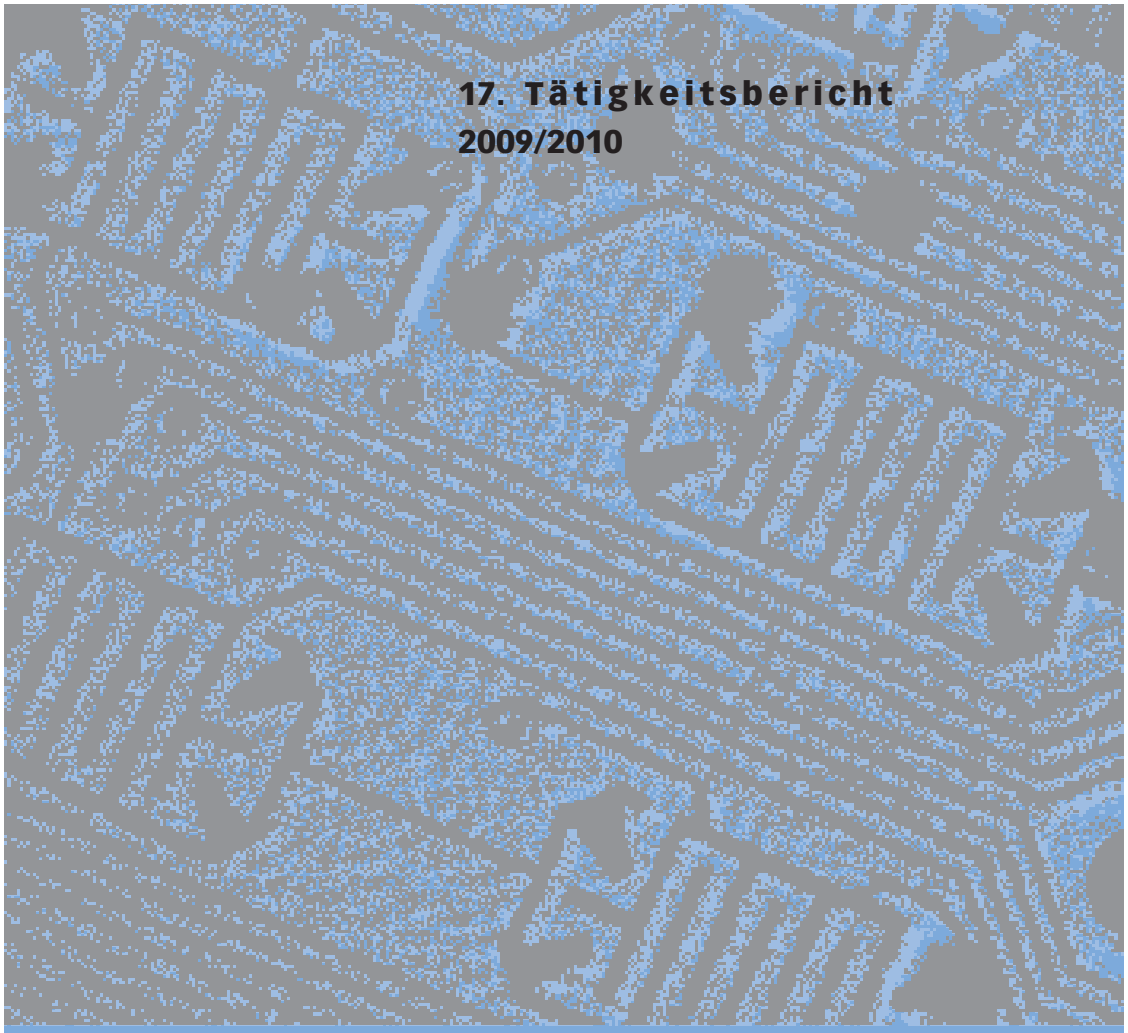


# 17. Tätigkeitsbericht 2009/2010

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

# Tätigkeitsbericht 2009/2010 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 2009 und 31. März 2010 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. 410.017.d/f

