweckmässigkeit der Massnahme gegeben ist. Wir zweifelten an der Effizienz der Anlage.

Schliesslich wiesen wir darauf hin, dass die Gesichtserkennung nur etwas bringen könne, wenn sie mit anderen Massnahmen (Fanbetreuer, Beizug der Polizei usw.) verbunden werde.

Für die Verknüpfung von Videoaufnahmen in den Stadien mit Biometrie resp. Gesichtserkennung gaben wir folgende Beurteilung ab:

Gemäss den Angaben der Arbeitsgruppe war ebenfalls geplant, die Gesichtserkennung (nach der Eingangskontrolle) während des Spiels weiterzuführen. Dabei würden die Gesichtserkennungsgeräte mit in den Stadien bereits vorhandenen Videoeinrichtungen verknüpft. Auch hier würden die «Nichttreffer» nicht gespeichert. Ziel wäre es, allfällige Treffer der Kantonspolizei zu melden, die danach die Personen aufsuchen würde.

Diesbezüglich stellt sich die Frage der Verhältnismässigkeit. Auf jeden Fall gelten auch hier die oben genannten Voraussetzungen. Wiederum ist der EDÖB für die Beurteilung der Datenbearbeitung durch die Kantonspolizei nicht zuständig.

Erneut ersuchten wir die Arbeitsgruppe, sicherzustellen, dass im Rahmen ihres Projekts die vorgenannten Datenschutzvoraussetzungen eingehalten werden. Wie bereits erwähnt, sind die jeweiligen Datenbearbeiter (Bundesamt für Polizei, Organisatoren gemäss BWIS usw.) für die Einhaltung der Datenschutzgesetzgebung verantwortlich. Allerdings ist nach einer bestimmten Zeit die Gesichtserkennung durch die Organisatoren resp. Sicherheitsverantwortlichen einer Evaluation zu unterziehen und die datenschutzrechtliche Situation im Hinblick auf die Zweckmässigkeit und die Verhältnismässigkeit der Massnahme nochmals abzuklären.

Zu allen anderen Punkten des Pilotprojekts, zum Beispiel zur Frage der Gesichtserkennung an öffentlichen Orten, haben wir nicht Stellung genommen, da dies von der Arbeitsgruppe nur am Rande erwähnt wurde und das Vorhaben für uns noch zu wenig konkretisiert war. Dort stellen sich weitere und viel heiklere Datenschutzprobleme, die noch abgeklärt werden müssten.

1.5 Gesundheit

1.5.1 Weitergabe von ärztlichen Gutachten

Die Weitergabe eines ärztlichen Gutachtens stellt einen heiklen Vorgang dar. Es werden besonders schützenswerte Personendaten an einen Dritten übergeben. In einigen Fällen bestehen deshalb klare spezialgesetzliche Grundlagen für die integrale Weitergabe ärztlicher Gutachten ohne die explizite Zustimmung der betroffenen Person. Bestehen keine solchen Grundlagen, so müssen die allgemeinen Datenschutzbestimmungen eingehalten werden. Insbesondere ist das Prinzip der Verhältnismässigkeit zu beachten.

Gemäss dem Prinzip der Verhältnismässigkeit dürfen Personendaten nur soweit bearbeitet werden, als diese für einen bestimmten Zweck objektiv geeignet und tatsächlich erforderlich sind. Bei der Weitergabe eines ärztlichen Gutachtens muss also der Absender, auch wenn er grundsätzlich zur Bekanntgabe von Informationen berechtigt ist, prüfen, welche Angaben er an den konkreten Empfänger übermitteln darf. Enthält ein ärztliches Gutachten Informationen, die für das Erreichen des konkreten Zwecks des Empfängers nicht geeignet und nicht erforderlich sind, so muss der Absender diese entfernen oder unkenntlich machen. Sonst wird das Prinzip der Verhältnismässigkeit verletzt. So darf der «case manager» einer Unfallversicherung zwar grundsätzlich Informationen aus einem Gutachten an einen beteiligten Haftpflichtversicherer weitergeben. Jedoch hat er Angaben, die für den Versicherer im konkreten Fall ohne Bedeutung sind, unkenntlich zu machen oder schlicht zu entfernen. So kann es zum Beispiel sein, dass ein von der Unfallversicherung erstelltes Gutachten Hinweise auf die Freizeitaktivitäten einer geschädigten Person enthält. Diese Informationen dürfen dem Haftpflichtversicherer nur übermittelt werden, wenn sie für die Beurteilung einer Rückgriffsforderung wirklich von Belang sind. Das ist beispielsweise dann der Fall, wenn eine bei einem Verkehrsunfall geschädigte Person ein Hobby betreibt, das mit besonderen körperlichen Risiken verbunden ist und den beim Verkehrsunfall entstandenen Körperschaden möglicherweise massgeblich beeinflusst hat.

1.5.2 Online-Datenbank mit Patientendaten

Der Betrieb einer Datensammlung, welche Krankheitsverläufe von Patienten dokumentiert, erfordert gezielte datenschutzrechtliche Vorkehrungen. Das trifft ganz besonders zu, wenn die Bearbeitung online erfolgt. Die Funktionen der Datenbearbeitung müssen beschrieben werden und die Beteiligten über das Verfahren informiert sein. Es gilt, mit angemessenen Massnahmen die Persönlichkeitsrechte der Patienten zu gewährleisten.

Bei der Behandlung von Patienten mit Langzeiterkrankungen entstehen grosse Informationsmengen. Eine Möglichkeit, die Daten zu verwalten, besteht darin, sie via Papierformulare in eine Datensammlung zu übertragen. Eine andere Möglichkeit, welche hier besprochen wird, ist der Zugriff über ein öffentliches Netz. Sowohl die behandelnden Ärzte als auch die betroffenen Patienten erhalten zur Bearbeitung der Daten Zugriff auf die Datensammlung. Bei den zu bearbeitenden Informationen handelt es sich ohne Frage um besonders schützenswerte Daten. Deshalb erfordert ihre Bearbeitung besondere Massnahmen. Diese lassen sich in drei Bereiche einteilen: die Identifizierung der Teilnehmer, der Umfang des Datenzugriffs und die Zuteilung von Zugriffsrechten.

Bei einem uns vorgestellten System handelt es sich um ein Langzeitregister im Bereich rheumatischer Erkrankungen. Die vom Betreiber geforderten und getroffenen Massnahmen sind als das absolute Minimum für eine Online-Datenbank mit Patientendaten zu betrachten.

- Die Identifizierung des Arztes bzw. Patienten: Nach schriftlichem Antrag auf Zugriff werden die Daten des Antragsstellers überprüft und ihm ein verschlüsselter Link per Email geschickt. Mit diesem kann er sein Benutzerkonto aktivieren.
- Der Umfang des Datenzugriffs: In einer Patienteninformation ist genau beschrieben, welcher Arzt auf die Daten des Patienten Zugriff hat. Ein Arzt hat nur auf die Daten seiner Patienten Zugriff, der Patient nur auf seine eigenen. Die Speicherung und der Transport der Daten erfolgen chiffriert.
- Die Zuteilung der Zugriffsrechte: Sie erfolgt nur mit der Einwilligung des Patienten. Bei einem Arztwechsel entscheidet der Patient, ob der bisher behandelnde Arzt weiterhin auf seine Daten zugreifen kann. Wenn der Patient aus dem System austritt, müssen auf seinen Antrag hin alle seine Daten gelöscht werden.

Zentrale Elemente im vorgestellten Verfahren sind die Patienteninformation und die Einverständniserklärung. Zunächst wird der Patient darüber informiert, welchem Ziel die Bearbeitung dient, wie die Daten erfasst und ausgewertet werden, was bei einem Arztwechsel geschieht und wie er die Datenbearbeitung beenden kann. Dann darf die Datenbearbeitung erst nach der schriftlichen Einwilligung des Patienten beginnen. Dieser kann die Einwilligung jederzeit widerrufen, ohne dass ihm daraus ein Nachteil entsteht.

1.5.3 Standards und Architektur der eHealth-Strategie Schweiz

Der Bundesrat hat am 27. Juni 2007 die «Strategie eHealth Schweiz» verabschiedet. In ihr werden unter anderem zwei Ziele genannt: die für die Umsetzung der Strategie notwendigen Standards und eine geeignete eHealth-Architektur zu definieren. Der daraus resultierende Auftrag ging an das Teilprojekt «Standards und Architektur», dessen Ergebnisse als Grundlage für die anderen Teilprojekte dienen. Deshalb haben wir uns entschieden, aktiv an «Standards und Architektur» mitzuwirken.

Einige Ereignisse im Gesundheitswesen der Schweiz stellen für den Datenschutz eine grosse Herausforderung dar. Die Umsetzung der «Strategie eHealth Schweiz», welche vom Bundesrat am 27. Juni 2007 verabschiedet wurde, gehört mit Sicherheit dazu.

Grundlage für einen effizienten und effektiven Datenschutz bildet die Erkenntnis, dass er einen der Sensibilität der bearbeiteten Personendaten angemessenen Stellenwert erhält. Der Bundesrat räumt in seinem Strategiepapier der Datensicherheit und dem Datenschutz höchste Priorität ein. Für ihn bedeutet «die Bearbeitung medizinischer Daten einen Eingriff in die Grund- bzw. Persönlichkeitsrechte der betroffenen Personen (z.B. der Patientinnen und Patienten). Damit der Eingriff legitim ist, müssen rechtliche, organisatorische und technische Massnahmen getroffen werden. Die Qualität dieser Massnahmen hat einen starken Einfluss auf das Vertrauen in die elektronischen Gesundheitsdienste.»

Unter diesen positiven Voraussetzungen haben wir uns entschieden, sowohl im Teilprojekt «Standards und Architektur» als auch im Teilprojekt «Rechtliche Grundlagen» aktiv mitzuarbeiten.

Das Teilprojekt «Standards und Architektur» will zwei Ziele der Strategie erreichen:

- «Bis Ende 2008 sind die Standards definiert für einen elektronischen Auszug behandlungsrelevanter Informationen aus der persönlichen Krankengeschichte. Die für die Einführung notwendigen Voraussetzungen sind beschrieben.»
- «Bis Ende 2012 ist die elektronische Übermittlung von medizinischen Daten unter den Teilnehmern im Gesundheitssystem strukturiert, medienbruchfrei und verlustfrei etabliert. Alle akut-somatischen Spitäler, alle integrierten Versorgungsnetze und die Mehrheit der frei praktizierenden Ärzte verwenden den elektronischen Auszug behandlungsrelevanter Informationen aus der persönlichen Krankengeschichte.»

Eine erste Aufgabe bestand darin, Vorschläge zur Strategieumsetzung interessierten Kreisen zur Vernehmlassung vorzulegen. Diese beinhalten unter anderem auch die Umsetzung der datenschutzrechtlich relevanten Grundsätze (mehr Informationen finden sich unter www.ehealth.admin.ch). Hervorzuheben ist jedoch, dass die datenschutzrechtlichen Aspekte bereits in den einzelnen Prozessen integriert sind. Als Grundsätze und Richtlinien haben sie für alle Akteure nicht nur eine rechtliche, sondern auch eine organisatorische und technische Verpflichtung. Kurz, die Datenschutzprozesse werden in der eHealth-Architektur fest «verdrahtet» sein.

Das wird auch nötig sein. Das Interesse an den elektronisch verwalteten Gesundheitsdaten ist gross, auch seitens Organisationen, die keinen rechtlichen Anspruch auf diese Daten geltend machen können. Deshalb besteht das Risiko, dass der berechtigt hohe Datenschutzanspruch des Bundesrates unterhöhlt wird. Dem gilt es nicht nur mit nützlichen Standards und einer passenden Architektur entgegenzuwirken, sondern auch mit den entsprechenden politischen und rechtlichen Rahmenbedingungen. Die Mitarbeit des EDÖB im Teilprojekt «Rechtliche Grundlagen» ist dabei sicher notwendig. Wir werden auch in Zukunft der Umsetzung der Strategie des Bundesrates einen hohen Stellenwert beimessen. Im Interesse der Patienten muss die Gelegenheit genutzt werden, mit eHealth bestehende datenschutzrechtliche Baustellen im Gesundheitswesen aufzuheben und nicht neue Baugruben auszuheben.

1.5.4 Die Einwilligung der betroffenen Personen bei medizinischen Forschungsprojekten

Die Daten für die Forschung sind den Forschenden grundsätzlich anonym zur Verfügung zu stellen. Sofern dies nicht möglich ist, ist die Einwilligung der Betroffenen einzuholen. Ist dies unmöglich, besteht die Möglichkeit, Forschungsprojekte mit Hilfe einer Bewilligung der Expertenkommission für das Berufsgeheimnis in der medizinischen Forschung durchzuführen. Es existieren heute Systeme, die unterschiedliche Abläufe berücksichtigen, damit den Forschern die Daten in anonymisierter Form zur Verfügung gestellt werden können.

Grundsätzlich muss man für die Forschung mit medizinischen Personendaten immer im Besitze der Einwilligung des betroffenen Patienten sein, ausser, man könne den Forschenden die Daten in anonymisierter Form zur Verfügung stellen. Personendaten sind dann anonymisiert, wenn sie nicht mehr einer bestimmten oder bestimmbaren Person zugeordnet werden können. In dieser Form unterliegen sie auch nicht mehr dem Datenschutzgesetz. Sofern weder eine Einwilligung eingeholt werden kann, etwa weil die Betroffenen verstorben sind, noch die Forschung mit anonymisierten Daten möglich ist, besteht immer noch die Möglichkeit, mit Hilfe einer generellen Bewilligung oder einer Sonderbewilligung, welche von der Expertenkommission für das Berufsgeheimnis in der medizinischen Forschung (Expertenkommission) mit den entsprechenden Auflagen ausgestellt werden kann, Forschung zu betreiben. Kontrollen unsererseits sowie Anfragen von Bürgern haben allerdings aufgezeigt, dass diese Vorgaben unterschiedlich interpretiert werden. Zum Teil geht man davon aus, dass eine Bewilligung der Expertenkommission genügt, damit namentlich keine Einwilligung mehr bei den Betroffenen eingeholt werden muss. Ein solches Vorgehen ist aber widerrechtlich.

Mit Personendaten sollte der Forschende gar nicht erst in Kontakt kommen, weil diese für die Forschungsvorhaben nicht notwendig sind. Es sind deshalb entsprechende Systeme zu gestalten, die es den Forschenden ermöglichen, mit anonymisierten Daten zu arbeiten. Die Anonymisierung von Personendaten kann oder muss je nach Situation unterschiedlich erfolgen. Bei Personendaten auf Papier wäre es ideal, wenn man dem Forscher nur die beispielsweise durch einen Archivmitarbeiter anonymisierten Daten zur Verfügung stellen könnte. Diese Dokumente könnten je nach Bedürfnis auch durch ein Pseudonym ergänzt werden, so dass allfällige, für den Patienten wichtige Erkenntnisse diesem mitgeteilt werden können.

Die Erhebung von Forschungsdaten aus «elektronischen» Datenbanken kann grundsätzlich anonym erfolgen, indem man die Daten aus der Datensammlung so erhebt, dass keine identifizierenden Daten in die Forschungsdatensammlung übernommen werden. Muss später allenfalls noch einmal auf die Ausgangsdaten zugegriffen werden, kann man auch im vorliegenden Fall mit Pseudonymen arbeiten, welche eine Re-Identifikation der Ursprungsdaten ermöglichen würde.

Auch für Register, wie bspw. Krebsregister, bestehen heute datenschutzkonforme Lösungen. Wichtige Informationen zum Anonymisieren und Pseudonymisieren im medizinischen Bereich finden sich in der Schriftenreihe der Telematikplattform für Medizinische Forschungsnetze mit der Bezeichnung «Generische Lösungen zum Datenschutz für die Forschungsnetze in der Medizin» (vgl. dazu www.tmf-net.de/Produkte/Uebersicht.aspx).

1.5.5 Erhebung von Personendaten zu Forschungszwecken aus elektronischen Datensammlungen eines Spitals

In der Folge wird eine Lösungsmöglichkeit aufgezeigt, wie Daten zu Forschungszwecken datenschutzkonform aus unterschiedlichen elektronischen Datensammlungen eines Spitals erhoben und den Forschern zur Verfügung gestellt werden können. Aufgrund der Zentralisierung fördert eine solche Lösung auch die Transparenz im Umfeld der medizinischen Forschung im jeweiligen Spital.

In einigen Spitälern bestehen mehrere elektronische Datensammlungen, mit deren Daten Forschungsprojekte durchgeführt werden. Sinnvollerweise wendet sich der Forscher an den Verantwortlichen der Datensammlung, damit sie gemeinsam die relevanten Daten erheben können. Dabei ist darauf zu achten, dass keine (direkt) identifizierenden Daten wie bspw. Name, Vorname oder Adresse erhoben werden. Die Nummer, die den Patienten im Spital eineindeutig identifiziert, darf erhoben werden, diese soll aber für die Forscher nicht einsehbar sein. Die Daten befinden sich nun auf einem Laptop und können auf einen zentralen Forschungsrechner übertragen werden. Dieser überprüft, ob die (direkt) identifizierenden Daten eliminiert wurden. Ist dies nicht der Fall, so wird dies protokolliert und dem Datensammlungsverantwortlichen sowie dem Forschungsprojektleiter mitgeteilt. Im Weiteren wird der Spitalnummer nun eine andere, nicht sprechende Zeichenfolge (Pseudonym) zugeordnet, so dass eine allfällige Rückidentifikation des Patienten möglich ist, wenn dieser bspw. aufgrund von Forschungserkenntnissen informiert werden muss. Auf dem Forschungsrechner sind auch diejenigen Betroffenen festgehalten, welche ihre Personendaten nicht zur Verfügung stellen wollen. Das System überprüft die in den Rechner übertragenen Daten

auf Patienten, welche ihre Daten für Forschungsprojekte gesperrt haben. Sofern solche vorhanden sind, werden sie aus dem Forschungssystem gelöscht. Erst nachdem diese Prozesse durchlaufen wurden, werden die Daten für die Forscher freigegeben. Sie haben dann online auf das System Zugriff und können nun das Forschungsprojekt durchführen. Selbstverständlich sind die sensitiven Bereiche in einem solchen System entsprechend zu schützen. Dies gilt insbesondere für den Prozess der Zuordnung der Spitalnummer zum Pseudonym.

Eine solche Zentralisierung der Forschungsvorhaben hat auch den Vorteil, dass die Transparenz im Forschungsbereich innerhalb eines Spitals erhöht wird. Aufgrund der Tatsache, dass die jeweiligen Spitäler unterschiedlich strukturiert sind und nicht die gleichen Sachmittel einsetzen, bestehen unterschiedliche Lösungsmöglichkeiten.

1.6 Versicherungen

1.6.1 Totalrevision des Versicherungsvertragsgesetzes

Der Bundesrat hat die Botschaft zur Totalrevision des Versicherungsvertragsgesetz (VVG) verabschiedet. Die Gesetzesrevision verbessert die Bestimmungen zur vorvertraglichen Information. Neu ist die Informationspflicht über das Widerrufsrecht für alle Versicherungsverträge eingefügt worden. Die Bestimmungen über die Datenschutzinformationen wurden wörtlich übernommen. Gemäss Vorschlag sind zudem die vorvertraglichen Informationen dem Versicherten neu zwingend vor der ihn bindenden Willenserklärung abzugeben. Unsere Anträge und Erläuterungen wurden mehrheitlich berücksichtigt.

Bereits mit der Teilrevision des Bundesgesetzes über den Versicherungsvertrag (VVG) hat man die vorvertraglichen Informationspflichten der Versicherer verstärkt und die Anliegen des Datenschutzes aufgenommen (vgl. unseren 11. Tätigkeitsbericht 2003/2004, Ziff. 6.2.3). So müssen die Versicherer seit dem 1. Januar 2007 über den Zweck und die Art der Datensammlung sowie über Empfänger und Aufbewahrung der Daten informieren. Der Inhalt dieser Bestimmung findet sich wortgetreu im VVG-Entwurf. Dies hat zu einer schrittweisen Verbesserung der Datenschutzbestimmungen im Versicherungsbereich geführt (Teilrevision VVG, 1. Januar 2007 sowie Teilrevision DSG, 1. Januar 2008). Mit der Totalrevision werden nun Form und Zeitpunkt der vorvertraglichen Informationen im VVG bestimmter geregelt. Alle diese Angaben und Unterlagen sind dem Versicherungsnehmer neu zwingend schriftlich, verständlich und rechtzeitig mitzuteilen, so dass dieser sie vor der bindenden Willenserklärung einsehen kann.

Unsere Erläuterungen zu den vorvertraglichen Informationspflichten betreffend Datenschutz wurden umfassend in den Botschaftstext eingefügt. Wir haben darin auf die verstärkten Transparenzbestimmungen des revidierten Datenschutzgesetzes verwiesen. Die Information und die Erkennbarkeit sind Hauptpfeiler der Neuerungen. Neben der versicherungsrechtlichen Informationspflicht bei Vertragsabschluss erhält die datenschutzrechtliche Information bei der Beschaffung aller Daten ein höheres Gewicht, auch wenn die ausdrückliche Information im DSG nur bei besonders schützenswerten Daten und Persönlichkeitsprofilen vorgeschrieben ist. Sofern die Beschaffung normaler Personendaten erkennbar ist, muss nicht ausdrücklich informiert werden. Dabei bemisst sich die Erkennbarkeit im Einzelfall nach dem Grundsatz von Treu und Glauben und dem der Verhältnismässigkeit. Wird berücksichtigt, dass eine angemessene Information die Voraussetzung einer gültigen Einholung der Einwilligungen ist, zeigt

sich, dass die Information auch im eigenen Interesse der Versicherungsgesellschaft erfolgen muss. Der Begriff der Zustimmung orientiert sich dabei an demjenigen der «Einwilligung des aufgeklärten Patienten». Wir haben in unseren Stellungnahmen empfohlen, sich bei der Ausarbeitung von Datenschutzmerkblättern auf die Europarats-Empfehlung Rec (2002) 9 über den Schutz von zu Versicherungszwecken erhobenen und verarbeiteten Daten zu stützen.

Neu wird im VVG-Entwurf die vorvertragliche Informationspflicht über das Widerrufsrecht vorgeschlagen. Diese Information ist erforderlich, weil der Versicherungsnehmer neu das Recht haben soll, innerhalb von vierzehn Tagen seinen Antrag auf Abschluss, Änderung oder Verlängerung zu widerrufen.

Im VVG-Entwurf nicht vorgesehen ist die gesetzliche Verankerung des Vertrauensarztes. Für genetische Daten ist im Gesetz über die genetische Untersuchung am Menschen (GUMG) der «beauftragte Arzt» bereits ausdrücklich vorgesehen. Da die Bezeichnung Vertrauensarzt aber aus der Sozialversicherung stammt und der Privatassekuranz fremd ist, wurde im GUMG der Begriff beauftragter Arzt gewählt. Beauftragter Arzt, Gesellschaftsarzt und Vertrauensarzt sind alles Ärzte, die dieselbe Funktion ausüben. Gemeint ist stets der für die Versicherungsgesellschaft tätige Arzt. Im VVG fehlt eine gesetzliche Regelung, wonach der Versicherte analog zu Art. 42 Abs. 5 des Krankenversicherungsgesetzes (KVG) verlangen kann, dass Gesundheitsdaten nur medizinischem Personal bekannt gegeben werden dürfen. Zwar gibt es in der Praxis der Versicherungsgesellschaften bereits den Gesellschaftsarzt, den medizinischen Dienst oder den beratenden Arzt. Leider ist dies aber nicht allen Beteiligten bewusst, und weder für Versicherte noch für Ärzte ist immer eindeutig klar, dass medizinische Daten ausschliesslich an medizinisches Personal weiterzuleiten sind. Deshalb sollten Versicherte in ihren Einwilligungserklärungen ausdrücklich erwähnen, dass sie der Weitergabe von Gesundheitsdaten nur von Arzt zu Arzt zustimmen. Die Ärzte ihrerseits sollten genetische Daten gemäss GUMG nur an den beauftragten Arzt weitergeben. Die anderen medizinischen Daten dürften sie nur an den Gesellschaftsarzt, den medizinischen Dienst bzw. den beratenden Arzt der Versicherungsgesellschaft weiterleiten. Die Weitergabe der Daten hat in verschlossenen und entsprechend adressierten Briefumschlägen zu erfolgen.

1.6.2 Zur Funktion des Vertrauensarztes in den verschiedenen Versicherungsbereichen

Als juristische Beratungsstelle wird der EDÖB auch immer wieder mit Problemen aus dem Bereich des Datenschutzes im Gesundheitswesen kontaktiert. Zum Dauerbrenner sind dabei die Fragen über den Einsatz des Vertrauensarztes in den verschiedenen Versicherungsbereichen geworden.

Die Revision des Krankenversicherungsgesetzes (KVG) vom 18. März 1994 hat dem Gesundheitswesen die Rechtsfigur des Vertrauensarztes beschert. Seit seiner Einführung ist es immer wieder zu Missverständnissen um seine Position und Aufgabe innerhalb des Gesundheitswesens gekommen. Wir haben es uns seit je zur Aufgabe gemacht, die wahre Bedeutung des Vertrauensarztes im KVG hervorzuheben. So haben wir im Berichtsjahr vor der Schweizerischen Gesellschaft der Vertrauensärzte (SGV) in einem Referat erneut auf die Wichtigkeit des Vertrauensarztes hingewiesen. Gemäss unseren Ausführungen bewegt sich der Vertrauensarzt (VA) als besonderes Organ des Krankenversicherungsgesetzes im Spannungsfeld zwischen den Interessen der Versicherten, der Leistungserbringer und der Versicherer. In seinem Urteil unabhängig, darf er den zuständigen Stellen der Versicherer nur diejenigen Angaben weitergeben, die notwendig sind, um über die Leistungspflicht zu entscheiden. Der Leistungserbringer ist stets berechtigt und auf Verlangen der versicherten Person sogar in jedem Fall verpflichtet, medizinische Angaben nur dem Vertrauensarzt bekannt zu geben.

Wir haben zudem betont, dass sich die gesetzlich vorgeschriebene Unabhängigkeit zunächst in der Organisation eines vertrauensärztlichen Dienstes (VAD) niederschlagen müsse. So müssen Lokale des VAD genügend abgetrennt und abschliessbar sein. Die Post darf nur durch Stellen des VAD geöffnet werden und es muss jederzeit sicher gestellt sein, dass besonders schützenswerte Personendaten den VAD nicht verlassen können. Ein unabhängiges Telefon- und Telefaxnetz ist unabdingbar, und das Informatiksystem muss physisch so organisiert werden, dass die vom VAD erstellten Dokumente nur auf eigenen Speichermedien archiviert werden, die wiederum nur den Mitarbeitern des VAD zugänglich sind. Als eindeutig unvereinbar erachten wir die Unterstellung des VA unter den Chef Leistungen der jeweiligen Versicherung. Dem VA muss zudem die alleinige Kompetenz zur Anstellung seines Hilfspersonals zukommen. Eindeutig haben wir uns dahingehend geäussert, dass sich Vertrauensärzte als Gesellschaftsärzte stets darauf beschränken sollten, nur im Bereich der Zusatzversicherungen aktiv zu sein, um sämtliche Interessenskollisionen mit anderen Versicherungsbereichen (Krankentaggeld, berufliche Vorsorge) zu vermeiden.

Sodann haben wir auch auf die Rolle der Ärzte in weiteren Versicherungszweigen hingewiesen. Die «Institution» des VA ist gesetzlich nur gerade für die obligatorische Grundversicherung geregelt. Das KVG verpflichtet die Krankenversicherer, VA zu bestellen. Bereits im Bereich der Krankenzusatzversicherung gelangt das Versicherungsvertragsgesetz (VVG), in der Unfallversicherung das Bundesgesetz über die Unfallversicherung (UVG) zur Anwendung. VVG, UVG, diverse Sozialversicherungsgesetze (IV, AHV) und weitere Versicherungszweige müssen zweckbestimmt immer wieder medizinisches Fachwissen von Ärzten nutzen, verfügen aber über keine gesetzliche Regelung, welche den Beizug oder die Einsetzung von Vertrauensärzten vorsieht. Vertrauensärzte der Krankenversicherer, Ärzte der SUVA, der Regionalen ärztlichen Dienste (RAD), der Medizinischen Abklärungsstelle der Invalidenversicherung (MEDAS) oder beratende Ärzte der Privatversicherer wie auch von Firmen und Behörden, verstehen sich in erster Linie als Ärzte und dadurch als Mittler zwischen Versicherer, Leistungserbringer und Patient. Im juristischen Beratungsumfeld des Gesundheitswesens wurden wir auch in diesem Berichtsjahr wiederholt mit der Frage konfrontiert, ob sich das Modell des Vertrauensarztes, wie es im KVG gesetzlich vorgeschrieben ist, nicht analog in diesen weiteren Versicherungszweigen verankern liesse (vgl. dazu auch Ziff. 1.6.1). Vorausgesetzt dass Pflichten und Rechte ebenso wie die Unabhängigkeit der Organisation gewährleistet würden, sprächen sicher keine gewichtigen Gründe dagegen. Allerdings sind organisatorische Massnahmen zur Gewährleistung der Unabhängigkeit unser Ansicht nach zwar wichtig, aber allein genügen sie nicht, um die Rechte des Patienten in allen Fällen ausreichend zu schützen. Die Problematik liegt nämlich einerseits in der schwierigen Auslegung des Begriffs der «medizinischen Daten» begründet und anderseits in der interpretationsbedürftigen Verpflichtung des Vertrauensarztes, dem jeweiligen Versicherer nur jene Angaben weiter zu geben, die absolut notwendig sind, um über die Leistungspflicht entscheiden zu können.

1.6.3 Erhebung des EDÖB und des BAG zur datenschutzrechtlichen Situation bei anerkannten sozialen Krankenversicherern

Gemeinsam mit dem Bundesamt für Gesundheit (BAG) haben wir im Rahmen unserer Aufsichtstätigkeit bei sämtlichen anerkannten sozialen Krankenversicherern eine Erhebung über die datenschutzrechtliche Situation durchgeführt.

Abklärungen des BAG und des EDÖB bei einzelnen Krankenversicherungen haben mehrfach ergeben, dass datenschutzrechtliche Mängel bestehen. Die beiden Aufsichtsorgane wirkten in der Folge wiederholt darauf hin, dass sich die Krankenversicherer datenschutzkonform verhalten. Im Rahmen der Aufsichtstätigkeit haben wir und das BAG nun im Berichtsjahr mittels einer Arbeitsgruppe bei den anerkannten sozialen Krankenkassen eine Erhebung über die datenschutzrechtliche Situation durchgeführt. Im Dezember 2007 sandten wir allen Krankenversicherern einen ausführlichen Fragebogen mit 70 Fragen zu. Diese flächendeckende Erhebung sollte Aufschluss geben über die datenschutzrechtliche Organisation und die Handhabung des Datenschutzes im Krankenversicherungsbereich.

Nach Eingang der Antworten konnten wir uns in einem ersten Schritt ein umfassendes Bild von der datenschutzrechtlichen Situation bei den Krankenversicherern machen. In einem zweiten Schritt besteht nun die Absicht, den Krankenversicherern bei der Verbesserung ihrer datenschutzkonformen Organisationsstruktur behilflich zu sein.

Nicht zuletzt sollen aufgrund der Erhebung Anregungen zum freiwilligen Datenschutzaudit sowie zur freiwilligen Datenschutzzertifizierung der Krankenversicherer nach revidiertem DSG ausgearbeitet werden. Um den Datenschutz und die Datensicherheit zu verbessern, können die Krankenversicherer ihre Systeme, Verfahren und Organisation einer Bewertung durch anerkannte unabhängige Zertifizierungsstellen unterziehen, sind aber von Gesetzes wegen nicht dazu verpflichtet.

Die Auswertung und Analyse der ausführlichen Antworten und detaillierten Belege waren aufwändig. Die 93 Krankenversicherer (Stand Ende 2007) haben mehrheitlich fristgerecht gute und vollständige Antworten und Belege abgeliefert. Deren Auswertung liegt in Form eines ca. 50 seitigen Berichtes vor und bietet – mit den allgemeinen Aufsichtsdaten des BAG – eine gute Grundlage für die Optimierung des Datenschutzes bei den Krankenversicherern. Dabei ist mit allem Nachdruck festzuhalten, dass die Krankenversicherer die alleinige Verantwortung tragen, dass ihre hochsensiblen Daten datenschutzkonform bearbeitet werden und keine Sicherheitsprobleme entstehen. Die beiden Aufsichtsbehörden sind bereit, die Krankenversicherer dabei zu unterstützen.

Als wichtiger Aspekt der Analyse ist vorausschickend zu erwähnen, dass heute die meisten Krankenversicherer innerhalb einer Versicherungsgruppe oder eines Krankenkassenverbandes zusammenarbeiten. Diese «Gruppenbildung» galt es bei den Auswertungsergebnissen zu berücksichtigen. Sie haben eindeutig ergeben, dass die Krankenversicherer zum jetzigen Zeitpunkt über keine einheitlichen Konzepte und Instrumente für die Einhaltung des Datenschutzes verfügen.

Die Analyse des eigentlichen «Herzstücks» der Untersuchung - das Datenschutzmanagement und die Datenschutzorganisation der Krankenversicherer - hat insbesondere folgende Resultate ergeben:

Über ein Datenschutzkonzept verfügen 59% der Krankenkassen, welche 90% der Bevölkerung versichern. Ein solches Konzept gibt Auskunft über die mittel- und langfristige Strategie, wie die Anforderungen des DSG im Betrieb wahrgenommen bzw. die Umsetzung sichergestellt werden. Es beschreibt die Organisation des Datenschutzes, und daraus leiten sich die konkreten Aufgaben des Datenschutzbeauftragten und der für die Datensammlungen zuständigen Personen ab. Ein Datenschutzkonzept ist nicht gesetzlich vorgeschrieben.

Über Bearbeitungsreglemente zu ihren schützenswerten Datensammlungen verfügen nur 26% der Krankenkassen (bei denen aber 62% der Bevölkerung versichert sind). Entsprechend existieren bei mindestens 38% der Versicherten keine Vorgaben, wie mit schützenswerten Daten umzugehen ist. Hier sind weder Datenschutz noch Datensicherheit gewährleistet. Gemäss Gesetzgebung ist jedoch für jede meldepflichtige Datensammlung ein Bearbeitungsreglement zu erstellen und aktuell zu halten. Das Sicherstellen der Vollständigkeit und der Aktualität der Bearbeitungsreglemente ist eine Hauptaufgabe des Datenschutzbeauftragten des Krankenversicherers und dient als eigentliche Grundlage für den gesetzeskonformen Betrieb bzw. die gesetzeskonforme Nutzung einer Datensammlung mit schützenswerten Personendaten.

Die Datenschutzverantwortlichen von 62% der Krankenversicherer (die 91% der Bevölkerung versichern) verfügen über eine befriedigende Ausbildung. Eine genügende Ausbildung leitet sich aus den Pflichten der Datenschutzverantwortlichen ab. In den anderen Fällen ist der Rolleninhaber nicht autonom und steht in einem Interessenkonflikt. Bei 40 Krankenversicherern verfügt der Datenschutzverantwortliche nicht über ein schriftliches Pflichtenheft seiner Rolle.

80% der Krankenversicherer mit 91% der Versicherten verfügen über einen Datenschutzverantwortlichen. Dieses Resultat ist zu begrüssen. Betriebe ohne Datenschutzverantwortlichen sind verpflichtet, alle ihre Datensammlungen mit schützenswerten Personendaten dem EDÖB anzumelden und aktuelle Bearbeitungsreglemente zu unterhalten.

Bezüglich aller Ergebnisse ist festzuhalten, dass das Abschneiden der einzelnen Krankenversicherer nicht von deren Grösse oder einer Gruppenbildung abhängt. Im Gegenteil, gerade kleine Kassen haben etwa gute bis sehr gute Bearbeitungsreglemente vorgelegt. Trotz der aufgezeigten Mängel gilt es anzuerkennen, dass die Krankenversicherer für die ganze Datenschutzproblematik sensibilisiert sind und auch mehrfach die Bereitschaft bekundet haben, sich in diesem Bereich zu verbessern. So hat sich denn auch eine klare Mehrheit bereit erklärt, sich einem regelmässigen freiwilligen Datenschutzaudit zu unterziehen. Im Weiteren haben bereits heute einzelne Krankenversicherer – in Kenntnis des zu erwartenden Grossaufwands – die Absicht bekundet, sich zu gegebener Zeit einer freiwilligen Datenschutzzertifizierung zu unterziehen. Diese stösst aber dennoch auf weniger Akzeptanz als ein Datenschutzaudit. Übrigens ist auch die Bereitschaft zu Datenschutzaudit bzw. -zertifizierung nicht von der Grösse der Kasse abhängig.

Es würde im Rahmen dieser Berichterstattung zu weit führen, auf die einzelnen Sachverhalte näher einzugehen. Wichtige Resultate betreffen die Wirtschaftlichkeitskontrolle, den vertrauensärztlichen Dienst, das im Bundesgesetz über die Krankenversicherung (KVG) nach wie vor nicht geregelte Case Management sowie das über Erwarten umfangreiche Outsourcing der Krankenversicherer, d.h. die im Auftrag der Kassen von Dritten durchgeführten Aufgaben über die ganze Bandbreite von anfallenden Tätigkeiten. Wir werden zusammen mit dem BAG darüber in ausführlicher Form berichten. In den nächsten Monaten werden wir insbesondere die diversen offenen Fragen weiter bearbeiten und allgemeine Anregungen an die Adresse der Krankenversicherer abgeben.

1.7 Arbeitsbereich

1.7.1 Einführung des Familienzulagenregisters

Seit dem 1. Januar 2009 ist das neue Bundesgesetz über die Familienzulagen in Kraft. Darin ist die Einführung eines Familienzulagenregisters vorgesehen. Wir haben zur entsprechenden Gesetzesvorlage keine Einwände angebracht.

Das Familienzulagenregister wird nach den Informationen über das Kind, für das eine Zulage bezogen wird, ausgerichtet. Mit der Schaffung dieses Registers soll in erster Linie der Missbrauch im Sinne von Doppelbezügen von Familienzulagen verhindert werden. Damit es dieses Ziel erreicht, müssen alle Familienausgleichskassen dem Register regelmäßig die notwendigen Daten und Mutationen liefern.

Der Datenkatalog des Familienzulagenregisters wird voraussichtlich weder besonders schützenswerte Daten enthalten, noch gesamthaft ein Persönlichkeitsprofil darstellen. Wir haben die entsprechende Gesetzesvorlage geprüft und keine datenschutzrechtlichen Einwände angebracht.

1.7.2 Revision des Regierungs- und Verwaltungsorganisationsgesetzes

Die Bundesverwaltung ist dabei, den Schutz der Benutzer ihrer Telekommunikationsinfrastruktur vor unzulässiger Datenbearbeitung gesetzlich zu verankern. Zugleich wird die gesetzliche Grundlage geschaffen, damit die Bundesverwaltung die Daten für bestimmte Zwecke bearbeiten kann. Wir haben bei den Entstehungsarbeiten mitgewirkt.

Bundesangestellte und Dritte, welche die Telekommunikationsinfrastruktur des Bundes benützen oder per Videoüberwachung geschützte Verwaltungsgebäude betreten, hinterlassen elektronische Spuren. Nebst Randdaten, die beim Auf- und Abbau elektronischer Verbindungen entstehen, können dabei auch Inhaltsdaten generiert werden, die im Einzelfall einen besonders schützenswerten Charakter haben können.

Die Aufzeichnung und Bearbeitung der Daten aus der elektronischen Infrastruktur der Bundesverwaltung erfolgte bisher ohne formelle gesetzliche Grundlage. Wir haben empfohlen, diese Lücke mit der Revision des Regierungs- und Verwaltungsorganisationsgesetzes (RVOG) zu schliessen.

Der Revisionsentwurf sieht vor, dass die Bundesverwaltung grundsätzlich alle Daten aufzeichnen darf, die bei der Benutzung der elektronischen Infrastruktur entstehen. Eingegrenzt wird die Datenbearbeitung durch die Auflistung von Voraussetzungen und die abschliessende Aufzählung der zulässigen Bearbeitungszwecke. Bundesorgane sollen unserer Meinung nach die Daten über den Auf- und Abbau elektronischer Verbindungen nur weiterbearbeiten dürfen, um etwa die Informations- und Dienstleistungssicherheit zu gewährleisten oder die Einhaltung von Nutzungsreglementen zu kontrollieren. Die personenbezogene Auswertung darf nach unserem Dafürhalten nur erfolgen, wenn ein konkreter Verdacht auf eine missbräuchliche Verwendung der elektronischen Infrastruktur besteht.

Bei den Entstehungsarbeiten der Gesetzesvorlage wirkten wir aktiv mit. Sie wurde anfangs 2009 durch den Bundesrat in die Vernehmlassung geschickt.

1.7.3 Revision des Bundespersonalgesetzes

Die Revision des Bundespersonalgesetzes soll die formelle Grundlage für die Bearbeitung von schützenswerten Personendaten und Persönlichkeitsprofilen im Personaldatenverarbeitungssystem BV PLUS schaffen. Unsere Empfehlungen anlässlich der ersten Ämterkonsultation blieben auch im neuen Regelungsentwurf weitgehend unberücksichtigt.

Im Rahmen der ersten Ämterkonsultation zur Revision des Bundespersonalgesetzes (BPG) haben wir verschiedene Einwände bezüglich der Regelungsdichte angebracht (vgl. unseren 15. Tätigkeitsbericht 2007/2008, Ziff. 1.7.4). Anlässlich der zweiten Ämterkonsultation mussten wir feststellen, dass unsere Einwände weitgehend unberücksichtigt geblieben sind. Keinen Eingang fand so auch im neuen Entwurf unsere Empfehlung zur Regelung der neuen Aufgaben des BV PLUS und des Abrufverfahrens von Beurteilungsdaten und anderen besonders schützenswerten Personendaten mittels dem Benutzerzugang E-Gate. Problematischerweise wurden zudem sämtliche weiteren Zugriffe per Abrufverfahren, welche im ersten Regelungsentwurf vorgesehen waren, aus dem neuen Entwurf entfernt.

Die vom Bundesrat am 19. September 2008 eröffnete Vernehmlassung dauerte drei Monate. Die Botschaft zur Revision des BPG soll nach heutiger Planung in der ersten Hälfte 2009 durch den Bundesrat genehmigt und zuhanden des Parlaments verabschiedet werden.

1.7.4 Umgang mit persönlichen Pensionskassenausweisen

Eine Pensionskasse stellt die persönlichen Ausweise ihrer versicherten Personen an den jeweiligen Arbeitgeber zu. Er verteilt die Pensionskassenausweise anschliessend an seine Arbeitnehmer. Die Pensionskasse ist jedoch nicht befugt, die Ausweise an den Arbeitgeber zu senden. Er benötigt die auf dem Pensionskassenausweis aufgelisteten Informationen weder versicherungsrechtlich noch arbeitsrechtlich. Wir betrachten die Zustellungspraxis dieser Pensionskasse als nicht datenschutzkonform, weshalb wir eine Empfehlung erlassen werden.

Wie uns mitgeteilt wurde, schickt eine Pensionskasse die persönlichen Ausweise Ihrer Versicherten an den jeweiligen Arbeitgeber, und zwar an jene Adresse, die ihr der Arbeitgeber mitteilt. Die auf diese Weise zugestellten Pensionskassenausweise werden anschliessend intern an die Arbeitnehmer weitergeleitet. Da die Ausweise nicht persönlich adressiert sind, kann der Arbeitgeber mit der Feinverteilung vom Inhalt Kenntnis nehmen.

Unserer Einschätzung nach ist die gegenwärtige Zustellungspraxis dieser Pensionskasse nicht datenschutzkonform. Die Informationen auf dem Pensionskassenausweis sind nur für den Versicherten bestimmt. Weder versicherungsrechtlich noch arbeitsrechtlich ist der Arbeitgeber auf diese Daten angewiesen. Die Pensionskasse hat die Zustellung so zu gestalten, dass der Arbeitgeber keinen Zugriff auf den Pensionskassenausweis erhält.

Wir haben mit der Pensionskasse Kontakt aufgenommen und sie um eine Stellungnahme gebeten. Die Pensionskasse führte zunächst organisatorische Gründe an, um diese Praxis zu rechtfertigen. Daraufhin unterbreiteten wir der Pensionskasse Vorschläge zur pragmatischen Lösung dieses organisatorischen Problems. Die Pensionskasse folgt unseren Vorschlägen jedoch nicht, mit der Begründung, der Einblick in diese Daten sei für den Arbeitgeber aus versicherungs- und arbeitsrechtlichen Gründen erforderlich. Wir erwiderten, dass die Pensionskasse keinen Rechtfertigungsgrund für die Zustellung der Ausweise an den Arbeitgeber hat und dass diese Daten für den Arbeitgeber weder zur Umsetzung des Gesetzes über die berufliche Vorsorge noch zur Durchführung des Arbeitsverhältnisses erforderlich seien und diese Praxis den Datenschutz verletze.

Der mehrfache Schriftenwechsel hat schliesslich zu keiner Lösung geführt. Deshalb werden wir zuhanden dieser Pensionskasse eine Empfehlung ausarbeiten.

1.7.5 Fragenkatalog bei Aufnahme in eine Pensionskasse

Gesundheitsdaten dürfen bei der Aufnahme in eine Pensionskasse nur im Bereich der überobligatorischen Versicherung erhoben werden. Bei der Aufnahme in die obligatorische Versicherung darf die Pensionskasse keine solchen Daten verlangen, da hier eine gesetzliche Aufnahmepflicht besteht.

Zu beurteilen war die Frage, ob Pensionskassen mit einem Fragenbogen Gesundheitsdaten aufnahmewilliger Person erheben dürfen. Aus dem Fragenbogen war nicht klar ersichtlich, ob es sich um eine obligatorische oder eine überobligatorische Versicherung nach dem Bundesgesetz über die berufliche Alters-, Hinterlassenen- und Invalidenvorsorge (BVG) handelt.

In unserer Stellungnahme haben wir auf den wichtigen Unterschied zwischen obligatorischer und überobligatorischer Versicherung nach BVG hingewiesen. Im Bereich der obligatorischen Versicherung dürfen keine Gesundheitsdaten erhoben werden, da eine gesetzliche Aufnahmepflicht besteht. Demzufolge sind Personen ungeachtet des Gesundheitszustandes in die Pensionskasse aufzunehmen, sofern die Bedingungen des BVG erfüllt sind.

Hingegen dürfen für die Aufnahme in eine überobligatorische Versicherung nach BVG Gesundheitsdaten angefordert werden. Hier dürfen die Versicherer für die Risiken Tod und Invalidität einen Vorbehalt aus gesundheitlichen Gründen machen, weshalb bei dieser Versicherung die gesundheitliche Risikoabklärung im Aufnahmeverfahren eine grosse Rolle spielt. Die Person, die eine überobligatorische Versicherung abschliessen will, muss der Pensionskasse vor der Aufnahme Tatsachen mitteilen, die geeignet sind, den Entschluss des Versicherers zu beeinflussen. Demgegenüber muss die Versicherung die antragstellende Person informieren, zu welchem Zweck die Gesundheitsdaten erhoben werden. Wie viele und welche Gesundheitsdaten für eine Risikobeurteilung beschafft werden dürfen, ist eine Frage der Verhältnismässigkeit. Es dürfen nur so viele Daten erhoben werden, wie für die Zweckerreichung notwendig sind. Es kann nach dem Grundsatz von Treu und Glauben erforderlich sein, dass die antragstellende Person noch weitere Informationen liefern muss. Allenfalls ist mitzuteilen, ob die gestellten Fragen freiwillig oder obligatorisch sind und mit welchen Folgen die Person zu rechnen hat, wenn sie die Angabe verweigert.

1.7.6 Personalbewirtschaftungssystem der Bundesverwaltung

Die Überprüfung des Datenverarbeitungssystems der Bundesverwaltung BV PLUS hat beim systemverantwortlichen Eidgenössischen Personalamt und beim Personaldienst der Bundeskanzlei als Endbenutzer keine wesentliche Probleme ans Tageslicht gebracht. Im Kompetenzbereich des Bundesamtes für Informatik ist die Überprüfung noch nicht abgeschlossen.