## Inhaltsverzeichnis



* Originaltext auf Französisch

* Originaltext auf Französisch

* Originaltext auf Französisch

# Vorwort

## Goldgräberstimmung im Internet – das Ende der Privatsphäre?

Es vergeht kaum eine Woche, ohne dass Internetgiganten wie Google oder Facebook neue beeindruckende Dienstleistungen und Tools anbieten. Sie funktionieren immer nach dem gleichen Muster: Der Dienst ist gratis für alle, die Anbieter generieren ihre Einnahmen über die Werbung. Die Werbeeinnahmen steigen, je mehr Personen solche Dienste in Anspruch nehmen und je gezielter ihre Bedürfnisse analysiert werden können. Auf der Suche nach möglichst vielen Nutzern und Werbemöglichkeiten ziehen die Anbieter sämtliche Register. Einige Beispiele aus jüngster Vergangenheit:

- Facebook offeriert ein Synchronisierungstool, mit welchem die Mitglieder ihre Agenden und Adressbücher auf seiner Plattform abgleichen können. Die so hochgeladenen Kontakte stehen aber nicht nur den Nutzern selbst, sondern auch Facebook zur Verfügung. Auf diese Weise erhält das Unternehmen auch Zugang zu Informationen über Personen, die davon nichts wissen und auch ihr Einverständnis nicht gegeben haben.
- Auch Google ist mittlerweile in den lukrativen Markt der Social Networks eingestiegen und offeriert Gmail-Nutzern mit «Google-Buzz» ein Tool, welches es ihnen erlaubt, ebenfalls mit «Freunden» Informationen auszutauschen. Einen Aufschrei gab es deswegen, weil Google die Grundeinstellungen so eingerichtet hatte, dass der gesamte Emailverkehr jener 176 Millionen Gmail-Nutzer, die dieses Tool anklickten, öffentlich wurde.
- Twitter wird mit einer Lokalisierungsfunktion erweitert. Über Twitter kann man den «Followern» künftig nicht nur seine Gedanken und Aktivitäten mitteilen, sondern ihnen auch seinen Aufenthaltsort kundtun: Über Webbrowser werden die Twitter-Nutzer auf Schritt und Tritt verfolgt und die Koordinaten übermittelt. Abgesehen davon, dass Twitterfreunde so jederzeit wissen, wo man sich befindet, weiss das natürlich auch Twitter und kann zielgenaue Werbung lancieren: Wer sich beispielsweise in der Nähe eines Kleidershops befindet, erhält interessante Angebote per SMS.
- Mit dem von Google kürzlich lancierten Mobiltelefon «Android» erhält man eine kostenlose Strassennavigation mit pfiffiger Suchtechnik: Es genügt zu sagen, «Navigiere zur Ausstellung ‹Körperwelten› in Zürich!» und das Gerät navigiert uns ins Puls 5 an der Giessereistrasse 18. Keine Frage, dass damit gewaltige Werbemöglichkeiten geschaffen werden.

- Google pröbelt mit «Goggle» bereits an einer Handy-Software zur automatischen Gesichtserkennung. Via Suchmaschine wird recherchiert, ob die fotografierte Person in irgendeiner Datenbank des Internets vorhanden ist, und die Ergebnisse werden dann aufs Mobiltelefon übermittelt.

Das Mobiltelefon mit Ortungsfunktion ermöglicht künftig überall, ortsbezogene Informationen zu erhalten, Sehenswürdigkeiten zu identifizieren, Freunde zu finden und Personen zu identifizieren. Die reale Welt wird gleichsam zur digitalen Benutzeroberfläche, welche Informationen jederzeit und überall verfüg- und abrufbar macht. Früher ging man «ins Internet» – in den Cyberspace als virtuellen Raum. Künftig ist das Netz überall, ein Outernet, wie der Trendforscher Nils Müller den Begriff den künftigen Gegebenheiten anpasst.

Die Auswertung der Daten der vielen Millionen Nutzerinnen und Nutzer wird für die Internetgiganten zur eigentlichen Goldgrube. Sie kennen die Vorlieben ihrer Kunden, wissen, wo sie sich bewegen, mit wem sie in Kontakt sind, was sie interessiert und was sie denken. Die heutigen hocheffizienten Analysesoftwares entdecken in diesen Informationen Algorithmen, welche die Erstellung nahezu perfekter Persönlichkeits- und Konsumprofile ermöglichen. Damit wird zielgenaues Werben (in Bezug auf Ort, Zeit, Produkt und Person) in noch nie da gewesenem Ausmass ermöglicht. Es ist deshalb nicht verwunderlich, dass die traditionellen Werbeträger, allen voran die Medien, weltweit um ihre Werbeeinnahmen fürchten; in den USA hat die Onlinewerbung die gedruckte bereits überholt. Weiter nicht verwunderlich ist, dass man sich in den Gremien der OECD und bei den Wettbewerbshütern inzwischen Sorgen macht über die marktbeherrschende Stellung der Internetgiganten. Selbst in den USA beginnen sich staatliche Institutionen dieser Problematik zu widmen.

Interessant bei dieser Entwicklung ist die Frage, wie die neuen Angebote unser Kommunikationsverhalten beeinflussen werden. Wenn Algorithmen zunehmend unser Leben beeinflussen, uns sagen, wer wir seien und was wir tun sollten, wird die individuelle Selbstbestimmung als Essenz eines freiheitlich liberalen Gesellschaftsmodells in Frage gestellt. Über die Auswirkungen dieser algorithmusgesteuerten Wahrnehmung und Entscheidfindung auf die demokratischen Entscheidungsmechanismen sind Studien in Bearbeitung; ich bin gespannt auf deren Erkenntnisse.

Es bringt nichts, angesichts solcher Entwicklungen in Kulturpessimismus zu verfallen und nur noch schwarz zu sehen, auch wenn nicht zu leugnen ist, dass sie eine grosse Herausforderung für all jene bedeuten, die sich dem Schutz der Privatsphäre

verpflichtet fühlen. Gefordert ist aber nicht nur der Datenschutz, sondern die Gesellschaft insgesamt:

*Zunächst die Nutzerinnen und Nutzer selber*: Sie müssen sich erstens vor Augen führen, dass die von ihnen preisgegebenen persönlichen Informationen Geld wert sind. Zweitens müssen sie abwägen, ob es das Angebot wert ist, (soviel) Persönliches ins Internet zu stellen. Selbstverantwortung wahrnehmen heisst, vor allem das Kleingedruckte zu lesen und sich zu vergewissern, welche Informationen man wirklich freigeben will – im Bewusstsein, dass damit sehr detaillierte Persönlichkeitsprofile kreiert werden können. Die Nutzer müssen auch wissen, dass sie keine Informationen über Freunde und Bekannte – wie Fotos von Familienfesten oder Betriebsausflügen – ohne Einwilligung aller Beteiligten aufs Netz schalten dürfen.

*Gefordert ist der Gesetzgeber:* Er muss zur Kenntnis nehmen, dass alle diese Internetangebote grundsätzlich eine möglichst weitgehende Offenlegung persönlicher Daten anstreben, weil sie möglichst viele Werbeeinnahmen generieren wollen. Deshalb sind die Grundeinstellungen dieser Produkte nicht privacy-orientiert. Aus Sicht eines wohlverstandenen Persönlichkeitsschutzes darf es nicht sein, dass derjenige aktiv werden muss, der seine Privatsphäre schützen will. Es muss genau umgekehrt sein: Jeder Anbieter muss per Gesetz verpflichtet werden, jene Technologie und jene Einstellungen zu wählen, die den grösstmöglichen Schutz der Privatsphäre garantieren. Nutzer, die darauf verzichten wollen, können dies tun, sie müssen aber von sich aus aktiv werden und die Grundeinstellungen ihrer Accounts anpassen. Wichtig ist in diesem Zusammenhang der Hinweis, dass nationalstaatliche Regelungen allein das Problem nicht in den Griff kriegen werden. Gefragt sind auch Lösungsansätze auf internationaler Ebene.