Im Rahmen unserer Tätigkeit als Datenschutzaufsichtsbehörde überprüften wir Ende 2007 bei den systemverantwortlichen Stellen sowie bei einem End-User die Einhaltung der Datenschutzbestimmungen bei der Anwendung des Datenverarbeitungssystems BV PLUS. Bei den überprüften, systemverantwortlichen Stellen handelt es sich um das Eidg. Personalamt (EPA) und das Bundesamt für Informatik und Technologie (BIT), beim Endbenutzer um den Personaldienst der Bundeskanzlei. Die Überprüfung hat sich auf die Fragenkomplexe der Datensicherheit und des Datenkatalogs beschränkt.

Beim Endbenutzer tauchten keine nennenswerten datenschutzrechtlichen Probleme auf, weshalb die Überprüfung rasch erfolgreich abgeschlossen werden konnte.

Beim EPA stellte sich die Frage, ob eine Einwilligung der Mitarbeitenden in die Abwicklung der Mitgliederbeitragszahlungen an Verbände mittels BV PLUS vorliegt. Nach Angaben des EPA geben die Mitarbeitenden den Verbänden bei Verbandsbeitritt schriftlich ihr Einverständnis, dass ihre Verbandsmitgliedschaft dem entsprechenden Personaldienst der Bundesverwaltung bekannt gegeben wird. Kopien der Einwilligungserklärungen seitens der Verbände erhält der Personaldienst jedoch nicht. Wir haben daher das EPA angewiesen, den Departementen zu empfehlen, solche Kopien zu verlangen.

Beim BIT stellten wir in verschiedenen Gebieten Verbesserungspotential fest. Im Bereich Organisation fiel uns auf, dass das vor Jahren erstellte Bearbeitungsreglement kaum nachgeführt wurde. Auch fehlt ein Sachverständiger für Daten- oder Informationssicherheit im Bereich SAP. Ausserdem haben wir angeregt, die Lohndaten der in Bern steuerpflichtigen Bundesangestellten auf ihrem Weg zur Steuerverwaltung des Kantons Bern verschlüsselt zu übertragen. Des Weiteren wurde dem BIT empfohlen, die Up- und Downloads von Daten vom Zentralrechner auf den Arbeitsplatzrechner einerseits sowie die Zugriffe von Benutzern mit erhöhten Systemprivilegien andererseits zu protokollieren und periodisch auszuwerten.

1.8 Handel und Wirtschaft

1.8.1 Revision des Schuldbetreibungs- und Konkursrechts

Die Anzeige von Daten auf dem Betreibungsregisterauszug ist gegenwärtig unserer Ansicht nach zu undifferenziert geregelt. Daher haben wir im Rahmen der Ämterkonsultation zur Revision des Schuldbetreibungs- und Konkursrechts (Sanierungsverfahren) vorgeschlagen, die Anzeigefristen anzupassen. Wir sind der Meinung, dass deren Staffelung auf der einen Seite den datenschutzrechtlichen Anforderungen besser entspricht und auf der anderen Seite Anreize liefern kann, offene Rechnungen schneller zu begleichen.

Gemäss der derzeitigen gesetzlichen Regelung informiert der Betreibungsregisterauszug fünf Jahre lang über Betreibungsdaten. Lediglich in drei Ausnahmefällen wird überhaupt keine Auskunft erteilt: a. wenn die Betreibung nichtig oder aufgrund einer Beschwerde oder eines Urteils aufgehoben worden ist; b. wenn der Schuldner mit einer Rückforderungsklage obsiegt hat, oder c. wenn der Gläubiger die Betreibung zurückgezogen hat. In der heutigen Praxis werden selbst diejenigen Betreibungen, welche nicht fortgesetzt werden (immerhin gut ein Drittel aller eingereichten Betreibungen), fünf Jahre lang im Betreibungsregisterauszug aufgeführt. Dasselbe gilt für ordnungsgemäss bezahlte Betreibungen (zwar als «erledigt» vermerkt). Eine solche wenig differenzierte Regelung erscheint aufgrund der Sensitivität von Betreibungsregisterdaten unangemessen und aus datenschutzrechtlicher Sicht unverhältnismässig. In der Praxis wird in vielen Kantonen ohne anderlautenden Wunsch bereits heute lediglich über die letzten drei Jahre Auskunft erteilt. Dies erscheint auf der einen Seite nicht ausreichend (so werden zum Beispiel bei Grundpfandbetreibungen mit einem Rechtsstreit noch laufende Betreibungen oft nicht mehr angezeigt) und auf der anderen Seite zu weitreichend (es ist beispielsweise nicht ersichtlich, warum erledigte Betreibungen während fünf Jahren im Betreibungsregister aufgeführt werden sollten).

Wir schlagen zur Realisierung eines zeitlich gestaffelten Einsichtsrechts vor, dass Art. 8a Abs. 4 des Schuldbetreibungs- und Konkursrechts (SchKG) wie folgt geändert wird: «Das Einsichtsrecht Dritter erlischt ein Jahr nach Abschluss des Verfahrens, wenn die Betreibung gemäss Art. 12 Abs. 2 SchKG erledigt wurde. Es erlischt drei Jahre nach Abschluss des Verfahrens, wenn die Betreibung gemäss Art. 88 SchKG nicht fortgesetzt wurde. In allen anderen Fällen erlischt das Einsichtsrecht Dritter fünf Jahre nach Abschluss des Verfahrens. Gerichts- und Verwaltungsbehörden können im Interesse eines Verfahrens, das bei ihnen hängig ist, weiterhin Auszüge verlangen.»

Der finanzielle Leumund einer betroffenen Person spielt in der Geschäftswelt eine nicht zu unterschätzende Rolle. Insbesondere im Rahmen der immer stärkeren Verbreitung von Kreditauskünften gewinnt der finanzielle Leumund an Bedeutung. Aufgrund des immer transparenter werdenden Zahlungsverhaltens der betroffenen Personen werden die entsprechenden Informationen immer sensibler.

Durch diese Neuregelung würde der Leumund von Schuldnern, welche ihre Schuld durch Zahlung beglichen haben, bereits nach einem Jahr wieder hergestellt. Hingegen blieben fruchtlose Betreibungen volle fünf Jahre im Betreibungsregister aufgeführt. Eine solche Regelung trägt zum einen den heutigen Gegebenheiten besser Rechnung und kann zum anderen bei betroffenen Schuldnern durchaus auch die Anreizwirkung entfalten, im Interesse ihres finanziellen Leumunds ihren Verpflichtungen schneller nachzukommen.

1.8.2 Private Publikation von Handelsregisterdaten

Die Publikation von Handelsregisterdaten durch Private im Internet fördert die Öffentlichkeitswirkung des Handelsregisters und ist daher vom Bundesverwaltungsgericht als rechtmässig beurteilt worden. Wir sind allerdings der Meinung, dass die Öffentlichkeitswirkung nicht mit einer maximalen Publizitätswirkung gleichzusetzen ist. Daher fordern wir private Anbieter von Handelsregisterdaten auf, Massnahmen zu ergreifen, welche zu einer geringeren Publizität führen.

Gemäss dem Urteil des Bundesverwaltungsgerichts vom 26. Februar 2008 wird die Bearbeitung und unbeschränkte Speicherung der Handelsregisterdaten durch private Anbieter gutgeheissen. Das öffentliche Weiterverbreitungsinteresse an Handelsregisterinformationen bestehe zeitlich unbeschränkt und unabhängig davon, ob die Datenquelle öffentlichen oder privaten Ursprungs ist, solange die Daten inhaltlich nicht verändert werden.

Trotz des Urteils hat einer der wichtigsten privaten Anbieter von Handelsregisterinformationen im Web in der Schweiz einige unserer zentralen Forderungen freiwillig umgesetzt. So ist es praktisch nicht mehr ohne Login möglich, nach Personen zu suchen oder nach Unternehmen, die gelöscht wurden.

Dennoch stören sich nach wie vor viele Personen daran, dass bei Internetrecherchen nach dem Namen natürlicher Personen oder Unternehmen Handelsregisterinformationen von Wirtschaftsauskunfteien an prominenter Stelle erscheinen, welche zum Teil nicht mehr aktuell sind. Insbesondere bei Konkursen haben die Betroffenen ein grosses Interesse, dass diese Daten nicht prominent auf Suchmaschinen erscheinen.

Wir anerkennen die Öffentlichkeitswirkung des Handelsregisters, welche im Obligationenrecht gesetzlich verankert ist. Zur Vereinfachung des freien Wirtschaftsverkehrs erfüllt ein für jedermann frei und einfach zugängliches Handelsregister seinen Zweck in der jetzigen Form. Dennoch ist die Öffentlichkeit des Handelsregisters nach Ansicht des EDÖB nicht mit einer grösstmöglichen Publizität gleichzusetzen.

Private Anbieter von Handelsregisterinformationen haben ein Interesse daran, dass ihre Webseite möglichst oft besucht wird, um so Werbeeinnahmen zu generieren. Aus diesem Grund optimieren sie meist ihre Webseiten dahingehend, dass sie in Suchmaschinen möglichst oft gefunden werden. Folglich tauchen bei der Suche nach einer Firma über eine Suchmaschine an prominenter Stelle die sie betreffenden Handelsregistereinträge auf. Diese grösstmögliche Publizitätswirkung ist nach unserer Meinung nicht mehr vom Zweck des Handelsregisters gedeckt und stellt daher eine widerrechtliche Datenbearbeitung dar. Aus diesem Grund werden wir im laufenden Jahr diese Thematik erneut aufgreifen, um die Persönlichkeit der betroffenen Personen besser zu schützen, ohne dabei die Öffentlichkeitswirkung des Handelsregisters einzuschränken.

1.8.3 Auskunfts- und Löschungsrecht bei Handelsfirmen

Auf zahlreiche Beschwerden hin haben wir bei gewissen Handelsfirmen – namentlich im Versandhandel – interveniert, um sie auf ihre Pflicht zur Einhaltung des DSG und insbesondere zur Gewährleistung des Auskunfts- und Löschungsrechts auf Verlangen der betroffenen Personen hinzuweisen.

Gemäss DSG dürfen Handelsfirmen keine Daten gegen den ausdrücklichen Willen der betroffenen Person bearbeiten und insbesondere keine Werbesendungen an Personen richten, die dies ausdrücklich abgelehnt haben. Die betroffene Person kann also jederzeit die Löschung ihrer Personendaten verlangen, wenn diese Marketingzwecken dienen. Die Verwendung der Adresse zu Werbezwecken kann von Anfang an generell untersagt werden (etwa durch Anbringen eines Sternchens im Telefonbuch oder durch Eintrag in der Robinson-Liste) oder nachträglich mit einem besonderen Verbot belegt werden. Dies ist namentlich der Fall, wenn der Empfänger die Werbesendung mit einer besonderen Anmerkung an den Absender zurückschickt.

Zudem ist jeder Inhaber einer Datensammlung aufgrund des DSG verpflichtet, jeder betroffenen Person auf Verlangen die über sie vorhandenen Personendaten, den Zweck und gegebenenfalls die Rechtsgrundlage des Bearbeitens sowie die Kategorien der bearbeiteten Personendaten, der an der Sammlung Beteiligten und der Datenempfänger mitzuteilen. Dieses Verfahren ist in der Regel kostenlos.

Wir haben verschiedene Unternehmen angeschrieben, um sie auf ihre gesetzlichen Verpflichtungen zur Löschung der Daten auf Verlangen der betroffenen Personen und zur Beantwortung der Auskunftsgesuche entsprechend dem Gesetz aufmerksam zu machen. Ausserdem haben wir die fraglichen Unternehmen darauf hingewiesen, dass die betroffenen Personen gegebenenfalls die Möglichkeit haben, ihre Rechte vor Gericht geltend zu machen. In einigen besonderen Fällen haben wir auch die Möglichkeit, den Sachverhalt abzuklären und für Unternehmen, die diese Rechte nicht beachten, Empfehlungen abzugeben.

1.8.4 Empfehlung in Sachen Mietercheck

Im Verlauf des Jahres 2008 haben wir bei einer Wirtschaftsauskunftei eine Sachverhaltsabklärung durchgeführt. Die betreffende Firma bietet neu eine Dienstleistung an, welche es Vermietern ermöglichen soll, Mieterangaben zu prüfen und das Risiko von Mietzinsausfällen zu vermindern. Mängel haben wir bei der Bonitätsrelevanz der angebotenen Daten und bei der Gewährung des Auskunfts- und Löschungsrechtes festgestellt. Deshalb haben wir eine Empfehlung erlassen.

Eine Wirtschaftauskunftei bietet neu unter dem Namen Mietercheck eine Dienstleistung an, mit welcher Vermieter online Auskünfte über potentielle Mieter einholen können. Damit soll es Vermietern möglich sein, Mieterangaben zu prüfen und Mietzinsausfälle zu verhindern.

Zur Einschätzung der Bonität potentieller Mieter benutzte Mietercheck einen Score, der nicht nur die Daten der betroffenen Person, sondern auch jene ihres Umfeldes auswertete. Mietercheck bewertete die betroffenen Personen mit einem Ampelsystem und bot den Vermietern Handlungsanweisungen hinsichtlich des Vertragsabschlusses an.

Durch eine betroffene Person auf den Mietercheck aufmerksam gemacht, nahmen wir umgehend mit der Firma Kontakt auf. Gleichzeitig rückte die Datenbearbeitung der Wirtschaftsauskunftei in den Medienfokus.

Wie eine Sachverhaltsabklärung zeigte, hat die Firma inzwischen einige Anpassungen an ihrer Dienstleistung vorgenommen. So wurden insbesondere der Score und die soziokulturellen Daten entfernt. Dennoch hat unsere Abklärung ergeben, dass die Datenbearbeitung nicht datenschutzkonform ist, weshalb wir mehrere Empfehlungen erlassen haben.

Die Firma sollte erstens die Bewertung der Zahlungserfahrungen transparenter gestalten. Für die betroffene Person ist nämlich weder erkennbar, wie ihre Zahlungserfahrungen eingestuft werden, noch dass der Mietercheck diese zusätzlich mit einer Ampel bewertet.

Zweitens ist die Bonitätsbewertung einer Person aufgrund ihrer Beziehungen zu einer Firma auf jene Fälle zu beschränken, welche die Bonität der betroffenen Person tatsächlich beeinflussen. Denn nicht jede Beziehung einer Person zu einer Firma muss bonitätsrelevant sein.

Drittens müssen diese Beziehungen für die betroffene Person und die Kunden erkennbar sein. Schliesslich haben wir erkannt, dass eine generelle Verknüpfung von Personendaten mit Firmendaten unverhältnismässig ist.

Viertens haben wir empfohlen, dass die Firma nicht mehr alle bekannten Adressen einer Person auflistet und hieraus die durchschnittliche Wohndauer berechnet. Die Dauer eines Mietverhältnisses kann von Faktoren abhängen, die nicht mit Zahlungsschwierigkeiten in Zusammenhang stehen, wie etwa die Arbeit des Mieters inklusive seiner Familienmitglieder, das Lebensumfeld, das Wohnungsangebot etc. Zum einen ist die durchschnittliche Wohndauer kein bonitätsrelevantes Datum und zum anderen lässt sich aus ihr auch nicht schliessen, dass der Mieter ein potentieller «Mietnomade» sei. Zudem haben wir darauf hingewiesen, dass die Angaben über Wohnsitzwechsel über mehrere Jahre hinweg als Persönlichkeitsprofil zu werten sind.

Fünftens haben wir die Entfernung der Bonitätsdaten von Personen verlangt, die mit einem potentiellen Mieter im selben Haushalt wohnen. Die Verknüpfung von Bonitätsdaten aller in einem Haushalt lebenden Personen mit Daten der abgefragten Person ist unseres Erachtens unverhältnismässig. Einerseits spielen die Bonitätsdaten der Mitbewohner nur dann eine Rolle, wenn der Mietvertrag von diesen Personen mit unterzeichnet wird. Anderseits sind ihre Bonitätsdaten grundsätzlich nicht dazu geeignet, Rückschlüsse über die Kreditwürdigkeit der abgefragten Person zu ziehen. Ausserdem ist letztere nicht in der Lage, zu erkennen, dass die Datenbank ihre Daten mit den Daten aller mit ihr im Haushalt lebenden Personen verknüpft.

Die sechste Empfehlung bezieht sich auf die Erteilung des Zuganges zur Datenbank. Wir haben gefordert, dass der Zugang nur zweckentsprechend, d.h. nur professionellen Vermietern gewährt werden darf. Einer Mieterkautionsversicherung, die selber nicht professioneller Vermieter ist, darf die Firma nur jene bonitätsrelevanten Daten anbieten, welche die Versicherung für den Abschluss oder die Abwicklung ihrer Verträge benötigt.

Mit der jetzigen Abfragemöglichkeit sind bei der Suche mehr Daten als notwendig abrufbar. Deshalb haben wir der Auskunftei empfohlen, die Abfrage technisch so einzuschränken, dass die Kunden stufenweise, je nach Anzahl Suchtreffer, weitere Kriterien eingeben müssen.

Schliesslich haben wir das Unternehmen aufgefordert, betroffenen Personen, die ein Auskunftsbegehren stellen, sämtliche Informationen auszuhändigen. Vermieter können über Mietercheck Daten von betroffenen Personen abrufen, die diesen bisher nicht mitgeteilt werden. Darunter befinden sich auch Daten, die nur verknüpft sind oder laufend aus den Beständen berechnet werden. Die betroffene Person erkennt nicht, welche Daten die Firma tatsächlich bearbeitet, und kann deshalb auch nicht hinreichend von ihrem Recht auf Datenberichtigung und Datenlöschung Gebrauch machen.

Im Anhang, Ziff. 4.1.6, ist die Empfehlung abgedruckt. Die Firma hat dazu Stellung genommen. Ob die Angelegenheit dem Bundesverwaltungsgericht zum Entscheid vorgelegt wird, ist zum jetzigen Zeitpunkt noch offen.

1.8.5 Bekanntgabe von Personendaten an Dritte durch Vereine und Veranstalter von Sportanlässen

Vereine oder Veranstalter eines Anlasses können die Adressen ihrer Mitglieder oder der Teilnehmer nicht ohne weiteres ihren Sponsoren oder anderen Dritten bekannt geben. Eine Bekanntgabe von Personendaten zu Marketingzwecken kann nur durch die freiwillige Einwilligung nach angemessener Information der betroffenen Personen gerechtfertigt werden. Wir haben die Verantwortlichen auf die gesetzlichen Voraussetzungen einer Datenbearbeitung aufmerksam gemacht und ihnen empfohlen, ihre Statuten und Reglemente entsprechend anzupassen.

In diesem Jahr sind zahlreiche Beschwerden von Vereinsmitgliedern sowie Teilnehmern von Sportanlässen betreffend die Bekanntgabe ihrer Adressen zu Marketingzwecken an Dritte (Sponsoren, Krankenkassen) bei uns eingegangen. Die betroffenen Personen wurden nicht – oder nur ungenügend – informiert und hatten nicht die Möglichkeit, sich einer solchen Bekanntgabe zu widersetzen. Im Anschluss an gewisse zu diesem Thema erschienene Presseartikel erhielten wir überdies zahlreiche Fragen von Vereinen oder Veranstaltern von Sportanlässen. Wir haben die betroffenen Personen und die Verantwortlichen über die gesetzliche Situation in diesem Bereich sowie über ihre Rechte beziehungsweise ihre Pflichten informiert.

Die Verwendung der Personendaten von Vereinsmitgliedern oder Teilnehmern an einer Sportveranstaltung untersteht dem Gesetz über den Datenschutz. Eine Bearbeitung von Personendaten muss auf einem Rechtfertigungsgrund beruhen und den allgemeinen Prinzipien des DSG genügen. Insbesondere müssen die Bekanntgabe der Daten und ihre Zweckbestimmung für die betroffenen Personen erkennbar sein. Die Bekanntgabe darf zudem nicht gegen ihren ausdrücklichen Willen und ohne Rechtfertigungsgrund erfolgen. Die Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei ihrer Erhebung angegeben wird, in einem Gesetz vorgesehen ist oder aus den Umständen hervorgeht.

Was die Bearbeitung der Daten von Teilnehmern einer Sportveranstaltung anbelangt, können Personen, die sich für einen Sportanlass anmelden, in der Regel damit rechnen, dass die im Rahmen der Anmeldung übermittelten Daten zu Zwecken verwendet werden, die unmittelbar mit dem ordentlichen Ablauf der Veranstaltung zusammenhängen. Zu diesen Zwecken zählen die Zusendung von Informationen über die Organisation des Wettlaufs, die Zuteilung einer Startnummer, die Zeitmessung, das Klassement usw. Die Datenbearbeitung lässt sich in diesem Fall ohne weiteres aus den Umständen ableiten und ist somit erkennbar; eine besondere Information in dieser Hinsicht ist demnach grundsätzlich nicht notwendig. Die Bearbeitung der Personendaten zu unmittelbar mit der Organisation des Wettlaufs verbundenen Zwecken ist grundsätzlich durch stillschweigendes Einverständnis der Teilnehmer gerechtfertigt.

Die Bekanntgabe von Personendaten an einen bestimmten Fotografen, an Sponsoren oder andere Dritte ergibt sich dagegen nicht aus den Umständen und erfordert somit eine spezifische Information. Allein die Einwilligung der betroffenen Personen kann eine Bekanntgabe von Daten an Dritte zu Marketingzwecken rechtfertigen. Das Einverständnis ist nur gültig, wenn der Betroffene seinen Willen frei und nach ordnungsgemässer Information zum Ausdruck bringt. Die betroffenen Personen müssen die Bekanntgabe ihrer Adressen an Dritte verweigern können.

Die betroffenen Personen sollten – spätestens bei der Anmeldung – über die Bekanntgabe ihrer Personendaten an Dritte, über deren Identität und über die Zweckbestimmung der Bekanntgabe (z.B. Werbung) informiert werden. Zudem ist ihnen die Möglichkeit zu geben, sich dieser Datenübermittlung zu widersetzen. Die Erwähnung einer Bekanntgabe an Dritte muss für die Betroffenen gut sichtbar sein. Eine blosse Anmerkung ganz am Ende des Teilnahmereglements und ohne Verweigerungsmöglichkeit entspricht nicht den Datenschutzprinzipien.

Wir haben den Veranstaltern von Sportanlässen empfohlen, auf dem Anmeldeformular zu der Veranstaltung ein Feld vorzusehen, das anzukreuzen ist und bedeutet: «Ja, ich bin mit der Bekanntgabe meiner Personendaten an die Sponsoren zu Marketingzwecken einverstanden», und im Veranstaltungsreglement genaue Angaben über die Identität der Sponsoren zu machen.

Bezüglich der Verwendung der Personendaten von Vereinsmitgliedern gilt: Das Verzeichnis der Adressen von Vereinsmitgliedern darf nur an Dritte zu Marketingzwecken weitergegeben werden, soweit diese Bekanntgabe erkennbar ist und die betroffenen Personen ihre Einwilligung gegeben oder sich nicht dagegen ausgesprochen haben.

In der Regel empfehlen wir den Vereinen, diese Art der Bekanntgabe in ihren Statuten, zum Zeitpunkt des Beitritts oder auch durch eine besondere Information zu kommunizieren. Die Betroffenen müssen ausserdem über ihre Möglichkeit, sich jederzeit einer derartigen Verwendung ihrer Personendaten zu Marketingzwecken zu widersetzen, informiert werden.

Detaillierte Informationen zu diesem Thema haben wir im «Merkblatt über den Umgang mit Mitgliederdaten in einem Verein» veröffentlicht. Dieses kann auf unserer Webseite www.derbeauftragte.ch unter Dokumentation – Datenschutz – Merkblätter abgerufen werden.

1.9 International

1.9.1 Umsetzung Schengen: Der Datenschutz auf Bundesebene

Nach unserer Mitarbeit bei der Evaluierung des Schweizer Datenschutzes durch die Europäische Union haben wir mit dem Aufbau unserer Aufsichts- und Informationstätigkeiten im Rahmen von Schengen begonnen. Wir haben eine Koordinationsgruppe für die Zusammenarbeit mit den kantonalen Datenschutzbehörden eingesetzt. Zudem haben wir eine Kontrolle bei einer diplomatischen Vertretung der Schweiz im Ausland durchgeführt und Informationsdokumente auf unserer Webseite veröffentlicht.

Bevor die durch das Beitrittsabkommen zu Schengen (im März 2008 in Kraft getreten) begründete Zusammenarbeit operativ wurde, haben wir uns an der Evaluierung der Fähigkeit der Schweiz zur Umsetzung des Schengener Besitzstands beteiligt. Im Juni 2008 vertrat die Europäische Union die Auffassung, dass insgesamt die auf der Schengen-Zusammenarbeit beruhenden Datenschutzanforderungen in der Schweiz erfüllt seien. Damit wurde die Beteiligung der Schweiz am Schengener Informationssystem (SIS) Tatsache.

Die Europäische Union hat indessen gewisse Empfehlungen an die Schweiz gerichtet. Diese betrafen namentlich die Unabhängigkeit der Datenschutzbehörden, deren Zusammenarbeit untereinander, ihre Ressourcen, ihre Kontrolltätigkeiten sowie die Sensibilisierung der Nutzer des SIS und die Öffentlichkeitsinformation. Der Sachverständigenausschuss wies insbesondere auf die Notwendigkeit einer grösseren Unabhängigkeit des EDÖB sowie einer Aufstockung seiner Haushaltsmittel und seines Personalbestands hin, um ihn in die Lage zu versetzen, die ihm in diesem Kontext neu zufallenden Aufgaben wahrzunehmen.

In Zusammenarbeit mit verschiedenen Bundesämtern haben wir an der Umsetzung einiger der empfohlenen Massnahmen mitgewirkt. Im Wesentlichen hat der Bundesrat beschlossen, uns ab 2010 drei neue Arbeitsstellen zuzuteilen. Im Rahmen der Revisionsvorlage zum Bundespersonalgesetz ist vorgesehen, den Beauftragten für eine Amtszeit von vier Jahren zu ernennen; dies sollte die Gewähr für eine grössere institutionelle Unabhängigkeit des EDÖB bieten. Weitere Massnahmen stehen zur Diskussion, wie etwa die Ernennung des Beauftragten durch den Bundesrat mit Ratifizierung durch das Parlament sowie die budgettechnische Funktionsweise der Dienststelle.

Im Anschluss an unsere Mitarbeit bei der Evaluierung durch die Europäische Union haben wir verschiedene Kontrollaktivitäten im Bereich der Datenbearbeitung, der Information der SIS-Nutzer und der Sensibilisierung der öffentlichen Meinung eingeführt. Um eine wirksame und zuverlässige Aufsicht zu gewährleisten, haben wir insbesondere die Zusammenarbeit mit den kantonalen Datenschutzbehörden ausgebaut, die ebenfalls für die Beaufsichtigung der kantonalen SIS-Nutzer zuständig sind. Eine Koordinationsgruppe der schweizerischen Datenschutzbehörden, deren Vorsitz wir führen, dient in Zukunft als Plattform für die Kontroll- und Informationstätigkeiten der erwähnten Behörden im Bereich der Zusammenarbeit Schengen/Dublin.

Auf der Grundlage der bei unserer ersten Kontrolle bei der diplomatischen Vertretung der Schweiz in der Ukraine gesammelten Erfahrungen (vgl. Ziff. 1.9.2) werden wir unsere Aufsichtstätigkeiten fortsetzen und weiter entwickeln. So sollen Inspektionen bei den Bundesorganen, die Daten im Rahmen des SIS bearbeiten, geplant und durchgeführt werden, so etwa beim Bundesamt für Polizei, beim Bundesamt für Migration und bei den diplomatischen Vertretungen der Schweiz im Ausland.

Abgesehen von der Beaufsichtigung des SIS und der an der Verwaltung und Nutzung des Systems beteiligten Dienststellen sind wir auch für die Gewährleistung der tatsächlichen Wahrnehmung der Rechte der von der Bearbeitung von Personendaten Betroffenen zuständig. Daher haben wir ein Informationsblatt über die Rechte der von der Bearbeitung ihrer Personendaten im SIS betroffenen Personen ausgearbeitet und auf unserer Webseite www.derbeauftragte.ch unter Themen – Datenschutz – Schengen veröffentlicht.

1.9.2 Umsetzung Schengen: Kontrolle des EDÖB bei der Schweizer Vertretung in der Ukraine

In unserer Eigenschaft als Aufsichtsbehörde der zur Verwendung des Schengener Informationssystems (SIS) befugten Bundesorgane haben wir bei der diplomatischen Vertretung der Schweiz in Kiew (Ukraine) eine Kontrolle durchgeführt. Dabei ging es um die Bearbeitungsverfahren von Personendaten bei der Ausstellung von Visa und Aufenthaltsbewilligungen zum Zwecke der Einreise von Staatsangehörigen von Drittländern in den Schengen-Raum über die Schweiz. Unsere Empfehlungen betrafen hauptsächlich die Ausbildung des zur Nutzung des SIS berechtigten Personals, den Schutz und die technische Sicherheit der Bearbeitungen von Personendaten, die Verträge mit externen Leistungserbringern und die Wahrnehmung der Rechte der betroffenen Personen. Gegenwärtig prüfen wir die Umsetzung der Empfehlungen in Zusammenarbeit mit dem EDA und dem Bundesamt für Migration.

Als Aufsichtsbehörde der Bundesorgane im Datenschutzbereich sind wir beauftragt, die Bearbeitung von Personendaten des Schengener Informationssystems (SIS) zu kontrollieren, insbesondere die Bearbeitungen durch die zur Nutzung des SIS befugten Bundesorgane, und dies gemäss den aufgrund der Schengen-Zusammenarbeit geltenden Anforderungen. Wir führen unter anderem Datenschutzkontrollen bei den diplomatischen und konsularischen Vertretungen der Schweiz im Ausland durch. Diese Inspektionen beziehen sich auf die Bearbeitungsverfahren von Personendaten bei der Ausstellung von Visa und Aufenthaltsbewilligungen zum Zwecke der Einreise von Staatsangehörigen von Drittländern in den Schengen-Raum. Dieses Verfahren bedingt die Nutzung des SIS durch das Personal der schweizerischen Vertretungen.

In diesem Zusammenhang führten wir von Mai bis Oktober 2008 eine Kontrolle bei der diplomatischen Vertretung der Schweiz in Kiew durch. Auf der Grundlage unserer Feststellungen haben wir einen Bericht vorgelegt und Verbesserungsvorschläge sowie Empfehlungen an das Eidgenössische Departement für auswärtige Angelegenheiten (EDA) gerichtet. Diese betrafen zum einen die Ausbildung des zur Nutzung des SIS befugten Personals sowie den Schutz von Personendaten und die technische Sicherheit bei ihrer Bearbeitung. Zum anderen äusserten wir uns zur Bearbeitung von Personendaten durch externe Leistungserbringer (auf Auftrag) und zur wirksamen Umsetzung der Rechte all jener Personen, deren Daten bearbeitet werden.

Wir erinnerten insbesondere an die Notwendigkeit einer spezifischen Personalausbildung bei den Behörden mit einer Zugriffsberechtigung zum SIS im Rahmen der Durchführung der Schengen-Zusammenarbeit. Bevor diese Mitarbeiter zur Bearbeitung der

im SIS aufbewahrten Daten befugt sind, müssen sie nämlich über die Sicherheits- und Datenschutzvorschriften angemessen unterrichtet und über die diesbezüglichen Rechtsverletzungen und Strafmassnahmen informiert werden.

Wir haben uns für einen verstärkten Schutz bei der Behandlung von Personendaten ausgesprochen, insbesondere bei der Bekanntgabe der von den schweizerischen Vertretungen an die Schweizer Behörden und an Privatpersonen übermittelten Daten, namentlich bezüglich der technischen Sicherheit bei der Datenbekanntgabe über ein gesichertes Verschlüsselungssystem.

Des weiteren haben wir die schweizerischen Vertretungen aufgefordert, in ihren Leistungsverträgen mit externen Unternehmen zur Vergabe von Aufträgen für gewisse Bearbeitungen von Personendaten Bestimmungen über die Sicherheit und den Schutz dieser Daten vorzusehen (betreffend die Zweckbindung und die Vertraulichkeit der Datenbearbeitung, die technische Sicherheit der Daten, wie etwa die Bekanntgabe mittels eines gesicherten Verschlüsselungssystems, den Schutz gegen ungesetzliches Bearbeiten, die Aufbewahrung und Löschung der Daten usw.).

Um schliesslich die Wirksamkeit der Rechte der durch die Bearbeitung von Personendaten betroffenen Personen zu gewährleisten, haben wir empfohlen, das diplomatische und konsularische Personal über die gesetzlichen Verfahren zur Ausübung der Rechte der von der Datenbearbeitung betroffenen Personen ordnungsgemäss zu informieren.

Derzeit koordinieren wir die Umsetzung der Verbesserungsvorschläge und Empfehlungen in Zusammenarbeit mit dem EDA sowie mit dem Bundesamt für Migration, das von einigen der Massnahmen ebenfalls betroffen ist.

1.9.3 Internationale Zusammenarbeit

Personendaten machen nicht an den Landesgrenzen Halt. Zur Gewährleistung eines effektiven Datenschutzes ist es daher entscheidend, dass die nationalen Datenschutzbehörden zusammenarbeiten und auch auf internationaler Ebene aktiv sind. So beteiligen wir uns insbesondere an den Arbeiten des Europarates, der Europäischen und der Internationalen Konferenz der Datenschutzbeauftragten, der Frankophonen Vereinigung der Datenschutzbehörden und der gemeinsamen Kontrollinstanzen von Schengen und Eurodac.

Europarat

Wir haben an den Arbeiten des beratenden Ausschusses des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen 108) und seines Büros mitgewirkt. Der Ausschuss setzte seine Gespräche über das Grundrecht auf Schutz der Daten fort, das in einer verbindlichen Rechtsurkunde verankert werden könnte (beispielsweise im Zusatzprotokoll zur Europäischen Menschenrechtskonvention EMRK). Obwohl der Ausschuss in seiner Mehrheit eine solche Urkunde befürwortet, hat er eine vorläufige Unterbrechung der Diskussionen beschlossen, um namentlich die Inkraftsetzung des Vertrags von Lissabon abzuwarten, der dieses Grundrecht festschreibt und den Beitritt der Europäischen Instanzen zur EMRK vorsieht. Der Ausschuss, beziehungsweise sein Büro, hat die Arbeiten zur Abfassung einer Empfehlung aufgenommen, die ausführt, wie im Rahmen einer Erstellung von Profilen verwendete Personendaten zu schützen sind. Die Informatikinstrumente und Informationstechnologien machen es nämlich möglich, ausgehend von Datenerhebungen Mechanismen zur Kategorisierung von Personen zu schaffen, auf diese Weise Personendaten abzuleiten und Daten betreffend die Interaktionen der einzelnen Personen mit ihrer physischen und digitalen Umwelt zu bearbeiten. Mittels dieser Techniken können namentlich die Verhaltensweisen und Gefühlsregungen der Personen aufgezeichnet und leichter interpretiert werden. Die Profilierung kann somit die Würde der Person, ihre Rechte und Grundfreiheiten, einschliesslich ihrer wirtschaftlichen und sozialen Rechte, in schwerwiegender Weise beeinträchtigen. Der Ausschuss hält die Festlegung von Bestimmungen für notwendig, um die Profilierungsaktivitäten in einen Regelungsrahmen zu stellen. Schliesslich appellierte der Ausschuss an das Komitee der Minister, um das Übereinkommen 108 und sein Zusatzprotokoll zu fördern, indem es namentlich Drittstaaten zum Beitritt zu diesen Urkunden auffordert, wie es das Übereinkommen gestattet. Der Beitritt von Drittstaaten wäre ein erster Schritt in Richtung einer universellen Urkunde im Bereich des Datenschutzes.

Europäische Konferenz der Datenschutzbeauftragten

Die Europäische Konferenz der Datenschutzbeauftragten fand vom 17. bis 18. April 2008 auf Einladung der italienischen Datenschutzbehörde in Rom statt. Die Konferenz ist ein Diskussionsforum zwischen europäischen Datenschutzbehörden zu aktuellen Themen. Sie befasste sich insbesondere mit der Bedrohung der Privatsphäre aufgrund der Sicherheitspolitiken, der Bedürfnisse der Wirtschaft und der technologischen Entwicklungen. Sie verabschiedete ausserdem die Geschäftsordnung ihrer Arbeitsgruppe «Polizei und Justiz» und eine Resolution betreffend Personenkontrollen bei der Ein- und Ausreise im Schengen-Raum. Diese Entschliessung fordert die zuständigen Stellen auf, die Effektivität und Wirksamkeit der vorhandenen Massnahmen zu prüfen, bevor eine Verstärkung der die Rechte und Grundfreiheiten der Einzelpersonen beeinträchtigenden Massnahmen erwogen wird. Sie verlangt den vorgängigen Nachweis der Notwendigkeit und Verhältnismässigkeit neuer Massnahmen. Im Rahmen eines Podiumsgesprächs zum Thema Privatsphäre und Sicherheit machten wir die Konferenz auf das wachsende Risiko eines Ungleichgewichts zu Lasten der Rechte und Grundfreiheiten aufmerksam, eine Folge der Sicherheitspolitiken, mit denen das Ziel der Sicherheit dennoch nicht unbedingt erreicht wird. Auch wenn ein ausreichendes Sicherheitsniveau Voraussetzung für einen wirkungsvollen Schutz der Menschenrechte ist, sollte doch der Umfang der zu ergreifenden Massnahmen neu dimensioniert werden. Zudem ist daran zu erinnern, dass Sicherheit auf der Achtung der Rechte und Freiheiten jedes Einzelnen aufbaut. Ohne Datenschutz könnten Sicherheit und Demokratie einem Staat des Misstrauens, der Gewalt und der Repression weichen. Daher ist es unerlässlich, die bereits getroffenen Massnahmen gründlich auf ihre Wirksamkeit und Effizienz zu prüfen und ihre Auswirkungen zu untersuchen, bevor neue Einschränkungen der Rechte und Grundfreiheiten vorgeschlagen werden. In diesem Rahmen müssen die Datenschutzbehörden ihre Zusammenarbeit verstärken und harmonisierte gemeinsame Stellungnahmen herausgeben. Sie müssen vermehrt Informations-, Kommunikations- und Sensibilisierungspolitik betreiben und den Prozess mitbestimmen, der in Massnahmen zur Einschränkung der Rechte der Einzelpersonen münden könnte.

Arbeitsgruppe «Polizei und Justiz»

Wir beteiligen uns regelmässig an den Tätigkeiten der Arbeitsgruppe «Polizei und Justiz» der Europäischen Konferenz der Datenschutzbeauftragten. Diese Gruppe hat die Aufgabe, die gesetzgeberischen Entwicklungen innerhalb der Europäischen Union im Bereich Polizei und Justiz, namentlich in Bezug auf die Entwicklung des Schengen-Besitzstandes, zu verfolgen. Sie bemüht sich um Gehör bei den verschiedenen zustän-

digen Behörden in der Europäischen Union und insbesondere beim Europäischen Parlament. Sie gibt Stellungnahmen und konkrete Vorschläge zur Gewährleistung eines wirksamen Datenschutzes ohne Beeinträchtigung der notwendigen polizeilichen und gerichtlichen Zusammenarbeit ab. Die Gruppe will auch in der Abstimmung der koordinierten Kontrolltätigkeiten zwischen den nationalen Datenschutzbehörden eine Rolle spielen und hat die Ausarbeitung eines Handbuchs für die Durchführung solcher Kontrollen an die Hand genommen.

Gemeinsame Kontrollbehörden Schengen und Eurodac

Seit dem 12. Dezember 2008 gehört die Schweiz zum Schengen-Raum. So sind wir Mitglieder der gemeinsamen Schengen-Kontrollbehörde (GK) und der Koordinationsgruppe Eurodac geworden, die aus den nationalen Datenschutzbehörden und dem europäischen Datenschutzbeauftragten besteht. Diese beiden Kontrollinstanzen ermöglichen einen umfassenden Informationsaustausch über die Auslegung der für Schengen und Dublin geltenden Datenschutzbestimmungen. Die GK hat namentlich die Aufgabe, die regelmässigen gemeinsamen Kontrollaktivitäten zu koordinieren, um die Einhaltung der Datenschutzbestimmungen des Schengen-Abkommens zu überprüfen und die notwendigen Empfehlungen an die Mitgliedstaaten und den europäischen Rat zu richten. Wir haben an einer ersten Inspektion betreffend die Signalemente von verschwundenen oder im Schengener Informationssystem zu schützenden Personen teilgenommen. Die Ergebnisse dieser Inspektion sind noch nicht bekannt. Im Rahmen der Koordinationsgruppe Eurodac haben wir uns an einer Erhebung über die Information der betroffenen Personen über ihre Rechte beteiligt. Der Schlussbericht ist noch nicht erstellt worden.

Internationale Konferenz der Datenschutzbeauftragten

Die 30. Internationale Konferenz der Datenschutzbeauftragten wurde von der Commission Nationale Informatique et Libertés (Datenschutzkommission von Frankreich) und dem deutschen Bundesbeauftragten für den Datenschutz und die Informationsfreiheit gemeinsam organisiert. Sie fand vom 15. bis 17. Oktober 2008 in Strassburg statt (www.privacyconference2008.org). Unter dem Thema «Der Schutz der Privatsphäre in einer Welt ohne Grenzen» wirkten rund 570 Teilnehmer aus 60 Ländern der ganzen Welt in Vertretung der Datenschutzbehörden, internationaler Organisationen, verschiedener Sektoren der Wirtschaft und akademischer und wissenschaftlicher Kreise an den Arbeiten mit. Sie pflegten einen Meinungs- und Informationsaustausch über die aktuellen Herausforderungen, die sich für den Datenschutz aufgrund der Si-

cherheitspolitiken, der sozialen Netzwerke, der Erwartungen der Unternehmen und der Wirtschaft im Allgemeinen oder der Digitaltechnologien stellen. Entscheidend erschien den Teilnehmern die Stärkung des gegenseitigen Vertrauens zur Entwicklung von Lösungen, Instrumenten und Produkten, die dem Recht auf Datenschutz Rechnung tragen und dessen Erfordernisse einbeziehen. Die Datenschutzbeauftragten haben sieben Resolutionen angenommen. Im Besonderen akkreditierten sie in einem entsprechenden Konferenzbeschluss Kroatien und Burkina Faso; dieser Staat hat als erster in Afrika ein Datenschutzgesetz erlassen und eine unabhängige Aufsichtsbehörde eingesetzt. Auf gemeinsamen Antrag des EDÖB und der spanischen Datenschutzbehörde nahm die Konferenz eine Entschliessung über die Dringlichkeit des Schutzes der Privatsphäre in einer Welt ohne Grenzen an und erarbeitete einen gemeinsamen Vorschlag zur Erstellung internationaler Normen zum Schutz der Privatsphäre und zum Schutz personenbezogener Daten. Diese Resolution (vgl. Anhang, Ziff. 4.1.7) schliesst an die Resolutionen der vorangegangenen Konferenzen und namentlich an die anlässlich der 27. Konferenz verabschiedete Erklärung von Montreux an (vgl. unseren 13. Tätigkeitsbericht 2005/2006, Ziff. 9.2.1 und 11.2.).

Die Datenschutzbeauftragten erinnerten daran, dass das Recht auf Datenschutz und auf Schutz der Privatsphäre ein Grundrecht jeder Person ist, ungeachtet ihrer Staatsangehörigkeit und ihres Wohnortes, und forderten erneut die Ausarbeitung einer zwingenden Rechtsurkunde im Bereich des Datenschutzes und des Schutzes der Privatsphäre. In diesem Sinne unterstützen sie namentlich die Bemühungen des Europarates im Hinblick auf den Beitritt von Nichtmitgliedstaaten zum Übereinkommen 108 und seinem Zusatzprotokoll. Die Entschliessung beauftragt auch eine Arbeitsgruppe, einen gemeinsamen Vorschlag zur Erstellung internationaler Normen zum Schutz der Privatsphäre und zum Schutz personenbezogener Daten auszuarbeiten und der nächsten Konferenz vorzulegen. Die konstituierende Sitzung dieser Arbeitsgruppe, der auch wir angehören, fand am 12. Januar 2009 in Barcelona statt. Sie bot Gelegenheit, die Arbeitsmethode festzulegen, Sachverständige aus verschiedenen Bereichen anzuhören und eine Bestandesaufnahme der anstehenden Probleme vorzunehmen. Die Konferenz verabschiedete überdies Entschliessungen über die Einrichtung einer Lenkungsgruppe zur Vertretung der Datenschutzbehörden bei Tagungen internationaler Organisationen, die Einrichtung einer Webseite der Konferenz, die Prüfung der Einführung eines internationalen Tages oder einer Woche für den Schutz der Privatsphäre und der personenbezogenen Daten, den Schutz der Privatsphäre von Kindern im Internet (vgl. Anhang, Ziff. 4.1.8) und zum Schutz der Privatsphäre in sozialen Netzwerkdiensten (vgl. Anhang, Ziff. 4.1.9).

Frankophone Vereinigung der Datenschutzbehörden

Wir sind auch in der frankophonen Vereinigung der Datenschutzbehörden (Association francophone des autorités de protection des données AFAPDP) tätig, in der wir das Amt eines der drei stellvertretenden Vorsitzenden innehaben. Nach ihrer Gründung am 24. September 2007 in Montreal nutzte die AFAPDP das erste Jahr ihrer Existenz, um sich zu organisieren und erste Tätigkeiten in Angriff zu nehmen, namentlich durch eine Mitwirkung innerhalb der institutionellen Netzwerke des französischsprachigen Raums, um das Recht auf den Schutz der Personendaten als wesentliches Element der heutigen Demokratie zu fördern. Die Vereinigung hat auch mit einem Informationsaustausch über die Stellungnahmen der Datenschutzbehörden zu aktuellen Themen begonnen und ein Inventar der Gesetzestexte in den Ländern des französischsprachigen Raums erstellt. Sie beteiligt sich weiter als Beobachterin an den Arbeiten des Europarates. Die AFAPDP hielt am Rande der 30. Internationalen Konferenz ihre 2. Generalversammlung in Strassburg ab. Dieser Versammlung ging eine frankophone Konferenz in Form von Workshops zur Sensibilisierung und Einführung in bewährte Praktiken voraus. Der erste Workshop war der Information der betroffenen Personen über ihre Rechte gewidmet. Ein zweiter Workshop befasste sich mit verschiedenen technischen Aspekten im Zusammenhang mit der Geolokalisierung, der Videoüberwachung und der Biometrie. So hatten wir die Gelegenheit, unsere Praxis im Bereich Videoüberwachung vorzustellen und auf die verfügbaren Techniken in Sachen Schutz der Privatsphäre aufmerksam zu machen.

1.9.4 Internationale Arbeitsgruppe Datenschutz im Telekommunikationsbereich

Zu den von der Berliner Gruppe im vergangenen Jahr angesprochenen Themen gehörten insbesondere die Problematik der sozialen Netzwerkdienste im Internet, die Ermittlung von Urheberrechtsverletzungen an den Tauschbörsen sowie die Bewertungsplattformen im Internet.

Im Verlauf des Jahres 2008 tagte die Internationale Arbeitsgruppe Datenschutz im Telekommunikationsbereich (oder «Berliner Gruppe») im März in Rom und im Oktober in Strassburg. Wegen der geografischen Nähe dieser Veranstaltungen konnte der EDÖB ausnahmsweise an beiden Tagungen teilnehmen.

Die Berliner Gruppe hat in Rom ein Dokument zum Thema der sozialen Netzwerkdienste im Internet (Facebook, Myspace etc.) verabschiedet. In den letzten Jahren sind solche Webseiten vor allem bei den jüngeren Generationen immer beliebter geworden. Das besagte Dokument (Rom Memorandum) hat das Ziel, die Risiken aufzuzeigen,

die mit diesen Webseiten unter dem Gesichtspunkt der Privatsphäre einhergehen können. Es enthält insbesondere eine Anzahl Empfehlungen, die sich an alle betroffenen Akteure richten, d.h. die Gesetzgeber, die Anbieter von sozialen Netzwerkdiensten sowie natürlich ihre Nutzerinnen und Nutzer. Darüber hinaus fand im Vorfeld zur Herbsttagung der Berliner Gruppe in Strassburg ein internationales Symposium über den «Schutz der Privatsphäre im Zeitalter der sozialen Netzwerkdienste» statt.

Die Thematik der Bearbeitung von Personendaten im Rahmen der Bekämpfung von Urheberrechtsverletzungen (vgl. unseren 15. Tätigkeitsbericht 2007/2008, Ziff. 1.3.1) sowie die Problematik der Bewertungsplattformen im Internet (vgl. dazu Ziff. 1.3.7) wurden ebenfalls erörtert.