*Gefordert sind auch die Medien und die Schulen*: Information und Aufklärung sind die einzigen Mittel, um Nutzerinnen und Nutzer in die Lage zu versetzen, selbstverantwortlich von den neuen Angeboten Gebrauch zu machen. Die Schulen sollten frühzeitig ein ausreichendes Fundament legen, damit Kinder und Jugendliche das Bewusstsein für den Wert ihrer Privatsphäre entwickeln können. Jede Bildungsstufe muss sich mit dem Phänomen der neuen Kommunikationsmittel auseinandersetzen und Handlungsanleitungen vermitteln.

*Gefordert sind nicht zuletzt auch die Anbieter solcher Dienste*: Im Interesse ihres guten Rufes müsste es ihnen ein Anliegen sein, datenschutzkonforme Produkte so auf den Markt zu bringen, dass sie der Nutzer nicht mehr verbessern muss.

Allerdings mache ich mir da keine Illusionen: Nur der Druck der Öffentlichkeit wird die grossen Player auf den Pfad der Tugend bringen.

Im Falle von Google Street View, der uns letztes Jahr intensiv beschäftigt hat und dies auch künftig tun wird, geht es genau um diese Frage: Welcher Perfektionsstand muss ein Produkt hinsichtlich des Schutzes der Privatsphäre aufweisen? Ist es richtig, dass man auf dem Netz intervenieren muss, wenn einem der angebotene Schutz nicht genügt? Diese Grundsatzfrage wird vom Bundesverwaltungsgericht vielleicht noch dieses Jahr beantwortet. Der Entscheid wird ein Massstab sein auch für andere Anbieter von Dienstleistungen im Internet.

Auch wenn sich viele zunehmend damit abzufinden scheinen, dass im Internetzeitalter wenig oder gar nichts mehr privat sein wird, dürfte die Schlussfolgerung, die Google-Chef Eric Schmidt kürzlich daraus zog, hoffentlich noch lange nicht mehrheitsfähig werden. Er sagte nämlich: «Wenn es etwas gibt, von dem Sie nicht wollen, dass es irgend jemand erfährt, sollten Sie es vielleicht gar nicht erst tun.» Das ist ganz im Sinne des Facebook-Gründers Mark Zuckerberg, der in einem Interview zum Besten gab, für ihn sei die Privatsphäre nicht mehr zeitgemäss.

Die Nutzerinnen und Nutzer hingegen setzen immer wieder Zeichen gegen einen zu liederlichen Umgang mit ihren persönlichen Daten. Sie protestieren, formieren sich zu Gruppen, bloggen – und erwirken durchaus auch Verbesserungen. Als Datenschutzbehörde unterstützen wir diese Tendenzen nach Kräften.

Hanspeter Thür

## Abkürzungsverzeichnis

| | |
|---|---|
| AHVG | Bundesgesetz über die Alters- und Hinterlassenenversicherung |
| ARE | Bundesamt für Raumentwicklung |
| ASTRA | Bundesamt für Strassen |
| ATSV | Verordnung über den Allgemeinen Teil des Sozialversicherungsrechts |
| BAFU | Bundesamt für Umwelt |
| BAG | Bundesamt für Gesundheit |
| BAKOM | Bundesamt für Kommunikation |
| BAZL | Bundesamt für Zivilluftfahrt |
| BFE | Bundesamt für Energie |
| BFM | Bundesamt für Migration |
| BFS | Bundesamt für Statistik |
| BGE | Bundesgerichtsentscheid |
| BGÖ | Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung |
| BIT | Bundesamt für Informatik und Telekommunikation |
| BJ | Bundesamt für Justiz |
| BK | Bundeskanzlei |
| BKP | Bundeskriminalpolizei |
| BLW | Bundesamt für Landwirtschaft |
| BSV | Bundesamt für Sozialversicherungen |
| BÜPF | Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs |
| BVG | Bundesgesetz über die berufliche Alters-, Hinterlassenen- und Invalidenvorsorge |
| BVGer | Bundesverwaltungsgericht |
| DSG | Bundesgesetz über den Datenschutz |
| EDA | Eidgenössisches Departement für auswärtige Angelegenheiten |