Alle von der Arbeitsgruppe veröffentlichten Dokumente können (auf englisch und auf deutsch) auf der Webseite www.iwgdpt.org oder www.datenschutz-berlin.de, Europa/International – International Working Group on Data Protection in Telecommunications (IWGDPT) abgerufen werden.

Auf der Basis des Rom Memorandum hat der EDÖB seinerseits ein Dokument zum Thema der sozialen Netzwerkdienste im Internet ausgearbeitet. Dieses ist auf unserer Webseite www.derbeauftragte.ch unter Themen – Datenschutz – Internet verfügbar.

2. Öffentlichkeitsgesetz: Jahresbilanz 2008

2.1 Zugangsgesuche bei der Bundesverwaltung

Die Anzahl der eingereichten Zugangsgesuche und der Schlichtungsanträge sind gemäss den Bundesämtern im Vergleich zum Vorjahr leicht zurückgegangen. Dabei stellt sich die Frage, ob tatsächlich alle Zugangsgesuche erfasst und gemeldet werden. Der Prozentsatz der vollständig oder zumindest teilweise gewährten Zugänge, die uns mitgeteilt wurden, entspricht in etwa jenem des Vorjahres. Bei den Schlichtungsverfahren liess sich in der Hälfte der Fälle ein für den Antragsteller günstigeres Resultat erreichen.

Bereits zum dritten Mal mussten uns die Stellen, die dem Öffentlichkeitsgesetz unterliegen, die Anzahl der eingereichten Zugangsgesuche und deren Beurteilung melden. Gemäss den uns mitgeteilten Zahlen sind im Jahr 2008 bei den Bundesbehörden 221 Zugangsgesuche eingereicht worden. In 115 Fällen gewährten die Behörden einen vollständigen und bei 35 Gesuchen einen teilweisen Zugang. 71 Zugangsgesuche wurden vollständig abgelehnt. Gegenüber dem Vorjahr haben sich diese Zahlen nicht grundlegend verändert (vgl. Statistik Ziff. 3.5).

Folgende Aussagen und Bemerkung lassen sich dazu machen:

- Bei 68% aller eingereichten Zugangsgesuche wurde ein vollständiger respektive ein teilweiser Zugang gewährt, bei 32% wurde er vollständig verweigert.
- Auch in diesem Berichtsjahr fällt die grosse Zahl der Verweigerungen und die relativ geringe Zahl der teilweise gewährten Zugänge auf. Selbst wenn sich der Anteil der teilweisen Zugangsgewährungen im Vergleich zum Vorjahr verdoppelt hat, so verweigern Bundesbehörden offenbar lieber vollständig den Zugang, anstatt – wie vom Öffentlichkeitsgesetz gefordert – das Verhältnismässigkeitsprinzip anzuwenden und einen teilweisen Zugang zu gewähren. Wir fragen uns, ob dies daran liegt, dass diese Art der Zugangsgewährung mit sehr viel mehr Aufwand verbunden sein kann (Passagen abdecken, anonymisieren etc.).
- Es gibt Verwaltungseinheiten, die uns seit der Einführung des Öffentlichkeitsgesetzes vor nunmehr 3 Jahren noch kein einziges Zugangsgesuch gemeldet haben. Dies kann verschiedene Gründe haben. Zum einen geben einzelne Bundesbehörden unumwunden zu, dass sie Anfragen aus der Öffentlichkeit, die ohne weiteres zum Zugang führen, «formlos» erledigen und darum auch

nicht in die Statistik aufnehmen. Darunter fallen nicht zuletzt Anfragen von Journalisten an die Informations- und Kommunikationsdienste der einzelnen Bundesämter. Zum andern ist nach wie vor davon auszugehen, dass zahlreiche Zugangsgesuche gar nicht als solche erkannt werden. In der Statistik erscheinen daher nur die aus der Sicht des Bundesamtes «relevanten» Fälle, d.h. jene, die schwierig in der Beurteilung sind oder besonders viel Aufwand verursachen (weil beispielsweise umfangreiche Berichte anonymisiert werden müssen). Die von den Bundesbehörden gemeldeten Zahlen – so unser Fazit – sind mit einer gewissen Vorsicht zu geniessen. Wahrscheinlich werden an die Bundesverwaltung tatsächlich mehr als die in der Statistik ausgewiesenen Zugangsgesuche gestellt und wohl auch positiv beurteilt.

- Als interessante Tendenz zeichnet sich ab, dass Ämter mehr Zugangsgesuche melden, wenn sie spezifische amtsinterne Ausbildungsveranstaltungen zum Öffentlichkeitsgesetz durchgeführt haben und/oder über ein Dokumentenmanagementsystem verfügen, das an die Bedürfnisse des Öffentlichkeitsgesetzes angepasst wurde (z.B. BAFU, BAKOM, EDÖB).
- Wie im letzten Berichtsjahr verlangten die Bundesämter auch in diesem Jahr in der Regel keine Gebühren für die Beurteilung der Zugangsgesuche. Nur bei 5 der 221 gemeldeten Zugangsgesuche wurde eine Gebühr im Gesamtbetrag von sFr. 1'280.- verlangt (im Vergleich zu sFr. 1'730.- im 2007).
- Weiterhin keine verlässlichen Angaben lassen sich über den bei den Ämtern und Departementen verursachten Zeitaufwand machen. Die Bundesbehörden sind nicht verpflichtet, den zeitlichen Aufwand für die Beurteilung eines Zugangsgesuchs zu melden. Die uns auf freiwilliger Basis gemachten Angaben sind daher nur bedingt aussagekräftig. Gemäss diesen Angaben hat der gemeldete Zeitaufwand im Vergleich zum Vorjahr beträchtlich zugenommen (273 Stunden im Jahr 2007, 509 Stunden im Jahr 2008).

2.2 Zugangsgesuche bei den Parlamentsdiensten

Auch die Parlamentsdienste unterstehen dem Öffentlichkeitsgesetz. Gemäss ihren Angaben wurde im Jahr 2008 kein Zugangsgesuch eingereicht.

2.3 Schlichtungsanträge beim EDÖB

2008 wurden insgesamt 25 Schlichtungsanträge eingereicht (vgl. Statistik Ziff. 3.8). Im Vorjahr waren es noch 36 Schlichtungsanträge.

Insgesamt konnten 27 Schlichtungsanträge aus den Jahren 2007 und 2008 abgeschlossen werden. In vier Fällen wurde mit den Beteiligten eine Schlichtung erzielt, und bei 16 Schlichtungsanträgen erliessen wir – da keine einvernehmliche Lösung möglich oder von vornherein ersichtlich war – Empfehlungen (z.T. wurden mehrere Schlichtungsanträge mit einer Empfehlung erledigt). In fünf Fällen kam die Behörde während des hängigen Schlichtungsverfahrens auf ihren negativen Entscheid zurück und gewährte doch noch den gewünschten Zugang. In zwei Fällen kam das Öffentlichkeitsgesetz nicht zur Anwendung.

Diese Zahlen lassen folgende Schlüsse und Bemerkungen zu:

- In 106 Fällen wurde der Zugang vollständig verweigert (71), respektive nur teilweise gewährt (35). Dem stehen 25 beim Beauftragten eingereichte Schlichtungsanträge gegenüber. Mit anderen Worten wird im Berichtsjahr bei einem knappen Viertel aller ganz oder teilweise abgelehnten Zugangsgesuche ein Schlichtungsantrag eingereicht. Im Vorjahr betrug diese Zahl noch ein Drittel. Erneut haben Rechtsanwälte und Journalisten am meisten Schlichtungsanträge eingereicht.
- Insgesamt konnte in der Hälfte der abgeschlossenen Schlichtungsverfahren (Schlichtungen und Empfehlungen) eine für den Gesuchsteller günstigere Lösung erzielt werden (d.h. Schlichtung respektive ein weitergehender Zugang als ursprünglich vom Bundesamt zugestanden).
- Die meisten Empfehlungen wurden von den Antragstellenden und den Bundesämtern akzeptiert; in vier Fällen verlangten die Antragsteller von der Behörde den Erlass einer Verfügung. Unseres Wissens wurde im Berichtsjahr gegen keine unserer Empfehlungen Beschwerde beim Bundesverwaltungsgericht eingereicht.

Mehr als nur eine Bundesbehörde wandte sich während des Schlichtungsverfahrens mit der Bitte an uns, ihnen das (vormals bei ihnen eingereichte) Zugangsgesuch zuzustellen, weil es im Amt nicht mehr auffindbar war. Mit Erstaunen nahmen wir zudem Aussagen zur Kenntnis, dass nicht alle Behörden mit einem Dokumentenmanagementsystem arbeiten.

2008 sind weniger Schlichtungsanträge als im Vorjahr eingegangen, weshalb ein Teil der Rückstände abgearbeitet werden konnte. Unbefriedigenderweise hat eine Antragstellerin oder ein Antragsteller noch immer zu lange auf die Durchführung eines Schlichtungsverfahrens zu warten. Dessen speditive Durchführung hängt allerdings

auch von der Kooperation der involvierten Bundesbehörden ab (z.B. durch umgehende Einreichung aller notwendigen Dokumente oder Bereitschaft zur Lösungsfindung in Schlichtungsverhandlungen). In jenen Fällen, in denen Zugang verlangt zu Dokumenten wird, die Personendaten Dritter enthalten, wäre es wünschenswert, dass Bundesämter diese Dritten entsprechend den Vorgaben des Öffentlichkeitsgesetzes auch tatsächlich anhören, anstatt den Zugang mit dem Argument des Schutzes der Privatsphäre von vornherein zu verweigern.

2.4 Empfehlungen

Nachfolgend werden die im Berichtsjahr erlassenen Empfehlungen im Bereich des Öffentlichkeitsgesetzes kurz zusammengefasst. Die vollständigen Versionen sind im Original auf unserer Webseite www.derbeauftragte.ch unter Dokumentation – Öffentlichkeitsprinzip zu finden. Drei wichtige Empfehlungen werden im Anhang veröffentlicht.

Empfehlung BAG / Vertrag Präpandemieimpfstoff (01. Februar 2008)

Das Gesuch eines Pharmaunternehmens um Zugang zu einem Vertrag (Kauf eines Präpandemie-Impfstoffes) mit einem anderen Unternehmen wurde vom Bundesamt für Gesundheit mit Verweis auf eine bereits ergangene Empfehlung in gleicher Sache abgelehnt. In einer neuen Empfehlung stützt der Beauftragte den Entscheid des BAG.

Empfehlung BAFU / Adresslisten und Abgabedeklarationen von Deponien und Abfallexporteuren (13. März 2008)

Das Bundesamt für Umwelt verweigerte den Zugang zu den besagten Dokumenten. Der Beauftragte empfahl dem Amt, gewisse Adresslisten zugänglich zu machen.

Empfehlung Stiftungsaufsicht / Revisionsbericht (11. Juni 2008)

Die Eidgenössische Stiftungsaufsicht verweigerte, gestützt auf das Berufs-, Geschäfts- und Fabrikationsgeheimnis, den Zugang zum Revisionsbericht, zur Bilanz sowie zur Erfolgsrechnung einer Stiftung. Der Beauftragte vertritt in seiner Empfehlung die Ansicht, dass der Zugang zu Recht verweigert wurde, da die besagten Dokumente detaillierte Angaben zur Vermögens- und Ertragslage der Stiftung enthalten und für deren Geschäftstätigkeit von zentraler Bedeutung sind.

Empfehlung EDA / Projektunterlagen DEZA (28. Juli 2008)

Der Antragsteller reichte verschiedene Zugangsgesuche zu laufenden Projekten des Schweizerischen Korps für humanitäre Hilfe (SKH) und der Direktion für Entwicklung und Zusammenarbeit ein (z.B. Tsunami-Wiederaufbau in Südasien). Der Beauftragte hatte letztendlich sechs komplexe Schlichtungsanträge zu beurteilen. In seiner Empfehlung gelangte er unter anderem zum Schluss, dass vom Antragsteller zu Recht eine Präzisierung des Zugangsgesuchs verlangt worden war, dass ein Bericht nicht erneut zu überarbeiten ist und dass ein weiterer Bericht anonymisiert werden muss. Die vollständige Empfehlung befindet sich unter Ziff. 4.2.1.

Empfehlung EDA / Bericht zur schweizerischen Energieaussenpolitik (29. August 2008)

Das Eidgenössische Departement für auswärtige Angelegenheiten verweigerte dem Antragsteller den Zugang zu einem Bericht zur schweizerischen Energieaussenpolitik und verwies auf verschiedene Ausnahmeklauseln des Öffentlichkeitsgesetzes. Der Beauftragte gelangte zum Schluss, dass eine Offenlegung von grossen Teilen des Berichts nicht zu einer Beeinträchtigung der vom EDA vorgebrachten Geheimhaltungsinteressen führt. Er empfahl, nur wenige Passagen abzudecken, ansonsten aber den Bericht zugänglich zu machen.

Empfehlung BFS / Statistikgeheimnis (31. Oktober 2008)

Die Antragstellerin ersuchte um Zugang zur Statistik über die Erfolgsquote von Maturanden aus der Westschweiz. Das Bundesamt für Statistik verweigerte den Zugang mit dem Hinweis auf das Statistikgeheimnis gemäss Art. 14 des Bundesstatistikgesetzes (BStatG). Der Beauftragte teilte die Ansicht des BFS und erliess eine entsprechende Empfehlung. Die vollständige Empfehlung befindet sich unter Ziff. 4.2.2 (Französisch).

Empfehlung BSV / Ausschreibung für Hörgeräte (28. November 2008)

Die Antragsteller wollten Einsicht in zwei Rechtsgutachten zur Ausschreibung für Hörgeräte durch das Bundesamt für Sozialversicherungen nehmen und stellten sowohl beim BSV als auch bei der Wettbewerbskommission (Weko) ein Zugangsgesuch. Der Beauftragte hielt in seiner Empfehlung fest, dass das Öffentlichkeitsgesetz nicht zur Anwendung gelangte, da die ersuchten Dokumente Teil eines laufenden Verfahrens waren.

Empfehlung Stiftungsaufsicht / Aufsichtstätigkeit (11. Dezember 2008)

Die Eidgenössische Stiftungsaufsicht verweigerte dem Antragsteller den Zugang zum Dossier über eine Stiftung, insbesondere zu den Akten über die Rückzahlung eines Deliktbetrags durch den ehemaligen Stiftungsratspräsidenten. Wie der Beauftragte in seiner Empfehlung festhielt, überwiegt vorliegend das Interesse der Öffentlichkeit am Zugang zu den besagten Dokumenten klar dasjenige der betroffenen Privaten (z.B. Stiftungsrat, ehemaliger Stiftungsratspräsident) am Schutz ihrer Privatsphäre. Die vollständige Empfehlung befindet sich unter Ziff. 4.2.3.

Empfehlung armasuisse / Zeughausverkauf (15. Dezember 2008)

Der Antragsteller ersuchte bei armasuisse, Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) um Einsicht in diverse Dokumente im Zusammenhang mit dem Verkauf des Zeughauses in Langnau im Emmental. armasuisse lehnte mit dem Hinweis ab, dass das Zugangsgesuch ein Geschäft betreffe, welches vor dem Inkrafttreten des BGÖ abgewickelt worden sei. Ein Teil der Dokumente wurde jedoch nach dem Inkrafttreten des BGÖ erstellt und auch schon einem Gesuchsteller zugänglich gemacht. Der Beauftragte empfahl daher, mit Verweis auf das Prinzip des gleichen Zuganges für jede Person, dem Antragsteller Einsicht in die die Dokumente zu gewähren.

Empfehlung EDA / Visainspektionsberichte (23. Dezember 2008)

Das Eidgenössische Departement für auswärtige Angelegenheiten stellte dem Antragsteller auf Wunsch zwei Visainspektionsberichte von Moskau und Mumbai zu, wobei diese jedoch eingeschwärzte Passagen enthielten. Der Beauftragte hatte zu prüfen, ob diese Passagen zu Recht eingeschwärzt wurden, und empfahl, nur wenige Passagen abzudecken.

2.5 Schlichtungen

In folgenden Fällen konnte eine Schlichtung erzielt werden:

Schlichtung BJ / Rassismus-Strafnorm:

Der Antragsteller ersuchte beim Bundesamt für Justiz um Zugang zu diversen Unterlagen bezüglich eines Hearings über die Rassismus-Strafnorm. Nach einer konstruktiven Diskussion in der Schlichtungsverhandlung konnte der Antragsteller sein Gesuch weiter konkretisieren und erhielt die noch gewünschten Dokumente zugestellt.

Schlichtung EAV / Adressverzeichnisse:

Die Eidgenössische Alkoholverwaltung lehnte den Zugang zu Adressverzeichnissen der gewerblichen Brenner sowie der Inhaber von Grosshandelsbewilligungen ab, weil eine gesetzliche Grundlage für die Bekanntgabe von Personendaten an Dritte fehlte. In der Schlichtungsverhandlung konnte auf Vorschlag des Beauftragten eine Einigung erzielt werden. Demnach verfasste der Antragsteller einen Informationsbrief an die gewünschten Adressaten und die EAV versandte diesen Brief. Auf diese Weise musste die EAV dem Antragsteller das Adressverzeichnis nicht bekannt geben.

Schlichtung SBF / Maturanden-Statistik:

Die Antragstellerin ersuchte das Staatssekretariat für Bildung und Forschung um Auskunft über die Erfolgsquoten von Westschweizer Maturanden an öffentlichen und privaten Schulen. Die Beteiligten einigten sich an der Schlichtungsverhandlung darauf, dass die Behörde die privaten Schulen bezüglich der Herausgabe der Statistik anfragt und diese mit dem Einverständnis der jeweiligen Schule der Antragstellerin weiterleitet.

Schlichtung BFS / Stellenbesetzung:

Das Bundesamt für Statistik (BFS) verweigerte dem Antragsteller aus Datenschutzgründen den Zugang zu Informationen betreffend eine Stellenbesetzung im BFS. Nach telefonischer Vermittlung durch den Beauftragten konnten dem Antragsteller die gewünschten Dokumente zugestellt werden.

3. Der EDÖB

3.1 WebDatareg: Die Inbetriebnahme des Registers der Datensammlungen

Nachdem wir die Anmeldungen von Datensammlungen durch die Bundesämter nachgeführt hatten, liessen wir den Privatpersonen und Unternehmen, die Bundesaufgaben wahrnehmen, eine Kopie der vorhandenen Anmeldungen zur Überprüfung und gegebenenfalls zur Berichtigung der Daten zukommen. Darauf haben wir die erforderlichen Korrekturen vorgenommen und darüber hinaus den Internet-Teil durch die Einführung eines Moduls erweitert, das die Anmeldung von Datensammlungen durch die zahlreichen externen Bundesorgane ermöglicht. Neben der Online-Registrierung kann man mit dieser Anwendung auch nach bereits gemeldeten Datensammlungen suchen sowie die Anmeldungen einsehen und ausdrucken.

Im Laufe des vergangenen Geschäftsjahrs (vgl. unseren 15. Tätigkeitsbericht 2007/2008, Ziff. 3.1) haben wir bereits alle betroffenen Bundesämter mit dem Intranet-Bereich der Anwendung vertraut gemacht, damit sie noch vor dem Sommer 2008 auf elektronischem Weg ihre neuen Datensammlungen anmelden und nötigenfalls bereits vorhandene Anmeldungen ändern könnten.

Entsprechend unserer Planung liessen wir sodann im Frühjahr 2008 allen privaten Unternehmen sowie denjenigen, die Bundesaufgaben wahrnehmen (wie zum Beispiel Krankenkassen und Unfallversicherungen), eine Kopie der vorhandenen Anmeldungen zukommen mit der Bitte, deren Richtigkeit zu prüfen. Dieser umfangreiche Massenversand (über 600 Sendungen) hatte eine ganze Menge Rücksendungen, Fragen und Probleme zur Folge, sowie eine erhebliche Anzahl Anträge auf Berichtigung der angemeldeten Daten. Sobald die Neuerungen und Änderungen im Register aufgenommen waren, haben wir die Funktionalitäten des Internet-Teils der Anwendung zusätzlich erweitert und ein Anmeldungsmodul eingeführt für die Datensammlungen der zahlreichen Bundesorgane die nicht dem internen Netz des Bundes (Intranet) angeschlossen sind (so genannte externe Bundesorgane).

Der Internet-Teil von WebDatareg ging im November 2008 online. Seither ist es möglich, die Datensammlungen mittels eines PDF- oder XML-Formulars beim EDÖB anzumelden und die Details jeder im Register enthaltenen Anmeldung zu suchen, einzusehen und auszudrucken. Nach Eingang einer schriftlichen, unterzeichneten Bestätigung, mit der sich der Anmeldende authentifiziert, importieren wir seine Anmeldungs-

daten in das Register und sorgen dabei auch für die Übersetzung der Bezeichnung und des Zwecks der Datensammlung in die beiden anderen Landessprachen (diese Übersetzung wird nur für die Anmeldungen von Privatpersonen gewährleistet; die externen Bundesorgane haben diese Elemente bereits mitzuliefern).

Die Einführung des Internet-Teils von WebDatareg wurde von allen Betroffenen auf Anhieb begrüsst, namentlich wegen seiner stabilen und intuitiven Funktionsweise. Wir haben zudem mit unserem Hosting-Dienstleister, dem Bundesamt für Informatik und Telekommunikation (BIT), ein statistisches Analysemodul definiert, um die Besuchsstatistiken erstellen und überwachen zu können. Mit WebDatareg können wir nun ein modernes und leistungsfähiges Instrument für die Anmeldung von neuen Datensammlungen anbieten, das auch die bequeme Suche nach bereits im Register enthaltenen Sammlungen ermöglicht. Wir sind überzeugt, dass es uns damit gelungen ist, das Register der Datensammlungen als wertvolles Instrument der Öffentlichkeitsinformation zu aktualisieren und aufzuwerten.

3.2 3. Europäischer Datenschutztag

Am 28. Januar 2009 fand der 3. Europäische Datenschutztag statt. In diesem Rahmen wurden wiederum mehrere Datenschutzthemen in diversen Radiosendungen in der ganzen Schweiz aufgegriffen. Zudem waren wir an verschiedenen Veranstaltungen präsent.

Beweggrund des vom Europarat ins Leben gerufenen Datenschutztages ist die Sensibilisierung der Bevölkerung für den Schutz der Privatsphäre. Dieser Schutz hat mehrere Facetten. Zum einen arbeiten Gesetzgeber und Datenschutzbeauftragte an entsprechenden Rahmenbedingungen für die Bearbeitung von Personendaten. Zum anderen wird im Zusammenhang mit dem Internet das selbstverantwortliche Handeln der einzelnen Personen zunehmend wichtiger.

So hatte der Vortrag vom EDÖB, Hanspeter Thür, am Europa Institut der Universität Zürich die ersten Erfahrungen mit dem revidierten Datenschutzgesetz zum Thema, während Radiosendungen in der Deutschschweiz, der französischen und der italienischen Schweiz verschiedene aktuelle Themen aufgriffen, unter anderem soziale Netzwerke im Internet, Cybermobbing und Suchmaschinen. Weitere Themen waren Kundenkarten, die geplante Gesundheitskarte und generell die Sensibilisierung der Bevölkerung für den Datenschutz. Letztere ist ein konstantes Ziel unserer Arbeit.

3.3 Publikationen des EDÖB – Neuerscheinungen

Unsere Webseite ist ein wichtiges Instrument für die Öffentlichkeitsarbeit. Auch im vergangenen Berichtsjahr haben wir das Angebot an Informationen stetig erweitert und Ergebnisse unserer Arbeit veröffentlicht. In der Reihe der neuen Publikationen befinden sich unter anderem das «U.S.-Swiss Safe Harbor Framework», Erläuterungen zu «Pay as you drive»-Systemen, Sozialen Netzwerken und andern Internetplattformen sowie ein Leitfaden für biometrische Erkennungssysteme.

Mit der Revision des Bundesgesetzes über den Datenschutz (DSG) trat auch die revidierte dazu gehörende Verordnung Anfang 2008 in Kraft. Wir haben im Berichtsjahr auf unserer Webseite www.derbeauftragte.ch unter Der EDÖB – Rechtliche Grundlagen den Kommentar hierzu veröffentlicht. Zudem haben Inhaber von Datensammlungen neu die Möglichkeit, ihre Verfahren und Produkte sowie ihre Organisation zertifizieren zu lassen. Im letzten Jahr kamen wir dem gesetzlichen Auftrag nach und erliessen Richtlinien, Erläuterungen und weitere Begleitmaterialien für die Datenschutzzertifizierung. Sie finden die Dokumente unter Themen – Datenschutz.

Die Gesetzesrevision führte weiter zu Änderungen bei der Übermittlung von Personendaten ins Ausland. Unter Themen – Datenschutz – Übermittlung ins Ausland haben wir eine kurze und eine ausführliche Version von Erläuterungen zum Thema aufgeschaltet. Am selben Ort ist auch das in Zusammenarbeit mit dem Seco mit den USA ausgehandelte «U.S.-Swiss Safe Harbor Framework» zu finden.

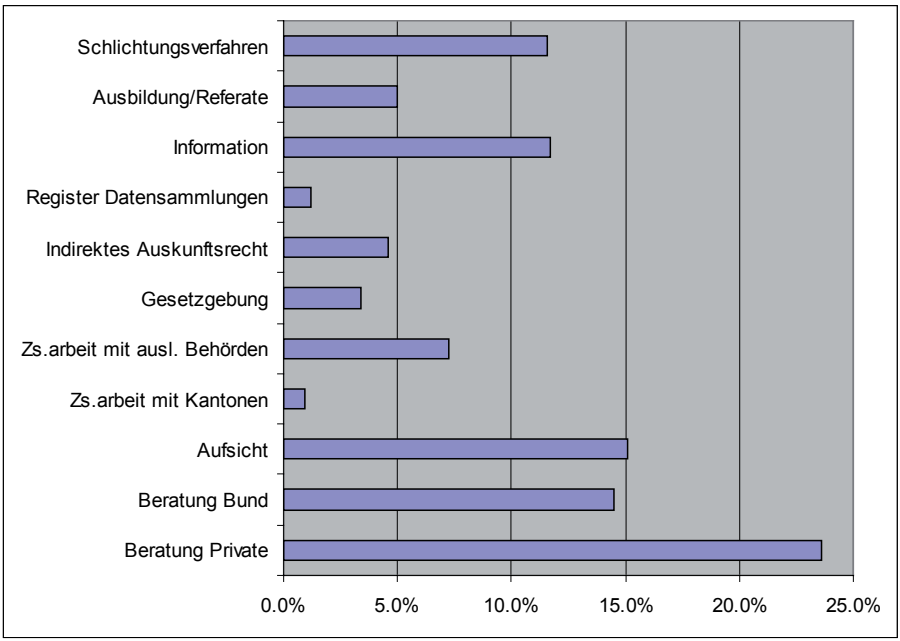
Neue Technologien stellen den Datenschutz vor grosse Herausforderungen. Deshalb haben wir Erläuterungen zu verschiedenen aktuellen Entwicklungen verfasst. Eine solche Neuerung sind «Pay as you drive»-Lösungen bei Motorfahrzeugversicherungen. Wo mittels einer Black-Box das Fahrverhalten von Versicherten aufgezeichnet wird, sind die datenschützerischen Grundsätze einzuhalten. Im Bereich des digitalen Fernsehens gilt dasselbe für die Aufzeichnung des Nutzungsverhaltens von Zuschauerinnen und Zuschauern. Hier können sensible Profile über betroffene Personen erstellt werden, die mit besonderer Sorgfalt zu behandeln sind. Ein neues Schlagwort ist der mCommerce – immer mehr Leute nutzen Bezahlsysteme, die es ermöglichen, per Mobiltelefon Rechnungen zu begleichen. Die damit verbundenen Risiken und zu beachtende Massnahmen haben wir unter dem Titel «Erläuterungen zu Mobile Payment» veröffentlicht. Weiter nutzen immer mehr Menschen die Angebote der Internet-Telefonie, das so genannte «Voice over IP» (VoIP). Da hier die Gespräche über die üblichen Internetkanäle erfolgen, besteht ein grosses Risiko der unrechtmässigen Abhörung. Hier müssen gerade einzelne User entsprechende Sicherheitsvorkehrungen treffen.

Das Internet ist auch in anderen Hinsichten ein Thema: Zum einen boomen Soziale Netzwerke wie Facebook oder MySpace mit bereits mehr oder weniger bekannten Risiken für die Persönlichkeit der betroffenen oder auch unbeteiligter Personen. Zum anderen verbreiteten sich im Berichtsjahr mehrere Bewertungssites auf internationaler oder regionaler Ebene, auf denen allerlei beurteilt wurde, vom Nachbarn über die Leistungen der Ärztin bis zur Vorlesung an der Universität. Auch zu diesen Themen legen wir unsere aktuellen Überlegungen dar, und zwar sowohl in entsprechenden Erläuterungen als auch in den beiden Ausgaben unseres Newsletters datum des Berichtsjahrs. Eine letzte neuere Entwicklung, die uns beschäftigt hat, ist der Jugendschutz an Automaten. In Deutschland haben Automatenbetreiber und Kreditinstitute Lösungen entwickelt, um auch an Automaten eine wirksame Alterskontrolle durchführen zu können. Wir betrachten diese Lösungen aus datenschutzrechtlicher Sicht. Zu finden sind alle diese Erläuterungen unter Themen – Datenschutz in den entsprechenden Unterrubriken.

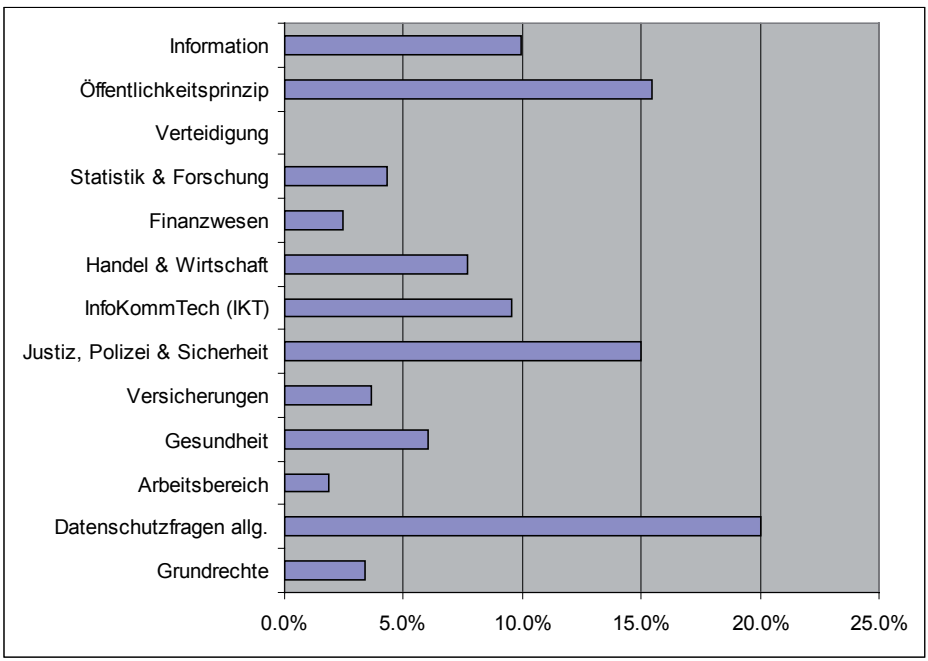
Ein Abbild unserer Zeit ist die zunehmende Tendenz, biometrische Zugangs- und Erkennungssysteme zu installieren. Deshalb haben wir für Entwickler und Anwender solcher Systeme einen entsprechenden Leitfaden publiziert. Er ist unter Dokumentation – Datenschutz – Leitfäden zu finden.

3.4 Statistik über die Tätigkeit des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (Zeitraum: 1. April 2008 bis 31. März 2009)

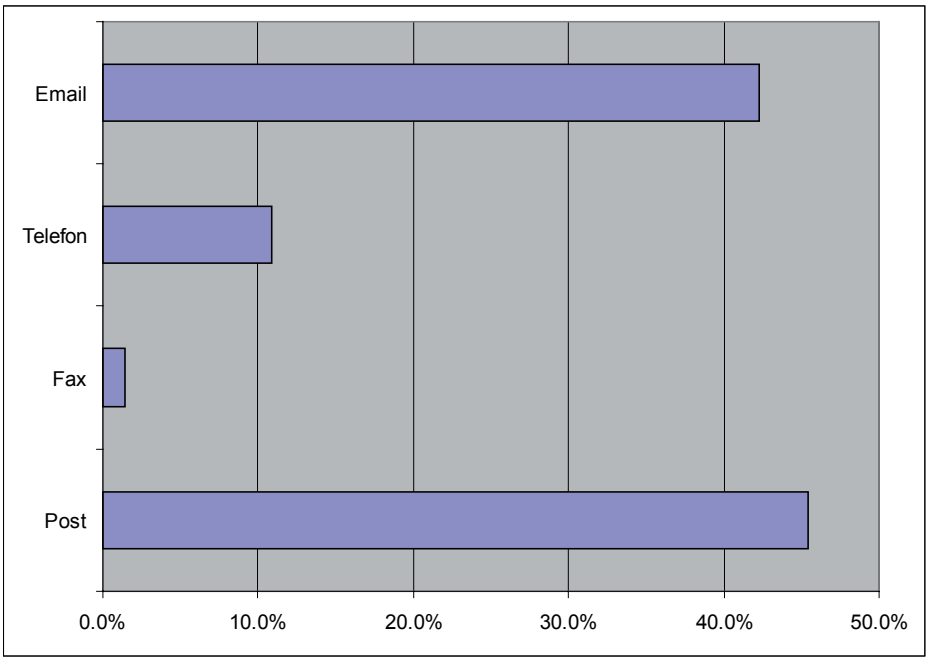
Aufwand nach Aufgabengebiet



Aufwand nach Sachgebiet



Herkunft der Anfragen



3.5 Statistik über die bei den Departementen eingereichten Zugangsgesuche nach Art. 6 des Öffentlichkeitsgesetzes (Zeitraum: 1. Januar 2008 bis 31. Dezember 2008)

Departement	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt / aufgeschoben
BK	31	22	3	6
EDA	20	11	7	2
EDI	29	9	11	9
EJPD	34	19	12	3
VBS	18	10	3	5
EFD	18	8	7	3
EVD	11	7	2	2
UVEK	60	29	26	5
TOTAL 2008 (in %)	**221** (100%)	**115** (52%)	**71** (32%)	**35** (16%)

TOTAL 2007 (in %)	**249** (100%)	**147** (59%)	**82** (33%)	**20** (8%)

Schweizerische Bundeskanzlei BK

Betroffener Fachbereich	Anzahl	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt / aufgeschoben
BK	8	6	0	2
EDÖB	23	16	3	4
TOTAL	**31**	**22**	**3**	**6**

Eidgenössisches Departement für auswärtige Angelegenheiten EDA

Betroffener Fachbereich	Anzahl	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt / aufgeschoben
EDA	20	11	7	2
TOTAL	**20**	**11**	**7**	**2**

Eidgenössisches Departement des Innern EDI

Betroffener Fachbereich	Anzahl	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt / aufgeschoben
GS EDI	5	4	1	0
EBG	0	0	0	0
BAK	1	0	1	0
BAR	0	0	0	0
METEO CH	0	0	0	0
BAG	8	3	1	4
BFS	0	0	0	0
BSV	7	0	4	3
SBF	2	1	0	1
ETH Rat	0	0	0	0
SWISSMEDIC	5	1	3	1
SNF	0	0	0	0
SUVA	1	0	1	0
TOTAL	**29**	**9**	**11**	**9**

Eidgenössisches Justiz- und Polizeidepartement EJPD

Betroffener Fachbereich	Anzahl	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt / aufgeschoben
GS EJPD	5	0	4	1
BJ	4	4	0	0
FEDPOL	5	3	0	2
METAS	0	0	0	0
BFM	15	12	3	0
BA	3	0	3	0
SIR	0	0	0	0
IGE	2	0	2	0
ESBK	0	0	0	0
ESchK	0	0	0	0
RAB	0	0	0	0
TOTAL	**34**	**19**	**12**	**3**

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS

Betroffener Fachbereich	Anzahl	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt / aufgeschoben
GS VBS/BIG	11	8	0	3
Verteidigung/ Armee	3	0	2	1
armasuisse	1	0	1	0
BABS	1	0	0	1
BASPO	2	2	0	0
TOTAL	**18**	**10**	**3**	**5**

Eidgenössisches Finanzdepartement EFD

Betroffener Fachbereich	Anzahl	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt / aufgeschoben
GS EFD	2	0	2	0
EFV	0	0	0	0
EPA	0	0	0	0
ESTV	3	2	1	0
EZV	1	0	0	1
EAV	3	1	0	2
BBL	0	0	0	0
BIT	0	0	0	0
BPV	3	0	3	0
EFK	6	5	1	0
PUBLICA	0	0	0	0
ZAS	0	0	0	0
TOTAL	**18**	**8**	**7**	**3**

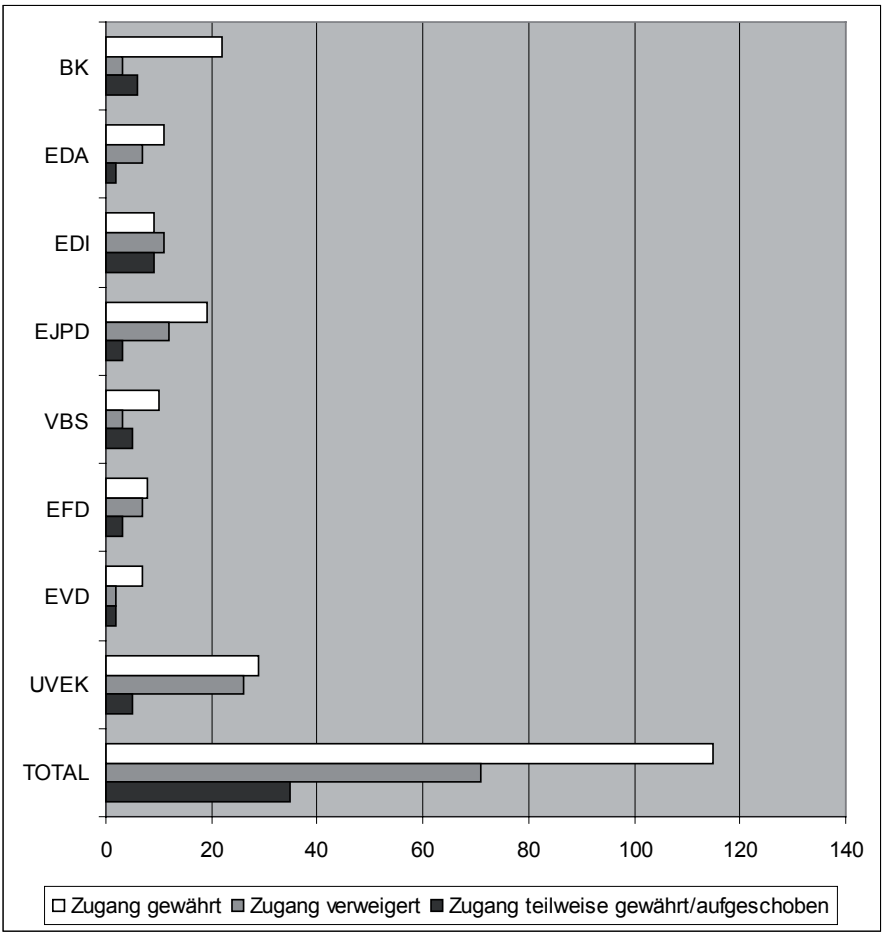
Eidgenössisches Volkswirtschaftsdepartement EVD

Betroffener Fachbereich	Anzahl	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt / aufgeschoben
GS EVD	4	4	0	0
SECO	2	2	0	0
BBT	1	0	0	1
BLW	2	1	1	0
BVET	1	0	0	1
BWL	0	0	0	0
BWO	0	0	0	0
PUE	0	0	0	0
WEKO	1	0	1	0
ZIVI	0	0	0	0
BFK	0	0	0	0
TOTAL	**11**	**7**	**2**	**2**

Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK

Betroffener Fachbereich	Anzahl	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt / aufgeschoben
GS UVEK	2	0	1	1
BAV	4	1	2	1
BAZL	20	11	9	0
BFE	2	0	2	0
ASTRA	1	0	1	0
BAKOM	8	5	3	0
BAFU	15	6	6	3
ARE	0	0	0	0
COMCOM	0	0	0	0
ENSI	5	3	2	0
PostReg	1	1	0	0
UBI	2	2	0	0
TOTAL	**60**	**29**	**26**	**5**

Behandlung der Zugangsgesuche



3.6 Statistik über die bei den Parlamentsdiensten eingereichten Zugangsgesuche nach Art. 6 des Öffentlichkeitsgesetzes (Zeitraum: 1. Januar 2008 bis 31. Dezember 2008)

Parlamentsdienste PD

Betroffener Fachbereich	Anzahl	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt / aufgeschoben
PD	0	0	0	0
TOTAL	**0**	**0**	**0**	**0**

3.7 Anzahl Schlichtungsgesuche nach Kategorien der Antragsteller (Zeitraum: 1. Januar 2008 bis 31. Dezember 2008)

Kategorie Antragsteller	2008
Rechtsanwälte	7
Medien	6
Privatpersonen (bzw. keine genaue Zuordnung möglich)	6
Interessenvertreter (Verbände, Organisationen, Vereine usw.)	3
Universitäten	2
Unternehmen	1
Total	**25**

3.8 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:	2 Personen
Kanzlei:	3 Personen

4 Anhänge

4.1 Datenschutz

4.1.1 Erläuterungen zu Sozialen Netzwerken

Vorwiegend junge Menschen wickeln heutzutage einen Teil ihres Soziallebens im Internet ab. Begünstigt wird dieser Trend durch die rasante Entwicklung im Bereich der neuen Kommunikationstechnologien. Wo immer mehr Privates ins Internet gestellt wird, ist auch der Datenschutz gefordert. Der EDÖB erläutert im vorliegenden Dokument Risiken und Gefahren der Social Networking Sites für die Privatsphäre und gibt an die Adresse der Involvierten Empfehlungen ab für einen verbesserten Schutz der Personendaten.

Benutzerinnen und Benutzer des Internets sind zunehmend nicht mehr nur «Konsumenten», die von Providern zur Verfügung gestellte Informationen auf statischen Websites suchen und downloaden, sondern benutzen das Internet interaktiver denn je und arbeiten kräftig an dynamischen Websites mit. Diese Entwicklung wird unter dem Begriff Web 2.0 zusammengefasst. Sowohl die steigende Verbreitung der Breitbandtechnologie, die die Prozesse des Up- und Downloadens bedeutend beschleunigt hat, wie auch die Entwicklung von Social Software hat diese veränderte Nutzung des Internets begünstigt. Immer mehr User sind in der Lage, in entscheidendem Umfang eigene Inhalte ins Internet zu stellen und sich zudem untereinander zu vernetzen.

In diesem Zusammenhang sind verschiedene Social Networking Sites (SNS) entstanden. Es sind dies umfangreiche Portale, in denen sich angemeldete Benutzerinnen und Benutzer treffen, Freundschaften schliessen und Nachrichten, Fotos und Filme austauschen. Dazu füllt man ein persönliches Profil aus unter Angabe von mehr oder weniger detaillierten Auskünften über die eigene Person, Vorlieben und Überzeugungen. Die bekanntesten Sozialen Netzwerke (Facebook, MySpace, StudiVZ etc.) gewinnen stetig zahlreiche Neumitglieder hinzu.

SNS stellen den Datenschutz vor neue Herausforderungen. Datenschutzgesetze waren ursprünglich darauf ausgerichtet, Personendaten vor der unrechtmässigen oder übermässigen Bearbeitung durch den Staat, später auch durch die Wirtschaft zu schützen. Mit den SNS sind nun zwei grundlegend neue Aspekte aufgetaucht:

1. Die genannten persönlichen Informationen werden von den Benutzern selber und also mit ihrer eigenen Einwilligung in die Internetprofile geladen.

2. Privatpersonen erhalten einen umfassenden Zugriff auf die Personendaten anderer Privatpersonen. Daraus können verschiedene Risiken entstehen.

SNS bergen viele Vorzüge für die Gesellschaft, so zum Beispiel die Möglichkeit, Networking zu betreiben, Kontakte über Landesgrenzen hinaus zu knüpfen oder eigene Inhalte zu publizieren. Es ist daher nicht die Absicht dieser Erläuterungen, SNS grundsätzlich zu verurteilen zu stellen. Das Ziel ist die Sensibilisierung der Behörden, Provider und User für einen korrekten und datenschutzkonformen Umgang mit Personendaten bei Sozialen Netzwerken.

Risiken und Gefahren

Die Benutzung des Internets ist aus der heutigen beruflichen und privaten Welt in unseren Breitengraden nicht mehr wegzudenken. Das Medium birgt verschiedene bekannte Gefahren, die auch in Sozialen Netzwerken drohen. Übeltäter können sich dabei die spezifischen Voraussetzungen der SNS zunutze machen. Zu diesen Voraussetzungen gehört unter anderem eine Neubesetzung der Begriffe Vertrauen und Vertraulichkeit. Wo Freundschaft zunehmend quantitative Aspekte hat, ist es unter Vorspiegelung falscher Tatsachen oder gar Annahme einer falschen Identität einfach, zum «Freund» von jemandem zu werden und also in Besitz von Informationen zu gelangen, die einem das Gegenüber in einem Gespräch von Angesicht zu Angesicht vielleicht nicht mitteilen würde. Die Behauptung solcher Netzwerke, man verlagere einzig die alltägliche Kommunikation unter Freunden ins Internet, suggeriert eine Intimität, die in einem weltweiten Medium nicht gegeben ist, zumal wenn die Zugangshürden zum Netzwerk niedrig sind.

Wer SNS unvorsichtig und ohne Vorkehrungen benutzt, setzt sich folgenden Risiken aus:

1. Das Internet kennt kein Vergessen: Benutzerprofile können von anderen Usern heruntergeladen und gespeichert werden, was die Löschung des Ursprungsprofils quasi nutzlos macht, bleiben so die Daten doch erhalten. So entsteht eine Unzahl von privaten Datensammlungen, und die Gefahr wächst, dass die Daten anders eingesetzt werden könnten als ursprünglich beabsichtigt. Aus-

serhalb der SNS bekannt gemacht können sie beispielsweise der betroffenen Person erheblich schaden. Solch private Sammlungen ermöglichen auch das Nachverfolgen von Anpassungen, die ein Profilinhaber vornimmt, und die Kategorisierung der Daten nach bestimmten Kriterien, z.B. mittels Suchfunktion.

2. Die SNS-Provider haben Zugriff nicht nur auf die Personendaten, sondern auch auf die Metadaten (Verbindungsdauer, grobe geografische Herkunft der IP-Adresse, Verweildauer und Bewegungen auf der Site, etc.). Bei vielen SNS-Anbietern ist unklar, was mit all diesen Daten geschieht. Klar ist: Personen- und Metadaten zusammen können ausführliche Persönlichkeitsprofile ergeben, deren Verkauf grosse Gewinne abwerfen dürfte.

3. Fotos mit erkennbaren Personen und zugeordneten Namen dienen der eindeutigen Identifikation der Abgelichteten. Mit spezieller Gesichtserkennungs-Software können SNS und andere Plattformen nach spezifischen Personen abgesucht werden. Diese können dann auch da, wo sie anonym bleiben wollen, z.B. auf einer Dating-Website, identifiziert oder dank des Fotos auf der SNS mit ihrem Lebenslauf auf einer Firmenwebsite in Verbindung gebracht werden.

4. In eine ähnliche Richtung geht die Gefahr des CBIR (content based image retrieval): Die automatische Wiedererkennung von Merkmalen im Hintergrund eines Bildes, z.B. ein spezifisches Gemälde oder Haus, kann zur geografischen Lokalisierbarkeit einer Fotosituation führen und die Bekanntgabe der Adresse, Stalking oder andere kriminelle Handlungen zur Folge haben.

5. Einige SNS erlauben weitgehende Verlinkungen mit Profilen oder Email-Adressen von Drittpersonen – durchaus auch solchen, die keine Mitglieder des Netzwerks sind – notabene, ohne deren Erlaubnis einzuholen. Dies kann zur Gefahr für die Privatsphäre jeder Person werden.

6. Benutzerkonti können praktisch nicht unwiderruflich gelöscht werden (siehe oben Punkt 1). Zum einen werden Profile z.T. nur «deaktiviert» statt gelöscht. Zum anderen hinterlassen aktive Benutzer viele zusätzlichen Informationen auf anderen Seiten des Netzwerks. Diese allumfassend zu löschen ist praktisch unmöglich. So verlieren Benutzerinnen und Benutzer die Kontrolle über ihre Daten.

7. Weitere Gefahren sind das so genannte Cross Site Scripting und schädliche Software (malware). Unter Ausnutzung von Computersicherheitslücken werden bspw. fehlerhafte Programmcodes eingeschmuggelt mit dem Ziel, an sensible Daten des Users zu kommen oder seinem Computer oder Profil Schaden zuzufügen.

8. Benutzer mehrerer SNS können die Bewirtschaftung ihrer Postfächer vereinfachen, indem sie alle in einer einzigen Webapplikation eingeben. So können sie mit einem Benutzernamen und einem Passwort alle aktuellen Nachrichten der eigenen Profile auf einen Blick einsehen, was praktisch sein mag, jedoch Sicherheitsbedenken weckt.

9. Bei den meisten SNS sind die Registrationshürden sehr niedrig: Man macht einige Angaben zur Person, die nicht verifiziert werden und also erfunden sein können. Einmal drin, ist es unter Umständen sehr einfach, Kontakte zu schliessen und in die Freundeskreise anderer aufgenommen zu werden. Das birgt Gefahren der Infiltration dieser Communities zu verschiedenen negativen Zwecken:

   a. Phishing: Übeltäter können so an zahlreiche Informationen kommen und zielgerichtete Phishing-Attacken lancieren mit dem Ziel, beispielsweise Zugangsdaten zu wichtigen Accounts, Bankinformationen etc. zu ergattern.

   b. Spammer können ebenso Profile eröffnen wie harmlose Benutzer. Daher droht auch in SNS-internen Kommunikationssystemen das altbekannte Problem des Spamming.

   c. Identitätsdiebstahl wird einfach gemacht: Man legt sich ein Profil mit dem Namen einer bekannten Person an und profitiert von deren Berühmtheit – oder schädigt ihren Ruf durch bösartiges Verhalten. Gleichermassen kann man ein Profil im Namen einer Person aus Schule oder Nachbarschaft eröffnen und ihr schaden, indem man sie lächerlich macht oder in ihrem Namen Bösartigkeiten verschickt.

10. Cyberstalking ist ein altes Phänomen neu verpackt: Die elektronischen Kontaktmöglichkeiten der SNS können böswillig dazu benutzt werden, jemanden zu bedrängen. Ausserdem kann die Menge an Daten, die die Benutzerinnen

und Benutzer über sich selber bekannt geben, durchaus dazu führen, dass jemand die Adresse seines Opfers herausfindet, seine Lebensgewohnheiten kennen lernt und die Person physisch verfolgen kann.

11. Auch Cyberbullying ist die Internet-Version eines in der Realität seit längerem bekannten Phänomens. Der Angreifer kann sich hinter einem gefälschten Profil verstecken, anonym bleiben und dabei die Möglichkeiten nutzen, die SNS bieten, um jemanden bösartig zu belästigen oder zu demütigen. Dies kann erst noch für andere Mitglieder der Community sichtbar getan werden, was den Schaden für das Opfer vergrössert.

Social Networking Services sind meistens gratis, aber sie sind keine gemeinnützigen Einrichtungen. Es findet ein «Handel» statt: Dienstleistungen für Benutzerinnen und Benutzer im Tausch gegen deren Daten. Hinter den Portalen steckt eine geballte Marktmacht, stecken führende internationale Unternehmungen, die unter dem Druck von Investoren und Aktionären wachsende Profite generieren müssen. Das einzige, was ein Social Networking Service anzubieten hat, sind Personendaten – und der Börsenwert eines SNS spricht Bände über deren Wert.

Soziales Netzwerken im Internet ist ein relativ neues Phänomen, und es werden laufend Erfahrungen gesammelt damit. Es ist daher auch wahrscheinlich, dass künftig neue Gefahren und Sicherheitslöcher auftauchen werden.

Empfehlungen an Behörden[1]:

Aus der Sicht des Datenschutzes sind folgende Empfehlungen zentral:

- Benutzerinnen und Benutzer solcher Social Networking Services sollen mit Kampagnen für die Gefahren sensibilisiert werden. Software-Hersteller sollen ermutigt werden, die Sicherheit der Personendaten zu berücksichtigen.
- Einführung eines Rechts der User, SNS pseudonymisiert zu benutzen;
- Erhöhte Transparenz: Im Hinblick auf existierende Datenschutzgesetze ist es angebracht, die Datenbearbeitungsmethoden der SNS-Anbieter unter die Lupe zu nehmen und allenfalls Korrekturen anzuregen. Die User sollten klar

[1] Folgende Empfehlungen basieren im Wesentlichen auf dem Rome Memorandum der International Working Group on Data Protection in Telecommunications. Siehe bibliografische Angaben am Textende.

unterrichtet werden über den Zweck der Datenbearbeitungen, eine allfällige Weitergabe der Daten oder die Geltendmachung von Auskunfts- und Berichtigungsrecht.

- Vorsicht mit Verboten: Statt die Benutzung von SNS zu verbieten, sollten Schulen sie (partiell) zulassen; so würde das Social Networking nicht gänzlich unkontrolliert vonstatten gehen. Zudem könnte die Aufklärung von Kindern, Lehrkräften und Eltern damit einhergehen.
- SNS-Provider sollten verpflichtet werden, Datenlecks bekannt zu geben. Damit wären die User informiert, und es würde sich zugleich zeigen, wie hoch der Sicherheitsstandard der SNS ist.
- Datenschutzunterricht: In Anbetracht des wachsenden Gebrauchs moderner Kommunikationsmittel durch Kinder und Jugendliche gehört Datenschutz unbedingt an die Schulen.

Empfehlungen an Anbieter:

- Stärkere Authentifizierung der Benutzerinnen und Benutzer: Das könnte bspw. via Postbestätigung passieren.
- Verbesserung der Möglichkeiten für User, Missbrauch und Regelverstösse auf der Webseite zu melden; bspw. mittels eines Buttons auf jeder Seite.
- Wahl passender Standardeinstellungen: Erfahrungsgemäss verändern wenige User die Grundeinstellungen von sich aus, daher ist es aus datenschützerischer Sicht zentral, dass die Einstellungen standardmässig datenschutzkonform sind.
- Schaffung und Promotion der Möglichkeit für User, unter Pseudonym zu surfen;
- Klare Informationen bezüglich der Datenbearbeitungen und allfälliger Weitergaben an Dritte; zudem müssen sich die Anbieter an gegebene Versprechen halten. Nur so kann Vertrauen entstehen.
- Einführung von Bewertungssystemen: Schaffung einer Möglichkeit für die User, sich gegenseitig zu bewerten. Es kann durchaus sinnvoll sein, sich im Kontakt mit Menschen, die man nicht persönlich kennt, auf die Erfahrungen von anderen zu stützen, die sich in solchen Ratings äussern. Die Online-Reputation gewinnt dadurch an Bedeutung, ein guter Ruf, verdient durch gutes Verhalten, wird erstrebenswert.

- Installation automatischer Filterwerkzeuge, die auf bestimmte Merkmale reagieren.
- Bessere Kontrolle des Users über seine Daten:
    - Schaffung einer praktischen Möglichkeit, Daten komplett zu löschen.
    - Das Untersagen des Anbringens von so genannten «tags» mit Personendaten (z.B. Bildbeschriftungen) ohne die Erlaubnis der betroffenen Person.
    - Wahlmöglichkeit für den User, welche seiner Daten in der SNS-Suchfunktion aufscheinen dürfen.
    - Generelle Kontrolle des Users darüber, was mit seinen Profil- und Bewegungsdaten passiert.

Empfehlungen an die Benutzinnen und Benutzer:

- Seien Sie vorsichtig bei der Veröffentlichung Ihrer Personendaten (Name, Adresse, Telefonnummer) und anderer persönlicher Informationen (bspw. politische Überzeugungen) auf einer SNS. Benutzen Sie Pseudonyme.
- Fragen Sie sich vor der Veröffentlichung immer, ob Sie in einem Bewerbungsgespräch mit den entsprechenden Daten konfrontiert werden möchten – und zwar auch noch in zehn Jahren. Schon heute suchen angeblich 2/3 der HR-Manager in SNS und Google nach Informationen über Bewerberinnen und Bewerber.
- Respektieren Sie die Privatsphäre Dritter, veröffentlichen Sie weder deren Personendaten noch beschriften Sie Fotos mit deren Namen.
- Informieren Sie sich über die Anbieter des Portals und wie die Privatsphäre der Nutzer gewährleistet wird. Hat der Dienst ein Datenschutz- oder -sicherheitsgütesiegel? Beobachten Sie das Verhalten des Anbieters kritisch.
- Wählen Sie in Ihrem Profil bei Ihren eigenen Einstellungen datenschutzkonforme Optionen. Geben Sie Ihre Informationen und Fotos nur für einen beschränkten Personenkreis frei. Stellen Sie heikle Inhalte nicht ins Internet.
- Benutzen Sie verschiedene Logins und Passwörter für verschiedene Dienste.
- Behalten Sie die Internetaktivitäten Ihrer Kinder im Auge.

Verschiedene europäische Datenschutzgremien haben sich bereits eingehend mit der Thematik befasst. Weitere Informationen finden Sie unter:

Frauenhofer-Institut für sichere Informationstechnologie SIT. Privatsphärenschutz in Soziale-Netzwerke-Plattformen. Darmstadt, 23. September 2008 (PDF).

http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf

http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf

http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_reputation_based_system.pdf

4.1.2 Erläuterungen zu Bewertungsplattformen im Intranet (November 2008)

1. Einleitung

Das Internet stellt heute die weltweit grösste Community dar und verwirklicht durch den freien Zugang zu Informationen jeglicher Art das Konzept eines global verfügbaren Wissensspeichers. Durch die Offenheit des Internets können fast zu jedem beliebigen Thema Informationen abgerufen werden, von den neusten wissenschaftlichen Erkenntnissen über brandaktuelle Zeitungsartikel bis hin zu Lokalinformationen über den Bäcker um die Ecke oder den alten Bekannten aus der Schulzeit.

Mit dem Aufkommen von sozialen Netzwerken unter dem Stichwort Web 2.0 sind eine Unzahl von Anwendungen (wie z.B. Bewertungsplattformen) geschaffen worden, mit denen Internetnutzer Informationen austauschen können. Bei solchen Anwendungen ist der Seitenbetreiber nicht mehr Informationslieferant; er stellt nur noch das Gefäss (seine Website) zur Verfügung als Plattform für die User, die darin eigene Inhalte für jedermann oder bestimmte Gruppen veröffentlichen können. In den meisten Fällen findet dabei keinerlei redaktionelle Kontrolle durch den Betreiber der Website statt.

Die Trennung von Gefäss und Inhalt in einem solchen Ausmass ist ein Novum des Internets, welches insbesondere bei der Garantie und Durchsetzung von Persönlichkeitsrechten eine erhebliche Rolle spielt. Viele Betreiber sind heute für die Inhalte der Websites nicht mehr verantwortlich und können sie auch nicht kontrollieren. Zudem wächst die Anzahl Internetseiten täglich. Dies sind zwei grosse Herausforderungen für den Persönlichkeitsschutz im Allgemeinen und den Datenschutz im Speziellen.

1.1 Entwicklungen und Herausforderungen bei Bewertungsplattformen

Ein Interesse an Bewertungen von und Informationen über Leistungen bestand schon lange vor dem Aufkommen des Internets. So greifen wir seit vielen Jahren zu Testberichten und Benotungen (wie bspw. vom Konsumentenschutz oder in Reise- oder Restaurantführer).

Traditionelle Anbieter von Bewertungen verfolgen meistens einen qualitativen Evaluationsansatz. Sie beauftragen Experten, eine Leistung oder ein Produkt gemäss gewissen Vorgaben detailliert zu begutachten, fassen die Resultate in einem Bericht zusam-

men und veröffentlichen ihn als Expertenmeinung im eigenen Namen. Damit ist der Anbieter – insbesondere in qualitativer Hinsicht – für den Inhalt der Veröffentlichung verantwortlich.

Daneben existiert der quantitative Bewertungsansatz, bei dem aus einer Vielzahl von Antworten statistisch signifikante Ergebnisse abgeleitet werden, um auf deren Basis Schlussfolgerungen über die Qualität von Produkten und Leistungen zu ziehen. Der quantitative Ansatz ist für Anbieter von traditionellen Bewertungen meist zu aufwändig und zu kostspielig, da eine grosse Anzahl an Nutzern/Konsumenten befragt werden muss.

Mit dem Aufkommen des Internets haben quantitative Ansätze an Bedeutung gewonnen, da die Sammlung von Informationen über ein elektronisches Medium zu geringsten Kosten möglich ist. Bei der Beurteilung der Qualität solcher quantitativen Erhebungen sind die dahinter stehenden mathematischen Modelle bezüglich der Aussagekraft der Ergebnisse von entscheidender Bedeutung. Somit ist die Qualität der hieraus resultierenden Bewertung von dem Prozess der Datenbearbeitung abhängig, während sie beim qualitativen Ansatz von den Fähigkeiten des Experten abhängt.

Durch das Aufkommen von Bewertungswebsites im Internet hat sich eine Mischform zwischen beiden Evaluationsansätzen entwickelt. Einerseits geben die Webseiten einen Bewertungsrahmen vor, welcher darauf abzielt, in strukturierter Form Informationen von einer grösseren Anzahl Nutzer zu sammeln, anderseits bieten sie den Nutzern die Möglichkeit, in Kommentarfeldern qualitative Aussagen zu machen. Die Auswertung und Darstellung solcher Evaluationen erfolgt allerdings oft nach dem Muster qualitativer Erhebungen, da meist nicht die notwendige Anzahl an Befragungen erreicht wird, um statistisch signifikante Aussagen treffen zu können. Doch sind die Evaluatoren vorwiegend nicht speziell befähigte Experten, die aufgrund ihres Wissens und einer Systematik bewerten, sondern gewöhnliche Internetnutzer, die ihre Meinung kundtun.

In diesem Zusammenhang stellt sich also die Frage, inwiefern die im Rahmen solcher Evaluationen erhobenen Informationen aussagekräftig und repräsentativ sind.

1.2 Bewertungsplattformen im Internet

Im Internet findet man verschiedene Formen von Bewertungsseiten. Oft sind diese in anderen Plattformen (wie z.B. online-Shops oder online-Auktionshäuser) integriert. Es gibt aber auch eigenständige, die nur die Bewertung der betroffenen Zielgruppe oder Person zum Zweck haben (wie z.B. Ärztebewertungen, Bewertungen von Unterrichtskursen, etc.).

1.2.1 Integrierte Bewertungsplattformen

Integrierte Bewertungsplattformen werden vorwiegend in Verbindung mit dem Kauf eines Produkts (z.B. Kauf über einen Marktplatz, Ersteigerung über ein Auktionshaus) oder einer Dienstleistung (z.B. Nutzung einer Website zum Videosharing) angeboten. Nach der Abwicklung des Online-Geschäfts werden Verkäufer und/oder Kunde bzw. Konsument gebeten, eine Bewertung abzugeben. Diese besteht meist aus einer Note und einem Kommentar.

Der Zweck solcher Bewertungsplattformen liegt darin, eine spezifische Aktion unmittelbar zu beurteilen. Die Beurteilung findet direkt nach dem Konsum statt, der Konsument kann dem Produkt oder Service direkt zugeordnet werden. Aus diesem Grund sind integrierte Plattformen in der Regel unproblematisch, solange über die Bewertungsfunktion keine ehrverletzenden, unnötig herabsetzenden oder beleidigenden Werturteile abgegeben werden. Zudem sind solche Bewertungsplattformen technisch meist so ausgestaltet, dass eine Bewertung nur dann möglich ist, wenn zuvor eine Transaktion stattgefunden hat (sei es durch den Konsum eines Videos oder durch den Kauf eines Produkts oder Services). In vielen Fällen kann (z.B. weil die Transaktion kostenpflichtig ist) zudem eine Bewertung nur dann abgegeben werden, wenn sich der jeweilige Benutzer registriert hat.

Aus ökonomischer Sicht bezwecken integrierte Bewertungsplattformen vorwiegend, die Reputation der Anbieter von Produkten oder Services auf der Verkaufsplattform aufzubauen. Da im Internet kaum ein persönlicher Kontakt möglich ist und ein direkter persönlicher Eindruck in der virtuellen Welt schwer zu vermitteln ist, werden Bewertungsplattformen beispielsweise genutzt, um beim Konsumenten das Vertrauen in die Verkäufer zu stärken. Damit wird die Unsicherheit der Nutzer reduziert.

1.2.2 Eigenständige Bewertungsplattformen

Im Gegensatz dazu haben eigenständige Bewertungsplattformen vorwiegend den Zweck, die Öffentlichkeit über die Qualität einer bestimmten Leistung zu informieren. Die Anwendungsbereiche sind vielfältig und reichen von der Beurteilung von Kochrezepten und Pauschalreisen bis hin zur Bewertung von einzelnen Firmen und Personen innerhalb einer Kategorie, wie z.B. Ärzte, Lehrer und Professoren.

Die einzelnen Bewertungswebsites unterscheiden sich in ihrer Funktionsweise nur unwesentlich. In den meisten Fällen wird auf der Website ein zu bewertendes Element (z.B. Professor, Kurs, Arzt oder aber auch ein Bild) dargestellt, welches von den Benutzern an Hand eines vorgefertigten Formulars mittels Likert-Skala (z.B. Note 1 bis 6) und Kommentarfeld bewertet werden kann.

Je nach Ausgestaltung der Website können Benutzer selbst das zu bewertende Element auf der Website eintragen, oder es wird vom Betreiber der Website zur Verfügung gestellt. Die nachfolgende Tabelle zeigt, auf welche Arten das zu bewertende Element.publiziert werden kann.

Einstellen des zu bewertenden Elements (z.B. Professor, Kurs, etc.)		
Eingabe durch betroffene Person	Eingabe durch Betreiber der Website	Eingabe durch Betreiber der Website

Tabelle 1: Eingabe des zu bewertenden Elements

Um Bewertungen abgeben zu können, müssen sich Nutzer in der Regel auf den Websites registrieren. Allerdings ist auf einem Teil der Seiten auch eine anonyme Abgabe von Bewertungen möglich. Die unterschiedlichen Möglichkeiten der Abgabe einer Bewertung sind in der nachfolgenden Tabelle dargestellt (Tabelle 2).

Abgabe der Bewertung		
Abgabe anonym möglich	Abgabe nach Registrierung möglich	Abgabe nur aufgrund einer speziellen Berechtigung möglich

Tabelle 2: Ausgestaltung der Bewertungsmöglichkeiten

Die in den beiden Tabellen aufgeführten Kategorien können zur Klassifizierung und datenschutzrechtlichen Beurteilung der jeweiligen Bewertungswebseiten beigezogen werden. Je nach Ausgestaltung der Seite stellen sich daher für die Betreiber unterschiedliche Anforderungen an die Sammlung von Bewertungen sowie deren öffentliche Bekanntgabe im Internet.

2 Ausgewählte Beispiele

Nachfolgend werden drei verschiedene auf dem Internet verfügbare eigenständige Bewertungswebseiten vorgestellt und beschrieben.

2.1 Bewertung von Bildern und Videos

Bestimmte Webpages bieten Personen die Möglichkeit, ein Bild oder Video von sich bzw. von einer anderen Person auf die Website zu stellen und dieses von den Usern bewerten zu lassen. Besucher der Website erhalten zufällig ein Bild oder Video angezeigt und werden aufgefordert, dieses mit einer Note zwischen 1 und 10 zu bewerten. Nach der Abgabe der Bewertung wird das bisherige Umfrageergebnis angezeigt.

Bei korrekter Verwendung der Website gibt die betroffene Person selbst das zu bewertende Element (ein Foto von sich selbst) ein und stellt es den Besuchern der Website zur Bewertung zur Verfügung. Die User können ihre Bewertung nach Betrachtung des Bildes anonym abgeben.

Aus datenschutzrechtlicher Sicht ist eine solche Website unproblematisch, solange gewährleistet wird, dass nur die betroffene Person Bilder über sich veröffentlicht. Auf der Website hat der jeweilige User ausschliesslich die Möglichkeit, das ihm angezeigte Bild oder Video zu bewerten. Daher kann die Bewertung auch anonym erfolgen.

2.2 Bewertung von Ärzten

Ein anderes Beispiel ist eine Website zur Bewertung von Ärztinnen und Ärzten. Auf einer solchen Seite könnten Besucher zum Beispiel anhand von Name, Vorname, Ort, Kanton und Spezialisierung nach Ärzten suchen und für diese danach in drei verschiedenen Kategorien (Empfang und Team, Verwaltung, Arzt) eine Bewertung abgeben. In jeder Kategorie kann der Besucher den Arzt beispielsweise anhand von einer gewissen Anzahl von Kriterien auf einer Likert-Skala von 1 bis 6 (wobei 1 der schlechteste und 6 der beste Wert ist und zudem auch die Bewertung «Keine Meinung» zur Verfügung steht) bewerten.

Der Name des betroffenen Arztes wird von den Betreibern der Website zur Verfügung gestellt. Die Benutzer der Website können ihre Bewertungen anonym abgeben. Eine Abgabe der Bewertung, ohne jemals bei dem betroffenen Arzt gewesen zu sein, ist ohne weiteres möglich.

Aus datenschutzrechtlicher Sicht können bei diesem Beispiel zwei unterschiedliche Problembereiche identifiziert werden. Auf der einen Seite ist nicht gewährleistet, dass der betroffene Arzt überhaupt weiss, dass er im Internet evaluiert wird. Auf der anderen Seite ist es problematisch, dass die Bewertungen anonym abgegeben werden können. Somit ist nicht gewährleistet, dass allfällig geübte Kritik aus unmittelbaren, eigenen Erfahrungen bei dem Arzt erwächst.

2.3 Bewertung von Hochschulkursen

Des Weiteren kommen im Rahmen der Bewertung von Lehrern und Professoren Webseiten auf, über welche registrierte Nutzer Kurse und Dozenten evaluieren können. Hierzu melden sie betreffende Kurse bzw. Dozenten auf der Plattform an und bewerten diese dann entsprechend auf einer Likert-Skala von «sehr schlecht» bis «sehr gut» in Kategorien wie «Fairness», «Unterstützung», «Material», «Verständlichkeit», «Spass», «Interesse» und «Verhältnis Aufwand/Note». Zudem hat der Nutzer die Möglichkeit, den Kurs weiterzuempfehlen und einen Kommentar abzugeben.

Der Name des Dozenten wird entweder durch diesen selbst oder durch Benutzer der Plattform zur Verfügung gestellt. Die Benutzer der Website können ihre Bewertung nur mit einem Login abgeben. Eine Abgabe der Bewertung, ohne jemals an einem Kurs teilgenommen zu haben, ist ohne weiteres möglich.

Kritisch zu betrachten ist aus datenschutzrechtlicher Sicht, dass jeder registrierte Nutzer Kurse erfassen kann. So können beispielsweise Kurse von Dozenten ohne deren Wissen evaluiert werden, was gegen das Erkennbarkeitsprinzip verstösst. Nutzer können aber auch Kurse bewerten, welche sie nie besucht haben, oder sie können aus persönlichen Gründen übertrieben schlechte Bewertungen abgeben. Zwar ist eine Registrierung auf der Website notwendig, doch der Nutzer kann eine anonyme Emailadresse verwenden und damit letztendlich seine Bewertungen anonym abgeben, obwohl die Betreiber der Website dies eigentlich untersagen.

3 Datenschutzrechtliche Grundproblematik und Risiken

Datenschutzrechtliche Problematik

Jede Veröffentlichung von Personendaten auf einer Webseite stellt eine Datenbearbeitung gemäss Art. 3 lit. e des Bundesgesetzes über den Datenschutz (DSG, SR 235.1) dar. Für den Betreiber einer Bewertungswebsite spielt es hierbei keine Rolle, ob er selbst (bzw. seine Mitarbeiter) oder Dritte diese Daten bearbeiten. Er muss sich auch deren

Datenbearbeitung zurechnen lassen, da er das Raster vorgibt und somit massgeblichen Einfluss auf die Bewertung und die Darstellung der Ergebnisse nimmt. Zudem ist er (gemäss Art. 3 lit. i DSG) Inhaber der Datensammlung, entscheidet er doch über deren Zweck und Inhalt. Dabei gilt es zu prüfen, ob die Grundsätze der Datenbearbeitung, insbesondere deren Erkennbarkeit (Art. 4 Abs. 4 DSG), eingehalten wurden. Zudem bedarf es, wenn kein überwiegendes privates oder öffentliches Interesse und keine gesetzliche Grundlage vorliegen, für die Datenbearbeitung der Einwilligung der betroffenen Person (Art. 13 DSG). Für den Betrieb von Bewertungswebseiten ist kein Rechtfertigungsgrund ersichtlich, darum ist grundsätzlich die Einwilligung der betroffenen Person notwendig.

Persönlichkeitsrechtliche Problematik

Für eine persönlichkeitsrechtliche Beurteilung von Bewertungswebseiten braucht es grundsätzlich eine Grundrechtsabwägung zwischen der freien Meinungsäusserung und den Persönlichkeitsrechten der betroffenen Person.

Bei der freien Meinungsäusserung wird grundsätzlich zwischen Tatsachenbehauptungen und Werturteilen unterschieden. Tatsachenbehauptungen müssen der Wahrheit entsprechen, beweisbar sein und werden grundsätzlich nicht als persönlichkeitsverletzend eingestuft. Werden jedoch Tatsachen behauptet, welche nicht allgemein bekannt und von sensiblem Gehalt sind, kann deren Veröffentlichung die Privatsphäre der betroffenen Person verletzen.

Werturteile sind im Vergleich hierzu Äusserungen persönlicher Ansichten oder Schlussfolgerungen über eine bestimmte Person oder einen Sachverhalt. Gemäss ständiger Rechtssprechung durch das Bundesgericht sind Werturteile zulässig, solange diese vertretbar erscheinen und nicht unnötig herabsetzend oder beleidigend sind.

Bei den auf eigenständigen Bewertungswebseiten dargestellten Evaluationsergebnissen handelt es sich meist um Werturteile, da in der Regel weder die Erhebungsarten (in quantitativer oder qualitativer Hinsicht) anerkannten statistischen Methoden genügen noch die Evaluatoren eine ausreichende inhaltliche Nähe zum beurteilten Element aufweisen, um die Ergebnisse als Tatsachenbehauptungen zu qualifizieren. Resultiert daraus eine Persönlichkeitsverletzung, muss der Betreiber der Website dafür geradestehen.

3.1 Risiken für Betreiber von Bewertungsplattformen

Für die Betreiber bestehen je nach Art der Bewertungsplattform unterschiedliche datenschutzrechtliche Risiken, welche anhand der Kategorisierungen in Tabelle 1 und Tabelle 2 sowie der Art der Evaluation (quantitativ, qualitativ, ereignisbezogen) beschrieben werden können.

Risiken aufgrund einer fehlenden Erkennbarkeit/Zustimmung der Datenbearbeitung

Damit eine betroffene Person durch eine Datenbearbeitung bedingte Persönlichkeitsverletzungen frühzeitig erkennen kann, schreibt das DSG in Art. 4 Abs. 4 vor, dass die Beschaffung von Personendaten und insbesondere der Zweck ihrer Bearbeitung für die betroffene Person erkennbar sein muss. Aus diesem Grund muss der Betreiber der Bewertungsplattform dafür sorgen, dass eine betroffene Person die Datenbearbeitung im Vornherein erkennen kann.

Falls die zu evaluierenden Informationen von der betroffenen Person selbst veröffentlicht worden sind, kann der Betreiber der Plattform von deren Zustimmung ausgehen. Werden hingegen die zu evaluierenden personenbezogenen Informationen durch den Betreiber oder einen beliebigen User auf der Plattform veröffentlicht, ist dies für den Betroffenen erst einmal nicht erkennbar. Wenn der Betreiber in einem solchen Fall die betroffenen Personen nicht informiert und ihre Einwilligung nicht einholt, verletzt er gemäss Art. 12 Abs. 2 lit. a DSG (i.V.m. Art. 4 Abs. 4 DSG) bzw. Art. 12 Abs. 2 lit. b DSG deren Persönlichkeit. Wenn besonders schützenswerte Personendaten oder Persönlichkeitsprofile bearbeitet werden, muss gemäss Art. 4 Abs. 5 DSG die Einwilligung ausdrücklich erfolgen. In anderen Fällen kann sie implizit geschehen, wenn gewährleistet ist, dass die betroffene Person angemessen informiert wurde und freiwillig einwilligt.

Risiken aufgrund von persönlichkeitsverletzenden Evaluationen

Evaluationen auf Bewertungswebseiten sind in der Regel als Werturteile zu qualifizieren (siehe oben) und dürfen nicht unnötig herabsetzend oder beleidigend sein. Der Betreiber einer solchen Seite gibt die einzelnen Evaluationen in der Regel nicht selbst ein und aggregiert sie meist automatisiert. In der Folge kann er nicht abschätzen, ob die auf seiner Webseite präsentierten Evaluationsergebnisse unnötig herabsetzend oder beleidigend sind (z.B. wenn Evaluationsergebnisse von bestimmten Nutzern ungerechtfertigt negativ beeinflusst werden). Je weniger statistisch signifikant die Evaluation ist und je grösser die inhaltliche Distanz zwischen Evaluator und Evaluationsobjekt, desto höher ist auch das Risiko einer Persönlichkeitsverletzung der betroffenen Person.

Persönlichkeitsverletzungen können weiter durch die Eingabe von unnötig herabsetzenden oder beleidigenden Kommentaren auf der Bewertungswebseite entstehen. Der Betreiber der Seite muss ausreichende Vorsichtsmassnahmen treffen, um entsprechende Kommentare umgehend zu löschen.

Die Risiken solcher Persönlichkeitsverletzungen steigen, wenn Bewertungen anonym abgegeben werden können. Bei registrierten Benutzern ist dieses Risiko geringer, besteht aber weiter, da meist eine Registrierung unter Verwendung einer falschen Emailadresse möglich ist.

3.2 Risiken für betroffene Personen

Die von einer Evaluation betroffene Person kann in ihrer Persönlichkeit verletzt werden, insbesondere, wenn die Ergebnisse ein falsches Bild abgeben oder wenn Nutzer systematische Falschbewertungen vornehmen. Die Gefahr einer falschen Tatsachenbehauptung ist umso grösser,

1. je geringer die Anzahl der abgegebenen Bewertungen ist (fehlende statistische Signifikanz),
2. je weniger qualifiziert der begutachtende Evaluator ist (fehlende Kompetenz),
3. je geringer der inhaltliche Bezug des Evaluators und der zu evaluierenden Sache ist (fehlende inhaltliche Nähe).

Daher hängt das Risiko einer Falschbewertung für die von einer Evaluation betroffenen Personen von der Ausgestaltung der Bewertungswebsites ab. Können zum Beispiel Bewertungen anonym abgegeben werden, so können auch Nutzer eine Evaluation durchführen, welche weder über die Kompetenz noch über ausreichende Informationen verfügen. Wenn eine Bewertungsplattform noch dazu die Ergebnisse schon bei einer geringen Anzahl von durchgeführten Bewertungen veröffentlicht, steigt das Risiko einer systematischen Falschbewertung.

3.3 Risiken für Personen, welche Bewertungen abgeben

Nutzer einer Bewertungsplattform müssen sich bei der Abgabe von Bewertungen bewusst sein, dass es sich meist um ein gemischtes Werturteil handelt und dieses nicht unnötig herabsetzend oder beleidigend sein darf. Ansonsten müssen sie mit einer Klage wegen Persönlichkeitsverletzung oder schlimmstenfalls mit einer Strafklage wegen Ehrverletzung rechnen.

Kann der Nutzer hingegen seine Bewertung anonym abgeben, ist für ihn das Risiko, belangt zu werden, gering. Dennoch muss er sich bewusst sein, dass es theoretisch über seine IP-Adresse möglich ist, ihn nach Abgabe der Bewertung zu identifizieren.

4 Massnahmen und Empfehlungen

Grundsätzlich sollten Betreiber ihre Bewertungsplattformen so ausgestalten, dass das Risiko einer Datenschutz- bzw. Persönlichkeitsverletzung möglichst minimiert wird. Droht eine Persönlichkeitsverletzung, müssen sowohl der Betreiber als auch die betroffene Person schnell handeln, um Schaden für alle Beteiligten abzuwenden oder zu begrenzen. Zur datenschutzkonformen Ausgestaltung der Datenbearbeitung stehen dem Betreiber, der betroffenen Person und dem Nutzer der Bewertungsplattform die nachfolgend beschriebenen Möglichkeiten zur Verfügung.

4.1 Massnahmen für den Betreiber der Bewertungswebseite

Grundsätzlich muss der Betreiber einer Bewertungswebseite diese so ausgestalten, dass Persönlichkeitsverletzungen möglichst verhindert werden. Um die je nach Ausgestaltung der Webseite zu treffenden Massnahmen zu identifizieren, werden die Kategorisierungen von Tabelle 1 und Tabelle 2 herangezogen.

4.1.1 Die betroffene Person initiiert die Evaluierung und gibt sie frei

Wenn die betroffene Person das zu bewertende Element auf eine Webseite lädt und zur Bewertung durch die Nutzer frei gibt, so erfolgt die Evaluation mit deren Einverständnis. Der Betreiber der Webseite muss dann lediglich dafür sorgen, dass Nutzer keine ehrverletzenden oder beleidigenden Äusserungen publizieren. Wird ihm ein entsprechender Missstand gemeldet, so muss er diesen unverzüglich beheben.

4.1.2 Dritte stellen die Evaluierung bereit

Wenn entweder der Betreiber der Webseite oder ein Nutzer der Webseite zu bewertende Elemente (welche einen Personenbezug aufweisen) einstellen kann, so ist dies für die betroffene Person erst einmal nicht erkennbar und erfolgt ohne deren Zustimmung. Daher muss der Betreiber die betroffene Person informieren, bevor die Evaluation durchgeführt wird, und (falls er nicht über einen ausreichenden Rechtfertigungsgrund verfügt) von ihr die Zustimmung zur Durchführung der Evaluation einholen.

4.1.3 Dritte können die Bewertung anonym abgeben

Spezielle Anforderungen an die Datenerhebung gelten, wenn anonyme Bewertungen möglich sind. Um in einem solchen Fall überhaupt verwertbare Informationen zu erhalten, muss die Evaluation so durchgeführt werden, dass die Ergebnisse robust und statistisch signifikant sind. Dies ist allerdings nur bei einer grossen Anzahl von unabhängigen Evaluationen möglich. Zudem müssen die bewertenden Nutzer eine gewisse inhaltliche Nähe zum bewerteten Element aufweisen. Der Betreiber muss daher dafür sorgen, dass die Evaluationsergebnisse erst veröffentlicht werden, wenn eine genügend grosse Anzahl an Bewertungen abgegeben wurde und diese von verschiedenen Personen stammen, die inhaltlich zur Evaluation befähigt sind (z.B. weil sie das zu bewertende Bild gerade im Browser gesehen haben).

Grundsätzlich ist bei anonym abgegebenen personenbezogenen Bewertungen aufgrund des Risikos einer Persönlichkeitsverletzung höchste Vorsicht geboten.

4.1.4 Dritte müssen sich zur Abgabe von Bewertungen registrieren

Nachdem sich eine betroffene Person registriert hat, kann sie in der Regel keine anonymen Bewertungen mehr abgeben, sofern sie sich nicht mit falschen Daten eingeschrieben hat. Aus diesem Grund muss der Betreiber einer Bewertungswebseite Massnahmen ergreifen, um das Risiko einer anonymen Registrierung und damit das Risiko einer Persönlichkeitsverletzung zu minimieren.

Auch ein wahrheitsgemäss registrierter Nutzer kann eine Evaluation durchführen, obwohl er das zu bewertende Objekt überhaupt nicht kennt. Immerhin kann er aber bei Streitfällen identifiziert und es können Massnahmen gegen ihn ergriffen werden.

4.1.5 Der Nutzer wird zur Evaluation ermächtigt

Ist die Bewertungsplattform so ausgestaltet, dass der Nutzer eine Bewertung nur dann abgeben kann, wenn die betroffene Person ihn zur Bewertung zugelassen hat, so braucht der Betreiber der Seite keine weiteren Massnahmen zu ergreifen.

Wird dem Betreiber einer Bewertungswebseite allerdings ein Misstand gemeldet (beleidigender Kommentar seitens eines Nutzers), so hat er diesen unverzüglich zu beheben.

Die nachfolgende Tabelle gibt nochmals einen Gesamtüberblick über die Ausgestaltungsmöglichkeiten von Bewertungswebseiten.

Ausgestaltung der Bewertung / Massnahmen des Daten-/ Persönlichkeitsschutzes		Keine	Zustimmung durch betroffene Person	Erkennbarkeit Rechtfertigungsgrund	Hohe Anzahl an Bewertungen	Qualifizierte Begutachter	Inhaltliche Nähe zum Evaluationsobjekt
Eingabe des zu bewertenden Elements	Eingabe durch betroffene Person	√	√	√			
	Eingabe durch Betreiber der Website	x	√	√			
	Eingabe durch beliebigen User	x	√	√			
Abgabe derBewertung	anonym	!! !			√	x	!
	nach Registrierung	!			√	√	√
	nach spezieller Ermächtigung	√			√	√	√

Tabelle 3: Möglichkeiten der Gestaltung von Bewertungswebseiten

Aus datenschutzrechtlicher Sicht sind Bewertungswebseiten, bei welchen die betroffene Person die Evaluation selbst veröffentlicht und gezielt Nutzer zur Evaluation einladen kann, am wenigsten problematisch.

Wenn das zu evaluierende Element nicht durch die betroffene Person veröffentlicht wird, muss diese vor Beginn der Evaluation darüber informiert und ihre Zustimmung eingeholt werden.

Anonyme Bewertungen können aus Sicht des EDÖB nur unter ganz speziellen Voraussetzungen zugelassen werden, sind aber in der Regel abzulehnen.

4.2 Massnahmen für betroffene Personen

Da von einer Evaluation betroffene Personen grundsätzlich vorgängig darüber informiert und um ihre Zustimmung gebeten werden müssen, dürf(t)en keine ihr unbekannten Evaluationen stattfinden. Zudem hat die betroffene Person gegenüber dem Betreiber der Bewertungsplattform jederzeit die Möglichkeit, ihre Zustimmung zurückzuziehen und die Evaluation samt Ergebnissen löschen zu lassen, es sei denn, der Betreiber kann Gründe geltend machen, welche die Weiterbearbeitung der Daten rechtfertigen.

Erfährt eine Person, dass im Internet eine sie betreffende Evaluation (welcher sie nicht zugestimmt hat) stattfindet, kann Sie gegenüber dem Betreiber jederzeit ihr Löschungsrecht geltend machen und ihn auffordern, die Evaluation unverzüglich zu beenden sowie die Ergebnisse nicht weiter zu veröffentlichen. Dazu stellt der EDÖB unter www.derbeauftragte.ch Musterbriefe zur Löschung von Daten zur Verfügung. Kommt der Betreiber dem Löschungsbegehren nicht nach, kann die betroffene Person ihr Rechte von einem Zivilrichter durchsetzen lassen.

4.3 Massnahmen für Nutzer von Bewertungswebseiten

Die Bewertung von Leistungen im Internet hat Auswirkungen auf die evaluierte Person. Ein Nutzer trägt mit seiner Teilnahme an einer Evaluation aktiv zur öffentlichen Meinungsbildung über die Evaluierten bei. Gerade deshalb sollten solche Webseiten in keinem Fall dazu verwendet werden, den bewerteten Personen «eins auszuwischen». Vielmehr sollten Evaluatoren sich ihrer Verantwortung bewusst sein und nur Bewertungen abgeben, wenn sie über ausreichende Informationen verfügen und kompetent sind.

4.1.3 Erläuterungen zum digitalen Fernsehen, zu ITV und IPTV (Mai 2008)

Bis zur Gegenwart haben sich hauptsächlich die beiden Technologien des digitalen Fernsehens (DVB) und des Fernsehens über das Internet (IPTV) durchgesetzt, so dass dem Publikum ein breites Angebot an Programmen zur Verfügung steht. Die in den letzten Jahren aufkommende Konvergenz der Medien Telefon, Internet und Fernsehen eröffnet neue Geschäftsmöglichkeiten für Telekommunikations- und Medienanbieter. Durch den Breitbandzugang zum Internet steht den Konsumenten und Fernsehanbietern ein Rückkanal zur Verfügung, welcher die interaktive Gestaltung von Fernsehprogrammen ermöglicht.

Vorwiegend zwei Entwicklungen haben ein interaktives digitales Fernsehen ermöglicht. Zum einen kann sich durch die immer grössere Bandbreite des Internets das Internet-TV in DVB-Qualität entwickeln. Zum anderen kann das digitale Fernsehen durch den Einzug des Internets in immer mehr Haushalte einen breitbandigen Rückkanal nutzen.

Digitales Fernsehen mit breitbandigem Rückkanal

Durch den heute zur Verfügung stehenden Rückkanal ist es dem Anbieter technisch möglich, mit dem Zuschauer in direkten Kontakt zu treten und diesem so einen individualisierten Fernsehzugang zu ermöglichen. Unter dem Begriff «Video-on-demand» bieten einige (vor allem Pay-TV-) Sender den Zuschauern bereits die Möglichkeit an, sich durch freie Filmwahl das eigene Programm zusammenzustellen.

Weiterhin ist es denkbar, dass der Kunde während dem Fernsehen Zusatzinformationen abrufen kann. So wäre es beispielsweise heute schon möglich, den Lebenslauf des gerade handelnden Schauspielers abzurufen oder direkt eine Buchung in einem im Programm gezeigten Hotel vorzunehmen.

Der Rückkanal ermöglicht aber auch dem Kabelnetzbetreiber, Informationen über das Fernsehverhalten und somit über die Interessen des Kunden zu erheben, um ihm individualisierte Werbeangebote zu unterbreiten.

Internet-TV in DVB-Qualität

Die heute vorhandenen Breitbandverbindungen ermöglichen es, Videoangebote über das Internet in einer angemessenen, aber mittelmässigen Qualität bereitzustellen. Obwohl allerdings über Webseiten wie z.B. YouTube.com oder peekvid.com verschiedene Videoangebote zur Verfügung gestellt werden, existieren heute nur wenige Fernseh-

sender, welche ihr Programm vollständig über das Internet anbieten, da zum einen hierfür noch keine ausreichende Nachfrage besteht, und zum anderen vielerorts die Bandbreite noch nicht ausreichend ist, um den Empfang in einer dem DVB-Standard äquivalenten Qualität zu ermöglichen.

Heutzutage nutzen zum Beispiel Online-Zeitungen die Möglichkeiten des IPTV, um neben den auf ihrer Seite publizierten Artikeln ihre Nachrichten auch als Video-Stream zu verbreiten und einfache Sendungen zu produzieren. Daneben existiert eine ganze Reihe von Webseiten, wo digitalisierte (Heim-)Videos oder Filme und Fernsehserien online zum Download angeboten werden.

Das Internet ist seit jeher ein zweiseitiges Kommunikationsmedium, welches die Interaktion des Nutzers mit dem Anbieter erlaubt. Daher ist es für die interaktive Gestaltung von Fernsehprogrammen geeignet. Zudem nutzt der Konsument bereits einen Computer und ist auf eine aktive Kommunikation mit Maus oder Tastatur eingestellt, was die Nutzung von interaktiven Angeboten eher begünstigt. Im Gegensatz hierzu wird der durchschnittliche Digital-TV-Nutzer eine intensive Interaktion mit dem Fernsehgerät eher als störend empfinden.

Risiken

Aus datenschutzrechtlicher Perspektive stellen sich durch die Möglichkeiten der Sammlung von personenbezogenen Nutzungsdaten verschiedene Fragen, welche nachfolgend erörtert werden.

Risiken für Zuschauer

Aufgrund des dauerhaften und breitbandigen Rückkanals wird es in Zukunft möglich sein, Daten über das Nutzungsverhalten des Fernsehzuschauers zu erheben, ohne dass dieser davon Kenntnis hat. Er weiss also weder welche Daten so über ihn und seinen Fernsehkonsum gesammelt noch welche Personendaten vom Kabelnetzbetreiber gespeichert werden.

Somit kann vom einzelnen Fernsehzuschauer ein Zuschauerprofil erstellt werden, welches über seine Wünsche und Neigungen weitgehende Auskünfte gibt. Da es sich hierbei mitunter um höchst sensible Personendaten handeln kann (z.B. Informationen über die sexuellen Neigungen einer Person) muss der Fernsehzuschauer aus Sicht des EDÖB jederzeit erkennen können, wann personenbezogene Daten erhoben werden, und er muss die Möglichkeit haben, diese jederzeit zu unterdrücken.

Diese Risiken bestehen vorwiegend beim digitalen Fernsehen mit breitbandigem Rückkanal, da über das Kabelnetz eine ganze Reihe an Fernsehsendern übertragen wird und der Kabelnetzbetreiber prinzipiell Daten über das gesamte Konsumverhalten des Zuschauers erheben kann.

Auch beim IPTV könnte das Konsumverhalten des Nutzers durch den jeweiligen Betreiber aufgezeichnet werden. Da aber nicht alle Angebote aus einer Quelle stammen, ist das Risiko einer Überwachung des gesamten Konsumverhaltens weitaus geringer.

Risiken für die Kabelnetzbetreiber

Die Kabelnetzbetreiber müssen sich bewusst sein, dass sie für die Erhebung von personenbezogenen Daten das Einverständnis des Kunden einholen müssen, wenn nicht öffentliche oder private Interessen überwiegen oder eine rechtliche Grundlage für die Datenbearbeitung besteht. Dem Fernsehnutzer muss dabei transparent dargelegt werden, welche Daten über ihn zu welchem Zweck wann, wo und wie bearbeitet werden. Grundsätzlich hat der Zuschauer ein Recht darauf, dass nur ein Minimum an bestimmten oder bestimmbaren Personendaten zur Aufgabenerfüllung (wie beispielsweise für die Rechnungsstellung) verwendet wird. Für Zusatzdienste hingegen sind anonymisierte oder pseudonymisierte Daten zu benutzen. In jedem Fall muss für den Zuschauer die unbeobachtete Nutzung des Fernsehens ohne Nachteile möglich sein.

Vor allem durch personalisierte Werbeangebote, welche auf das Profil des jeweiligen Kabelanschlusses abgestimmt sind, könnten sich einzelne Zuschauer gestört fühlen, was zu Beschwerden führen könnte.

Die grössten Risiken für die Kabelnetzbetreiber werden im drohenden Vertrauensverlust der Fernsehzuschauer bei einer übermässigen Datensammlung durch den Betreiber gesehen. Dies könnte dazu führen, dass Fernsehzuschauer in der Zukunft verstärkt auf Satellitenempfang (DVB-S) umsteigen, da hier kein Rückkanal zur Verfügung steht.

Risiken für Anbieter von interaktiven DVB-Diensten

Auch Anbieter von interaktiven DVB-Diensten müssen bei der Datenerhebung die Grundsätze des Datenschutzes beachten und dürfen nur diejenigen personenbezogenen Daten über Nutzer erheben, welche sie zur Bereitstellung ihrer Dienste benötigen. In diesem Zusammenhang kann weitgehend auf die bisherige Praxis des Datenschutzes im digital commerce verwiesen werden.

Massnahmen

In den meisten Fällen werden für die Bereitstellung von interaktivem Kabelfernsehen keine personenbezogenen Daten benötigt, welche über das Nutzungsverhalten des Fernsehzuschauers Auskunft geben. Eine Ausnahme könnte beispielsweise die Nutzung von Angeboten im Pay-per-View-Modus sein, falls der Kunde eine detaillierte Einzelabrechnung wünscht. Daher muss der Fernsehzuschauer in den weitaus meisten Fällen seine Einwilligung für die Datenbearbeitung durch die Kabelnetzbetreiber oder Anbieter von DVB-Dienstleistungen geben.