| | |
|---|---|
| EDI | Eidgenössisches Departement des Innern |
| EDÖB | Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter |
| EFD | Eidgenössisches Finanzdepartement |
| EJPD | Eidgenössisches Justiz- und Polizeidepartement |
| ELGK | Eidgenössische Kommission für allgemeine Leistungen und Grundsatzfragen |
| EPA | Eidgenössisches Personalamt |
| ESTV | Eidgenössische Steuerverwaltung |
| EVD | Eidgenössisches Volkswirtschaftsdepartement |
| fedpol | Bundesamt für Polizei |
| FINMA | Eidgenössische Finanzmarktaufsicht |
| GEWA | Datenverarbeitungssystem zur Bekämpfung der Geldwäscherei |
| GK | Gemeinsame Kontrollinstanz Schengen |
| HFG | Bundesgesetz über die Forschung am Menschen |
| IDHEAP | Institut de hautes études en administration publique |
| ISB | Informatikstrategieorgan Bund |
| IschV | Verordnung über den Schutz von Informationen des Bundes |
| ISIS | Staatsschutz-Informationssystem |
| IVF-ET | In-Vitro-Fertilisation / Embryotransfer |
| IVI | Institut für Viruskrankheiten und Immunprophylaxe |
| JANUS | Gemeinsames Informationssystem der kriminalpolizeilichen Zentralstellen des Bundes |
| MWSTG | Bundesgesetz über die Mehrwertsteuer |
| MWSTV | Mehrwertsteuerverordnung |
| N-SIS | Nationaler Teil des Schengener Informationssystems |
| OECD | Organisation for Economic Co-operation and Development (Organisation für wirtschaftliche Zusammenarbeit und Entwicklung) |
| OR | Obligationenrecht |

| | |
|---|---|
| PGP | Pretty Good Privacy (Ph. Zimmerman) |
| RFID | Radio Frequency Identification |
| RSA | Rivest-Shamir-Adelman (Algorithmus) |
| RTVV | Radio- und Fernsehverordnung |
| RVOG | Regierungs- und Verwaltungsorganisationsgesetz |
| S/MIME | Secure / Multipurpose Internet Mail Extensions |
| SAKE | Schweizerische Arbeitskräfteerhebung |
| SAS | Schweizerische Akkreditierungstelle |
| SchKG | Bundesgesetz über Schuldbetreibung und Konkurs |
| SIRENE | Supplementary Information Request at the National Entry |
| SIS | Schengener Information System |
| StGB | Schweizerisches Strafgesetzbuch |
| SUVA | Schweizeische Unfallversicherungsanstalt |
| UID | Unternehmens-Identifikationsnummer |
| UIDG | Bundesgesetz über die Unternehmensidentifikationsnummer |
| UVEK | Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation |
| UVG | Bundesgesetz über die Unfallversicherung |
| UWG | Bundesgesetz gegen den unlauteren Wettbewerb |
| VBS | Departement für Verteidigung, Bevölkerungsschutz und Sport |
| VDSZ | Verordnung über die Datenschutzzertifizierungen |
| WADA | World Anti-Doping Agency |
| ZEMIS | Zentrales Migrationsinformationssystem |
| ZGB | Zivilgesetzbuch |

# 1. Datenschutz

## 1.1 Grundrechte

### 1.1.1 Zertifizierung von Datenschutzmanagementsystemen: Akkreditierungen

**Die Schweizerische Akkreditierungsstelle (SAS) hat erste private Unternehmen für die Datenschutzzertifizierung von Organisation und Verfahren akkreditiert. Wir haben sie dabei begleitet. Die akkreditierten Unternehmen werden auf der Internetseite der SAS publiziert.**