Um die Informationssicherheit beim Digitalfernsehen zu gewährleisten, sollte die Verwendung von Personendaten technisch und organisatorisch einzig auf den Vertragsabschluss und die Serviceleistungen beschränkt werden. Im Hinblick auf letztere muss der Kunde zusätzlich die Möglichkeit haben, zu bestimmen, welche personenbezogenen Daten über seinen Fernsehkonsum gespeichert werden. Auch sollte der Zuschauer nach Meinung des EDÖB selbst entscheiden können, ob er beispielsweise eine detaillierte Aufstellung der konsumierten Filme erhalten möchte.

Heute kann der einzelne Fernsehzuschauer keine Massnahmen zur Verhinderung eines unerwünschten Datentransfers zum Anbieter des digitalen Fernsehens ergreifen. Künftig wären bspw. spezielle Firewalls für das Fernsehgerät denkbar. Sie könnten eine solche Übertragung entweder direkt unterbinden oder den Zuschauer darauf aufmerksam machen, dass ein Datentransfer stattfindet und ihm die Möglichkeit geben, seine Einwilligung zu verweigern.

Daneben erachtet es der EDÖB als sehr wichtig, dass die Kabelnetzbetreiber die Systeme von Anfang an datenschutzkonform ausgestalten. Dies bedeutet, dass weitgehend auf die Erhebung von Personendaten verzichtet wird oder dass bereits erhobene anonymisiert werden. Im Weiteren muss das Kabelnetz die Informationssicherheit gewährleisten.

Auch im digitalen Fernsehen muss die unbeobachtete Nutzung des Fernsehens ohne Nachteile möglich bleiben. Daher schlägt der EDÖB folgende Massnahmen vor:

Weitgehender Verzicht auf Personendaten

Die personenbezogene Datenerhebung im Rahmen der Nutzung des digitalen Fernsehens sollte technisch auf ein Minimum beschränkt werden und nur da möglich sein, wo dies unbedingt notwendig ist. Dies ist aus Sicht des EDÖB beim Vertragsabschluss und bei den Serviceleistungen der Fall. Zudem sollte der Kunde selbst darüber ent-

scheiden können, ob er beispielsweise im Hinblick auf seinen Fernsehkonsum Einzelabrechnungen erhalten möchte oder nicht. Um dies zu ermöglichen müssen die Anbieter von Fernsehprogrammen ihren Kunden entsprechend informieren.

Zudem sollten die Anbieter dafür sorgen, dass technisch nur diejenigen Mitarbeitenden Zugriff auf die personenbezogenen Daten haben, welche diesen unbedingt benötigen.

Vor allem zu Marketingzwecken und für personalisierte Werbung sind aus Sicht des EDÖB keine personenbezogenen Daten notwendig. Daher sind die für diese Zwecke erhobenen Daten entweder zu anonymisieren oder mindestens zu pseudonymisieren, so dass eine Zuordnung des Fernsehverhaltens zu einzelnen Personen nicht möglich ist.

Transparente Information der Betroffenen

Kabelnetzbetreiber müssen die betroffenen Personen transparent sowohl über die Datenbearbeitungen als auch das Informationssystem in Kenntnis setzen. Dies beinhaltet auch die Angabe, welche Daten wann und wo bearbeitet (bspw. an wen weitergeleitet) und wann sie gelöscht werden. Selbstverständlich gilt auch gegenüber den Betreibern von Kabelnetzen oder Anbietern von IPTV-Diensten das Auskunftsrecht der Betroffenen. Hierbei ist es, ebenfalls aus Transparenzgründen, notwendig, die Kunden darauf aufmerksam zu machen, dass und wann über den Rückkanal personenbezogene Daten von Ihnen gesammelt werden können. Zudem muss den Kunden die Möglichkeit eröffnet werden, einen Transfer personenbezogener Daten vom Fernsehgerät an den Anbieter zu unterbinden.

4.1.4 Erläuterungen zu «Pay as you drive» und dem Einsatz von Black Boxen in Motorfahrzeugen (Mai 2008)

Moderne Versicherungstarife für Motorfahrzeuge setzen sich aus mehreren Kriterien zusammen, mit welchen Versicherer versuchen, eine risikogerechte Prämie anzubieten. Bisher haben sie zur Risikoeinschätzung vorwiegend Informationen basierend auf bestimmten Zustandsdaten (Fahrzeugtyp, PS, etc.) und ereignisbezogene Verhaltensdaten (wie Schadensfälle oder Administrativmassnahmen) erhoben. Unter dem Namen «Pay as you drive» (PAYD) evaluieren in letzter Zeit allerdings immer mehr Versicherungen die zusätzliche Nutzung von ereignisunabhängigen Verhaltensdaten (wie das tägliche Fahrverhalten), um den einzelnen Kundinnen und Kunden individualisierte Motorfahrzeugsversicherungen anzubieten.

Die technischen Lösungen zur Erhebung der gewünschten Verhaltensdaten reichen von einer einfachen Erfassung der gefahrenen Kilometer über eine Tankkarte an der jeweiligen Tankstelle bis hin zu einem vollautomatischen und kommunikationsfähigen Datenaufzeichnungsgerät (Black Box), welches sämtliche Fahrzeugbewegungen und Reaktionen des Lenkers aufzeichnet und an das Versicherungsunternehmen weiterleitet. Nachfolgend werden die datenschutzrechtlichen Herausforderungen der vier wichtigsten PAYD-Lösungen kurz vorgestellt:

- Milage Monitoring: Der Versicherungsnehmer verfügt über eine Servicekarte, mit welcher er (z.B. beim Tanken) regelmässig den Kilometerstand seines Fahrzeuges an den Versicherer übermittelt, der den Tarif entsprechend anpasst.
- Journey Monitoring: Neben den gefahrenen Kilometern werden, entweder per GPS oder auf Autobahnen via Mautsystem, zusätzlich Route und Tageszeit erfasst. Entsprechend der Risikoeinschätzung der gewählten Route und Tageszeit wird dann der Versicherungstarif angepasst.
- Passive Black Box: Es handelt sich um ein im Fahrzeug installiertes Aufzeichnungsgerät, welches zusätzlich das Fahrverhalten (abruptes Bremsen, Beschleunigen, etc.) aufzeichnet und speichert. Nach dem Auslesen der Daten kann ein individueller Versicherungstarif berechnet werden.
- Aktive Black Box: Dieses Gerät verfügt zusätzlich über eine Kommunikationseinheit und übermittelt der Versicherung laufend Daten.

Da durch diese neuen technischen Möglichkeiten nahezu beliebig viele Daten über das Bewegungsverhalten der betroffenen Personen erhoben werden können, stellen sich besondere datenschutzrechtliche Fragen. Der EDÖB macht auf denkbare Risiken beim Einsatz von PAYD-Tarifen aufmerksam und zeigt Möglichkeiten auf, wie aus datenschutzrechtlicher Perspektive mit diesen Risiken umgegangen werden sollte.

Risiken

Risiken für Versicherungsnehmer

Mit der Einführung von PAYD-Lösungen könnte es zu tief greifenden Veränderungen im Versicherungsmarkt für Motorfahrzeuge kommen. Es stellt sich die Frage, in wieweit sich ein Kunde einer PAYD-Lösung überhaupt entziehen könnte. Der in der ökonomischen Theorie bekannte Effekt der «adverse selection» könnte Versicherungsnehmer mit geringem Risiko dazu veranlassen, aufgrund der Preisvorteile einen PAYD-

Tarif zu wählen. Bei den herkömmlichen Tarifen verblieben lediglich die risikoreichen teuren Versicherten und solche, denen die PAYD-Datenbearbeitungen zu weit gehen, was zu einem signifikanten Anstieg der Prämien führen könnte. Je nachdem wie stark ein solcher Preisanstieg wäre, könnten sich Versicherte gezwungen fühlen, in den PAYD-Tarif zu wechseln, um keine übermässigen finanziellen Nachteile zu erleiden. Das würde bedeuten, dass sich Versicherte faktisch nicht mehr gegen die Erstellung eines auf ihrer Fahrweise beruhenden Persönlichkeitsprofils wehren könnten.

Über die Motorfahrzeugversicherung hinaus könnte ein solcherart erstelltes Risikoprofil auch für weitere Versicherungen verwendet werden. Es könnte insbesondere in die Risikoberechnung bei Lebens-, Invaliditäts- und Unfallversicherungen Eingang finden, was im schlimmsten Fall dazu führen könnte, dass der Versicherungsgeber es ablehnt, die betroffene Person aufzunehmen, und diese keine Möglichkeit mehr hat, sich gegen entsprechende Risiken zu versichern. Dies ist schwerwiegend, weil zur Erstellung eines Risikoprofils die Datenerhebung über eine gewisse Zeit hinweg notwendig ist. Je nach Planungshorizont des Versicherungsgebers könnte sich durch Verhaltensänderungen des Versicherungsnehmers sein tatsächliches Risikoprofil ändern. Je nachdem, wie lange die Versicherungsgesellschaft die Verhaltensdaten der betroffenen Person speichert und zur Auswertung heranzieht, könnten sich dadurch Verzerrungen im aufgezeichneten Persönlichkeitsprofil des Versicherten ergeben.

Die stärkere Segmentierung der Tarifmodelle könnte zudem dazu führen, dass sich die Schere zwischen hohen und niedrigen Beiträgen weiter öffnet.

Risiken für Versicherer

Vor allem in der Transformationsphase zwischen den bisherigen Tarifen und den PAYD-Tarifen könnte es bei Versicherungen, welche sich entschliessen, PAYD nicht einzuführen, zu einer systematischen Abwanderung von Versicherungsnehmern kommen. Dies könnte sich für die Versicherungen negativ auf die Risikostrukturen auswirken, was dann letztendlich zu einer Erhöhung der Beitragssätze führen könnte. Hierdurch würden weitere Versicherungsnehmer animiert, zu anderen Anbietern mit PAYD-Tarifen zu wechseln. Das Resultat wäre eine ungleiche Risikoverteilung, da diejenigen Versicherungen, welche PAYD anbieten, sowohl einen Informationsvorsprung hätten als auch vermehrt Kunden mit geringerem Risiko anziehen würden. Kunden mit einem höheren Risikoprofil würden vermehrt bei Versicherungen mit lediglich traditionellen Tarifen verbleiben.

Auf der anderen Seite kann auch die Einführung einer PAYD-Lösung beim Versicherungsgeber zu höheren Kosten führen. Dies ist auf der einen Seite dann der Fall, wenn dieser die Kosten für den Einbau einer Black Box zu tragen hat. Auf der anderen Seite

können je nach Art der gewählten Lösung zusätzliche Kosten für den Betrieb und die Verwaltung der gesammelten Daten entstehen – insbesondere, wenn das Versicherungsunternehmen sie zentral speichert.

Massnahmen

In naher Zukunft ist davon auszugehen, dass das Angebot aufgrund noch fehlender Standards bei PAYD sehr heterogen ausfallen wird. Ausserdem erwarten wir, dass die herkömmlichen Tarifmodelle zumindest auf mittlere Frist erhalten bleiben werden und lediglich die bisher bereits bestehenden ereignisbezogenen Tarifelemente, welche Rückschlüsse auf das Fahrverhalten zulassen (wie gefahrene Kilometer, Führerausweisentzüge, Unfälle, etc.) in die Versicherungsprämie einfliessen werden. Daher wird eine weitergehende PAYD-Versicherungsprämie, welche unabhängig von bestimmten Ereignissen das Fahrverhalten analysiert, lediglich eine Option bleiben, welche ein Versicherungsnehmer wählen kann, wenn er davon finanziell profitieren möchte.

Grundsätzlich dürfen personenbezogene Daten, welche mittels eines PAYD-Systems erhoben werden, immer nur mit dem Einverständnis des Versicherungsnehmers bearbeitet werden. Daher ist es zunächst zentral, dass er vor dem Entschluss für ein PAYD-Modell detailliert über die Art und den Umfang der über ihn zu bearbeitenden Personendaten informiert wird. Insbesondere muss die betroffene Person wissen, welche Daten wann, wie und in welcher Häufigkeit erhoben, gespeichert oder ausgewertet werden, sei es mittels einer Black Box oder auf andere Weise.

Die Erfahrung hat allerdings gezeigt, dass neue Möglichkeiten der Datenerhebung, sobald sie einmal eingeführt sind, schnell neue Begehrlichkeiten wecken können. Daher ist es notwendig, klare gesetzliche Regelungen zu schaffen, unter welchen Umständen beispielsweise Strafverfolgungsbehörden Zugriff auf die in einer solchen Black Box gespeicherten Daten haben sollen.

Empfehlungen

Grundsätzlich müssen bei der Sammlung von ereignisunabhängigen Nutzungsdaten, welche über das Fahrverhalten Aufschluss geben, insbesondere durch Installation von Black Boxen, die Datenschutzgrundsätze beachtet werden. Hierbei gilt es, von vorne herein festzulegen, zu welchem Zweck die Daten verwendet werden, und eine entsprechende Selektion der unbedingt notwendigen Daten vorzunehmen. Damit soll vermieden werden, dass alle möglichen Informationen auf Vorrat gesammelt werden.

Zudem darf die Sammlung ereignisunabhängiger Verhaltensdaten nicht zu einem «gläsernen Fahrer» führen, über dessen Fahrverhalten ein detailliertes Personenprofil erhoben wird. Genauso wenig darf ein komplettes Bewegungsprofil des Fahrers erstellt werden. Um exzessive personenbezogene Auswertungen zu vermeiden, sollte zudem auf die zentrale Datenspeicherung verzichtet werden. Denn damit könnten die Bewegungsprofile verschiedener Fahrer verglichen werden, was dann Rückschlüsse auf ganz andere Lebenssachbereiche zulassen würde.

Da es für Aussenstehende zudem oft nicht nachvollziehbar ist, was beispielsweise in einer Black Box aufgezeichnet wird, ist es sowohl für den Versicherer wie auch für den Versicherungsnehmer eine Vertrauensfrage, wie mit diesen sensiblen Personendaten umgegangen wird.

Beschränkung der Abrufbarkeit von Daten (Vorauswertung)

Da ereignisunabhängige Fahrverhaltensdaten meist über ein Aufzeichnungsgerät erhoben werden, welches über eine eigenständige Recheneinheit verfügt (wie z.B. eine Black Box), könnte bereits eine Vorauswertung innerhalb dieser Recheneinheit vorgenommen werden. Anstatt alle Primärdaten aufzuzeichnen, würden dann nur noch berechnete Sekundärdaten, welche der Versicherer zur Ausgestaltung seines PAYD-Tarifs benötigt, verwendet. Dies hätte den Vorteil, dass die Datenauswertung dezentral erfolgen würde und der Versicherer nur noch aggregierte Daten abrufen könnte. Aus solchen wäre es dem Versicherer dann kaum noch möglich, mit geänderten Auswertungsalgorithmen weitergehende und eventuell zweckfremde Auswertungen vorzunehmen, was bei der Auswertung von Primärdaten ohne weiteres möglich ist.

Beschränkter Zugriff auf die in der Black Box gespeicherten Daten

Eine im Fahrzeug installierte «Black Box» muss grundsätzlich vor Missbrauch und vor externen Zugriffen geschützt sein. Da sie personenbezogene Daten speichert, sollte lediglich der Benutzer des Fahrzeugs über diese Daten verfügen können. So muss eine Black Box, welche über eine Kommunikationseinheit verfügt, dahingehend geschützt sein, dass kein unberechtigter Dritter über diese Kommunikationseinheit Daten abrufen kann.

4.1.5 Empfehlung betreffend der Internetseite www.okdoc.ch der Firma Bonus.ch AG

Siehe Abschnitt 4.1.5 im französischen Teil des Berichtes

4.1.6 Empfehlung an die Dienstleistung «Auskunftservice A» der Firma X

Bern, den 16.12.2008

Empfehlung

gemäss

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

betreffend

die Dienstleistung «Auskunftservice A» der Firma X

I. Sachverhalt

1. Die Firma X und ihre Dienstleistung «Auskunftservice A»

1 Die Firma X ist eine Tochtergesellschaft der Firma Y. Im Rahmen ihrer Tätigkeit als Wirtschaftsauskunftei sammelt und speichert sie Daten, um sie Dritten zur Bonitätsprüfung ihrer Kunden und Geschäftspartnern zur Verfügung zu stellen.

2 Die Firma X bietet die in ihrer Datenbank gespeicherten Daten zielgruppenspezifisch über die Internetplattform als Dienstleistung «Auskunftservice A» an. Der «Auskunftservice A» ist eine Applikation, mit welcher die gespeicherten Daten automatisiert aufbereitet und ausgewertet werden können. Diese Auswertung kann über die Plattform X-Online im Abrufverfahren bezogen werden. Damit können zugangsberechtigte Personen über Suchmasken Bonitäts- und Wirtschaftsinfor-

mationen der betroffenen Personen abfragen, um Mieterangaben zu prüfen und Mietzinsausfälle zu vermeiden. Ausserdem können ergänzende Informationen, wie Betreibungsauskünfte, Arbeitgeber- und Vermieter-Referenzen, eingeholt bzw. angefordert werden.

2. Chronologischer Ablauf der Sachverhaltsabklärung

3 Der EDÖB wurde erstmals am 01.04.2008 durch eine Mitteilung einer betroffenen Person auf die Existenz des «Auskunftservice A» aufmerksam gemacht, worauf-hin er am 08.04.2008 zwecks Sachverhaltsabklärung mit der Firma X Kontakt aufnahm.

4 Parallel hierzu bereitete das Schweizer Fernsehen einen Beitrag zum «Auskunftservice A» vor. In einer Sendung wurde dann der «Auskunftservice A» thematisiert. Auch wurde ein vorher aufgezeichnetes Interview mit dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten Hanspeter Thür ausgestrahlt.

5 Am 04.06.2008 nahmen Vertreter des EDÖB die Datenbearbeitung der Firma X betreffend «Auskunftservice A» vor Ort in Augenschein. Die Ergebnisse der Sitzung wurden in einem Sitzungsprotokoll[1] zusammengefasst, welches durch die Firma X mit einigen Ergänzungen[2] gutgeheissen wurde.

3. Umfang der Sachverhaltsabklärung

6 Zwischen der ersten Kontaktaufnahme am 08.04.2008 und der Augenscheinnahme des «Auskunftservice A» durch den EDÖB hat die Firma X verschiedene Anpassungen und Änderungen der Dienstleistung vorgenommen. Demzufolge wird vor diesem Hintergrund auf die ursprüngliche, von den Medien aufgegriffene Version des «Auskunftservice A» in den Erwägungen des EDÖB nur insoweit eingegangen, als dies notwendig ist.

7 Obwohl die Praxis der Firma X hinsichtlich der Gewährung des Auskunfts- und Löschungsrechtes bereits im Jahr 2006 vom EDÖB überprüft wurde, nahm der EDÖB die Sachverhaltsabklärung zum «Auskunftservice A» zum Anlass, diese vor dem Hintergrund des geänderten und erweiterten Dienstleistungsangebots erneut ab-

[1] Beilage 1, Sitzungsprotokoll.
[2] Beilage 2, Schreiben vom 17.07.2008.

zuklären. Dies war vorwiegend deshalb notwendig, da die Firma X im Rahmen des «Auskunftservice A» ihren Kunden nicht nur wie bisher die von ihr gespeicherten Daten anbietet, sondern zudem speziell aufbereitete, miteinander verknüpfte und mit einem Rating versehene Daten zur Verfügung stellt.

8 Diese Sachverhaltsabklärung ist keine Bewertung der gesamten Tätigkeit der Firma X, sondern sie bezieht sich nur auf die Beurteilung des «Auskunftservice A».

4. «Auskunftservice A»

4.1 «Auskunftservice A» in der ursprünglichen Form

9 In der ursprünglichen Form präsentierte sich der «Auskunftservice A» dem EDÖB aufgrund der von verschiedenen Personen eingereichten Unterlagen, der von der Firma X zugesandten Unterlagen, der vom EDÖB selbst recherchierten Unterlagen sowie der Informationen aus der Sendung des Schweizer Fernsehens.

10 Die Firma X stellt auf ihrer Webseite ein Webinterface[3] zur Verfügung, mit welchem man über eine Suchmaske nach bei ihr gespeicherten Personen suchen kann. Dadurch können die folgenden Profil- bzw. Bewertungsdaten einer gespeicherten Person abgerufen werden: *Entscheidung, Entscheidungsmatrix, Score, Zahlungserfahrungen, bekannte Adressen, gleicher Haushalt (gleicher Name oder gleiche Telefonnummer), Firmenbeziehungen, Umfeld und Ähnlichkeitstreffer.* Die einzelnen Profildaten werden in der nachfolgenden Tabelle 1 kurz erläutert:

11 Tabelle 1

Kategorien	Beschreibung
Entscheidung	Aus den bei der Firma X zu einer betroffenen Person gesammelten Daten wird ein Bonitätsrating in Form einer Ampel mit den nachfolgenden Ausprägungen berechnet: rot (Handlungsanweisung: Vertrag nicht abschliessen), gelb (Handlungsanweisung: Zusatzabklärungen treffen) und grün (Handlungsanweisung: Vertrag abschliessen).

[3] Beilage 3, Factsheet vom 08.04.2008.

Entscheidmatrix	In der Entscheidmatrix werden die einzelnen zur Berechnung des Entscheidfeldes herangezogenen Daten mit einer Ampel (rot, gelb, grün) bewertet. Im Einzelnen sind dies die Felder: Score, Trefferart, Status, Firmenbeziehung mit negativen Daten, durchschnittliche Wohndauer an einer Adresse, Blacklistenprüfung, weitere Familienmitglieder, Bonität Familienmitglieder und Ähnlichkeitstreffer. Zusammengefasst werden die jeweiligen Einzelergebnisse unter der Kategorie Entscheidung. Zudem werden unter der Kategorie Entscheidungsgrund, die entscheidungsrelevanten Daten der Entscheidmatrix inklusive deren Wert aufgeführt.
Score	Der Score ist ein numerischer Wert, welcher aus den Datenfeldern Zahlungserfahrungen einer Person, Umfeld, Mobilität sowie Soziodemographie berechnet wird und liegt zwischen 250 und 700 Punkten. Er wird graphisch auf einer dreifarbigen (rot, gelb, grün) waagrechten Achse dargestellt.
Zahlungserfahrungen	Hier werden die der Firma X bekannten und gespeicherten bonitätsrelevanten Ereignisse aufgeführt. Diese sind Anzahl Zahlungserfahrungen, aktuellster Fall, Forderungssumme und offener Betrag Forderungsstatus (Konkurs, Betreibung), Auskünfte (Betreibungsregister) sowie Inkassomeldungen.
Bekannte Adressen	Aufgeführt werden die aktuelle Adresse und sämtliche der X bekannten Adressen inklusive Wohndauer sowie die durchschnittliche Wohndauer
Im gleichen Haushalt lebende Personen	In dieser Rubrik werden Daten von denjenigen Personen aufgelistet, die den gleichen Telefonanschluss nutzen (gleiche Telefonnummer) oder die den gleichen Namen an derselben Adresse tragen mit Angabe des Jahrganges, inklusive deren Informationen über allfällige Negativeinträge.
Firmenbeziehungen	Beziehungen zwischen gesuchter Person und Firmen werden bewertet. Angezeigt werden Handelsregistereinträge zu der jeweiligen Person sowie sonstige der Firma X bekannte negative Firmeneinträge.
Umfeldanalyse	Hierbei wird ein prozentualer Wert im Vergleich mit dem Umfeld auf grund des Nachnamens, des Hauses, der Strasse, des Ortes und des Landes errechnet.
Ähnlichkeitstreffer	Anzeige von Personen mit ähnlichem Namen inkl. Geburtsdatum.

Ausserdem haben die Nutzer des «Auskunftservice A» die Möglichkeit, zusätzlich Betreibungsregisterauskünfte online zu bestellen.

4.2 «Auskunftservice A» in der angepassten bzw. aktuellen Form

12 Bis zur Sachverhaltsabklärung hat die Firma den «Auskunftservice A» so modifiziert, dass dieser sich wesentlich von der früheren Version unterscheidet[4]. Nachfolgend werden die Eigenschaften des «Auskunftservice A» in der angepassten Form vorgestellt:

13 Tabelle 2

Kategorien	Beschreibung
Entscheidung	Aus den bei der Firma X zu einer betroffenen Person gesammelten Daten wird ein Bonitätsrating in Form einer Ampel mit den nachfolgenden Ausprägungen berechnet: rot (hohe Risiken vorhanden), gelb (sorgfältige Prüfung empfohlen. Der Entscheid impliziert nicht, dass eine verschlechterte Bonität vorliegt) und grün (keine Risiken gefunden).
Entscheidmatrix	In der Entscheidmatrix werden die einzelnen zur Berechnung des Entscheidfeldes herangezogenen Daten mit einer Ampel (rot, gelb, grün) bewertet. Im Einzelnen sind es folgende Felder: Score, Trefferart, Status, Firmenbeziehung mit negativen Daten, durchschnittliche Wohndauer an einer Adresse, weitere Familienmitglieder, Bonität Familienmitglieder und Ähnlichkeitstreffer. Zusammengefasst werden die jeweiligen Einzelergebnisse unter der Kategorie Entscheidung. Zudem werden unter der Kategorie Entscheidungsgrund, die entscheidungsrelevanten Daten der Entscheidmatrix inklusive deren Wert aufgeführt. Zudem wird bei den Bewertungen ein Hilfetext eingeblendet, sofern die Ampel gelb oder rot anzeigt.

[4] Beilage 4, Factsheet vom 04.06.2008; Beilage 5, Blatt «Infoboxen Auskunftservice A in Decisionmatrix».

Zahlungserfahrungen	Hier werden die bei der Firma X bekannten und gespeicherten bonitätsrelevanten Ereignisse aufgeführt. Diese sind: Anzahl Zahlungserfahrungen, aktuellster Fall, Forderungssumme und offener Betrag, Forderungsstatus (Konkurs, Betreibung), Auskünfte (Betreibungsregister) sowie Inkassomeldungen.
Alte Adresse(n) [Bekannte Adressen]	Aufgeführt werden die aktuelle Adresse und sämtliche der Firma X alten (bekannten) Adressen inklusive Umzugsmeldung sowie die so errechnete durchschnittliche Wohndauer angezeigt.
Gleicher Haushalt gleicher Name oder gleiche Telefonnummer)	In dieser Rubrik werden die Daten von denjenigen Personen angegeben, welche den gleichen Telefonanschluss nutzen (gleiche Telefonnummer) oder den gleichen Namen an der Adresse tragen mit Angabe des Jahrganges.
Firmenbeziehungen	Beziehungen zwischen gesuchter Person und Firmen werden bewertet. Angezeigt werden Handelsregistereinträge zu der jeweiligen Person sowie sonstige der Firma X bekannte negative Firmeneinträge.
Ähnlichkeitstreffer (Verwechslungsgefahr)	Anzeige von Personen mit ähnlichem Namen inkl. Geburtsdatum.

14 Insgesamt wurden die nachfolgend aufgeführten Änderungen am «Auskunftservice A» durchgeführt:

a Die Erklärungen zum Ampelsystem in der Kategorie Entscheidung wurden, wie in der Tabelle 2 aufgeführt, geändert. Zudem wird die Ampel nur noch dann rot, wenn über die betroffene Person negative Zahlungserfahrungen vorhanden sind oder wenn der Personenstatus (minderjährig, bevormundet, verstorben) einem rechtsgültigen Vertragsabschluss entgegensteht.

b Das Ampelsystem in der Kategorie Entscheidmatrix wurde mit Erklärungen versehen, so dass zu jeder Bewertung und deren Zustandekommen ein kleiner Erläuterungstext eingeblendet wird[5].

c Entfernt wurden die Kategorien Score und Umfeld sowie das Feld Blacklistenprüfung in der Kategorie Entscheidungsmatrix.

[5] Beilage 4; Beilage 5.

d Die Zahlungserfahrungen werden neu mit den Buchstaben A, B, C und D wie folgt bewertet:

i. A «nichts bekannt»;

ii. B «geringfügige Fälle bekannt»;

iii. C «erhebliche Fälle bekannt» und

iv. D «schwerwiegende Fälle bekannt».

Nach Auskunft der Firma X beruhen diese Zahlungsbewertungen einzig aufgrund der vorliegenden Zahlungserfahrungen der gesuchten Person. Bei diesem Rating wird die Aktualität der Zahlungserfahrungen (aktuelle wiegen schwerer als frühere), die Gewichtigkeit des Zahlungsereignisses (ein Konkurs wiegt schwerer als ein Inkassofall) und die Anzahl der Zahlungserfahrungen (viele negative wiegen schwerer als einzelne) berücksichtigt[6].

II. Erwägungen

1. Anwendbarkeit des Datenschutzgesetzes und Zuständigkeit des EDÖB

148 15 Gemäss Art. 2 Abs. 1 Ziffer a des Bundesgesetzes über den Datenschutz (DSG, SR 235.1) gilt das DSG für das Bearbeiten von Daten natürlicher oder juristischer Personen durch private Personen. Gemäss Art. 3 lit. e DSG wird unter «Bearbeiten» jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren und Vernichten von Daten verstanden. Als Personendaten gelten gemäss Art. 3 lit. a DSG alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen. Im Rahmen ihrer Tätigkeit als Wirtschaftsauskunftei bearbeitet die Firma X Adress- und Bonitätsdaten von natürlichen und juristischen Personen und gibt diese an Dritte bekannt (Art. 3 Ziff. f DSG). Deshalb ist das DSG auf den vorliegenden Sachverhalt anwendbar (Art. 2 in Verbindung mit Art. 3 Ziff. a, e und f DSG).

16 Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) hat gemäss Art. 29 DSG die Aufsicht über die Bearbeitung von Personendaten durch Private: Er kann insbesondere nach Art. 29 Abs. 1 lit a DSG von sich aus oder auf Meldung Dritter den Sachverhalt abklären, wenn Bearbeitungsmethoden geeig-

[6] Beilage 1, S. 4; Beilage 2, S. 3 Schreiben Firma X vom 17.07.2008; Beilage 4; Beilage 5.

net sind, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen (Systemfehler). Stellt er aufgrund einer Sachverhaltsabklärung fest, dass eine Datenbearbeitung gegen das Datenschutzgesetz verstösst, kann er empfehlen, die Datenbearbeitung zu ändern oder zu unterlassen (Art. 29 Abs. 3 DSG).

17 Durch Meldung verschiedener Personen wurde der EDÖB auf den «Auskunftservice A» aufmerksam gemacht. Aufgrund der Vielzahl der potenziell betroffenen Personen (zwei Drittel der Bewohnerinnen und Bewohner in der Schweiz leben zur Miete[7]) ist die Datenbearbeitung durch die Firma X geeignet, die Persönlichkeit einer Vielzahl von natürlichen und juristischen Personen zu verletzen. Aus diesem Grund ist der EDÖB im vorliegenden Fall berechtigt, aufgrund seiner Abklärungen eine Empfehlung im Sinne von Art. 29 Abs. 3 DSG zu erlassen.

2. Datenbearbeitung im Rahmen der Dienstleistung «Auskunftservice A»

2.1 Vorbemerkungen

18 Der EDÖB geht im Rahmen seiner Erwägungen lediglich auf den «Auskunftservice A» in seiner angepassten Form ein. Auf ihrer Website verweist die Firma X allerdings nach wie vor auf den «Auskunftservice A» in seiner ursprünglichen Form. So erscheinen in den Beschreibungen immer noch Hinweise auf die Elemente Score sowie Blacklistenprüfung[8]. Die Hinweise auf der Website «Integration der eigenen Blacklist verhindert Ausfälle» und «Score» (professionelle Berechnung der Ausfallwahrscheinlichkeit) sollten entfernt werden.

2.2 Zulässigkeit der Datenbearbeitung zum Zwecke von Mietauskünften

Allgemeines

19 Wer Personendaten bearbeitet darf gemäss Art. 12 Abs. 1 DSG die Persönlichkeit der betroffenen Person nicht widerrechtlich verletzen. Insbesondere darf er nach Art. 12 Abs. 2 DSG Personendaten nicht entgegen den allgemeinen Datenschutzgrundsätzen (Art. 4, 5 und 7 Abs. 1 DSG) bearbeiten, nicht ohne Rechtfertigungsgrund Daten einer Person gegen deren ausdrücklichen Willen bearbeiten

[7] Bundesamt für Wohnungswesen (BWO), Briefing Mietrecht: 8 http://www.bwo.admin.ch/dokumentation/00101/00184/index.html?lang=de
[8] www.Firma X, besucht am 3.11.2008.

und nicht ohne Rechtfertigungsgrund besonders schützenswerte Personendaten oder Persönlichkeitsprofile Dritten bekannt geben. In der Regel liegt dann keine Persönlichkeitsverletzung vor, wenn die betroffene Person ihre Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat (Art. 12 Abs. 3 DSG). Keine widerrechtliche Persönlichkeitsverletzung ist gemäss Art. 13 Abs. 1 DSG gegeben, wenn sie durch Einwilligung, überwiegendes öffentliches und privates Interesse oder Gesetz gerechtfertigt ist. Auch wenn sich der Dateninhaber grundsätzlich auf einen Rechtfertigungsgrund berufen kann, sind die allgemeinen Datenschutzgrundsätze zu beachten.

Rechtfertigungsgründe

20 Als Rechtfertigungsgrund gemäss Art. 13 Abs. 1 DSG kommt für Mietauskünfte neben der Einwilligung der betroffenen Person ein überwiegendes privates Interesse der bearbeitenden Person in Frage, wenn zur Prüfung der Kreditwürdigkeit einer anderen Person weder besonders schützenswerte Personendaten noch Persönlichkeitsprofile bearbeitet und Dritten nur Daten bekannt gegeben werden, die sie für den Abschluss oder die Abwicklung eines Vertrages mit der betroffenen Person benötigen (Art. 13 Abs. 2 Bst. c DSG). Unter diesen Bedingungen ist für die Kreditprüfung durch Dritte (Auskunfteien) und die Bekanntgabe eine Speicherung der Daten auf «Vorrat» zulässig. Gemäss Zweckmässigkeitsprinzip dürfen allerdings nur die Daten bearbeitet werden, die zur Prüfung der Kreditwürdigkeit erforderlich sind[9].

21 Ein weiterer Rechtfertigungsgrund nach Art. 13 Abs. 2 Bst. a DSG ist jener des Vertragsabschlusses. Demnach kann ein überwiegendes privates Interesse die Bearbeitung von Daten rechtfertigen, wenn diese die Verminderung des Risikos bei einem Vertragsabschluss bezweckt. Dieser Rechtfertigungsgrund kann bei allen Vertragsformen angerufen werden[10]. Auch wenn die Kreditauskunftei auf «Vorrat» Daten rechtmässig bearbeiten darf, ist die Bekanntgabe an Dritten nur an bestehende oder unmittelbar werdende Vertragspartner der betroffenen Person erlaubt. Hierbei obliegt es der Person, welche Daten bekannt gibt, zu prüfen, ob der Dritte ein tatsächliches Interesse an diesen Daten geltend machen kann. Die Anforderungen an den Interessenausweis sind nach dem Verhältnismässigkeitsprinzip je nach Sensitivität der Daten anzupassen.

[9] Basler Kommentar zum Datenschutzgesetz (BSK-DSG), Corrado Rampini, Art. 13 N 36.
[10] BSK-DSG, Corrado Rampini, Art. 13 N 30 f.

22 Nach Art. 4 Abs. 2 DSG haben die Datenbearbeitungen nach Treu und Glauben zu erfolgen. Gegen diesen Grundsatz verstösst beispielsweise derjenige, der Daten nicht offen bearbeitet, ohne dabei gegen eine Rechtsnorm zu verstossen[11]. Demzufolge muss eine Datenbearbeitung transparent sein. Nach dem Erkennbarkeitsprinzip muss die Beschaffung von Personendaten und insbesondere der Zweck der Bearbeitung für die betroffene Person erkennbar sein (Art. 4 Abs. 4 DSG). Die Anforderungen, die dabei an die Erkennbarkeit gestellt werden, sind nach den Umständen sowie den Grundsätzen der Verhältnismässigkeit und von Treu und Glauben zu beurteilen[12]. Ist die Beschaffung aufgrund der Umstände für die betroffene Person weniger deutlich erkennbar, muss die betroffene Person umso eher mit angemessenen Mitteln auf die Erhebung und ihre wesentlichen Rahmenbedingungen aufmerksam gemacht werden[13].

23 Nach dem Verhältnismässigkeitsprinzip (Art. 4 Abs. 2 DSG) darf ein Datenbearbeiter nur diejenigen Daten bearbeiten, die er für einen bestimmten Zweck tatsächlich benötigt und die im Hinblick auf den Bearbeitungszweck und die Persönlichkeitsbeeinträchtigung in einem vernünftigen Verhältnis stehen[14]. Wenn die Datenbearbeitung das angestrebte Ziel erreicht (Zwecktauglichkeit) und die privaten Interessen der Betroffenen schont (geringstmöglicher Eingriff) ist das Prinzip der Verhältnismässigkeit eingehalten.

24 Nach dem Grundsatz der Zweckmässigkeit (Art. 4 Abs. 3 DSG) dürfen Daten nur für den objektiven Zweck bearbeitet werden, der bei der Beschaffung angegeben worden ist oder der aus den Umständen ersichtlich oder gesetzlich vorgesehen ist. Die betroffene Person muss es nicht hinnehmen, dass über sie Daten ohne nähere Zweckbestimmung auf «Vorrat» erhoben werden[15].

[11] BSK-DSG, Urs Maurer-Lambrou/Andrea Steiner, Art. 4 N 7 und BBl 1988 II 449.
[12] BBl 2003 2125.
[13] BBl 2003 2126.
[14] BSK DSG Urs Maurer-Lambrou/Andrea Steiner, Art. 4 N 11.
[15] BSK DSG Urs Maurer-Lambrou/Andrea Steiner, Art. 4 N 14; BGE 125 II 473 E. 4.

25 Der Zweck von Mieterauskünften, wie sie der «Auskunftservice A» bereitstellt, ist die Verhinderung von Mietzinsausfällen. Der «Auskunftservice A» soll dem Bedürfnis der Bonitätsprüfung für die Mieterselektion dienen[16]. Auf der Website wird als Zweck die Überprüfung von Mieterinformationen erwähnt. Als Kreditauskunftei stützt sich die Firma X bei ihrer Datenbearbeitung auf ein überwiegendes privates Interesse, namentlich auf den Rechtfertigungsgrund der Bonitätsprüfung gemäss Art. 13 Abs. 2 Bst. c DSG. Diesbezüglich ist auch ein Datenaustausch entgegen dem Willen der betroffenen Person zum Zweck der Prüfung der Kreditwürdigkeit der betroffenen Person möglich.

26 In diesem Zusammenhang ist zu prüfen, ob die Datenbearbeitung den allgemeinen Datenschutzgrundsätzen entspricht. Die damalige Eidgenössische Datenschutzkommission (EDSK) hat die Datenbearbeitung im Rahmen von Mietverhältnissen in zwei Entscheiden im Zusammenhang mit der Ausgestaltung von Mietformularen konkretisiert[17]. Demnach dürfen nur Daten verwendet werden, die der Vermieter aus objektiven Gründen für die Mieterevaluation tatsächlich benötigt. Zudem darf der Vermieter bestimmte Unterlagen und Bestätigungen von Angaben (Betreibungsregisterauszüge) erst dann verlangen, wenn er mit dem Interessenten definitiv einen Mietvertrag abschliessen will[18].

27 Der EDÖB kommt daher zum Schluss, dass Mieterauskünfte, wie der «Auskunftservice A», aus datenschutzrechtlicher Sicht grundsätzlich möglich sind, solange die Grundsätze der Datenbearbeitung (Art. 4, 5 Abs. 1 und 7 Abs. 1 DSG) eingehalten werden und diese ausschliesslich dazu verwendet werden, Bonitätsdaten auszutauschen. Werden hingegen weitere Daten (die nicht direkt bonitätsrelevant sind) zum Zweck der Mieterevaluation ausgetauscht, kann sich der Anbieter einer solchen Dienstleistung nicht auf ein überwiegendes privates Interesse gemäss Art. 13 Abs. 2 lit. c DSG berufen und benötigt hierfür einen anderen Rechtfertigungsgrund.

[16] Beilage 6.
[17] VPB 62.42B und VPB 68.153; diese Beurteilungen sind in das Merkblatt Mietwohnungen des EDSB (EDÖB) eingeflossen.
[18] BSK DSG Urs Maurer-Lambrou/Andrea Steiner, Art. 4 N 25.

3. Datenschutzrechtliche Prüfung des «Auskunftservice A»

3.1 Informationen rund um den «Auskunftservice A»

28 Die Firma X informiert in ihrem Merkblatt «Datenschutzrechtliche Aspekte der Firma X Datenbank», dass ihre Datensammlung beim EDÖB angemeldet sei[19]. Zudem weist die Firma X auch in ihren Antwortschreiben an Auskunftsersuchende darauf hin, dass die Datenbank dem DSG entspreche und beim eidgenössischen Datenschutzbeauftragten angemeldet sei[20]. In den Allgemeinen Geschäftsbedingungen (AGB) wird weiterhin erklärt, dass die Firma X sich verpflichte, alle Datenschutzanforderungen einzuhalten. Dazu gehöre unter anderem die Registrierung in Bern als Auskunftei, die Verschlüsselung der Kommunikation über https und der Schutz der Daten vor unberechtigtem Zugriff[21]. Auf dem Merkblatt «Häufig gestellte Fragen» schreibt die Firma X als Antwort, warum der Kunde nicht darüber informiert worden sei, dass er in eine Datenbank eingetragen wurde: «Datenbanken, die beim eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten angemeldet sind, brauchen die betroffenen Personen nicht zu informieren, wenn sie jemanden in die Datenbank aufnehmen»[22].

29 Nach Art. 11a DSG sind Datensammlungen von Privatpersonen beim EDÖB anzumelden, wenn diese regelmässig besonders schützenswerte Personendaten an Dritte bekanntgeben. Nach revidiertem Datenschutzgesetz ist das auch dann der Fall, wenn die betroffene Person Kenntnis von der Datenbearbeitung hat. Allerdings muss für die betroffene Person gemäss Art. 4 Abs. 4 DSG immer erkennbar sein, dass Daten über sie bearbeitet werden.

30 Der Text der Firma X kann den Eindruck erwecken, dass ihre Tätigkeit vom EDÖB bewilligt worden ist. Die Anmeldung nach Art. 11c DSG ist lediglich eine formelle Pflicht. Es bedeutet nicht, dass der EDÖB eine Bewilligung erteilt und die Tätigkeit der Firma X überprüft und genehmigt hat (ausserdem hat der EDÖB von Gesetzes wegen keine Bewilligungskompetenz). Demzufolge entsprechen die Ausführungen der Firma X in dem Merkblatt «Datenschutzrechtliche Aspekte der Firma X Datenbank» und dem Merkblatt «Häufig gestellte Fragen» nicht den aktuellen gesetzlichen Gegebenheiten.

[19] Beilage 9, Merkblatt « Datenschutzrechtliche Aspekte der Firma X Datenbank».
[20] Beilage 7, Firma X Antwortschreiben Auskunftsbegehren.
[21] Beilage 8, Allgemeine Geschäftsbedingungen (AGB), Ziff. 5.4 und 6.2.
[22] Beilage 10, Merkblatt «Häufig gestellte Fragen».

31 Daher sind die Merkblätter «Datenschutzrechtliche Aspekte der Firma X Datenbank» und «Häufig gestellte Fragen» an das geltende Recht anzupassen.

3.2 Zahlungserfahrungen (Bonitätsscoring)

32 Die Firma X bewertet die Zahlungserfahrung anhand einer Skala von A bis D, wobei betroffene Personen in die Kategorie A eingestuft werden, wenn keine Zahlungsstörungen bekannt sind, in Kategorie B, wenn geringfügige Fälle bekannt sind, in Kategorie C, wenn erhebliche Fälle bekannt sind und in Kategorie D, wenn schwerwiegende Fälle bekannt sind. Hierbei wissen die betroffenen Personen nicht in welche Kategorie sie eingestuft werden. Zudem wissen weder sie noch die Kunden des «Auskunftservice A», wie die Fälle eingestuft werden und welche Informationen für die Einteilung der Kategorien herangezogen werden. Nach Aussagen der Firma X wird die Kategorisierung mathematisch aus den nachfolgenden Daten berechnet: Schwere der Zahlungsstörung (ein Konkurs wiegt schwerer als ein Inkassofall), Alter des Ereignisses (aktuellere wiegen schwerer als frühere) und Anzahl der Zahlungsstörungen (viele wiegen schwerer als einzelne)[23]. Indem die Firma X nicht zu erkennen gibt, welche Daten sie zur Kategorisierung der Zahlungserfahrungen heranzieht und wie sie die Betroffene einstuft, verletzt sie den Grundsatz der Erkennbarkeit gemäss Art. 4 Abs. 4 DSG.

33 Demzufolge sind die Bewertung der Zahlungserfahrungen in A, B, C und D, die Kriterien der Berechnung, die einzelnen Zahlungserfahrungen sowie die Ampelbewertung für die betroffenen Personen und die Kunden der Firma X transparent zu gestalten.

3.3 Status einer Person

34 Die Firma X führt auf, dass der Personenstatus dazu dient, eine minderjährige, bevormundete oder verstorbene Person zu erkennen[24].

[23] Beilage 1, S. 4; Beilage 2, S. 3; Beilage 4 (Kategorie Entscheidungsmatrix); Beilage 5.
[24] Beilage 4 (Kategorie Entscheidungsmatrix).

35 Es ist nicht ersichtlich, warum es notwendig sein sollte, das Merkmal «minderjährige bzw. verstorbene Person» in der Datenbank zu führen, zumal der Vermieter mit seinem Interessennachweis über die erforderlichen Informationen verfügt. Da dieses Merkmal eng mit der Suchfunktionalität zusammenhängt, wird auf die Erwägungen hinsichtlich der Suchfunktionalitäten (nachfolgend Rz 63 ff.) verwiesen.

3.4 Firmenbeziehungen mit negativen Daten

36 Die Firma X prüft, ob die betroffene Person in einer Beziehung zu Firmen mit Zahlungsstörungen steht. Hierbei muss, ihren Angaben zufolge, ein Status «gelb» keine verschlechterte Bonität implizieren. Die Firma X bittet ihre Kunden daher zu prüfen, ob die Art der Zahlungsstörung im Zusammenhang mit der Rechtsform, der Art und Grösse der Firma geeignet ist, die Bonität der Person zu beeinflussen[25].

37 Die Beziehung einer Person zu einer Firma kann nur unter ganz speziellen Umständen einen Einfluss auf die Bonität des Mietinteressenten haben. Zu denken ist hierbei insbesondere an Fälle, in denen die betroffene Person unbeschränkt haftender Gesellschafter an einer Kollektiv- oder Kommanditgesellschaft ist oder Inhaber einer Kapitalgesellschaft ist, deren Grundkapital noch nicht vollständig liberiert wurde. Im «Auskunftservice A» ist jedoch nicht ersichtlich, welcher Art die Beziehung einer Person zu einer Firma ist, welche Rechtsform die betreffende Firma hat und inwiefern sich die Beziehung zwischen der Person und der Firma gegenseitig bonitätsrelevant beeinflussen können. Deshalb ist der Grundsatz der Erkennbarkeit verletzt (Art. 4 Abs. 4 DSG). Zudem steht ein solcher Bonitätshinweis nur im Einklang mit dem DSG, wenn dieser tatsächlich geeignet ist, die Bonität der betroffenen Person zu beeinflussen. Nicht jede Verknüpfung einer betroffenen Person, mit einer Firma, welche Negativeinträge bei der Firma X aufweist, ist geeignet, Rückschlüsse auf die Bonität der betroffenen Person zu ziehen. Eine generelle Verknüpfung zwischen betroffenen Personen und Unternehmen verstösst gegen das Verhältnismässigkeitsprinzip (Art. 4 Abs. 2 DSG).

38 Deshalb sind die Beziehungen einer betroffenen Person zu einer Firma und die Bewertung der Bonität auf diejenigen Fälle zu beschränken, in welchen die durch die Verknüpfung gewonnen Informationen tatsächlich bonitätsrelevant sind. Zudem müssen die Verknüpfungsarten für die betroffenen Personen und die Kunden der Firma X erkennbar sein.

[25] Beilage 4 (Kategorie Entscheidungsmatrix); Beilage 5.