Nachdem unsere Richtlinien über die Mindestanforderungen an ein Datenschutzmanagementsystem (Zertifizierung von Organisation und Verfahren) am 1. September 2008 in Kraft getreten sind, haben private Unternehmen die Möglichkeit, sich akkreditieren zu lassen. Zuständig ist die Schweizerische Akkreditierungsstelle (SAS), die uns für das Akkreditierungsverfahren beizuziehen hat. So haben wir die SAS im Rahmen der Akkreditierung sowohl bei der Begutachtung vor Ort als auch bei Witness-Audits begleitet. In dieser Phase beschränkte sich unsere Rolle darauf, zu beobachten und allfällige Fragen der SAS und der Fachexpertin zu beantworten. Wir gewannen dadurch erste Eindrücke sowohl über die Akkreditierung als auch über die Zertifizierung in der Praxis. Solche Erfahrungen werden uns im Rahmen unserer Aufsichtsfunktion, die auch gegenüber zertifizierten Unternehmen bestehen bleibt, nützlich sein. Wir haben zudem gemerkt, wie wichtig es ist, von Anfang an das Zertifizierungsobjekt (d.h. den Umfang des zu zertifizierenden Bearbeitungsverfahrens) klar zu definieren.

Die akkreditierten Unternehmen werden von der SAS auf ihrer Website (www.sas.ch, unter akkreditierte Stellen) publiziert.

### 1.1.2 Zertifizierung von Produkten: Quo vadis?

**Wir haben durch das Bundesamt für Justiz beim Bundesrat einen Antrag betreffend Verlängerung der uns in der Verordnung über die Datenschutzzertifizierungen gesetzten Frist für den Erlass der Richtlinien eingereicht.**

Die schon letztes Jahr (vgl. unseren 16. Tätigkeitsbericht 2008/2009, Ziff. 1.1.1) angedeuteten Schwierigkeiten beim Erlass der Richtlinien für die Zertifizierung von Produkten haben sich nur teilweise geklärt. Wir haben uns deshalb entschieden, der Suche nach

optimalen Lösungen mehr Zeit einzuräumen und in diesem Sinne einen Antrag an den Bundesrat gestellt, die uns in Art. 5 Abs. 3 der Verordnung über die Datenschutzzertifizierungen (VDSZ) gesetzte Frist für den Erlass der Richtlinien zu verlängern.

Wir haben im Februar 2010 interessierte Kreise zu einer Informationsveranstaltung zum Stand unserer Arbeiten eingeladen. Danach haben wir eine Arbeitsgruppe gebildet und sind nun zuversichtlich, die Richtlinien im Anschluss an diese Arbeiten baldmöglichst erlassen zu können.

### 1.1.3 Volkszählung 2010

**2010 wird die Volkszählung, ermöglicht durch die Registerharmonisierung, erstmals nach dem neuen System durchgeführt. Neu werden im Rahmen der Volkszählung jedes Jahr grosse Datenmengen von Bürgerinnen und Bürgern erhoben und bearbeitet werden. Wir begleiteten verschiedene Projekte und konnten feststellen, dass die Akteure grundsätzlich für datenschutzrechtliche Fragestellungen sensibilisiert sind.**

Die Volkszählung 2010 wird erstmals nach einem durch die Registerharmonisierung ermöglichten System abgewickelt. Dabei werden die Basisdaten aus den kantonalen Einwohnerregistern, den wichtigsten Bundesregistern und dem eidgenössischen Wohn- und Gebäuderegister erhoben. Zusätzlich wird neben einer Stichprobenerhebung, von der 200'000 Bürgerinnen und Bürger betroffen sind, auch eine thematische Erhebung durchgeführt, in welcher 10'000-40'000 Personen über ihr Mobilitäts- und Verkehrsverhalten befragt werden. Letztlich werden noch kleinere Erhebungen, so genannte Omnibusse, zu ausgewählten Themen durch das Bundesamt für Statistik (BFS) veranlasst. Für die betroffenen Bürgerinnen und Bürger ist es wichtig zu wissen, dass die Volkszählung kein einmaliges grösseres statistisches Projekt ist, das nur alle 10 Jahre stattfindet. Zukünftig werden im Rahmen der Volkszählung durch das BFS alljährlich grosse Datenmengen erhoben und bearbeitet.