3.5 Durchschnittlichen Wohndauer an einer Adresse

39 Die Firma X führt die durchschnittliche Wohndauer im «Auskunftservice A», um ihren Kunden häufige Umzüge anzuzeigen. Ihrer Meinung nach können häufige Umzüge in kurzen Abständen Hinweise darauf geben, dass Zahlungsstörungen bei Betreibungsämtern bekannt sein könnten. In einem solchen Fall rät die Firma X Betreibungsauskünfte der früheren Wohnorte zu verlangen[26].

40 Für einen Vermieter kann es grundsätzlich von Vorteil sein, wenn dieser weiss, wie lange ein potentieller Mieter an einem Wohnort im Durchschnitt verweilt. Wie allerdings die EDSK im vorerwähnten Entscheid[27] festhält, hängt die Dauer eines Mietverhältnisses von verschiedenen Faktoren, wie Arbeit des Mieters inklusive der Familienmitglieder, Lebensumfeld, Geschmack des Mieters oder seiner Familie ab. Die EDSK hat die Frage nach der Länge des laufenden Mietverhältnisses als unverhältnismässig eingestuft. Neben der Tatsache, dass es sich bei der durchschnittlichen Wohndauer nicht um ein bonitätsrelevantes Datum im Sinne von Art. 13 Abs. 2 lit. c DSG handelt, ist diese zudem völlig ungeeignet, um hieraus Rückschlüsse auf einen potentiellen «Mietnomaden» zu ziehen.

41 Der EDÖB gibt zudem zu bedenken, dass die Aufstellung sämtlicher Wohnsitzwechsel ein Persönlichkeitsprofil gemäss Art. 3 lit. d DSG darstellt. Diesbezüglich ist ein überwiegendes privates Interesse der bearbeitenden Person gemäss Art. 13 Abs. 2 lit. c DSG explizit ausgeschlossen. Ob ein Persönlichkeitsprofil vorliegt, ist im Einzelfall aufgrund der konkreten Umstände zu beurteilen. Angaben zu Wohnsitzwechseln über einen Zeitraum von mehreren Jahren sind als Persönlichkeitsprofil zu werten[28].

42 Daher sind das Feld «Durchschnittliche Wohndauer an einer Adresse» und der Hinweis auf der Webseite «komplette SchuldnerHistorie aller uns bekannter Wohnorte» unverhältnismässig und zu entfernen.

[26] Beilage 3 (Kategorie Entscheidungsmatrix und alte Adresse(n)); Informationen Website.
[27] VPB 68.153, Erw. 13.
[28] BSK DSG Urs Belser, Art. 3 N 22.

3.6 Bonität von Haushaltsmitgliedern

43 Im «Auskunftservice A» erhalten die Kunden der Firma X Daten mutmassliche Haushaltsmitglieder der gesuchten Person angezeigt, bei denen Zahlungsstörungen vorliegen. Die Firma X führt hierzu aus, dass eine gelbe Ampel hierbei keine verschlechterte Bonität implizieren muss, sondern empfiehlt die Bonität dieser Haushaltsmitglieder (bei Vorliegen eines Interessensnachweises) zu verifizieren[29].

44 Die Bonität von Haushaltsmitgliedern kann beim Abschluss eines Mietvertrages dann eine Rolle spielen, wenn der Mietvertrag von solidarisch haftenden Personen unterschrieben werden soll. In diesem Fall kann auch jeweils ein Interessenachweis vorgelegt und die betreffende Person ihrerseits separat mit Namen und Geburtsdatum im «Auskunftservice A» abgerufen werden. Daher ist die Notwendigkeit einer solchen Verknüpfung der Daten nicht ersichtlich. Nach der Rechtsprechung[30] dürfen in einem Mietformular Name, Vorname, Geburtsdatum, Beruf und Arbeitgeber nur von Personen erfragt werden, die den Mietvertrag mit unterzeichnen. Da die Bonität der Haushaltsmitglieder nur dann eine Rolle spielt, wenn der Mietvertrag von diesen Personen unterzeichnet wird, ist die Verknüpfung von Bonitätsdaten der im selben Haushalt lebenden Personen als unverhältnismässig gemäss Art. 4 Abs. 2 DSG einzustufen. Zudem sind Bonitätsdaten über Haushaltsmitglieder grundsätzlich nicht dazu geeignet, Rückschlüsse auf die Kreditwürdigkeit der betroffenen Person zu ziehen, weshalb sich die Firma X hierfür nicht auf den Rechtfertigungsgrund gemäss Art. 13 Abs. 2 Bst. c DSG berufen kann. Die Anzeige der Bonitätsdaten von Hausmitgliedern stellt daher eine widerrechtliche Persönlichkeitsverletzung der betroffenen Person gemäss Art. 12 DSG dar, weshalb das Feld «Haushaltmitglieder Bonität» zu entfernen ist.

3.7 Datenbearbeitung zu weiteren Haushaltsmitgliedern

45 Die Firma X zeigt im «Auskunftservice A» an, ob im gleichen Haushalt möglicherweise Ehe- oder Konkubinatspartner wohnhaft sein könnten. Hierzu wird anhand einer gleichen Telefonnummer oder einem übereinstimmenden Namen an einer identischen Wohnadresse automatisiert auf eine solche Partnerschaft geschlos-

[29] Beilage 4, Kategorie Entscheidungsmatrix; Beilage 5.
[30] VPB 68.153 und VPB 62.42A.

sen und der Status der betroffenen Person als gelb bewertet. Die Firma X merkt zudem an, dass der Status gelb in dieser Kategorie noch keine verminderte Bonität implizieren muss[31].

46 Die Angabe, dass mehrere Personen die gleiche Telefonnummer nutzen oder mehrere Personen mit gleichem oder verschiedenem Namen an der gleichen Adresse wohnhaft sind, reicht nicht aus, um hieraus auf bonitätsrelevante Informationen schliessen zu können. Nach derzeitiger Rechtsprechung[32] dürfen in einem Mietformular Name, Vorname und Geburtsdatum nur von Personen erfragt werden, die den Mietvertrag mit unterzeichnen. Da die Bonität der Haushaltsmitglieder nur dann eine Rolle spielt, wenn sie den Mietvertrag unterzeichnen, ist die Datenbearbeitung weiterer Personen, die den Mietvertrag nicht unterschreiben, unverhältnismässig (Art. 4 Abs. 2 DSG). Ausserdem wissen die im gleichen Haushalt lebenden Personen nicht, dass ihre Identifikationsdaten miteinander in einer Datenbank verknüpft werden. Daher verstösst eine solche Datenbearbeitung zudem gegen das Erkennbarkeitsprinzip gemäss Art. 4 Abs. 4 DSG, weshalb das Feld «Weitere Haushaltsmitglieder» zu entfernen ist.

3.8 Ähnlichkeitstreffer

47 Von Seiten der Firma X werden bei jeder Personenauskunft Ähnlichkeitstreffer angegeben, wenn Personen den gleichen Namen oder dasselbe Geburtsdatum haben. Ziel ist es, nach Angaben der Firma X, das Verwechslungsrisiko zu minimieren[33].

48 Grundsätzlich sollte bereits die Suchfunktionalität nach Name, Vorname, Adresse und Geburtsdatum genügen, um eine betroffene Person eindeutig zu identifizieren, so dass die Notwendigkeit von Ähnlichkeitstreffern nicht gegeben ist. Zudem sind Ähnlichkeitstreffer in keinem Fall geeignet, um Rückschlüsse auf die Bonität der betroffenen Person zu ziehen, weshalb die Firma X diesbezüglich kein überwiegendes privates Interesse geltend machen kann (Art. 13 Abs. 2 lit. c DSG). Daher ist diese Information als unverhältnismässig gemäss Art. 4 Abs. 2 DSG zu qualifizieren und demzufolge ist das Feld «Ähnlichkeitstreffer» zu entfernen.

[31] Beilage 4, Kategorie Entscheidungsmatrix; Beilage 5.
[32] PB 68.153 und VPB 62.42A.
[33] Beilage 4, Kategorie Entscheidungsmatrix; Beilage 5.

4. Zur Gewährung des Zugangs zum «Auskunftservice A»

49 Als Bedingung für den Zugang prüft die Firma X, ob ein Antragssteller als professioneller Wohnungsvermieter qualifiziert werden kann und ob die vom Antragssteller genannte Firma tatsächlich existiert. In den AGB verpflichten sich die Vertragpartner (auch für den Testzugang), für jede getätigte Nachfrage einen Interessennachweis aufzubewahren und der Firma X diesen auf Ersuchen hin vorzulegen (Stichprobenkontrolle). Der Interessennachweis entspricht nach Auskunft der Firma X demjenigen für Betreibungsauskünfte nach SchKG (SR 281.1)[34]. Während die Firma X vor der Sitzung mit dem EDÖB grundsätzlich jedem Vermieter einen Zugang zum «Auskunftservice A» gewährte, wird diese Dienstleistung nur noch Firmen (professionelle Wohnungsvermieter) angeboten[35]. Inzwischen ist dem EDÖB allerdings bekannt geworden, dass auch Versicherungen, die Mietkautionsversicherungen anbieten, den «Auskunftservice A» nutzen können.

50 Bonitätsdaten dürfen gemäss Art. 12 Abs. 2 lit. c DSG nur zum Zweck der Prüfung der Kreditwürdigkeit im Rahmen des Abschluss und der Abwicklung eines Vertrages mit der betroffenen Person bearbeitet werden.

51 Obwohl der «Auskunftservice A» grundsätzlich von jedem Vermieter genutzt werden könnte, ist die Missbrauchsgefahr gross, wenn jeder beliebige Vermieter hierauf Zugriff hätte. Daher begrüsst der EDÖB die Beschränkung des Nutzerkreises. Eine Nutzung dieses Services durch eine Mieterkautionsversicherung ist dementsprechend nur dann möglich, wenn sich die Datenweitergabe nur auf Bonitätsdaten beschränkt. Weitergehende Informationen sind für die jeweilige Versicherung zwar für die Risikoabschätzung der betroffenen Person nützlich, werden allerdings nicht zum Abschluss oder zur Abwicklung einer solchen Versicherung benötigt.

52 Für die Überprüfung, ob die via «Auskunftservice A» bezogene Daten tatsächlich für den Abschluss eines Mietvertrages verwendet werden, ist datenschutzrechtlich einzig die Firma X verantwortlich, da sie den Zugang erteilt.

53 Der Zugriff auf den «Auskunftservice A» erfolgt, nachdem ein Vertrag mit der Firma X abgeschlossen wird. Wenn die Firma X die Interessennachweise der Zugangsberechtigten nur stichprobenhaft herausverlangt, übernimmt sie datenschutzrechtlich das Risiko, dass die Datenbekanntgabe an Kunden erfolgen kann, die im Einzel-

[34] Beilage 1, S, 5.
[35] Beilage 2, S. 3.

fall keinen Interessennachweis vorlegen können. Steht im Nachhinein fest, dass der betreffende Kunde keinen Interessennachweis erbringen kann, hat die Datenschutzverletzung bereits stattgefunden. Die Firma X kann in einem solchen Fall für entstandene Schäden haftbar gemacht werden.

54 Wenn die Kunden der Firma X gleichzeitig einen Betreibungsregisterauszug bestellen, der via Tochtergesellschaft Firma A eingeholt wird, muss vorgängig ein Interessennachweis von der Firma X bzw. der Firma A eingeholt werden, denn ohne diesen Nachweis wäre die Bestellung eines aktuellen Betreibungsregisterauszuges auch nicht möglich. In diesen Zusammenhang ist zu vermerken, dass gemäss EDSK Entscheid, ein Betreibungsregisterauszug im Zusammenhang eines Mietvertrages immer erst dann eingeholt werden darf, wenn mit dem Mieter definitiv ein Mietvertrag abgeschlossen werden soll. Diesbezüglich ist die Firma X datenschutzrechtlich dafür verantwortlich, dass ein Betreibungsregisterauszug erst dann verlangt und die in der Datenbank der Firma X entsprechend gespeicherten Daten erst dann abgerufen werden dürfen, wenn mit dem Mieter definitiv der Vertrag abgeschlossen werden soll.

55 Der Zugang zum «Auskunftservice A» ist für Mietkautionsversicherungen so einzuschränken, dass nur noch die für den Abschluss und die Abwicklung eines Vertrages relevanten Bonitätsdaten übermittelt werden. Die Firma X hat organisatorisch und technisch dafür zu sorgen, dass möglichst keine unberechtigten Abfragen im «Auskunftservice A» vorgenommen werden können.

5. Datensicherheit

56 Der Zugang zum «Auskunftservice A» erfolgt via Internet über einen passwortgeschützten und verschlüsselten (128 Bit SSL) Bereich. Vertraglich lässt sich die Firma X zudem in Ziff. 6.1 der AGB zusichern, dass das Passwort nur von den berechtigten Personen genutzt werden darf und eine Weitergabe an Dritte untersagt ist. Ausserdem trägt der Benutzer die Verantwortung, dass das Passwort in regelmässigen Abständen geändert wird und jeden Monat eine Bewegungsstatistik erstellt wird. Nach Aussage der Firma X wird jedoch eine Passwortänderung nach einer gewissen Frist (30 - 60Tage) erzwungen[36].

[36] Beilage 1, S. 5.

57 Die Firma X protokolliert sämtliche Zugriffe auf die Datenbank. Nach eigenen Angaben, deaktiviert sie den Zugang umgehend, wenn sie einen Missbrauch feststellt[37]. In einem dem EDÖB bekannten Fall wurde in Vorbereitung einer Sendung des Schweizer Fernsehens der Zugang missbräuchlich genutzt. Die Firma X hat zwar zunächst den Zugang korrekterweise gesperrt, diesen aber wieder frei geschaltet und damit in Kauf genommen, dass ohne Interessennachweis Abfragen möglich wurden.

58 Nach Art. 7 DSG müssen Personendaten gegen unbefugtes Bearbeiten durch angemessene technische und organisatorische Massnahmen geschützt werden. Insbesondere muss der Datenbearbeiter gemäss Art. 8 Abs. 1 der Verordnung zum Bundesgesetz über den Datenschutz (VDSG, SR 235.11) für die Vertraulichkeit, die Integrität und die Verfügbarkeit der Daten sorgen. Die Bekanntgabekontrolle (Art. 9 Abs. 1 Bst. d VDSG) gewährleistet die Firma X insofern, als sie die Zugriffe protokolliert und den Benutzern die Daten lediglich über einen verschlüsselten und passwortgesicherten Bereich zugänglich macht[38].

59 Diesbezüglich sorgt die Firma X aus technischer Sicht in ausreichendem Masse für die Datensicherheit. Aus organisatorischer Sicht wurde mindestens bei der Zugangserteilung an den Kassensturz die Datensicherheit gemäss Art. 7 DSG nicht gewährleistet.

60 Ein Ausschluss der Haftung und eine Delegation der datenschutzrechtlichen Verantwortung an die Benutzer betreffend der Datensicherheit sind vertraglich nicht möglich und verstossen gegen Art. 7 DSG, weshalb die AGB entsprechend anzupassen sind. Demzufolge hat die Firma X organisatorische Massnahmen zu treffen, damit ein unberechtigter Zugriff frühzeitig erkannt wird und der entsprechende Zugang zu ihrer Datenbank gesperrt wird und solange gesperrt bleibt, bis ein Missbrauch ausgeschlossen werden kann. Auch sind die AGB hinsichtlich der Pflicht des Datenbearbeiters bei der Datensicherheit gemäss Art. 7 DSG anzupassen.

[37] Beilage 1, S. 5.
[38] BSK-DSG, Kurt Pauli, Art. 7 N 13.

6. Datenrichtigkeit

61 In Ziffer 7.1 ihrer AGB schliesst die Firma X jede Haftung hinsichtlich Vollständigkeit und Richtigkeit der Daten ausdrücklich aus.

62 Gemäss Art. 5 Abs. 1 DSG hat derjenige, der Personendaten bearbeitet, sich über deren Richtigkeit zu vergewissern. Indem die Firma X jede Haftung hinsichtlich Vollständigkeit und Richtigkeit der Daten gemäss Ziff. 7.1 AGB ausschliesst, verstösst sie gegen Art. 5 Abs. 1 DSG. Ein solcher Ausschluss der Haftung und eine Delegation der datenschutzrechtlichen Verantwortung an die Benutzer sind vertraglich nicht möglich, weshalb die AGB hinsichtlich der Pflicht des Datenbearbeiters bei der Datenrichtigkeit gemäss Art. 5 Abs. 1 DSG anzupassen sind.

7. Suchfunktionalitäten

63 Die Suchfunktionalitäten im «Auskunftservice A» sind so ausgestaltet, dass allein aufgrund eines Attributmerkmals (Name, Strasse etc.) eine Suche ausgelöst werden kann, die zu Treffern führt. Die Suchergebnisse sind auf eine Liste von ca. 50 Namen begrenzt[39].

64 Mit der jetzigen Ausgestaltung der Suchfunktionalität können Zugangsberechtigte mehr Daten einsehen als notwendig. In den AGB legt die Firma X fest, dass der Zugangsberechtigte nur auf die tatsächlich benötigten Daten zugreifen darf, für die er einen Interessensnachweis erbringen kann[40].

65 Diesbezüglich hat einerseits der Kunde die datenschutzrechtliche Verantwortung, nur die Daten von Personen abzufragen, für die ein Interessennachweis vorhanden ist. Andererseits hat aber auch die Firma X eine datenschutzrechtliche Verantwortung. Sie muss nach dem Grundsatz der Verhältnismässigkeit gemäss Art. 4 Abs. 2 DSG und dem Grundsatz der Datensicherheit gemäss Art. 7 DSG dafür sorgen, dass nur tatsächlich benötigte Daten abgefragt werden können. Die Firma X muss also auch technische Massnahmen ergreifen, damit eine einschränkende Suche möglich ist. Demzufolge sind die Suchfunktionalitäten so auszugestalten, dass die Firma X stufenweise von den Kunden die Eingabe von Kriterien verlangt, die jeweils von der Anzahl der gelieferten Suchtreffer abhängig ist. Die Suchkriterien wären

[39] Beilage 1, S. 5.
[40] Beilage 8, Ziff. 6.1 AGB.

in der erweiterten Suche zunächst Name und Vorname, dann Geburtsdatum, weiter Wohnort und schliesslich Adresse. Da der Kunde über die notwendigen Informationen verfügt, ist eine solche Suche für ihn möglich. Dadurch werden keine Ähnlichkeitstreffer mehr angezeigt, da die Suche fortlaufend mittels Aufforderung erweitert werden kann, bis schliesslich die gesuchte Person angezeigt wird.

66 Mit einer solchen Lösung könnte im Einklang mit Art. 9 Abs. 1 Bst. g VDSG technisch und organisatorisch besser gewährleistet werden, dass Zugangsberechtigte nur auf tatsächlich benötigte Daten zugreifen können.

67 Demzufolge sind die Suchfunktionalitäten zwingend so zu auszugestalten, dass der Kunde bei der Suche nach einer Person stufenweise Kriterien eingeben muss, die jeweils von der Anzahl Suchtreffern abhängig sind.

8. Auskunfts- und Löschungsbegehren

68 Nach eigenen Angaben erledigt die Firma X Auskunfts- und Löschungsbegehren betreffend «Auskunftservice A» innerhalb von 2 bis 3 Tagen. Die Überprüfung der Identität des Auskunftsersuchenden erfolgt aufgrund der Kopie eines amtlichen Ausweises wie Pass, Identitätskarte oder Führerausweis[41]. Die Auskunft wird in der Regel in einem Standardbrief[42] und einem Auszug aus der Datenbank der Firma X erteilt, der folgende Daten enthält:

- Info über die Person (Status) mit Adresse, Telefonnummer, Faxnummer, Email, Geburtsdatum, Geschlecht und Geburtsort;
- Publikationen;
- Zahlungserfahrungen (Anzahl Zahlungserfahrungen, Aktuellster Fall, Forderungssumme, offener Betrag und Forderungsstatus);
- Auskünfte und Inkassomeldungen.

69 Im Standardantwortbrief wird mitgeteilt, dass die Datenbank der Firma X Personendaten enthält, die von den Kunden der Firma X zur Prüfung der Kreditwürdigkeit im Zusammenhang mit dem Abschluss eines Vertrages benötigt werden

[41] Beilage 1, S. 6.
[42] Beilage 11, Firma X Standardantwortbrief Auskunftsbegehren.

und ob über den Kunden negative Bonitätsdaten bekannt sind. Zudem wird auf das Merkblatt «Datenschutzrechtliche Aspekte der Firma X Datenbank» sowie das Blatt «Häufig gestellte Fragen» verwiesen. Diese Merkblätter sowie Hinweise auf Auskunfts- und Löschungsrechte werden von der Firma X nicht auf ihrer Webseite veröffentlicht.

70 Im Rahmen des Auskunftsersuchens erhält die betroffene Person von der lediglich ihre in der Datensammlung gespeicherten Personendaten[43]. Hingegen erhält die betroffene Person keinerlei Auskunft über Daten, welche die Firma X anhand der in ihrer Datensammlung vorhanden Daten berechnet (z.B. Scorings, Kennzahlen, etc.) oder verknüpft und welche sie Dritten bekannt gibt.

71 Nach Art. 8 DSG kann jede Person vom Inhaber einer Datensammlung Auskunft darüber verlangen, ob Daten über sie bearbeitet werden und ob der Dateninhaber sich auf einen Rechtfertigungsgrund für die Datenbearbeitung berufen kann. Die Gewährung des Auskunftsrechts ist die Voraussetzung, um zu erkennen, welche Daten über eine betroffene Person bearbeitet werden und um weitere (Datenschutz-)Rechte, wie beispielsweise das Löschungs- und Berichtigungsrecht, erst geltend machen zu können.

72 Das Auskunftsrecht bezieht sich hierbei auf alle Daten über eine Person in einer Datensammlung, die ihr zugeordnet werden können. Es erstreckt sich auf jede Art von Information, die auf die Vermittlung oder die Aufbewahrung von Kenntnissen ausgerichtet ist, ungeachtet, ob es sich dabei um eine Tatsachenfeststellung oder um ein Werturteil handelt und ob diese Information in einer Datenbank abgespeichert oder nur zur Ansicht jeweils berechnet wird. Entscheidend für die Qualifikation als Personendaten, die vom Auskunftsrecht erfasst sind, ist, dass sich die Angaben einer oder mehreren Personen zuordnen lassen. Wie der Bezug zur betroffenen Person hergestellt wird, ist hierbei ohne Bedeutung. Wesentlich ist, dass die Zuordnung ohne unverhältnismässigen Aufwand möglich ist[44]. Auskunft zu erteilen ist über alle Daten, die sich auf die auskunftsersuchende Person beziehen (Art. 3 Bst. a DSG) und die ihr zugeordnet werden können (Art. 3 Bst. g DSG). Wird die Auskunft verweigert, eingeschränkt oder aufgeschoben, muss nach Art. 9 Abs. 4 DSG hierfür ein Grund angegeben werden.

[43] Beilage 11.
[44] BSK DSG Urs Belser, Art. 3 N 5, VBP 62.57, E 4.

73 Gegenüber ihren Kunden bietet die Firma X neben den bei ihr gespeicherten Daten segmentspezifische Ratings (z.B. in Form von Ampeln) der betroffenen Personen an. Im Rahmen der Wahrnehmung ihres Auskunftsrechts erhalten hingegen die betroffenen Personen lediglich einen Auszug über die von der Firma X gespeicherten Adress- und Bonitätsdaten. Die Merkblätter «Häufig gestellte Fragen» und «Datenschutzrechtliche Aspekte der Firma X Datenbank» erwähnen nirgends, dass diese Daten der betroffenen Person weiterbearbeitet werden (z.B. in Form von Ratings oder dem Ampelsystem).

74 Zugangsberechtigte ersehen beim «Auskunftservice A» einen grösseren Datensatz als der betroffenen Person im Rahmen ihrer Auskunftsbegehren mitgeteilt werden. Somit ist für die betroffenen Personen nicht erkennbar, welche Daten über sie von der Firma X bearbeitet werden (Art. 4 Abs. 4 DSG). Gerade aus diesem Grund können die betroffenen Personen auch nicht ausreichend von ihrem Recht auf Datenberichtigung gemäss Art. 5 Abs. 2 DSG Gebrauch machen. Damit liegt eine widerrechtliche Persönlichkeitsverletzung vor. Indem Firma X in Auskunftsbegehren nicht alle objektiv erschliessbaren Daten den betroffenen Personen mitteilt, bzw. eine Einschränkung des Auskunftsrechts begründet, verletzt sie die Pflichten nach Art. 8 und 9 DSG. Es wird darauf hingewiesen, dass betroffene Personen gemäss Art. 15 DSG eine Klage beim Zivilrichter einreichen können. Zudem kann bei vorsätzlicher Verletzung der Auskunftspflicht auch eine Strafklage erhoben werden (Art. 34 Abs. 1 DSG).

75 Demzufolge sind den betroffenen Personen auf Auskunftsersuchen hin sämtliche Informationen auszuhändigen, welche von der Firma X bearbeitet werden (unabhängig davon, ob diese in deren Datensammlung gespeichert sind oder bei Bedarf aus dem Datenbestand berechnet werden) und die ersuchende Person betreffen (auch wenn es sich hierbei um Daten handelt, welche nicht im Datensatz der betroffenen Person gespeichert sondern nur verknüpft werden).

III. Empfehlungen

Aufgrund dieser Erwägungen empfiehlt der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB)

1. Das Merkblatt «Datenschutzrechtliche Aspekte der Firma X Datenbank» sowie das Merkblatt «Häufig gestellte Fragen» sind an das geltende Recht anzupassen.

2. Die Bewertung der Zahlungserfahrungen in A, B, C und D, die Kriterien der Berechnung, die einzelnen Zahlungserfahrungen sowie die Ampelbewertung sind transparent zu gestalten.

3. Die Beziehungen einer betroffenen Person zu einer Firma und die Bewertung der Bonität sind auf die Fälle zu beschränken, in welchen die durch die Verknüpfung gewonnenen Informationen tatsächlich bonitätsrelevant sind. Zudem müssen die Verknüpfungen für die betroffene Person und die Kunden der Firma X erkennbar sein.

4. Das Feld «Durchschnittliche Wohndauer an einer Adresse», der Hinweis auf der Website «komplette Schuldnerhistorie aller uns bekannter Wohnorte» sowie die Felder «Haushaltmitglieder Bonität», «Weitere Haushaltsmitglieder» und « Ähnlichkeitstreffer» sind zu entfernen.

5. Der Zugang zum «Auskunftservice A» ist für Mieterkautionsversicherungen so einzuschränken, dass nur noch die für den Abschluss und die Abwicklung des Vertrages relevanten Bonitätsdaten übermittelt werden.

6. Die Firma X hat organisatorische Massnahmen zu treffen, damit ein unberechtigter Zugriff frühzeitig erkannt wird und der entsprechende Zugang zu ihrer Datenbank gesperrt wird und solange gesperrt bleibt, bis ein Missbrauch ausgeschlossen werden kann.

7. Die AGB sind hinsichtlich der Pflicht des Datenbearbeiters bei der Datensicherheit gemäss Art. 7 DSG und sowie seiner Pflicht bei der Datenrichtigkeit gemäss Art. 5 Abs. 1 DSG anzupassen.

8. Die Suchfunktionalität ist zwingend so zu auszugestalten, dass der Kunde bei der Suche nach einer Person stufenweise Kriterien eingeben muss, die jeweils von der Anzahl Suchtreffern abhängig ist.

9. Den betroffenen Personen ist laut Auskunftsersuchen hin sämtliche Informationen auszuhändigen, welche von der Firma X bearbeitet werden (unabhängig davon, ob diese in deren Datensammlung gespeichert sind oder bei Bedarf aus dem Datenbestand berechnet werden) und die ersuchende Person betreffen (auch wenn es sich hierbei um Daten handelt, welche nicht im Datensatz der betroffenen Person gespeichert, sondern verknüpft werden).

Die Firma X teilt dem 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 Firstablauf (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

4.1.7 Entschliessung über die Dringlichkeit des Schutzes der Privatsphäre in einer Welt ohne Grenzen

30. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre Straßburg, 15. - 17. Oktober 2008

Entschließung über die Dringlichkeit des Schutzes der Privatsphäre in einer Welt ohne Grenzen und die Erarbeitung einer gemeinsamen Entschließung zur Erstellung internationaler Normen zum Schutz der Privatsphäre und zum Schutz personenbezogener Daten

Antragsteller:

Die Agencia de Protección de Datos (Spanien) und der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (Schweiz)

Unterstützt von:

Der Commission nationale de l'Informatique et des Libertés (Frankreich)

Dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Dem Garante per la Protezione dei Dati Personali (Italien)

Dem Staatlichen Inspektorat für den Datenschutz der Republik Litauen

Dem Amt für Datenschutz der Republik Tschechien

Der griechischen Datenschutzbehörde

Der niederländischen Datenschutzbehörde

Dem Europäischen Datenschutzbeauftragten

Dem Generalinspekteur für den Datenschutz (Polen)

Dem Datenschutzbeauftragten von Irland

Der Nationalen Direktion für den Datenschutz von Argentinien

Der Agence de protection des données de la Principauté d'Andorre

Dem Amt des Informationsbeauftragten (Vereinigtes Königreich)

Der Nationalen Kommission für den Datenschutz (Portugal)

Dem Beauftragten für den Schutz der Privatsphäre von Neuseeland

Dem Datenschutzbeauftragten von Guernsey

Dem Berliner Beauftragten für Datenschutz und Informationsfreiheit

Der Datenschutzbehörde des Baskenlandes (Spanien)

Der Datenschutzbehörde von Katalonien (Spanien)

Der Datenschutzbehörde von Madrid (Spanien)

Die Konferenz erinnert daran, dass:

- die auf ihrer 22. Konferenz in Venedig verabschiedete Erklärung;
- die auf ihrer 26. Konferenz in Breslau gefasste Entschließung;
- die auf ihrer 27. Konferenz in Montreux verabschiedete Erklärung;
- die auf ihrer 28. Konferenz vorgestellte Londoner Initiative;
- die auf ihrer 29. Konferenz gefasste Entschließung;

- den universellen Charakter des Rechts auf Datenschutz und auf den Schutz der Privatsphäre stärken wollen und zur Erstellung eines universellen Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten aufrufen.
- Insbesondere in der Erklärung von Montreux ruft die Konferenz die Organisation der Vereinten Nationen auf, ein zwingendes Rechtsinstrument auszuarbeiten, in dem das Recht auf Datenschutz und das Recht auf den Schutz der Privatsphäre ls durchsetzbare Menschenrechte im Einzelnen festgeschrieben werden. Ferner ruft die Konferenz den Europarat auf, gemäß Artikel 23 des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten die Nichtmitglied-

staaten dieser Organisation, die eine entsprechende Datenschutzgesetzgebung besitzen, aufzufordern, dem Übereinkommen (STE Nr. 108) und seinem Zusatzprotokoll (STE Nr. 181) beizutreten.

- In der Entschließung der 29. Konferenz haben die Datenschutzbeauftragten die Notwendigkeit unterstrichen, die Erarbeitung effizienter, universell anerkannter internationaler Normen zum Schutz der Privatsphäre zu unterstützen, als Mechanismus, um den Parteien zu helfen, die Konformität mit den gesetzlichen Anforderungen im Bereich des Datenschutzes und des Schutzes der Privatsphäre herzustellen und nachzuweisen.

Die Konferenz stellt fest, dass inzwischen ermutigende Anstrengungen gemacht wurden, um diese Ziele zu erreichen und dass insbesondere:

- Die Frage eines universellen Übereinkommens auf dem Arbeitsprogramm der Kommission für internationales Recht der Vereinten Nationen steht;

- Der Europarat den Beitritt von Nichtmitgliedstaaten befürwortet, deren Datenschutzgesetzgebung den Anforderungen des Übereinkommens STE Nr. 108 entspricht, und beschlossen hat, sich für dieses Regelwerk weltweit einzusetzen; so hat er die potenziell universelle Gültigkeit des Übereinkommens STE Nr. 108 betont, insbesondere auf dem Weltgipfel zur Informationsgesellschaft in Tunis im November 2005 und bei den Foren zur Internet-Governance 2006 in Athen und 2007 in Rio;

- Die OECD am 12. Juni 2007 eine Empfehlung zur grenzübergreifenden Zusammenarbeit bei der Anwendung der Rechtsvorschriften zum Schutz der Privatsphäre angenommen hat, die insbesondere darauf abstellt, die nationalen Rahmen zur Anwendung der Gesetze über den Schutz der Privatsphäre zu verbessern, um eine bessere Zusammenarbeit der nationalen Behörden mit den ausländischen Behörden zu ermöglichen, und wirksame internationale Mechanismen zu erarbeiten, um die grenzübergreifende Zusammenarbeit zur Anwendung der Gesetze zum Schutz der Privatsphäre zu erleichtern;

- Die Regionalkonferenzen der Unesco 2005 (Asien-Pazifik) und 2007 (Europa) den rioritären Charakter des Datenschutzes unterstreichen;

- Die Artikel 29-Gruppe der Europäischen Union Initiativen ergriffen hat, um das Verabschiedungsverfahren für zwingende Vorschriften für Unternehmen (BCR) und die Entwicklung vertraglicher Lösungen für den grenzübergreifenden Datenaustausch zu erleichtern.

- Die Staats- und Regierungschefs der «Frankophonie» sich zum Abschluss ihres 11. Gipfels im September 2006 in Budapest verpflichtet haben, auf nationaler Ebene die Arbeit an den erforderlichen gesetzlichen und verordnungsrechtlichen Regelungen zur Festschreibung des Rechtes der Menschen auf Datenschutz zu intensivieren und sich weltweit für die Ausarbeitung eines internationalen Übereinkommen einzusetzen, das die Effektivität des Rechts auf Datenschutz gewährleistet;

- Die APEC im November 2004 Leitprinzipien zum Schutz der Privatsphäre verabschiedet hat, um den Schutz der Privatsphäre zu verstärken und den Informationsfluss aufrechtzuerhalten. Im September 2007 hat die APEC eine Initiative «Privatsphäre» zur Entwicklung des Umsetzungsrahmens gestartet, um zertifizierte internationale Datenflüsse sicherzustellen, die den Bedürfnissen des Geschäftsverkehrs entsprechen, die Konformitätskosten senken, den Verbrauchern ein wirksames Instrument an die Hand geben, den Regulatoren effizientes Handeln ermöglichen und die Vorschriftenlast verringern;

- Die in Montreal am Rande der 29. Internationalen Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre gegründete Frankophone Vereinigung der Datenschutzbehörden (AFAPDP) in ihren Zielsetzungen die Ausarbeitung eines universellen Übereinkommens und die Bemühungen mit Blick auf den Beitritt von Nichtmitgliedstaaten des Europarats zum Übereinkommen STE Nr. 108 unterstützt;

- Das Iberoamerikanische Datenschutz-Netzwerk (RIPD) zum Abschluss seiner 6. Tagung im Mai 2008 in Kolumbien eine Erklärung angenommen hat, in der die internationalen Konferenzen für den Datenschutz und für die Privatsphäre aufgerufen werden, unabhängig von ihrer geografischen Zugehörigkeit ihre Bemühungen mit dem Ziel der Verabschiedung eines gemeinsamen Rechtsinstruments fortzusetzen;

- Die mittel- und osteuropäischen Datenschutzbehörden (APDCO) auf ihrer jüngsten Tagung im Juni 2008 in Polen ihren Willen bekundet haben, ihre Aktivitäten im Rahmen von APDCO fortzusetzen und zu verstärken und insbesondere gemeinsame Lösungen zu erarbeiten und die neuen Mitglieder bei der Implementierung ihrer Datenschutzgesetzgebung zu unterstützen.

Die Konferenz ist der Ansicht, dass:

- das Recht auf Datenschutz und den Schutz der Privatsphäre ein Grundrecht der Menschen ist, unabhängig von ihrer Staatsangehörigkeit und ihrem Wohnsitz;
- in der sich ausbreitenden Informationsgesellschaft das Recht auf Datenschutz und auf den Schutz der Privatsphäre in einer demokratischen Gesellschaft eine unerlässliche Voraussetzung ist, um die Achtung der Rechte der Personen, den freien Fluss von Informationen und eine offene Marktwirtschaft zu gewährleisten;
- die Globalisierung des Austauschs und der Verarbeitung personenbezogener Daten, die Komplexität der Systeme, die Schäden, die durch eine unangemessene Nutzung immer leistungsfähigerer Technologien entstehen können und der Anstieg der Sicherheitsmaßnahmen eine rasche und angemessene Antwort erfordern, um dieAchtung der Grundrechte und -freiheiten, insbesondere des Rechts auf Schutz der Privatsphäre, zu gewährleisten;
- die anhaltenden Disparitäten im Bereich des Datenschutzes und der Achtung der Privatsphäre weltweit, insbesondere wegen des Fehlens von Garantien in mehreren Staaten, dem Austausch personenbezogener Daten und der Schaffung eines effizienten, globalen Datenschutzes schaden;
- die Entwicklung internationaler Regeln, die die Achtung des Datenschutzes und des Schutzes der Privatsphäre einheitlich gewährleisten, eine Priorität darstellt;
- die Anerkennung dieser Rechte die Verabschiedung eines universellen, zwingenden Rechtsinstruments erfordert, das die in den verschiedenen bestehenden Instrumenten festgeschriebenen gemeinsamen Prinzipien des Datenschutzes und der Achtung der Privatsphäre bestätigt, auflistet und ergänzt und die internationale Zusammenarbeit zwischen Datenschutzbehörden verstärkt;
- die Umsetzung der von Organisationen wie der APEC oder der OECD entwickelten Leitlinien, insbesondere derjenigen, die die Annahme eines internationalen Rahmens zur Verbesserung der Achtung des Rechts auf Datenschutz und auf den Schutz der Privatsphäre bei grenzüberschreitenden Datenflüssen betreffen, eine positive Etappe zur Erreichung dieses Ziels darstellt;

- der Beitritt zu zwingenden Instrumenten mit universeller Gültigkeit, wie das Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (STE Nr. 108) und sein Zusatzprotokoll über die Kontrollbehörden und den grenzüberschreitenden Datenfluss (STE Nr. 181), die Grundprinzipien des Datenschutzes enthalten, den Austausch von Daten zwischen Parteien erleichtern kann; diese Instrumente sehen in der Tat Mechanismen und eine Plattform für die Zusammenarbeit zwischen den Datenschutzbehörden vor, tragen Sorge dafür, dass diese Behörden bei der Erfüllung ihrer Aufgaben völlig unabhängig sind und fördern die Einrichtung eines angemessenen Datenschutzniveaus;
- die 30. Internationale Datenschutzkonferenz eine geeignete Instanz für die Verabschiedung einer Strategie ist, die speziell auf die Verwirklichung dieser Ziele ausgerichtet ist.

Daher erneuert die Konferenz **ihren Appell**, ein zwingendes, universelles Rechtsinstrument zum Datenschutz und zum Schutz der Privatsphäre auszuarbeiten und **fasst dazu folgende Entschließungen:**

1. Die Konferenz unterstützt die Bemühungen des Europarats, das Grundrecht auf Datenschutz und auf den Schutz der Privatsphäre zu fördern. Die Konferenz fordert daher die Mitgliedstaaten dieser Organisation, die dies noch nicht getan haben, auf, die Ratifizierung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten und ihres Zusatzprotokolls zu prüfen. Die Konferenz fordert die Nichtmitgliedstaaten, die in der Lage sind, es zu tun, auf, zu erwägen, der Einladung des Europarats, dem Übereinkommen STE Nr. 108 und seinem Zusatzprotokoll beizutreten, Folge zu leisten. Mit Blick auf ihre Entschließung über die Errichtung einer Lenkungsgruppe zur Vertretung bei Tagungen internationaler Organisationen hat die Konferenz den Wunsch, auch einen Beitrag zu den Arbeiten des beratenden Ausschusses des Übereinkommens STE Nr. 108 zu leisten.

2. Die Konferenz unterstützt die Initiativen der APEC, der OECD und anderer regionaler Organisationen und internationaler Foren für die Entwicklung wirksamer Mittel zur Förderung besserer internationaler Standards für den Datenschutz und den Schutz der Privatsphäre.

3. **Die Konferenz beauftragt** eine Arbeitsgruppe, die von der den 31. Internationalen Konferenz ausrichtenden Behörde koordiniert wird und sich aus den interessierten nationalen Datenschutzbehörden zusammensetzt, einen **gemeinsamen Vorschlag zur Erstellung internationaler Normen zum Schutz der Privatsphäre und zum Schutz personenbezogener Daten** abzufassen und ihr auf ihrer nichtöffentlichen Sitzung vorzulegen, wobei folgender Kriterien vorgegeben werden:

   - Vornahme einer Bestandsaufnahme der Grundsätze und Rechte im Bereich des Schutzes personenbezogener Daten in den verschiedenen geografischen Gebieten der Welt, wobei besonders auf Gesetzestexte oder andere Texte abzustellen ist, die in den regionalen und internationalen Foren auf weitgehenden Konsens gestoßen sind;
   - Erarbeitung einer Zusammenstellung von Prinzipien und Rechten, die die bestehenden Texte widerspiegelt und ergänzt und dadurch die Erreichung eines Höchstmaßes an internationaler Akzeptanz zur Sicherung eines hohen Schutzniveaus ermöglicht;
   - Beurteilung der Sektoren, in denen diese Rechte und Prinzipien Anwendung finden, einschließlich der Varianten, die den Akzent auf die Harmonisierung ihrer Anwendungsbereiche legen;
   - Bestimmung der grundlegenden Kriterien, die ihre tatsächliche Anwendung gewährleisten, unter Berücksichtigung der Verschiedenheit der Rechtssysteme;
   - Prüfung der Rolle, die die Selbstregulierung spielen muss;
   - Formulierung wesentlicher Garantien für bessere und flexiblere internationale Datentransfers.

Bei dem Verfahren, das zur Abfassung dieses gemeinsamen Vorschlags führt, sollen die öffentlichen und privaten Organisationen und Instanzen zu einer breiten Beteiligung an den Arbeitsgruppen und an Foren und Anhörungen ermutigt werden, um zu einem möglichst umfassenden institutionellen und gesellschaftlichen Konsens zu gelangen. Besondere Aufmerksamkeit sollte den laufenden Arbeiten der Internationalen Organisation für Normung (ISO) und der Kommission für internationales Recht gewidmet werden.

4.1.8 Entschliessung zum Schutz der Privatsphäre von Kindern im Internet

30. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre Straßburg, 17. Oktober 2008

Entschließung zum Schutz der Privatsphäre von Kindern im Internet

Antragstellerin:

Die Datenschutzbeauftragte von Kanada

Unterstützt durchs:

Datenschutzbeauftragter, Neuseeland

La Commission Nationale de l'Informatique et des Libertés (Frankreich)

Datenschutzbeauftragter, Irland

Beauftragter für den Datenschutz und Informationsfreiheit, Berlin

Überall in der Welt gehen die Jugendlichen von zu Hause und von der Schule aus sowie über ihre kabellosen Geräte ins Internet. Sie nutzen das Internet zur sozialen Interaktion – sie tauschen Geschichten, Ideen, Fotos und Videos aus, sie bleiben den Tag über durch SMS-Mitteilungen in Kontakt mit ihren Freunden und sie beteiligen sich an Online-Spielen gemeinsam mit anderen Personen am anderen Ende der Welt.

Dabei werden die Jugendlichen auch mit den Schwierigkeiten und Herausforderungen bezüglich des Schutzes ihrer persönlichen Daten im Internet konfrontiert. Das Fehlen einer Regelung bei zahlreichen Internetdiensten macht die Sache schwierig. Viele der bei Jugendlichen beliebtesten Websites sammeln große Mengen personenbezogener Daten für Verkaufs- und Marketingzwecke.

Mit steigender Anzahl der im Internet angebotenen Anwendungen und Technologien wird die Menge der gesammelten und aufbewahrten personenbezogenen Daten immer größer. Heute sind sich die Jugendlichen oft nicht darüber bewusst, dass ihre Auskünfte, ihre Gewohnheiten und ihre Verhaltensweisen im Internet überwacht werden.

Untersuchungen zeigen, dass die Jugendlichen (wie auch zahlreiche Erwachsene) nur selten die Geheimhaltungserklärungen der von ihnen besuchten Websites lesen, was nicht überrascht, denn die Vertraulichkeitserklärungen zahlreicher Websites sind in einer technischen oder juristischen Fachsprache abgefasst, die für die meisten Leser schwer verständlich ist.

Wenn auch manche Jugendliche die mit ihren Online-Aktivitäten verbundenen Gefahren erkennen, so verfügen sie doch nicht über die Erfahrung, die technischen Kenntnisse oder die nötigen Instrumente, um diese Gefahren zu mindern. Oft kennen sie ihre gesetzlichen Rechte nicht.

Vor fast 20 Jahren hat die Generalversammlung der Vereinten Nationen 1989 ein Übereinkommen über die Rechte des Kindes verabschiedet. In diesem heißt es, dass die Staaten die Rechte des Kindes achten und schützen müssen, einschließlich ihres Rechtes auf den Schutz ihrer Privatsphäre.

Seit dieser Zeit bereiteten den Datenschutzbeauftragten die Verletzungen der Privatsphäre von Kindern im Internet immer mehr Sorgen.

In der am 20. Februar 2008 vom Ministerrat des Europarats angenommenen Erklärung zum Schutz der Würde, Sicherheit und der Privatsphäre von Kindern im Internet zeigt sich dieser von der Notwendigkeit überzeugt, Kinder über die lange Speicherdauer und über die Risiken der von ihnen ins Internet eingestellten Inhalte aufzuklären. Er erklärte darüber hinaus, dass, anders als bei der Strafverfolgung, keine fortbestehenden oder dauerhaft zugänglichen Aufzeichnungen über die von Kindern ins Internet eingestellten Inhalte existieren sollten, die deren Würde, Sicherheit und Privatsphäre angreifen oder ihnen auf andere Art und Weise jetzt oder zu einem späteren Zeitpunkt ihres Lebens schaden können.

Die Datenschutzbeauftragten haben zugleich erkannt, dass ein auf Erziehung ausgerichteter Ansatz, verbunden mit einer Regelung des Datenschutzes, eine der wirksamsten Methoden zur Bewältigung dieses Problems darstellt. So haben mehrere Länder innovative, auf Erziehung angelegte Konzepte umgesetzt, um der Herausforderung zu begegnen, die der Schutz der Privatsphäre von Kindern im Internet darstellt.

Kinder und Jugendliche haben ein Recht darauf, sich online sicher bewegen und positive Erfahrungen machen zu können, bei denen sie die Absichten der Personen, mit denen sie interagieren, kennen und verstehen.

Die auf der 30. internationalen Konferenz versammelten Beauftragten für den Datenschutz und für die Privatsphäre haben beschlossen:

- die Erarbeitung von Ansätzen zu fördern, die auf Erziehung angelegt sind, um die Lage in Bezug auf den Schutz der Privatsphäre im Internet auf nationaler wie auf internationaler Ebene zu verbessern;
- bemüht zu sein, dafür zu sorgen, dass Kinder und Jugendliche in der ganzen Welt Zugang zu einem sicheren Online-Umfeld haben, das ihre Privatsphäre respektiert;
- mit Partnern und Akteuren im eigenen Land und im Ausland zusammenzuarbeiten, in der Erkenntnis, dass die Zusammenarbeit mit den Fachleuten, die das tägliche Leben der Kinder beeinflussen, von entscheidender Bedeutung ist;
- miteinander zu arbeiten, um beispielhafte Praktiken auszutauschen und Aktivitäten zur Erziehung der Öffentlichkeit durchzuführen, um Kinder und Jugendliche stärker zu sensibilisieren hinsichtlich der Gefahren in Bezug auf den Schutz ihrer Privatsphäre, die mit ihren Online-Aktivitäten verbunden sind, und bezüglich der sich ihnen bietenden Möglichkeiten einer aufgeklärten Wahl, um ihre persönlichen Informationen zu kontrollieren;
- bei Erziehenden die Einsicht zu fördern, dass die Sensibilisierung für den Schutz der Privatsphäre einen wesentlichen Aspekt der Kindererziehung darstellt und in ihr Unterrichtsprogramm aufgenommen werden muss;
- zu fordern, dass die Behörden Gesetze erlassen, die die Sammlung, Verwendung und Mitteilung personenbezogener Daten von Kindern einschränken, einschließlich geeigneter Bestimmungen für den Fall von Verstößen;
- bei Online-Werbung für Kinder oder verhaltensbezogener Werbung geeignete Einschränkungen bei der Sammlung, Verwendung und Mitteilung personenbezogener Daten von Kindern zu fordern;
- die Betreiber von Websites für Kinder anzuhalten, ihr soziales Bewusstsein unter Beweis zu stellen, indem sie Vertraulichkeitserklärungen und Nutzungsvereinbarungen einführen, die klar, einfach und verständlich sind und indem sie die Nutzer über die Gefahren für den Schutz der Privatsphäre und die Sicherheit sowie über die ihnen auf der Website gebotenen Wahlmöglichkeiten aufklären.