Die Erhebungen nach neuem System werden erst ab Mitte des Jahres 2010 in eine produktive Phase treten. Wir haben das BFS in diesen Arbeiten begleitet und zu verschiedenen Konzepten, die den Datenschutz betreffen, Stellung genommen. Soweit wir dies beurteilen können, wurden unsere Anregungen umgesetzt. Wir werden die Volkszählung weiter eng begleiten und haben auch entsprechende Kontrollen geplant.

Die Post tritt im Rahmen der Vorarbeiten für die Volkszählung als private Dienstleistungserbringerin für die erstmalige Zuweisung des Wohnungsidentifikators auf. Gerade grössere Stadtgemeinden und auch einige Kantone haben diese Dienstleistung

in Anspruch genommen. Dabei stellten sich verschiedene datenschutzrechtliche Probleme, die wegen der Kompetenzenteilung zwischen Bund und Kantonen nicht einfach zu lösen waren. Wir haben die Post entsprechend beraten und sie bei Bedarf an die zuständigen Stellen verwiesen.

Neben der Post werden diverse andere externe Akteure an der Volkszählung beteiligt sein. Das BFS hat entsprechende Aufträge ausgeschrieben und vergeben, während wir die Verträge auf datenschutzrechtliche Schutzklauseln geprüft haben. Anlässlich dieser Überprüfung haben wir das BFS darauf aufmerksam gemacht, dass es die Umsetzung der datenschutzrechtlichen Bestimmungen kontrollieren muss. Ein weiteres Problem, das sich auch schon bei der letzten Volkszählung stellte, ist das Zweckbindungsgebot, das den externen Dienstleistungsunternehmen verbietet, die im Rahmen der Volkszählung zu statistischen Zwecken erhobenen Daten für andere Zwecke zu benutzen. Wir werden diesbezüglich unsere Aufsichtspflicht wahrnehmen.

### 1.1.4 SAKE – Statistische Umfrage des Bundes per Telefon

**Im Herbst 2009 galt für natürliche Personen erstmals eine Antwortpflicht für die SAKE, die Schweizerische Arbeitskräfteerhebung. Dieser Umstand und die Tatsache, dass die Erhebung telefonisch durch ein vom Bundesamt für Statistik (BFS) beauftragtes privates Institut durchgeführt wurde, führten zu einer Welle der Empörung und verunsicherte viele Bürgerinnen und Bürger. Wir standen dem BFS beratend zur Seite und nahmen dazu Stellung.**

Seit Oktober 2009 ist für Bürgerinnen und Bürger, welche im Rahmen der SAKE befragt werden, antworten obligatorisch. Mit dieser Erhebung werden Informationen zu den Arbeitsbedingungen, den Auswirkungen des freien Personenverkehrs und der Working-Poor-Quote in der Schweiz generiert.

Die Einführung der Antwortpflicht für die Bürgerinnen und Bürger führte ebenso zu grosser Verunsicherung wie der Umstand, dass die Erhebung am Telefon durch ein vom Bundesamt für Statistik (BFS) beauftragtes privates Institut durchgeführt wird. Die Unsicherheit wurde durch Medienberichte über hohe Bussen bei Verweigerung der Antworten noch vergrössert.

Wir haben das BFS bei der Beratung der besorgten Bürgerinnen und Bürger unterstützt und verschiedene Massnahmen vorgeschlagen, um das Vertrauen der Bevölkerung in die datenschutzkonforme Bearbeitung der erhobenen Daten zu festigen. Dabei legten wir den Schwerpunkt auf die grössere Sicherstellung der Authentifizierung des erhebenden Institutes. Auf unseren Vorschlag hin fügte das BFS dem vorangehenden

Informationsschreiben, das für die SAKE ausgewählte Personen vor ihrer Befragung erhalten, einen Code hinzu. Der angerufene Bürger kann das anrufende Institut um Angabe des Codes bitten und überprüfen, ob es das zur Erhebung der für die SAKE benötigten Daten berechtigte ist.