4.1.9 Entschliessung zum Datenschutz in sozialen Netzwerkdiensten

30. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre Straßburg, 15. - 17. Oktober 2008

Entschließung zum Datenschutz in Sozialen Netzwerkdiensten

Antragsteller:

Berliner Beauftragter für Datenschutz und Informationsfreiheit, Deutschland

Unterstützt durch:

Commission Nationale de l'Informatique et des Libertés (CNIL), Frankreich;

Bundesbeauftragter für Datenschutz und Informationsfreiheit, Deutschland;

Garante per la protezione dei dati personali, Italien;

College Bescherming Persoonsgegevens, Niederlande;

Privacy Commissioner, Neuseeland;

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB), Schweiz

Entschließung

Soziale Netzwerkdienste[1] haben in den letzten Jahre große Beliebtheit erworben. Diese Dienste bieten ihren Teilnehmern Interaktionsmöglichkeiten auf der Basis von selbst generierten persönlichen Profilen, die in einem noch nie da gewesenen Ausmaß die Veröffentlichung persönlicher Informationen zu den betreffenden Personen

[1] «Ein sozialer Netzwerkdienst stellt ab auf den Aufbau [...] sozialer Online-Netzwerke für Gruppen von Menschen, die gemeinsame Interessen und Aktivitäten teilen oder daran interessiert sind, die Interessen und Aktivitäten Anderer zu erkunden […]. Die meisten Dienste sind hauptsächlich webbasiert und bieten Nutzern eine Reihe verschiedener Interaktionsmöglichkeiten […]». Zitat aus Wikipedia: http://en.wikipedia.org/wiki/Social_network_service.

(und auch anderen Personen) mit sich bringen. Die sozialen Netzwerkdienste bieten zwar ein neues Spektrum von Möglichkeiten für Kommunikation und den Echtzeit-Austausch von nformationen jeder Art, die Nutzung dieser Dienste kann jedoch auch eine Gefährdung der Privatsphäre ihrer Nutzer - und Anderer - mit sich bringen, denn personenbezogene Daten einzelner Personen werden in bisher unbekannter Weise und Menge öffentlich (und global) zugänglich, einschließlich großer Mengen digitaler Fotos und Videos.

Der Einzelne läuft Gefahr, die Kontrolle über die Nutzung der Daten durch Andere zu verlieren, wenn sie erst einmal im Netzwerk publiziert sind: Während der Community-Bezug sozialer Netzwerke die Vorstellung erweckt, die Veröffentlichung der eigenen persönlichen Daten laufe in etwa auf das Gleiche hinaus, wie früher das Mitteilen von Information unter Freunden von Angesicht zu Angesicht, können Profildaten tatsächlich für alle Teilnehmer einer Community (deren Zahl in die Millionen gehen kann) verfügbar sein.

Derzeit gibt es wenig Schutz dagegen, dass personenbezogene Daten jeder Art aus Profilen kopiert werden – durch andere Mitglieder des Netzwerks oder durch unbefugte netzwerkfremde Dritte – und zum Aufbau von Persönlichkeitsprofilen verwendet werden oder dass die Daten anderweitig wieder veröffentlicht werden. Es kann sehr schwierig - und manchmal unmöglich - sein zu erreichen, dass Daten, wenn sie einmal publiziert sind, wieder vollständig aus dem Internet entfernt werden. Selbst nach ihrer Löschung auf der ursprünglichen Website (z.B. dem sozialen Netzwerk) können Kopien bei Dritten oder bei den Anbietern der sozialen Netzwerkdienste verbleiben. Personenbezogene Daten aus Nutzerprofilen können auch außerhalb des Netzwerks bekannt werden, wenn sie von Suchmaschinen indexiert werden. Hinzu kommt, dass manche Anbieter sozialer Netzwerkdienste über Applikationsprogrammierschnittstellen Drittanbietern Nutzerdaten zur Verfügung stellen, die dann unter der Kontrolle dieser Dritten stehen.

Ein Beispiel von Wiederverwendungen, das großes öffentliches Aufsehen erregt hat, ist die Praxis von Personalverantwortlichen, Nutzerprofile von Stellenbewerbern oder Angestellten zu durchsuchen. Presseberichten zufolge gibt bereits heute ein Drittel der Personalverantwortlichen an, bei ihrer Arbeit Daten aus sozialen Netzwerkdiensten zu nutzen, z. B. um die einzelnen Angaben von Bewerbern zu überprüfen und/oder zu ergänzen.

Profilinformationen und Verkehrsdaten werden von Anbietern sozialer Netzwerkdienste auch zur Weiterleitung zielgerichteter Werbung an ihre Nutzer verwendet.

Sehr wahrscheinlich werden in Zukunft noch weitere unerwartete Verwendungen von Informationen in Nutzerprofilen auftreten.

Zu weiteren, bereits jetzt identifizierten spezifischen Risiken für Datenschutz und Datensicherheit zählen erhöhte Risiken durch Identitätsbetrug, der durch die umfangreiche Verfügbarkeit personenbezogener Daten in Nutzerprofilen begünstigt wird, und durch eine mögliche Übernahme von Profilen durch unbefugte Dritte. Die 30. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre erinnert daran, dass diese Risiken bereits in dem Dokument «Bericht und Empfehlung zum Datenschutz in sozialen Netzwerkdiensten» («Rom-Memorandum»)[2] der 43. Tagung der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommuniktion (3. - 4. März 2008) und in dem ENISA Positionspapier Nr. 1 «Security Issues and Recommendations for Online Social Networks»[3] (Oktober 2007) analysiert wurden.

Die in der Internationalen Konferenz versammelten Datenschutzbeauftragten sind von der Notwendigkeit überzeugt, dass als Erstes eine intensive Informationskampagne unter Beteiligung aller öffentlichen und privaten Interessengruppen – von Regierungsstellen bis zu Bildungseinrichtungen wie Schulen, von Anbietern sozialer Netzwerkdienste bis zu Verbraucher- und Nutzerverbänden, einschließlich der Datenschutzbeauftragten selbst – durchgeführt werden muss, um den vielfältigen mit der Nutzung sozialer Netzwerkdienste verbundenen Gefahren vorzubeugen.

Empfehlungen

180 In Anbetracht der besonderen Natur der Dienste und der kurz- und langfristigen Gefahren für die Privatsphäre des Einzelnen richtet die Konferenz folgende Empfehlungen an Nutzer und Anbieter sozialer Netzwerkdienste:

Nutzer sozialer Netzwerkdienste

Organisationen, denen am Wohl der Nutzer sozialer Netzwerke gelegen ist – einschließlich Diensteanbieter, Regierungen und Datenschutzbehörden – sollten mithelfen, die Nutzer über den Schutz ihrer personenbezogenen Daten aufzuklären und die folgende Botschaften zu vermitteln.

1. Veröffentlichung von Daten

Nutzer sozialer Netzwerkdienste sollten sich sorgfältig überlegen, welche persönlichen Daten sie - wenn überhaupt - in einem sozialen Netzwerkprofil publizieren. Sie sollten bedenken, dass sie zu einem späteren Zeitpunkt mit einer Information oder

[2] http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf?1208438491
[3] http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf

mit Bildern konfrontiert werden könnten, z. B. wenn sie sich um eine Arbeitsstelle bewerben. Insbesondere sollten Minderjährige vermeiden, ihre Privatanschrift oder ihre Telefonnummer mitzuteilen.

Privatpersonen sollten sich überlegen, ob es nicht ratsam wäre, in einem Profil anstelle ihres wirklichen Namens ein Pseudonym zu verwenden. Dabei sollten sie jedoch nicht vergessen, dass auch die Benutzung von Pseudonymen nur einen begrenzten Schutz gewährt, da Dritte in der Lage sein können, ein solches Pseudonym aufzudecken.

2. Die Privatsphäre Anderer

Nutzer sollten auch die Privatsphäre Anderer achten. Sie sollten besonders vorsichtig sein bei der Veröffentlichung personenbezogener Daten Anderer (einschließlich Bildern, oder sogar mit Zusatzinformationen versehenen Bildern) ohne die Einwilligung der betreffenden Personen.

Anbieter sozialer Netzwerkdienste

Anbieter sozialer Netzwerkdienste tragen eine besondere Verantwortung dafür, die Belange von Personen, die soziale Netzwerke nutzen, zu beachten und zu wahren. Sie sollten nicht nur die Regelungen des Datenschutzrechts einhalten, sondern auch die folgenden Empfehlungen umsetzen.

1. Datenschutzvorschriften und -standards

Anbieter, die in verschiedenen Ländern oder sogar weltweit tätig sind, sollten die Datenschutzstandards der Länder einhalten, in denen sie ihre Dienste betreiben. Zu diesem Zweck sollten die Anbieter Datenschutzbehörden konsultieren, wenn und soweit dies notwendig ist.

2. Aufklärung der Nutzer

Anbieter sozialer Netzwerkdienste sollten ihre Nutzer über die Verarbeitung ihrer personenbezogenen Daten transparent und offen informieren. Es sollte auch aufrichtig und verständlich über mögliche Folgen einer Veröffentlichung persönlicher Daten in einem Profil und über verbleibende Sicherheitsrisiken sowie über gesetzliche Zugriffsrechte Dritter (einschließlich z.B. von Strafverfolgungsbehörden) aufgeklärt werden. Eine solche Aufklärung sollte auch Hinweise dazu enthalten, wie Nutzer mit personenbezogenen Daten von Dritten umgehen sollten, die in ihren Profilen enthalten sind.

3. Nutzerkontrolle

Anbieter sollten die Kontrolle der Nutzer über die Verwendung ihrer Profildaten durch andere Community-Mitglieder weiter verbessern. Sie sollten die Einschränkung der Sichtbarkeit ganzer Profile sowie von in Profilen enthaltenen Daten, und in Community-Suchfunktionen ermöglichen.

Die Anbieter sollten auch eine Kontrolle der Nutzer über die Nutzung von Profil- und Verkehrsdaten, z. B. für zielgerichtete Werbung, ermöglichen. Als ein Minimum sollten eine Opt-out-Möglichkeit für allgemeine Profildaten und eine Opt-in-Möglichkeit für sensible Profildaten (z.B. politische Überzeugungen, sexuelle Orientierung) und Verkehrsdaten geboten werden.

4. Datenschutzfreundliche Standardeinstellungen

Darüber hinaus sollten Anbieter datenschutzfreundliche Standardeinstellungen für Nutzerprofilinformationen anbieten. Standardeinstellungen spielen eine Schlüsselrolle beim Schutz des Privatsphäre der Nutzer: Es ist bekannt, dass lediglich eine Minderheit von Nutzern, die sich bei einem Dienst anmelden, irgendwelche Änderungen daran vornimmt.

Diese Einstellungen müssen bei einem sozialen Netzwerkdienst, der sich an Minderjährige wendet, besonders restriktiv sein.

5. Sicherheit

Anbieter sollten die Sicherheit ihrer Informationssysteme weiter verbessern und aufrechterhalten und die Nutzer gegen betrügerische Zugriffe auf ihre Profile schützen, indem sie für die Konzeption, die Entwicklung und den Betrieb ihrer Anwendungen anerkannte Methoden einschließlich unabhängigem Auditing und unabhängiger Zertifizierung verwenden.

6. Auskunftsrechte

Anbieter sollten Personen (gleichgültig ob Mitglieder des sozialen Netzwerkdienstes oder nicht) ein Recht auf Auskunft zu ihren personenbezogenen Daten gewähren und erforderlichenfalls diese Daten berichtigen.

7. Löschung von Nutzerprofilen

Anbieter sollten den Nutzern die Möglichkeit geben, ihre Mitgliedschaft auf einfache Weise zu beenden und ihre Profile sowie alle Inhalte oder Informationen, die sie in dem sozialen Netzwerk publiziert haben, zu löschen.

8. Pseudonyme Nutzung des Dienstes

Anbieter sollten als Option die Möglichkeit der Einrichtung und Verwendung pseudonymer Profile anbieten und zur Nutzung dieser Option ermutigen.

9. Zugriff durch Drittpersonen

Anbieter sollten wirksame Maßnahmen ergreifen, um das Durchsuchen und/oder massenweise Herunterladen (oder „bulk harvesting") von Profildaten durch Dritte zu verhindern.

10. Indexierbarkeit der Nutzerprofile

Die Anbieter sollten sicherstellten, dass Nutzerdaten von externen Suchmaschinen nur durchsucht werden können, wenn der Nutzer dazu seine ausdrückliche, vorherige und informierte Einwilligung erteilt hat. Die Nichtindexierbarkeit von Profilen durch Suchmaschinen sollte als Standard eingestellt sein.

4.2 Öffentlichkeitsprinzip

4.2.1 Empfehlung an das Eidgenössische Departement für auswärtige Angelegenheiten: «Projektunterlagen DEZA»

Bern, den 28. Juli 2008

Empfehlung

gemäss

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

zum Schlichtungsantrag von

X
(Antragsteller)

gegen

Eidg. Departement für auswärtige Angelegenheiten (EDA), Bern

I. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte stellt fest:

A. Schlichtungsantrag Nr. 1

1. Der Antragsteller teilte der Chefin des EDA und den Verantwortlichen der Direktion für Entwicklung und Zusammenarbeit (DEZA) mit E-Mail vom 20. März 2007 mit, er «*hätte gerne Auskunft über ALLE laufenden Projekte von SKH [Schweizerische Korps für humanitäre Hilfe; der Beauftragte] / DEZA, inklusive aller relevanten Projektdaten: Art, Ziel, Begründung, Begünstigte, involvierte Parteien und deren Vertreter in den diversen Funktionen und Fachgebieten, getroffene Vereinbarungen, Beginn, geplantes Ende, gegenwärtiger Stand der Umsetzung, Budget, Budgetrevisionen, getätigte Zahlungen, wichtige Meilensteine etc.*» Gleichzeitig bot sich der Antragsteller als Projektleiter für die Erstellung einer entsprechenden Datenbank an.

   Am 21. März 2007 bedankte sich das EDA (nachfolgend anstelle von DEZA und/oder SKH) beim Antragsteller für die «*angebotenen Dienste*» und zeigt sich bereit, ihm «*in einem persönlichen Gespräch das System zu erklären, mit dem wir arbeiten, bzw. zu arbeiten haben*.»

2. Am 7. April 2007 verlangte der Antragsteller, «*um die (…) verbleibende Zeit gut zu nutzen*,» Einblick in Projektdaten der Programme «Tsunami-Wiederaufbau in Südasien (Indonesien, Thailand, Sri Lanka)» und «Wälder und Agro-Ökosysteme der Andenregion (PROBONA)». Weiter führte er aus, ihn interessieren «*die folgenden Daten und Fakten obgenannter Programme, sowie sämtlicher zugehöriger Projekte und Teilprojekte: Name des Programms / Projekts / Teilprojekts, Land / Ort / Adresse / Kontaktdaten, Programm- / Projekt- / Teilprojektbudget, Saläranteile Zentrale / Kobü, Saläre CH Expatriates, Saläre lokal Angestellter, übrige Kosten lokal, übrige Kosten CH, aktuelle und geplante Laufzeit, Beschrieb, Rahmenbedingungen, Zielsetzungen, Meilensteine, Standards, Messgrössen / Indikatoren, aktueller Stand / Resultate, Vereinbarungen mit lokalen Partnern, Schlüsseldokumente, Kontaktpersonen CH, Kontaktpersonen lokal, lokale Partner / Begünstigte, Kontaktpersonen lokaler Partner / Begünstigter, lokale Beauftragte / Konsulenten, Kontaktpersonen lokaler Beauftragter / Konsulenten*.»

3. Am 13. April 2007 gelangte der Antragsteller erneut ans EDA und beharrte mit Verweis auf das Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsgesetz BGÖ, SR 152.3) «*auf der vollumfänglichen Beantwortung meiner ursprünglichen Anfrage*».

4. Mit Brief vom 18. April 2007 teilte das EDA dem Antragsteller mit: «*In Ihrem Gesuch verlangen Sie Einsicht in ganze Dossier, Ihr Gesuch betrifft unzählige Dokumente. Die von Ihnen gelieferten Angaben reichen nicht aus, um die verlangten Dokumente zu identifizieren*.» Das EDA forderte den Antragsteller mit Verweis auf die Art. 10 Abs. 3 BGÖ und Art. 7 der Verordnung vom 24. Mai 2006 über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsverordnung, VBGÖ, SR 152.31) und unter Ansetzung einer Frist auf, die Anfrage zu präzisieren. Weiter wies das EDA darauf hin, dass der Zugang zu Dokumenten gemäss Öffentlichkeitsgesetz grundsätzlich gebührenpflichtig ist.

5. Mit E-Mail vom 20. April 2007 zu Handen des EDA vertrat der Antragsteller die Ansicht, dass die von ihm gemachten Angaben zur Beantwortung seiner Anfrage vollends ausreichend seien.

6. Mit E-Mail vom 25. April 2007 verlangte der Antragsteller «als Nachtrag» zu seiner E-Mail vom 20. April 2007 ein Verzeichnis sämtlicher laufender Projekte von DEZA und SKH zukommen zu lassen. Weiter möchte er «*Einblick in alle direktionsinternen sowie externen Projekt-Monitoring- und Projekt-Schlussberichte von DEZA und SKH*», «*in sämtliche Reporte Y, über Projekte von DEZA und SKH in Sri Lanka, wie allen anderen Projektländern, ab Januar 2005 bis zum heutigen Datum*.» Ferner ersuchte er das EDA, ihm «*die aktuellsten, detaillierten (jedes einzelne Projekt und Teil-Projekt beinhaltend) und vollständigen buchhalterischen Übersichten über die Budgets und Mittelfluss zu all diesen Projekten und von DEZA und SKH insgesamt zukommen zu lassen, inklusive aller Salärkosten also der detaillierten und vollständigen Zuteilung und Verwendung des Gesamtbudgets von DEZA und SKH – sowie die direktionsinterne Begründung und Selbstevaluation dieser Zuteilung und Verwendung, sowie der erzielten Resultate*.»

7. Am 27. April 2007 teilte der Antragsteller dem EDA per E-Mail mit, dass ihn «*unter den erwähnten Evaluationen (…) insbesondere auch jene der GPK-S*» [Geschäftsprüfungskommission des Ständerates; der Beauftragte] interessiere und dass er «*sämtliche Dokumente wolle, die bei der DEZA und beim*

EDA dazu vorliegend sind.» Weiter interessierten ihn «*insbesondere die vollständigen Reise- und Spesenabrechnungen aller Mitarbeiter, von Januar 2005 bis dato, speziell der Direktoren*» sowie weiterer Mitarbeiter des SKH.

8. Das EDA teilte dem Antragsteller mit E-Mail vom 2. Mai 2007 mit, dass er «*Einblick in ganze Dossiers und nicht nur in einzelne Dokumente verlange*» und er seine Anfrage «*noch ausgeweitet (habe) indem Sie Einblick in zusätzliche Dokumente verlangten*.»

9. In einer E-Mail vom 3. Mai 2007 erwähnte der Antragsteller, dass er an der «*Anfrage nach Einsicht in die Ausschreibungen und Bewerbungen des SKH, und um[sic!] die Adressen der Korps-Angehörigen*» festhalte.

10. Auf eine weitere E-Mail des Antragstellers vom 8. Mai 2007 schlug ihm das EDA zur Klärung der Fragen eine Besprechung vor. Mit E-Mail vom 10. Mai 2007 nahm der Antragsteller die Einladung an und legte dem EDA gleichzeitig eine Auflistung vor, in der die gewünschten Dokumente und Dossiers in 4 Dringlichkeitsstufen eingeteilt waren.

    (Die Besprechung zwischen dem Antragsteller und Vertretern des EDA fand am 29. Mai 2007 statt.)

11. Am gleichen Tag, also am 10. Mai 2007, reichte der Antragsteller beim Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (Beauftragter) den Schlichtungsantrag Nr. 1 ein.

B. Schlichtungsantrag Nr. 2

1. Am 26. Juni 2007 verlangte der Antragsteller per E-Mail, «*mir von den gewünschten Schluss-Berichten vorab wenigstens den Einsatz-Schlussbericht von Z (2004-2007, Sri Lanka), sowie sämtliche nach Erlassdatum BGÖ verfassten Einsatz-Schlussberichte / End of Mission Report von Country Directors der DEZA in Indonesien zuzustellen*.»

    (Die Berichte werden im Weiteren mit Schlussbericht Sri Lanka und Schlussbericht Indonesien bezeichnet.)

2. Das EDA teilte dem Gesuchsteller am 4. Juli 2007 mit, dass die Anfrage, welche sich auf End of Mission-reports bezieht, genügend präzisiert sei und als neues Zugangsgesuchs behandelt werde.

3. Das EDA teilte dem Antragsteller mit Schreiben vom 17. August 2007 mit, dass das Zugangsgesuch folgendermassen beurteilt wurde:

   - «Einsichtnahme in Schlussberichte»

     Der Zugang zu den Schlussberichten Sri Lanka und Indonesien wurde mit Verweis auf die nachfolgenden Ausnahmeklauseln eingeschränkt:

     - Art. 7 Abs. 1 Bst. b BGÖ (Beeinträchtigung der zielkonformen Durchführung konkreter behördlicher Massnahmen),
     - Art. 7 Abs. 1 Bst. d BGÖ (Beeinträchtigung der aussenpolitischen Interessen und der internationalen Beziehungen),
     - Art. 7 Abs. 2 BGÖ und Art. 9 BGÖ («aus Gründen des Persönlichkeitsschutzes»).

   Den Schlussberichten beigefügt war jeweils eine Stellungnahme der DEZA. Darin weist die DEZA «*Als Arbeitgeberin des Verfassers dieses Berichtes (…) auf Folgendes hin, dass bei einem eventuellen Gebrauch des Berichtes (X) durch Dritte berücksichtigt werden muss*: *‚Schlussberichte sind (…) grundsätzlich Ausdruck der subjektiven Meinung des Verfassers. Sie dienen der persönlichen Vorbereitung des aus dem Einsatz zurückkehrenden Korpsangehörigen für das Abschlussgespräch (‚debriefing') an der SKH-Zentrale in Bern. (…) Demzufolge handelt es bei einem «Schlussbericht» um ein bewusst subjektiv gehaltenes, internes, Arbeitsdokument, welches als Vorbereitung für ein Mitarbeitergespräch zwischen ArbeitnehmerIn und Arbeitgeberin dient. Im Gespräch selbst werden dann die im Bericht enthaltenen Aussagen besprochen, allfällige Meinungsverschiedenheiten geklärt, Massnahmen ins Auge gefasst sowie der Einsatz formell abgeschlossen.*

   Ein ‚Schlussbericht' einer dem SKH angehörenden Person über einen absolvierten Einsatz widerspiegelt daher in keiner Weise die Sicht der DEZA, sondern einzig die subjektive Meinung dieser Person. Die DEZA verzichtet auf eine Stellungnahme zum Bericht.»

   - «Anhang und Antworten des SKH/der DEZA und des EDA zum Schluss-Bericht Z (Korrespondenz mit Z)»

     Der Zugang zur Korrespondenz des EDA mit Z wurde mit Verweis auf die nachfolgenden Ausnahmeklauseln verweigert:

- Art. 7 Abs. 1 Bst. b BGÖ (Beeinträchtigung der zielkonformen Durchführung konkreter behördlicher Massnahmen),
- Art. 7 Abs. 2 BGÖ («aus Gründen des Persönlichkeitsschutzes»).

- «Zugang zu den Beilagen zum Z-Bericht (CD als Beilage zum Z-Bericht)»

  Auf der CD befänden sich «unzählige Dokumente». Soweit diese nicht vor Inkrafttreten des Öffentlichkeitsgesetzes vom EDA erstellt oder bei ihm eingegangen sind, würden «*Praktisch alle Dokumente (…) Personendaten (enthalten), welche vor einer Einsichtnahme abgedeckt werden müssten. Möglicherweise müssten noch weitere Passagen aus Gründen von Art. 7 ff. BGÖ eingeschwärzt werden*.» Weiter führte das EDA dazu aus: «*Für die nach Inkrafttreten des Öffentlichkeitsgesetzes erstellten Dokumente, ist eine Anonymisierung nicht möglich, weil es sich um derart umfangreiche Dokumente handelt, dass eine Anonymisierung mit einem verhältnismässigen Aufwand nicht zu leisten ist. Wenn eine Anonymisierung nicht möglich ist und keine Zustimmung der betroffenen Personen vorliegt, so erlaubt das Öffentlichkeitsgesetz nur in Ausnahmefällen das Zugänglichmachen von Dokumenten mit Personendaten, nämlich nur wenn überwiegende öffentliche Interessen am Zugang bestehen. Unseres Erachtens bestehen vorliegend keine überwiegenden öffentlichen Interessen am Zugang der auf der CD gespeicherten Dokumente, welche ein Zugänglichmachen ohne vorgängige Anonymisierung rechtfertigen würden. In Anwendung von Art. 9 Abs. 2 BGÖ i.V. mit Art. 19 des Datenschutzgesetzes können wir Ihnen daher keinen Einblick zu den auf der CD gespeicherten Dokumente gewähren*.»

4. Der Antragsteller reichte am 6. September 2007 beim Beauftragten einen Schlichtungsantrag ein. Das gleiche Schreiben ging mit dem Betreff «Aufsichtseingabe» auch an die Geschäftsprüfungskommission (GPK) der Parlamentsdienste. Es enthielt folgenden «*Antrag an EDÖB und GPK*

   a) Der ganze Z-Bericht, inklusive Anhang und Beilagen, ist aufgrund öffentlichen Interesses freizugeben. Die betroffenen Personen sind um ihre Zustimmung zur Namensnennung zu ersuchen. Mindestens die Namen und Funktionen öffentlicher Figuren (d. h. der obersten Führung von SKH/DEZA/EDA, wenn nicht aller leitenden Mitarbeiter) dürfen aufgrund des Persönlichkeitsschutzes jedoch NICHT unkenntlich gemacht werden, weil hier Fragen von öffentlichem Interesse und nicht irgendwelche Privat-Angelegenheiten betroffen sind.

b) Der vorliegende Indonesien-Bericht ist scheinbar nur ein Entwurf. Es ist die Endfassung auszuhändigen.

c) Die Misswirtschaft, die systematische Unterschlagung von Information und die aktenkundig gewordenen Lügen von leitenden Mitarbeitern und Führungskräften von EDA DEZA SKH sind zu untersuchen und zu sanktionieren.

d) Über Art und aktuellen Status, Kosten und Kostensplit der Projekte der DEZA ist mittels einer Web-Projekt-Datenbank detailliert und überprüfbar zu informieren, so dass sich die Öffentlichkeit, die Begünstigten - und vor allem auch die Verantwortlichen innerhalb von EDA DEZA SKH selbst - jederzeit ein genaues Bild über die «vielfältigen Aktivitäten» der DEZA machen können: Projekt-Monitoring wie es selbstverständlich sein muss. (Vgl. hierzu meine entsprechende Eingabe an SKH/DEZA.)

e) Falls a) (vorläufig) nicht stattgegeben werden sollte, ist eine akzeptable, die Integrität des Originals respektierende «Bearbeitung» auszuhändigen, «eingeschwärzt», nicht «eingeweisst», inklusive des gesamten Anhangs, sowie (mindestens) der erwähnten Bestandteile der Beilagen.

f) *Die mir seitens EDA DEZA SKH am 29. Mai im Bundeshaus versprochenen Projekt-Übersichten und Evaluationen der DEZA sind baldmöglichst auszuhändigen.*

g) Dem EDÖB sind bei offenkundigem Bedarf sofort wenigstens die in der Vernehmlassung zum BGÖ vorgesehenen personellen Ressourcen zu gewähren, prinzipiell aber genügend, dass Schlichtungsbegehren innert der gesetzlich vorgesehenen Frist bearbeitet werden können.

h) Das Kompetenzzentrum Öffentlichkeitsprinzip des EDA ist so zu verstärken, dass Einsichtsgesuche innert vertretbarer Frist gradlinig, aufrichtig und kompetent bearbeitet werden können.

i) Falls einzelnen Punkten nicht stattgegeben werden sollte, ist eine anfechtbare Antwort mit Verfügung auszustellen.»

C. Schlichtungsanträge Nr. 3 - 6

1. Am 15. August 2007 verlangte der Antragsteller «*Einsicht in sämtliche seit 1. Januar 2006 verfassten Sri Lanka-Projekt und Missions-Reporte von Y*». Gemäss Angaben des EDA hat der Antragsteller das Gesuch im Dezember 2007 telefonisch zurückgezogen. Im März 2008 bat das EDA den Antragsteller, seinen Rückzug schriftlich zu bestätigen. Dieser antwortete umgehend, dass er sich an «das erwähnte Gespräch nicht mehr erinnern» könne, er halte jedoch an all seinen Gesuchen weiterhin fest.

   Das EDA teilte dem Antragsteller am 6. Mai 2008 mit, dass für das Einschwärzen respektive Anonymisieren der fraglichen Dokumente mit Gebühren in der Höhe von vorsichtlich Fr. 800.- zu rechnen sei. Das EDA forderte den Antragsteller auf, entsprechend Art. 16 Abs. 2 VBGÖ sein weiteres Interesse innerhalb von 10 Tagen zu bestätigen, ansonsten das Gesuch als zurückgezogen gelte.

   Der Antragsteller reichte am 6. Juni 2008 beim Beauftragten einen Schlichtungsantrag (Schlichtungsantrag Nr. 3) ein.

2. Am 6. November 2007 reichte er ein Gesuch um «*Akteneinsicht in den Auftrag / Vertrag an / mit PwC, sowie den vollständigen Untersuchungsbericht und die Honorarbestimmungen / Abrechnungen*» im Zusammenhang mit der «Evaluation der Tsunami-Hilfe von SKH DEZA EDA» ein.

   Das EDA wies in der Beantwortung des Zugangsgesuchs am 6. Mai 2008 darauf hin, dass nicht die Firma PricewaterhouseCoopers, sondern die Firma KPMG einen entsprechenden Auftrag erhalten habe. Es lehnte den Zugang gestützt auf Art. 7 Abs. 1 Bst. g BGÖ (Berufs-, Geschäfts- oder Fabrikationsgeheimnisse) sowie aufgrund der Tatsache ab, dass der Endbericht noch nicht fertig gestellt sei.

   Der Antragsteller reichte am 6. Juni 2008 beim Beauftragten einen Schlichtungsantrag (Schlichtungsantrag Nr. 4) ein.

3. Am 27. März 2008 reichte der Antragsteller ein Gesuch um Zugang zu folgenden Dokumenten ein:

   - «Guidelines for Donor Agencies Regarding Rehabilitation / Relocation of the Tsunami Affected Schools, Prepared by Planning and Performance Review Division, Ministry of Education, Sri Lanka» vom 18. Februar 2005 «sowie»

- MoU (Memorandum of Understanding) between the Swiss Government and the Government of Sri Lanka, on Repairs and Reconstruction of Schools damaged by Tsunami on December 26, 2004 (unterzeichnet am 10. März 2005, durch den Schweizer Botschafter in Sri Lanka), inclusive Annex «List of Schools Proposed for Rebuilding by the Swiss Government».

Das EDA lehnte das Zugangsgesuch mit E-Mail vom 6. Mai 2008 mit der Begründung ab, dass beide Dokumente vor Inkrafttreten des Öffentlichkeitsgesetzes (1. Juli 2006) vom EDA erstellt respektive empfangen wurden und sie somit nicht in den Anwendungsbereich des Öffentlichkeitsgesetz fallen (Art. 23 BGÖ).

Der Antragsteller reichte am 6. Juni 2008 beim Beauftragten einen Schlichtungsantrag (Schlichtungsantrag Nr. 5) ein.

4. Am 10. Juni 2008 reichte der Antragsteller folgenden Schlichtungsantrag (Schlichtungsantrag Nr. 6) ein:

«*BGÖ-Schlichtungsgesuch an den EDÖB, in Sachen Desinformation, Intransparenz, Misswirtschaft und Repression sachlicher, interner Kritik der DEZA, betreffend Einsichtsgesuche in*:

a) Antworten EDA/DEZA/SKH auf Schlussreport Z (s. nachfolgende E-Mails, als Anhang 1 und 2)

b) Transportbelege persönliche Effekten Z (s. nachfolgendes E-Mail, als Anhang 1)

c) Videoaufnahme Fachgruppentagung SKH, Jahrestagung HH 2007 (s. nachfolgendes E-Mail, als Anhang 2)

d) Bewerbungen und Arbeitsverträge SKH (s. nachfolgendes E-Mail, als Anhang 3)

e) Reisebelege Führungsverantwortliche EDA/DEZA/SKH (s. nachfolgendes E-Mail, als Anhang 3) sowie

f) Ersuchen um Kostenübernahme/-Erlass, bzw. Klärung Datenschutzmassnahmen Sponsoring»

D. Schlichtungsverfahren

1. Der Beauftragte führte zwei Schlichtungsverhandlungen mit dem Antragsteller und Vertretern des EDA durch, wobei in keinem Punkt eine Einigung erzielt werden konnte.

   An der ersten Schlichtungsverhandlung verwies das EDA auf die Vielzahl der laufenden und abgeschlossenen Projekte der DEZA.[1] Es führte u.a. aus, dass bereits die Gesamtdokumentation für ein einzelnes Projekt ausserordentlich umfangreich sei. Illustriert wurde dies anhand eines *Teil*projektes des Tsunami-Wiederaufbauprogramms, das alleine 13 Bundesordner umfasst. Im Weiteren präsentierte das EDA Listen mit allen Projekten und zeigte sich bereit, dem Antragsteller in der Spezifizierung behilflich zu sein.

   Der Antragsteller anerkannte sowohl während der zweiten Schlichtungsverhandlung als auch im Mailverkehr mit dem Beauftragten, dass sich einige der von ihm verfolgten Ziele nicht mit dem Öffentlichkeitsgesetz erreichen lassen. Trotzdem bekräftige er stets, an allen Zugangsgesuchen und Schlichtungsanträgen festzuhalten.

   So vertrat er beispielsweise in Bezug auf den ersten Schlichtungsantrag die Ansicht, dass «*die Transparenz der DEZA bei weitem nicht genügt. Misswirtschaft wird anhaltend kaschiert, interne sachliche Kritik wird unterdrückt, Öffentlichkeit und Parlament werden desinformiert*.» Daher halte er an seinem ersten Schlichtungsantrag fest. Das EDA war in diesem Punkte der Meinung, «dass es zu Recht eine Präzisierung des Zugangsgesuches verlangt hat (Art. 10 Abs. 3 i.V.m. Art. 7 BGÖ).»

2. Zusätzlich zu den Schlichtungsverhandlungen empfing der Beauftragte den Antragsteller zu einem Einzelgespräch und erläuterte ihm ausführlich den Anwendungsbereich und die Grenzen des Öffentlichkeitsgesetzes. Dabei erklärte der Beauftragte insbesondere die Fristenregelung des Öffentlichkeitsgesetzes und dessen Zusammenwirken mit dem Bundesgesetz über den Datenschutz (DSG, *SR* 235.1).

[1] Übersicht auf http://www.deza.admin.ch/de/Home/Projekte

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

A. Schlichtungsverfahren und Empfehlung 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. 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.

3. Der Antragsteller hat Zugangsgesuche nach Art. 6 BGÖ beim EDA eingereicht und ablehnende Antworten erhalten. Als Teilnehmer an einem vorangegangenen Gesuchsverfahren ist er zur Einreichung der Schlichtungsanträge Nr. 1 und 2 berechtigt. Sie wurden formgerecht (einfache Schriftlichkeit) und fristgerecht (innert 20 Tagen nach Empfang der Stellungnahme der Behörde) beim Beauftragten eingereicht.

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

4. Die Schlichtungsanträge Nr. 3[4], 4 und 5 wurden nicht innert 20 Tagen nach Empfang der einzelnen Stellungnahmen des EDA (alle datieren vom 6. Mai 2008) beim Beauftragten eingereicht. Der Antragsteller anerkannte dies und führte in seinen Schlichtungsanträgen dazu aus, dass das EDA die Frist zur Beantwortung seiner Zugangsgesuche deutlich überschritten habe, weshalb er das gleiche Recht für die Einreichung der Schlichtungsanträge beanspruche.

   Die Fristen für die Beantwortung eines Zugangsgesuchs sind in Art. 12 BGÖ festgehalten. Es handelt sich dabei um eine *Ordnungsfrist*.[5] Wird diese von der Behörde nicht eingehalten, so liegt eine unzulässige Rechtsverzögerung vor, weshalb ein Betroffener gestützt auf Art. 13 Abs. 1 Bst. b BGÖ i.V.m. Art. 13 Abs. 2 BGÖ nach Ablauf der der Behörde zur Stellungnahme verfügbaren Zeit einen Schlichtungsantrag einreichen kann.[6]

   Im Gegensatz zur eben erwähnten Ordnungsfrist der Behörde handelt es sich bei der Frist zur Einreichung eines Schlichtungsantrags (Art. 13 Abs. 2 BGÖ) um eine *Verwirkungsfrist*.[7] Diese Frist kann nicht verlängert werden, und der Antragsteller muss bei der Behörde allenfalls ein neues Gesuch stellen.

   Will der Antragsteller seine Rechte nicht verwirken, so muss er bei Nichterhalt einer Stellungnahme innert 20 Tagen ab Einreichen seiner Zugangsgesuche von Gesetzes wegen beim Beauftragten wiederum innert 20 Tagen einen Schlichtungsantrag einreichen. Dies hat er jedoch in den Fällen der späteren Schlichtungsanträge Nr. 3, 4 und 5 nicht getan, sondern erst, nachdem das EDA (verspätet) am 6. Mai 2008 Stellung genommen hatte. Nun hätte er erneut die Möglichkeit gehabt, innert 20 Tagen einen Schlichtungsantrag einzureichen. Das EDA hat ihn in seinen Stellungnahmen auf diese Frist hingewiesen. Anlässlich eines Telefongesprächs vom 23. Mai 2008 hat auch der Beauftragte den Antragsteller darauf aufmerksam gemacht. Trotzdem hat er seine Schlichtungsanträge Nr. 3, 4 und 5 nicht bis 26. Mai 2008, sondern erst am 6. Juni 2008 beim Beauftragten eingereicht.

   Folglich kann festgehalten werden, dass die Schlichtungsanträge Nr. 3, 4 und 5 nicht innert der in Art. 13 Abs. 2 BGÖ vorgeschriebenen Frist von 20 Tagen ab Empfang der Stellungnahme der Behörde beim Beauftragten eingereicht wurden. Der Beauftragte tritt nicht auf diese Schlichtungsanträge ein.

[4] Schlichtungsverfahren nur in Bezug auf die Höhe der verlangten Gebühren
[5] Brunner / Mader (Hrsg.), Stämpflis Handkommentar zum BGÖ, Art. 12, Rz. 15
[6] Handkommentar zum BGÖ, Art. 12, Rz. 15
[7] Handkommentar zum BGÖ, Art. 13, Rz. 34; BGE 124 II 265, 267

Dem Antragsteller bleibt es unbenommen, bei der zuständigen Behörde jederzeit wieder Zugangsgesuche in den gleichen Angelegenheiten einzureichen.

5. Soweit die im Schlichtungsantrag Nr. 6 geltend gemachten Begehren nicht bereits durch die Schlichtungsverfahren Nr. 2 – 5 abgedeckt sind, gilt es festzuhalten, dass dem Antrag kein eigentliches Zugangsverfahren beim EDA vorausgegangen ist. Somit ist der Antragsteller, da kein Teilnehmer an einem vorangegangenen Gesuchsverfahren, nicht zur Einreichung eines Schlichtungsantrags berechtigt.

   Der Beauftragte tritt auf den Schlichtungsantrag Nr. 6 nicht ein.

   Dem Antragsteller bleibt es unbenommen, bei der zuständigen Behörde entsprechende Zugangsgesuche einzureichen.

B. Sachlicher Geltungsbereich

1. Schlichtungsantrag Nr. 1

1.1. Der Gesuchsteller reichte am 10. Mai 2007 einen Schlichtungsantrag ein. Für seine Beurteilung stellte der Beauftragte einzig auf jene Tatsachen und Vorkommnisse ab, die sich bis zu seiner Einreichung ereignet haben.

Der Antragsteller und das EDA hatten auch nach der Einreichung dieses Schlichtungsantrags diverse weitere Kontakte (Treffen zwischen dem Antragsteller und dem EDA Ende Mai 2007, Telefongespräche, Mailverkehr, Einreichung weiterer Zugangsgesuche durch den Antragsteller etc.), die hier insofern berücksichtigt werden, als dass sie für den Schlichtungsantrag Nr. 2 relevant sind.

1.2. Der Antragsteller verlangte ursprünglich «*Auskunft über ALLE laufenden Projekte von SKH [Schweizerischen Korps für humanitäre Hilfe; der Beauftragte] / DEZA, inklusive aller relevanten Projektdaten*» (E-Mail vom 20. März 2007). Im weiteren Mailverkehr mit dem EDA hielt er stets an dieser Forderung fest, weitete sie zum Teil aus oder grenzte sie mit präzisierenden Angaben wieder ein.

Im Folgenden gilt es daher abzuklären, ob die vom Antragsteller in diversen E-Mails gemachten Angaben *zum Zeitpunkt der Einreichung des Schlichtungsantrags* als inhaltlich hinreichend formuliertes Zugangsgesuch beurteilt werden können.

1.3. Vorweg kann festgehalten werden, dass jederzeit ein Schlichtungsantrag eingereicht werden kann, wenn ein Gesuchsteller die Ansicht vertritt ist, dass die von einer Behörde verlangte Präzisierung nicht notwendig ist.[8] Er muss also nicht zwingend eine von der Behörde als definitiv bezeichnete Stellungnahme nach Art. 12 BGÖ abwarten.

1.4. Das Öffentlichkeitsgesetz sieht vor, dass das Zugangsgesuch hinreichend genau formuliert sein muss (Art. 10 Abs. 3 BGÖ). Was unter «hinreichend formuliert» zu verstehen ist, wird in Art. 7 VBGÖ genauer ausgeführt. Die Behörde muss aufgrund der vom Gesuchsteller im Zugangsgesuch erwähnten Angaben in der Lage sein, das verlangte amtliche Dokument zu identifizieren (Art. 7 Abs. 2 VBGÖ). Gelingt ihr dies nicht, so kann sie den Gesuchsteller zu einer Präzisierung seines Gesuchs auffordern (Art. 7 Abs. 3 VBGÖ). Gleichzeitig ist die Behörde verpflichtet, dem Gesuchsteller bei der genaueren Formulierung seines Gesuches behilflich zu sein (Art. 3 VBGÖ).

1.5. Selbst wenn das Öffentlichkeitsgesetz keine hohen Anforderungen an die Form und den Inhalt von Zugangsgesuchen stellt, so muss es doch für die Behörde überhaupt möglich sein, aufgrund des Gesuchs das gewünschte amtliche Dokumente spezifizieren zu können.

Das Öffentlichkeitsgesetz will Zugang *zu einem oder mehreren bestimmten, also genau spezifizierbaren amtlichen* Dokumenten gewähren. Es verschafft jedoch *keinen Anspruch auf eine nicht näher eingrenzbare Menge* von Verwaltungsinformationen. Zum inhaltlichen kommt ein rein praktisches Kriterium hinzu: Die Behörde muss in der Lage sein, die Zugangsgewährung zu einer derart riesigen Menge an amtlichen Dokumenten mit den ihr zur Verfügung stehenden Ressourcen überhaupt bewerkstelligen zu können. Noch nicht beantwortet ist sodann die Frage, ob die Gebühren für ein so umfassendes Zugangsgesuch überhaupt bezahlbar sind.

1.6. Ein Gesuch, das Zugang zu *allen* laufenden und/oder abgeschlossenen Projekten der DEZA beansprucht, zielt auf eine quantitativ nicht erfassbare Anzahl von Dokumenten ab und ist daher nicht hinreichend formuliert. Dass selbst der vom Antragsteller geforderte Zugang zum Programm «Tsunami-Wiederaufbau in Südasien (Indonesien, Thailand, Sri Lanka)» inhaltlich unzureichend

[8] Handkommentar zum BGÖ, Art. 10 RZ 40

spezifiziert ist, zeigte sich für den Beauftragten an der ersten Schlichtungsverhandlung, an der das EDA nachvollziehbar darzulegen vermochte, dass die Gesamtdokumentation zum Tsunami-Wiederaufbau in den betroffenen Ländern eine *Vielzahl* an Projekten und Unterprojekten beinhaltet.

Der Antragsteller hat mit seinen stetig neuen Forderungen nicht zu einer Klärung der Situation beigetragen. Dass er mit fast jeder E-Mail sein Zugangsgesuch inhaltlich abänderte, dieses als ganzes jedoch gleich umfangreich und wenig konkret beliess, führte nach Ansicht des Beauftragten nicht dazu, dass die vom Öffentlichkeitsgesetz verlangte konkrete inhaltliche Bestimmtheit des Zugangsgesuchs erreicht wurde.

Zudem kann dem EDA zum Zeitpunkt der Einreichung des Schlichtungsantrags Nr. 1 nach Ansicht des Beauftragten auch nicht vorgeworfen werden, es sei dem Antragsteller bei der Präzisierung seines Gesuchs nicht behilflich gewesen. So erachtet der Beauftragte die vom EDA angebotene Unterredung vom 29. Mai 2007 als eine angemessene Unterstützungsmassnahme im Sinne von Art. 3 VBGÖ. Im Anschluss an diese Besprechung reichte der Antragsteller dann auch weitere Zugangsgesuche ein, die inhaltlich hinreichend präzisiert waren.

Der Beauftragte gelangt daher zum Schluss, dass das EDA vom Antragsteller zu Recht eine Präzisierung seines Zugangsgesuchs verlangt hat.

2. Schlichtungsantrag Nr. 2

2.1. Vorweg gilt es festzuhalten, dass ein Schlichtungsbegehren nicht begründet werden muss. Ebenso wenig müssen dem Beauftragten konkrete Anträge unterbreitet werden, die dieser prüfen soll. Der Beauftragte beurteilt auch ohne entsprechende Begehren umfassend, ob die Behörde bei ihrer Beurteilung des Zugangsgesuches die Vorgaben des Öffentlichkeitsgesetzes korrekt berücksichtigt hat.

Der Beauftragte kann im Rahmen eines Schlichtungsverfahrens nur über jene Bereiche befinden, die in den Geltungsbereich des Öffentlichkeitsgesetzes fallen. Er hat dies dem Antragsteller in der Einzelunterredung sowie in den Schlichtungsverhandlungen eingehend dargelegt und begründet. Dabei hat er mehrmals den Unterschied zwischen aktiver und passiver Information[9] erläutert und erklärt, dass das Öffentlichkeitsgesetz grundsätzlich nur die passive

[9] Handkommentar zum BGÖ, Einleitung RZ 78

Information regelt und dem Bürger, der Bürgerin keinen spezifischen Anspruch auf eine aktive Information oder eine bestimmte Informationspolitik von Seiten der Bundesbehörden verschafft. Der Beauftragte äussert sich daher nicht mehr zu folgenden «*Anträgen*» des Antragstellers (s. o. Ziffer I.B.4.):

- Buchstabe c («Die Misswirtschaft, die systematische Unterschlagung von Information…»)
- Buchstabe d («Über Art und aktuellen Status, Kosten und Kostensplit der Projekte der DEZA ist mittels einer Web-Projekt-Datenbank detailliert und überprüfbar zu informieren,… »)
- Buchstabe f («Die mir seitens EDA DEZA SKH am 29. Mai im Bundeshaus versprochenen Projekt-Übersichten…»)
- Buchstabe g («Dem EDÖB sind bei offenkundigem Bedarf sofort wenigstens die in der Vernehmlassung zum BGÖ vorgesehenen personellen Ressourcen zu gewähren …»)
- Buchstabe h («Das Kompetenzzentrum Öffentlichkeitsprinzip des EDA ist so zu verstärken,…).

Zum Antrag Buchstabe i («Falls einzelnen Punkten nicht stattgegeben werden sollte, ist eine anfechtbare Antwort mit Verfügung auszustellen.»):

Kommt es im Schlichtungsverfahren zu keiner Einigung, erlässt der Beauftragte eine Empfehlung. Innert 10 Tagen nach Erhalt dieser Empfehlung kann der Antragsteller eine Verfügung verlangen (Art. 14 i.V.m. Art. 15 Abs. 1 BGÖ, s. u. Ziffer III.).

2.2. Angesichts des komplexen Sachverhaltes, der vom Antragsteller zahlreich eingereichten, hängigen Zugangsgesuche und Schlichtungsanträge sowie der bereits erfolgten Kontakte zwischen dem Antragsteller und dem EDA erschien es dem Beauftragten sinnvoll und notwendig, eine Schlichtungsverhandlung durchzuführen.

Im Laufe des Schlichtungsverfahrens zeigte sich, dass der Antragsteller bereits alle Dokumente, zu denen er Zugang beantragte, *direkt vom Ersteller des Schlussberichts Sri Lanka erhalten hatte*. Der Antragsteller bestätigte dies dem Beauftragten in der zweiten Schlichtungsverhandlung explizit. Weiter führte er aus, dass er über eine Vollmacht des Erstellers verfüge, die ihn ermächtige, im Namen des Erstellers des Schlussberichts Sri Lanka zu handeln. Der Antrag-

steller verfolgte nach eigenen Worten das Ziel, mittels des Öffentlichkeitsgesetzes in Erfahrung zu bringen, welche Teile des Schlussberichts Sri Lanka er veröffentlichen könne, um damit auf mutmassliche Missstände im EDA (resp. der DEZA und des SKH) hinzuweisen.

Im Verlaufe der zweiten Schlichtungsverhandlung zeigte sich einerseits immer deutlicher, dass der Antragsteller anerkannte, dass das Öffentlichkeitsgesetz nicht das richtige Mittel zur Erreichung des von ihm verfolgten Zieles ist. Anderseits hielt er inhaltlich stets an allen Schlichtungsanträgen fest.

Da keine Schlichtung zwischen den beiden Parteien erreicht werden konnte, muss der Beauftragte gemäss Art. 14 BGÖ eine Einschätzung zum Sachverhalt abgeben und eine Empfehlung erlassen, damit sowohl der Antragsteller wie auch die Behörde die Gelegenheit erhalten, die strittige Angelegenheit von einem Richter beurteilen zu lassen.

2.3. In Bezug auf das vom Antragsteller hauptsächlich verfolgte Ziel (nach seinen Aussagen das Aufdecken von Missständen in der DEZA) weist der Beauftragte darauf hin, dass er in seiner Funktion als Schlichtungsstelle materiell *nicht* darüber zu entscheiden hat, ob - und falls ja, in welchem Umfang - es zu Missständen gekommen ist. Er kann in diesem Zusammenhang den Antragsteller lediglich darauf hinweisen, dass die Geschäftsprüfungskommission des Parlaments die Oberaufsicht über die Geschäftsführung des Bundesrates und der Bundesverwaltung ausübt, und sie im Rahmen ihrer Tätigkeit das Verwaltungshandeln auch auf Rechtmässigkeit, Zweckmässigkeit und Wirksamkeit überprüfen muss (Art. 52 des Bundesgesetzes über die Bundesversammlung, SR 171.10).

2.4. Schlussbericht Sri Lanka (inklusive Beilagen und Korrespondenz von Z mit dem EDA)

2.4.1. Das EDA hat dem Antragsteller den Schlussbericht Sri Lanka zugestellt, wobei Textpassagen mit Verweis auf die Ausnahmebestimmungen von Art. 7 Abs. 1 Bst. b und d, Abs. 2 BGÖ und Art. 9 BGÖ abgedeckt respektive anonymisiert worden sind. Diese Passagen wurden vom EDA «eingeweisst». Es stellte dem Antragsteller ein Exemplar zu, das ein anderes Format aufwies als jenes, das er direkt vom Ersteller erhalten hatte.

2.4.2. Der Antragsteller hält fest, dass «eine akzeptable, die Integrität des Originals respektierende «Bearbeitung» auszuhändigen» sei. Er ist daher der Ansicht, dass (1.) das Dokument geschwärzt (und nicht geweisst) und (2.) das Format beibehalten werden muss.

Zu Recht wirft der Antragsteller in Zusammenhang mit dem Schlussbericht Sri Lanka Fragen (Einweissen von Textstellen anstelle von Einschwärzen, Beibehaltung des Originalformats, Anonymisierung der Namen von Chefbeamten) auf, die einer materiellen Klärung bedürfen.

2.4.3. Vorweg gilt es festzuhalten, dass das BGÖ keine klaren Vorgaben für die Anonymisierung oder die Abdeckung respektive für das Einschwärzen/Einweissen von Textpassagen enthält. Es entspricht jedoch dem Sinn und Zweck des Öffentlichkeitsgesetzes, wenn für den Gesuchsteller ersichtlich ist, welche Textpassagen in einem Dokument von der Behörde anonymisiert respektive abgedeckt worden sind. Eine Anonymisierung (bei Personendaten) oder Abdeckung von bestimmten Textpassagen (bei Fällen von Art. 7 BGÖ) muss daher in einer Art und Weise erfolgen, dass für den Gesuchsteller ersichtlich ist, welche Teile des Dokumentes so bearbeitet wurden. Dies kann einerseits durch Schwärzen oder durch eine andere Kennzeichnung erfolgen (bspw. durch Auslassungszeichen […]).

Ein Einweissen eines Textes hat zur Folge, dass nicht in jedem Fall nachvollzogen werden kann, welche Teile und in welchem Umfang Textpassagen abgedeckt worden sind. Der Beauftragte ist daher der Ansicht, dass aus diesem Grund auf das Einweissen von Texten grundsätzlich zu verzichten ist. Anders verhält es sich, wenn die Behörde die eingeweissten Stellen zusätzlich kennzeichnet.

2.4.4. Das Öffentlichkeitsgesetz spricht sich auch nicht explizit darüber aus, ob bei der Anonymisierung oder beim Abdecken von Texten das Format des Originaldokuments beibehalten werden muss.

Hinsichtlich des Zugangs zum Originaldokument – und damit auch zum Originalformat – sieht das Öffentlichkeitsgesetz vor, dass ein Gesuchsteller grundsätzlich wählen kann, wie er Einblick in die Dokumente erhalten möchte: Er kann sie entweder vor Ort einsehen oder Kopien davon anfordern (Art. 6 Abs. 2 BGÖ). Bei Einsichtnahme vor Ort besteht grundsätzlich ein Anspruch auf Zu-

gang zum Originaldokument.[10] Dieser ist allerdings nicht absolut, denn in bestimmten Fällen kann sich die Behörde gemäss Art. 4 Abs. 2 VBGÖ auch darauf beschränken, der Gesuchstellerin oder dem Gesuchsteller lediglich Einsicht in eine Kopie des amtlichen Dokuments zu gewähren, beispielsweise wenn der Zustand des Originals dies erfordert.[11] Gleich muss es sich verhalten, wenn Teile des Dokuments abgedeckt oder anonymisiert werden müssen. Es versteht sich von selbst, dass das Original durch die Anonymisierung respektive Abdeckung nicht beeinträchtigt werden darf. Eine Schwärzung von Textpassagen kann also in der Regel nicht direkt auf dem Original, sondern nur auf einer Kopie angebracht werden kann.

Im Weiteren gilt es zu beachten, dass das Öffentlichkeitsgesetz lediglich einen Anspruch auf *Integrität des Inhalts,* nicht aber einen Anspruch auf das Originalformat verschafft. Dies zeigt sich unter anderem auch daran, dass der Gesetzgeber technische Mittel zur Bearbeitung von Dokumenten (z.B. Abrufverfahren usw.) zulässt. Wenn ein Dokument für die Herausgabe an den Gesuchsteller noch bearbeitet werden muss (z.B. durch Löschen einer oder mehrerer Textpassagen), so führt dies bei elektronischen Dokumenten unweigerlich zu einer Änderung des Formats. Es ist nicht ersichtlich, weshalb eine Bundesbehörde, die eine elektronische Version des Originaldokuments auf Papier besitzt und diese vor der Gewährung des Zugangs anonymisieren respektive abdecken muss, die entsprechenden Bearbeitungsschritte nicht elektronisch vornehmen darf. Diese Form des Anonymisierens respektive des Abdeckens (Löschens) ist einfacher und benötigt in der Regel viel weniger Zeit.

Als Fazit kann Folgendes festgehalten werden:

- Grundsätzlich muss eine Behörde ein Dokument in einer Art und Weise anonymisieren respektive einzelne Textpassagen abdecken, dass für den Gesuchsteller erkennbar ist, welche Teile des Dokuments anonymisiert oder abgedeckt worden sind.
- Das Einschwärzen von Textpassagen ist dem Einweissen vorzuziehen.
- Das Format des zugänglich gemachten Dokuments muss nicht in jedem Fall dem Format des Originaldokuments entsprechen.

[10] Handkommentar zum BGÖ, Art. 6 Ziffer 33
[11] Vorordnung über das Öffentlichkeitsprinzip der Verwaltung, Erläuterungen des Bundesamtes für Justiz, Ziffer 3.3 Einsichtnahme vor Ort (Art. 4 VBGÖ)

2.4.5. Die Namen und die Funktionen von Verwaltungsangestellten (insbesondere von Entscheidungsträgerinnen und Entscheidungsträgern), die in amtlichen Dokumenten erwähnt werden, unterliegen, soweit diese Personen in Erfüllung einer öffentlichen Aufgabe gehandelt haben, nicht der Anonymisierungspflicht.[12]

2.4.6. Das EDA stellte dem Antragsteller einen anonymisierten respektive abgedeckten Schlussbericht Sri Lanka zu. Den Zugang zur CD mit den Beilagen des Berichts sowie zur Korrespondenz des EDA mit dem Ersteller verweigerte es aus verschiedenen Gründen.

Die konsequente und korrekte Anwendung des Öffentlichkeitsprinzips führt immer zu einer Mehrarbeit für die zuständige Verwaltungseinheit. Einige Zugangsgesuche verursachen mehr, andere weniger Aufwand. Der Gesetzgeber hat durch den Erlass des Öffentlichkeitsgesetzes klar gemacht, dass er eine transparente Bundesverwaltung wünscht, auch wenn damit für sie eine Mehrbelastung einhergeht. Der *alleinige* Umstand, dass der Zugang zu einem Dokument nur mit einem grossen Zeitaufwand gewährt werden kann, ist nach Ansicht des Beauftragten keine Rechtfertigung, das im Öffentlichkeitsgesetz vorgesehene Verfahren nicht ordnungsgemäss durchzuführen.[13]

Die Beantwortung dieses Zugangsgesuchs und das anschliessende Schlichtungsverfahren haben bei den betroffenen Stellen nicht nur zu einem hohen, sondern zu einem überdurchschnittlich hohen Arbeitsaufwand geführt. Nach Einschätzung des Beauftragten hat der Arbeitsaufwand für die Behandlung dieses Zugangsgesuchs und des Schlichtungsantrags ein vertretbares Mass überschritten. Zusätzlich zum Zeitfaktor muss der Beauftragte für eine umfassende Einschätzung auch weitere Kriterien berücksichtigen. Dies ist zum einen der Umstand, dass sich das EDA bemühte, auf die Zugangsgesuche und Anliegen des Antragstellers entsprechend den Vorgaben des Öffentlichkeitsgesetzes einzugehen, und sich an den Schlichtungsverhandlungen gesprächs- und kooperationsbereit gezeigt hat.

Zum anderen kann der Beauftragte bei seiner Einschätzung die bedeutende Tatsache nicht unbeachtet lassen, dass der Antragsteller bereits im Besitz aller Dokumente ist, zu denen er Zugang beantragt. Gemäss seinen eigenen Aussagen bezweckte er vom EDA den Erhalt einer Kopie, um sie mit dem Exemplar,

[12] Handkommentar zum BGÖ, Art. 9 RZ 14
[13] ebenso Handkommentar zum BGÖ, Art. 7 RZ 3

das er direkt vom Ersteller erhalten hat, zu vergleichen. Auf diese Weise wollte er in Erfahrung bringen, welche Teile des Berichts er Dritten weitergeben kann. Angesichts des grossen Umfangs der gewünschten Dokumentation sowie der Tatsache, dass aller Wahrscheinlichkeit nach ein eingeschränkter Zugang ein aufwändiges, konsequentes Einschwärzen beziehungsweise Anonymisieren erfordert, ist nach Ansicht des Beauftragten die vom Öffentlichkeitsgesetz geforderte Transparenz dadurch erreicht, dass der Antragsteller den Bericht bereits vom Ersteller erhalten hat.

Auch wenn der Beauftragte die Anliegen des Antragstellers in Teilen nachvollziehen kann, ist er der Ansicht, dass es aufgrund der Tatsache, dass der Antragsteller bereits im Besitz aller Dokumente ist, unverhältnismässig wäre und dem Grundsatz von Treu und Glauben widerspräche, vom EDA angesichts des Verlaufs der Angelegenheit zu fordern, die entsprechenden, umfangreichen Anonymisierungs- und Abdeckungsarbeiten vorzunehmen und die Dokumente herauszugeben. Unter diesen Umständen sieht auch der Beauftragte davon ab, den Schlussbericht Sri Lanka, die CD mit den Beilagen sowie die Korrespondenz zwischen dem Ersteller und dem EDA darauf hin zu überprüfen, ob die Bedingungen für Einschränkungen nach Art. 7 und 9 BGÖ erfüllt sind und in welchem Mass der Zugang zu gewährleisten ist.

2.5. Schlussbericht Indonesien

2.5.1. Das EDA händigte dem Antragsteller in Beantwortung seines Zugangsgesuchs einen eingeschwärzten Schlussbericht Indonesien aus. Auf jeder Seite war im Hintergrund der Vermerk «Entwurf» angebracht.

2.5.2. Der Antragsteller macht daher geltend, dass ihm eine Kopie der Endfassung und nicht ein Entwurf des Schlussberichts auszuhändigen sei.

Das EDA erklärte dazu in den Schlichtungsverhandlungen, dass der Vermerk «Entwurf» von jener Dienststelle angebracht worden war, die den Schlussbericht geschwärzt hatte, bevor sie ihn an die für die Zugangsgewährung zuständige Stelle weitergeleitet hatte. Der Vermerk bezog sich somit nicht auf den Inhalt des Dokuments, sondern auf die Einschwärzung. Aus Versehen sei daher dem Antragsteller ein Exemplar mit dem Vermerk «Entwurf» herausgegeben worden.

Der Antragsteller führte in der zweiten Schlichtungsverhandlung dazu aus, dass diese Erläuterungen des EDA zwar plausibel seien, «aufgrund dokumentierter Lügen des EDA, DEZA, SKH bleibt aber die Frage offen, ob das zugänglich gemachte Dokument (1.) das einzige und (2.) die Endfassung ist.»

An der zweiten Schlichtungsverhandlung überreichte das EDA dem Beauftragten eine Kopie jener E-Mail, mit welcher der Ersteller des Schlussberichts Indonesien dem EDA seinen definitiven Bericht zugestellt hat. Der Beauftragte konnte sich davon überzeugen, dass der dieser E-Mail angefügte Schlussbericht inhaltlich jener Kopie mit dem Vermerk «Entwurf» entspricht, die das EDA dem Antragsteller zugestellt hat.

2.5.3. Das EDA schwärzte Passagen des Schlussberichts Indonesien mit Verweis auf die Bestimmungen von Art. 7 Abs. 1 Bst. b (Beeinträchtigung der zielkonformen Durchführung konkreter behördlicher Massnahmen), Bst. d (Beeinträchtigung der aussenpolitischen Interessen und der internationalen Beziehungen) sowie von Art. 7 Abs. 2 i.V.m. Art. 9 BGÖ («aus Gründen des Persönlichkeitsschutzes») ein.

2.5.4. Bei der Beurteilung, ob eine Ausnahme von Art. 7 Abs. 1 BGÖ vorliegt, ist keine Abwägung zwischen den Interessen der Verwaltung an einer Geheimhaltung und dem Interesse des Gesuchstellers am Zugang vorzunehmen, sondern es muss geprüft werden, ob die Offenlegung des Dokuments erstens zu einer *erheblichen und reellen* Beeinträchtigung der in Art. 7 Abs. 1 BGÖ erwähnten Geheimhaltungsinteressen führt und ob zweitens ein *ernsthaftes* Risiko für den Eintritt dieser Beeinträchtigung besteht.[14] Wie der Beauftragte bereits in einer früheren Empfehlung[15] ausgeführt hat, darf die Behörde den Zugang nur verweigern oder einschränken, wenn diese Beeinträchtigung *mit hoher Wahrscheinlichkeit* auch eintreten wird. Mit anderen Worten ist ein Abdecken von Textpassagen nicht zulässig, wenn eine Beeinträchtigung der Geheimhaltungsinteressen von Art. 7 Abs. 1 BGÖ lediglich denkbar oder im Bereich des Möglichen ist.

In Bezug auf den Schlussbericht Indonesien nimmt der Beauftragte eine andere Einschätzung des Schadensrisikos vor als das EDA. Bei den meisten abgedeckten Stellen gelangt er zum Schluss, dass deren Offenlegung *nicht* zu einer *erheblichen und tatsächlichen* Beeinträchtigung der vom EDA geltend

[14] Handkommentar zum BGÖ, Art. 7 RZ. 4ff.
[15] Empfehlung vom 27. November 2006, Ziffer II.B.5

gemachten Geheimhaltungsinteressen führt. Dabei schätzt er das Schadensrisiko auch deshalb nicht als *ernsthaft* ein, weil die Schlussberichte zusammen mit einer Erklärung abgegeben werden, in der ausdrücklich darauf hingewiesen wird, dass die Schlussberichte «*in keiner Weise die Sicht der DEZA, sondern einzig die subjektive Meinung dieser Person*» widerspiegeln.

Der Beauftragte ist nicht berechtigt, in einem Schlichtungsverfahren oder in einer Empfehlung vertrauliche oder geheime Informationen und Details aus dem fraglichen Dokument bekannt zu geben. Grundsätzlich lässt sich sagen, dass kein ernsthaftes Schadensrisiko gegeben ist, wenn bereits allgemein bekannte Informationen und Ansichten über die Bevölkerung eines Landes ebenso wie allgemein zugängliche kulturelle und religiöse Hintergründe zugänglich gemacht werden.

Ausserdem gilt es stets zu beachten, dass durch die Einführung des Öffentlichkeitsprinzips beabsichtigt wurde, die demokratischen Kontrollrechte gegenüber der Verwaltung zu stärken. In diesem Sinne erachtet es der Beauftragte daher als richtig und wichtig, dass ein Bürger, eine Bürgerin u.a. einen uneingeschränkten Zugang zu Informationen erhält, die die Auswirkungen von Besuchen aus der Schweiz (z.B. von Parlamentarier, Mitglieder der Bundesverwaltung, Journalisten usw.) auf die Arbeit des SKH vor Ort aufzeigen.

Weiter kann bei dieser Gelegenheit grundsätzlich festgehalten werden, dass das Öffentlichkeitsgesetz den Bundesbehörden keine Handhabe dazu bietet, für sie nicht genehme oder wenig vorteilhafte Informationen zurückzuhalten. Insofern dürfen kritische Bemerkungen und Verbesserungsvorschläge zur Verwaltungstätigkeit nicht zurückgehalten werden.

2.5.5. Das Öffentlichkeitsgesetz sieht zum Schutz von Personendaten vor, dass diese vor der Zugangsgewährung «nach Möglichkeit» zu anonymisieren sind (Art. 9 Abs. 1 BGÖ).

Nicht in allen Fällen muss jedes Personendatum abgedeckt werden. So ist beispielsweise nicht ersichtlich, weshalb die Namen jener Hilfsorganisationen, die sich am Tsunami-Wiederaufbau in den einzelnen Regionen oder Ländern beteiligen, abgedeckt werden müssen, zumal deren Einsatz ja bereits öffentlich bekannt ist. Weiter sind, wie oben ausgeführt, die Namen von Entscheidungsträgern der Bundesbehörden nicht zu anonymisieren.

Anders ist die Sachlage zu beurteilen, wenn der Ersteller eines Schlussberichts *Wertungen und Einschätzungen* über die Arbeitsweise und die Persönlichkeit von anderen Mitarbeitenden oder über die Zusammenarbeit mit ausländischen Behörden und anderen, nationalen wie internationalen Hilfsorganisationen abgibt. In diesen Fällen sind die Personendaten (also Namen, Firmen und Bezeichnungen) aus Gründen des Schutzes der Privatsphäre grundsätzlich zu anonymisieren. Das Anonymisieren muss sich aber so weit als möglich auf Personendaten beschränken. Demnach dürfen bei Schilderungen (bspw. ‚Hauptprobleme und Fragen' im Schlussbericht) über heikle oder problematische Aspekte der Zusammenarbeit mit den Behörden vor Ort, mit den von der DEZA beauftragten Unternehmen oder mit anderen Hilfsorganisationen nur die Namen, Firmen und die Bezeichnungen anonymisiert, nicht aber der gesamte Abschnitt abgedeckt werden. Weiter gehendes Einschwärzen ist nur zulässig, wenn der Schutz der Privatsphäre eines Dritten dies unbedingt verlangt oder wenn Geheimhaltungsinteressen nach Art. 7 Abs. 1 BGÖ dies erfordern.

2.5.6. Aufgrund dieser Ausführungen empfiehlt der Beauftragte dem EDA, den Schlussbericht Indonesien entsprechend dem Vorschlag im Anhang zu anonymisieren und abzudecken (s. Anhang).

3. Auskunftsrecht nach Art. 8 DSG

Mit Bezugnahme auf die Vollmacht, die der Antragsteller vom Ersteller des Schlussberichts Sri Lanka erhalten hat, ist darauf hinzuweisen, dass der Ersteller jederzeit sein Auskunftsrecht nach Art. 8 des Bundesgesetzes über den Datenschutz (DSG, *SR* 235.1) geltend machen kann. In diesem Fall muss die betroffene Behörde ihm alle über ihn bearbeiteten Personendaten unter Vorbehalt der Ausnahmen von Art. 9 DSG herausgeben. Jede Einschränkung des Auskunftsrechts muss in Form einer Verfügung begründet werden. Gegen diese Verfügung kann die betroffene Person eine Beschwerde beim Bundesverwaltungsgericht einreichen.

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

1. Schlichtungsantrag Nr. 1

   Das Eidg. Departement für auswärtige Angelegenheiten hat vom Antragsteller zu Recht eine Präzisierung des Zugangsgesuchs verlangt.

   Schlichtungsantrag Nr. 2

   Schlussbericht Sri Lanka: Das Eidg. Departement für auswärtige Angelegenheiten muss den bereits zugänglich gemachten Schlussbericht Sri Lanka (inkl. Beilagen und Korrespondenz) nicht erneut überarbeiten.

   Schlussbericht Indonesien: Das Eidg. Departement für auswärtige Angelegenheiten schwärzt den Schlussbericht Indonesien entsprechend den Vorgaben von II.B.2.5 ein und stellt ihn dem Antragsteller zu.

2. Das Eidg. Departement für auswärtige Angelegenheiten erlässt eine Verfügung nach Art. 5 des Verwaltungsverfahrensgesetzes, wenn es mit der Empfehlung in Ziffer 1 nicht einverstanden ist.

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

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

   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 15. Juli bis und mit 15. August still. Die Frist beginnt somit am Montag, den 18. August 2008.

5. Diese Empfehlung wird veröffentlicht. Zum Schutz der Personendaten der am Schlichtungsverfahren Beteiligten werden die Namen des Antragstellers und der erwähnten Drittpersonen anonymisiert (Art. 13 Abs. 3 VBGÖ).

6. Die Empfehlung wird eröffnet:

   X

   Eidg. Departement für auswärtige Angelegenheiten
   3003 Bern

Hanspeter Thür

Anhang (nur EDA):

- Schlussbericht Indonesien

Kopie:

Geschäftsprüfungskommissionen (GPK)
Sekretariat GPK
Parlamentsgebäude
3003 Bern

4.2.2 Empfehlung an das Bundesamt für Statistik: «Statistikgeheimnis»

Siehe Abschnitt 4.2.2 im französischen Teil des Berichtes.

4.2.3 Empfehlung an das Eidgenössische Departement des Innern: «Stiftungsaufsicht / Aufsichtstätigkeit»

Empfehlung

gemäss

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

zum Schlichtungsantrag von

X
(Antragsteller)

gegen

Eidgenössische Stiftungsaufsicht,
Eidgenössisches Departement des Innern, Bern

I. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte stellt fest:

1. Der Antragsteller (Journalist) ersuchte am 10. Oktober 2007 gestützt auf das Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsgesetz BGÖ, SR 152.3) bei der Eidgenössischen Stiftungsaufsicht (Stiftungsaufsicht) um Zugang zu den «Akten der eidgenössischen Stiftungsaufsicht über die Paraplegiker-Stiftung, Nottwil. Insbesondere interessieren mich die Akten, die erstellt wurden seit dem 8. Juni 2007 und die Rückzahlung der Deliktsumme von Y, wie sie das Bundesgericht in seinem Entscheid festgehalten hat, an die Paraplekiger-Stiftung (…).» Der Journalist hatte in der Vergangenheit bereits eine Reihe von Presseartikeln zur Schweizer Paraplegiker-Stiftung (SPS) verfasst.

2. Die Stiftungsaufsicht verweigerte dem Antragsteller am 11. Oktober 2007 den Zugang «in alle einschlägigen, durch die Schweizer Paraplegiker-Stiftung eingereichten und durch die Eidgenössische Stiftungsaufsicht erstellten, amtlichen Dokumente und Auskünfte, insbesondere aber in alle, die mit der Rückzahlung gemäss Urteil des Schweizerischen Bundesgerichts zu tun haben. Die Verweigerung des Zugangs wird damit begründet, dass Ihr Gesuch Akten eines erstinstanzlichen Verwaltungsverfahrens (Art. 3 Abs. 1 Bst. b BGÖ) betrifft und unter die vom Öffentlichkeitsgesetz vorgesehenen Ausnahmebestimmungen (Art. 7 BGÖ) fällt.»

3. Mit Schreiben vom 13. Oktober 2007 ersuchte der Antragsteller den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (Beauftragter) um Schlichtung. Er führte dazu aus, dass die von der Stiftungsaufsicht angeführte Bestimmung von Art. 3 Abs. 1 Bst. b BGÖ nicht auf ihn anwendbar sei, da er keine Partei in einem Verwaltungsverfahren sei. Er erachte daher die Begründung «als schludrig und damit schikanös».

4. An der Schlichtungsverhandlung vom 26. November 2008 anerkannte die Stiftungsaufsicht, dass die Begründung für die Zugangsverweigerung (insbesondere der Verweis auf Art. 3 Abs. 1 Bst. b BGÖ) materiell nicht korrekt gewesen sei. Vielmehr hätte der Zugang mit Hinweis auf das in casu gegebene Geschäftsgeheimnis (Art. 7 Abs. 1 Bst. g BGÖ) und auf den Schutz von Personendaten (Art. 9 BGÖ) verweigert werden sollen.

An der Schlichtungsverhandlung wies die Stiftungsaufsicht u.a. darauf hin, dass es 11 Aktenordner zur SPS gebe und das Zugangsgesuch daher zu allgemein formuliert gewesen sei. Daraufhin konkretisierte der Antragsteller sein Gesuch, indem er um Zugang zu allen Dokumenten ersuchte, welche die Stiftungsaufsicht erstellt hat betreffend:

- die Rückerstattung des vom Bundesgericht festgestellten Deliktsbetrags durch Y
- die Abberufung von Y als Präsident der SPS (bis zum Zeitpunkt der Übernahme durch den neuen Stiftungsratspräsidenten).

Der Antragsteller und die Stiftungsaufsicht konnten sich nicht einigen.

5. Entsprechend dem konkretisierten Zugangsgesuch hat der Beauftragte folgende Dokumente zur Beurteilung nach den Vorgaben des Öffentlichkeitsgesetzes ausgewählt:

   - Schreiben der Stiftungsaufsicht vom 5. April 2007 an den Rechtsanwalt der SPS
   - Protokoll vom 23. April 2007 (Besprechung der Stiftungsaufsicht mit Vertretern des Stiftungsrates der SPS), erstellt von der Stiftungsaufsicht
   - Schreiben der Stiftungsaufsicht vom 3. Mai 2007 an das Amtsstatthalteramt Sursee
   - Schreiben der Stiftungsaufsicht vom 6. Juni 2007 an die SPS
   - Schreiben der Stiftungsaufsicht vom 14. August 2007 an die SPS
   - Aktennotiz/Aide-mémoire concernant la Fondation suisse pour paraplégiques (FSP), 13 septembre 2007, erstellt von der Stiftungsaufsicht
   - Schreiben der Stiftungsaufsicht vom 8. Oktober 2007 an das Amtsstatthalteramt Sursee
   - Schreiben der Stiftungsaufsicht vom 23. Oktober 2007 an die SPS
   - Schreiben der Stiftungsaufsicht vom 13. November 2007 an die SPS

Im Folgenden gilt es zu prüfen, ob die vollumfängliche Zugangsverweigerung durch die Stiftungsaufsicht in Übereinstimmung mit dem Öffentlichkeitsgesetz erfolgt ist.

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

A. Schlichtungsverfahren und Empfehlung 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 bei der Stiftungsaufsicht 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[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. Inhaltliche Bestimmtheit eines Zugangsgesuchs:

   Zur Frage der inhaltlichen Bestimmtheit eines Zugangsgesuchs hält Art. 10 Abs. 3 BGÖ fest, dass das Gesuch *hinreichend genau formuliert* sein muss, damit die Behörde das gewünschte Dokument überhaupt identifizieren kann. Gelingt dies der Behörde nicht, kann sie vom Gesuchsteller verlangen, dass er sein Gesuch präzisiert (Art 7 Abs. 3 der Verordnung über das Öffentlichkeitsprinzip der Verwaltung, Öffentlichkeitsverordnung, VBGÖ, SR 152.31). Dieses Vorgehen ist nur dann sinnvoll, wenn es dem Gesuchsteller zugemutet werden kann, Angaben zu liefern, die das Dokument eindeutiger bezeichnen (wie beispielsweise Erstellungsdatum oder betroffener Sachbereich; Art. 7 Abs. 2 VBGÖ). Eine Präzisierung setzt voraus, dass entsprechende Angaben in dieser Form auch allgemein zugänglich sind. Ist dies nur beschränkt oder überhaupt nicht der Fall, kann eine Behörde vom Gesuchsteller auch nicht verlangen, dass er sein Zugangsgesuch weiter präzisieren muss. Vielmehr gelangt in einem solchen Fall Art. 3 Abs. 1 VBGÖ zur Anwendung, gemäss dem die Behörde dem Gesuchsteller Auskunft über die verfügbaren amtlichen Dokumente geben und ihn bei seinem Vorgehen unterstützen muss. Am einfachsten ist dies zu bewerkstelligen, indem sie mit dem Gesuchsteller telefonisch Kontakt aufnimmt und mit ihm die notwendige Spezifizierung vornimmt. Weiter kann sie dieser Verpflichtung auch nachkommen, indem sie ihm einen Ausdruck mit der Auflistung aller Dokumente des Dossiers zustellt oder – sofern die Behörde über kein Dokumentenmanagementsystem verfügt – eine Liste der vorhandenen Dokumente erstellt.[3]

   In diesem Sinn hat der Beauftragte auch Dokumente ausgeschieden, die von der Stiftungsaufsicht zeitlich vor dem 8. Juni 2007 und nach dem Rücktritt des damaligen Stiftungsratspräsidenten (auf den 1. Oktober 2007, der Beauftragte) erstellt worden sind.

2. Ablehnende Stellungnahme:

   Wenn eine Behörde den Zugang verweigert oder beschränkt, muss sie dies summarisch *begründen* (Art. 12 Abs. 4 BGÖ).[4] Keine ausreichende Begründung liegt vor, wenn in der ablehnenden Stellungnahme lediglich ausgeführt wird, dass eine vom Öffentlichkeitsgesetz vorgesehene Ausnahmebestimmung (Art.

[3] ebenso Handkommentar zum BGÖ, Art. 10 Rz. 34
[4] s.a. BBl 2003 2022f.

7 BGÖ) vorliegt, oder wenn der blosse Wortlaut der Ausnahmebestimmung zitiert wird. Es ist daher zu fordern, dass die negative Stellungnahme in einer Weise zu motivieren ist, die es dem Gesuchsteller erlaubt, die Überlegungen der Behörde *zumindest in Grundzügen nachvollziehen* zu können.[5]

3. Öffentlichkeitsgesetz - Instrument zur Kontrolle der Verwaltung:

Gemäss der bundesrätlichen Botschaft zum Öffentlichkeitsgesetz sollte die Einführung des Öffentlichkeitsprinzips u.a. auch zu einer Verbesserung der Beziehungen zwischen dem Staat und der Bevölkerung beitragen. Darum sah er es als unerlässlich an, «dem Bürger oder der Bürgerin die Möglichkeit zuzugestehen, selber Informationen zu beschaffen und ihm oder ihr zu erlauben, den Wahrheitsgehalt amtlicher Verlautbarungen zu überprüfen.»[6] Der Bundesrat betrachtete denn auch das Öffentlichkeitsprinzip ausdrücklich als «zusätzliches, unmittelbares Instrument zur Kontrolle der Verwaltung durch die Bürgerinnen und Bürger».[7]

Vorliegend möchte der Antragsteller wissen, welche Massnahmen eine Aufsichtsbehörde von einer Stiftung gefordert und ergriffen hat, deren früherer Stiftungsratspräsident letztinstanzlich vom Bundesgericht wegen Veruntreuung verurteilt worden ist. Letztlich verlangt er nichts anderes als Transparenz über sämtliche Aktivitäten der Aufsichtsbehörde in Bezug auf die Ausübung ihrer Aufsichtstätigkeit in einem konkreten Fall. Sein Zugangsgesuch deckt sich somit mit den mit der Einführung des Öffentlichkeitsprinzips angestrebten Zielsetzungen.

4. Amtliche Dokumente:

Bei den in Ziffer I.5. aufgeführten Dokumenten handelt es sich um amtliche Dokumente im Sinne von Art. 5 Abs. 1 BGÖ. Dies gilt explizit auch für die Aktennotiz/Aide-mémoire vom 13. September 2007. Das Dokument, das vom Ersteller unterzeichnet ist, trägt die Überschrift «Aide-mémoire» und richtet sich an den Departementschef, den Generalsekretär und dessen Stellvertreter. Es enthält zum einen Ausführungen, Zahlen und Fakten zur laufenden Angelegenheit und hält zum anderen die Position der Stiftungsaufsicht fest.

[5] ebenso Handkommentar zum BGÖ, Art. 10 Rz. 34
[6] BBl 2003 1973
[7] BBl 2003 1974

Die Bezeichnung eines Dokuments als «Aktennotiz» bedeutet nicht automatisch, dass es «ausschliesslich der Autorin, dem Autoren oder einem eng begrenzten Personenkreis als Arbeitshilfsmittel» (Art. 1 Abs. 3 VBGÖ) dient und daher ein zum persönlichen Gebrauch bestimmtes Dokument ist. Indem es die wichtigsten Fakten sowie die Position der Stiftungsaufsicht zuhanden der Vorgesetzten auflistet, ist es als amtliches Dokument im Sinne von Art. 5 Abs. 1 BGÖ zu qualifizieren. Die Unterschrift und die definitive Übergabe des Dokuments an die Adressaten «zur Kenntnis- oder Stellungnahme oder als Entscheidgrundlage» (Art. 1 Abs. 2 Bst. b VBGÖ) belegen überdies, dass das Dokument fertig gestellt ist.

Die Aktennotiz/Aide-mémoire ist als amtliches, fertig gestelltes Dokument im Sinne von Art. 5 Abs. 1 BGÖ zu qualifizieren.

5. Geschäftsgeheimnis:

Die Stiftungsaufsicht ist der Ansicht, dass der Zugang zu den von ihr erstellten Dokumenten in Zusammenhang mit der Rückzahlung des Deliktbetrags und der Abberufung des Präsidenten *aufgrund des Geschäftsgeheimnisses gemäss Art. 7 Abs. 1 Bst. g BGÖ* verweigert werden muss.

Diese Ausnahmeklausel will jene wesentlichen Informationen, die für den Geheimnisträger von *zentraler Bedeutung* sind und die auch tatsächlich Geheimnischarakter aufweisen, vom Zugang ausnehmen. Dabei muss das *Geheimhaltungsinteresse* des Betroffenen legitim und sein *Geheimniswille* ersichtlich sein.[8]

Sowohl in den Print- wie auch in den elektronischen Medien wurde breit über die Urteile des Appellationgerichts des Kantons Basel-Stadt und des Bundesgerichts sowie über deren Folgen, also über die hier zu beurteilenden Sachverhalte (Rückzahlung des Deliktsbetrags und Abberufung des damaligen Stiftungsratspräsidenten), berichtet. Weiter haben sich auch die Betroffenen selbst verschiedentlich zu den Ereignissen öffentlich geäussert. Daher weisen nach Ansicht des Beauftragten diese Informationen, die sich in den hier zu beurteilenden amtlichen Dokumenten finden, keinen *Geheimnischarakter* auf. Sie sind Tatsachen, die aufgrund der erwähnten Ereignisse in der Öffentlichkeit allgemein bekannt sowie allgemein zugänglich sind.

[8] Bundesamtes für Justiz: «Leitfaden Gesuchsbeurteilung und Checkliste» vom 24.05.2006, S. 8

Die Ausnahmeklausel von Art. 7 Abs. 1 Bst. g BGÖ gelangt vorliegend nicht zur Anwendung.

6. Personendaten:

   Die in Ziffer I.5. aufgeführten amtlichen Dokumente enthalten Personendaten im Sinne von Art. 3 Bst. a des Bundesgesetzes über den Datenschutz (DSG, *SR* 235.1) zu folgenden Personen:

   - Y,
   - der SPS,
   - Z,
   - die Namen von Mitarbeitenden der Stiftungsaufsicht und des Amtstatthalteramtes Sursee,
   - der Rechtsanwalt der SPS,
   - weitere Personen, die keinen direkten respektiven nur einen begrenzten Bezug zur hier zu beurteilenden Angelegenheit aufweisen (z.B. betreffen sie einen Vergleich mit einer anderen Stiftung).

   Gemäss Art. 9 Abs. 1 BGÖ müssen amtliche Dokumente, die Personendaten enthalten, «nach Möglichkeit» anonymisiert werden. Ist dies nicht möglich, so ist das Zugangsgesuch gemäss Art. 9 Abs. 2 BGÖ nach Artikel 19 DSG zu beurteilen.

6.1. Namen der Mitarbeitenden der Stiftungsaufsicht und des Amtsstatthalteramtes Sursee:

   Die Namen und die Funktionen von Verwaltungsangestellten (insbesondere von Entscheidungsträgerinnen und Entscheidungsträgern), die in amtlichen Dokumenten erwähnt werden, unterliegen, soweit diese Personen in Erfüllung einer öffentlichen Aufgabe gehandelt haben, nicht der Anonymisierungspflicht.[9]

[9] Handkommentar zum BGÖ, Art. 9 RZ 14

6.2. Namen des Rechtsanwalts, der Stiftungsratsmitglieder und weiterer Personen:

Entsprechend Art. 9 Abs. 1 BGÖ können die in den fraglichen Dokumenten enthaltenen Personendaten des Rechtsanwalts, der im Protokoll vom 23. April 2007 erwähnten Mitglieder des Stiftungsrates der SPS und weiterer Personen problemlos anonymisiert respektive pseudonymisiert werden.

6.3. Namen von Y, der SPS und Z:

Nach Ansicht der Stiftungsaufsicht können diese Personendaten nicht anonymisiert werden, da aufgrund der konkreten Umstände weiterhin Rückschlüsse auf die Person der betroffenen Dritten möglich seien.

Wie vorgängig erwähnt, muss die Beurteilung des Zugangsgesuchs nach Art. 19 DSG erfolgen. Art. 19 Abs. 1*bis* DSG ermöglicht es Bundesbehörden, gestützt auf das Öffentlichkeitsgesetz Personendaten bekannt zu geben, wenn die betreffenden Personendaten im Zusammenhang mit der Erfüllung einer öffentlichen Aufgaben stehen und wenn an ihrer Bekanntgabe ein überwiegendes öffentliches Interesse besteht. Diese Bestimmung stellt eine Koordinationsnorm zu Art. 7 Abs. 2 BGÖ dar, der vorsieht, dass der Zugang zu amtlichen Dokumenten beschränkt wird, wenn durch seine Gewährung die Privatsphäre Dritter beeinträchtigt werden könnte. Ausnahmsweise muss deren Privatsphäre einem überwiegenden Interesse der Öffentlichkeit am Zugang zu den Dokumenten weichen.

Im Folgenden gilt es zu prüfen, ob (1°) die Zugangsgewährung zu einer Beeinträchtigung der Privatsphäre der betroffenen Dritten führt und (2°) ein allfälliges überwiegendes Interesse einen teilweisen oder vollumfänglichen Zugang zu den fraglichen Dokumenten rechtfertigt.

6.4. Beeinträchtigung der Privatsphäre:

Es stellt sich die Frage, ob angesichts der in der Öffentlichkeit bereits bekannten Einzelheiten dieses Falles eine *uneingeschränkte Gewährung* des Zugangs zu den fraglichen Dokumenten *die Privatsphäre* der betroffenen Dritten (Y, der SPS, Z) überhaupt *beeinträchtigen kann*.

Der vorliegende Fall zeichnet sich dadurch aus, dass

- über die Urteile des Appellationsgerichts des Kantons Basel-Stadt und des Bundesgerichts gegen den ehemaligen Stiftungsratspräsidenten in den Medien ausführlich berichtet worden ist.

- Y und auch die SPS selber wiederholt öffentlich Position dazu bezogen haben (Site der SPS http://www.paraplegiker.ch/sw31702.asp, Paraplegiker-Magazin[10]).

- Y nicht als Privatperson, sondern in seiner Funktion als ehemaliger Stiftungsratspräsident gehandelt hat, und er sich für sein Wirken in der Öffentlichkeit - gerade auch im Zusammenhang mit seiner Verurteilung durch das Bundesgericht und seiner Abberufung aus dem Stiftungsrat - weitergehende Eingriffe in seine Privatsphäre gefallen lassen muss.

- die SPS gemäss eigenen Angaben über einen «sehr grossen Rückhalt in der Bevölkerung» verfügt und 1,2 Millionen Haushalte des Landes der Z angehören.[11]

- die Stiftungsaufsicht eine Verfügung im Internet publiziert hat, die zwar nicht die hier erwähnten Sachverhalte zum Gegenstand hat, aber in der sie u.a. darauf hinweist, dass «die Eidgenössische Stiftungsaufsicht und die Öffentlichkeit bezüglich Rückerstattung des vom Bundesgericht festgestellten Deliktsbetrags getäuscht wurden, indem der überwiesene Betrag nicht aus der Vermögenssphäre von ■■■ stammte, sondern in Wirklichkeit durch die ■■■ geleistet wurde».[12]

Auf Grund dieser Tatsachen gelangt der Beauftragte zur Ansicht, dass die Gewährung des Zugangs zu den fraglichen amtlichen Dokumenten zu keiner Beeinträchtigung der Privatsphäre der betroffenen Dritten (Y, der SPS, Z) führt.

6.5. Vorliegen eines überwiegenden öffentlichen Interesses:

Selbst wenn man die Haltung vertreten würde, dass die Gewährung des Zugangs die Privatsphäre der Betroffenen tatsächlich beeinträchtigte, käme im vorliegenden Fall hinzu, dass nach Einschätzung des Beauftragten das öffentliche Interesse am Zugang jenes der betroffenen Dritten am Schutz ihrer Privatsphäre überwiegt. Die Verurteilung eines Stiftungsratspräsidenten wegen Veruntreuung sowie die Täuschung der «Eidgenössische(n) Stiftungsaufsicht und (der) Öffentlichkeit bezüglich Rückerstattung des vom Bundesgericht fest-

[10] Stellungnahme des Stiftungsrates SPS zum Bundesgerichtsurteil, veröffentlicht in «Paraplegie, Das offizielle Magazin der Schweizer Paraplegiker-Stiftung», Juni 2007, S. 6f.
[11] http://www.paraplegiker.ch/sw11888.asp
[12] Verfügung vom 20. Februar 2008 in Sachen Schweizer Paraplegiker-Stiftung (nur in deutscher Sprache); Zitat S. 6

gestellten Deliktsbetrags»[13] im konkreten Fall begründen ein besonderes Informationsinteresse der Öffentlichkeit im Sinne von Art. 6 Abs. 2 Bst. a VBGÖ. Als besonderer Umstand kommt die Tatsache hinzu, dass es sich bei der SPS um eine für schweizerische Verhältnisse ausserordentlich bekannte wie bedeutende Stiftung handelt, die jedes Jahr von einer beträchtlichen Anzahl von Personen («1.2 Millionen Haushalte») Millionenbeträge an Gönnerbeiträgen, Spenden sowie Zuwendungen aus Erbschaften und Legaten erhält. Des Weiteren besteht im vorliegenden Fall auch ein berechtigtes öffentliches Interesse an der korrekten Umsetzung des Öffentlichkeitsgesetzes: Es soll in Erfahrung gebracht werden können, welche Schritte die zuständige staatliche Aufsichtsbehörde in einem Fall, der in der Öffentlichkeit auf grosses Interesse gestossen ist, konkret unternommen hat.

6.6. Zusammenfassend kann daher festgehalten werden, dass:

- *die Stiftungsaufsicht den Zugang zu den in Ziffern I.5. aufgeführten Dokumenten gewährt,*
- *die Personendaten von Y, der SPS und Z nicht abgedeckt werden müssen, da deren Bekanntgabe zu keiner Beeinträchtigung ihrer Privatsphäre führt respektive ein überwiegendes Interesse am Zugang besteht (Art. 7 Abs. 2 BGÖ), und*
- *die Namen weiterer Personen abgedeckt werden müssen (Art. 9 Abs. 1 BGÖ).*

7. Rechtliches Gehör:

Der Beauftragte eröffnet diese Empfehlung allen Personen, die betroffene Dritte im Sinne von Art. 7 Abs. 2 BGÖ sind. Sie haben somit - wie der Antragsteller - die Möglichkeit, von der Stiftungsaufsicht den Erlass einer Verfügung zu verlangen und gegen diese eine Beschwerde beim Bundesverwaltungsgericht einzureichen.

[13] Zitat Verfügung vom 20. Februar 2008 der Stiftungsaufsicht

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

1. Die Eidgenössische Stiftungsaufsicht gewährt den Zugang zu allen in Ziffer I.5. aufgeführten Dokumenten.

   Die Personendaten von Y, der Schweizer Paraplegiker-Stiftung und Z sind zugänglich zu machen.

   Die Daten der übrigen in diesen Dokumenten erwähnten Personen müssen anonymisiert werden.

2. Die Eidgenössische Stiftungsaufsicht erlässt eine Verfügung nach Art. 5 des Verwaltungsverfahrensgesetzes, wenn sie in Abweichung von Ziffer 1 den Zugang nicht gewähren will.

   Die Eidgenössische Stiftungsaufsicht erlässt die Verfügung innert 20 Tagen nach Empfang dieser Empfehlung (Art. 15 Abs. 3 BGÖ).

3. Der Antragsteller und die von dieser Empfehlung betroffenen Personen (Y, die Schweizer Paraplegiker-Stiftung und Z) können innerhalb von 10 Tagen nach Erhalt dieser Empfehlung bei der Eidgenössischen Stiftungsaufsicht den Erlass einer Verfügung nach Artikel 5 des Verwaltungsverfahrensgesetzes verlangen, wenn sie mit der Empfehlung nicht einverstanden sind (Art. 15 Abs. 1 BGÖ).

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

4. Diese Empfehlung wird veröffentlicht. Entsprechend den Vorgaben von Art. 13 Abs. 3 VBGÖ muss der Beauftragte die Namen des Antragstellers und der betroffenen Drittpersonen anonymisieren.

5. 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 und mit dem 2. Januar still.

6. Die Empfehlung wird eröffnet:

- X

- Eidgenössisches Departement des Innern EDI
  Generalsekretariat GS-EDI
  Stiftungsaufsicht
  Inselgasse 1
  3003 Bern

- Y

- Schweizer Paraplegiker-Stiftung
  CH-6207 Nottwil

- Z

Hanspeter Thür