In einer Stellungnahme gegenüber dem BFS haben wir festgehalten, dass wir die telefonische Erhebungsmethode im Rahmen einer obligatorischen Befragung als problematisch erachten. Aus den zahlreichen an uns gerichteten Fragen und Beschwerden von Bürgerinnen und Bürgern ging klar hervor, dass ein solches Vorgehen durch den Staat als unverhältnismässiger Eingriff in die Privatsphäre empfunden wird. Wir begrüssen deshalb die diesbezügliche parlamentarische Debatte, angestossen in der Frühjahrssession 2010. Denn es ist unbestritten, dass telefonische Befragungen auch durch dubiose Firmen zur Beschaffung von Personendaten verwendet werden. Aus diesem Grund raten wir grundsätzlich davon ab, über das Telefon Personendaten leichtfertig und ohne genaue Prüfung von Ziel und Zweck der Erhebung preiszugeben. Es ist uns klar, dass diese Prüfung einiges an Umsicht und Durchsetzungsvermögen seitens der Bürgerinnen und Bürger verlangt. Auch deshalb setzen wir uns dafür ein, dass das BFS die telefonische Befragungsmethode nicht auf weitere obligatorische Erhebungen ausdehnt.





### 1.1.5 Das neue Humanforschungsgesetz

**Der Entwurf des Humanforschungsgesetzes wurde im Oktober 2009 vom Bundesrat verabschiedet und dem Parlament zur Beratung überwiesen. Vorgängig konnten wir in einer Ämterkonsultation dazu Stellung nehmen. Der Gesetzesentwurf sieht die Schaffung einer Ausweichklausel für Forschende im Bereich der Weiterverwendung von biologischem Material und gesundheitsbezogenen Personendaten vor. Dies ist aus unserer Sicht höchst bedenklich.**

Im Rahmen der Ämterkonsultation haben wir zum Entwurf des Bundesgesetzes über die Forschung am Menschen (Humanforschungsgesetz, HFG) Stellung genommen. Mit dem Gesetzesentwurf soll eine Lücke in der schweizerischen Gesundheitsgesetzgebung geschlossen werden. Diesen Umstand begrüssen wir, gerade weil dem Schutz der Menschenwürde im neuen Entwurf eine besondere Stellung eingeräumt wird. Leider wird im Gesetzesentwurf und auch im zugrunde liegenden Verfassungsartikel, über den im Frühling 2010 abgestimmt worden ist, aber nur die Datenbearbeitung im Rahmen der biologischen und medizinischen Forschung geregelt. Andere Bereiche der Forschung am Menschen, beispielsweise in der Sozialpsychologie, sind davon ausgenommen.

In unserer Stellungnahme haben wir das Bundesamt für Gesundheit (BAG) auf verschiedene datenschutzrechtliche Probleme hingewiesen. Wir möchten an dieser Stelle auf zwei Punkte näher eingehen. Zum einen werden die Aufgaben der Expertenkommission für das Berufsgeheimnis in der medizinischen Forschung an die kantonalen Ethikkommissionen delegiert. Die Bewilligung der Expertenkommission wurde regelmässig mit Auflagen zum Datenschutz verbunden, deren Umsetzung wir stichprobenartig überprüft haben. An den Sitzungen der Expertenkommission nahmen wir in beratender Funktion ohne Stimmberechtigung teil. Neu wird nun vorgeschrieben, dass die Ethikkommissionen so zusammengesetzt sein müssen, dass sie über die für ihre Aufgabenerfüllung notwendigen Fachkompetenzen und Erfahrungen verfügen. Der Bundesrat wird ermächtigt, diesbezüglich Vorschriften zu machen. Wir machten nun darauf aufmerksam, dass die Mitglieder der Ethikkommissionen neu unbedingt auch über Kenntnisse des Datenschutzrechtes verfügen sollten, damit diesem bei der Projektgestaltung von den Forschenden Rechnung getragen wird.

Zum anderen wird für die Weiterverwendung von biologischem Material und gesundheitsbezogenen Personendaten eine Ausweichklausel («escape clause») geschaffen. Dies bedeutet, dass Forschende in diesem Bereich die allgemeinen Datenschutzgrundsätze der Einholung der Einwilligung der betroffenen Person nach vorgängiger Information über Art und Zweck der Datenbearbeitung nicht mehr beachten müssen. Aus unserer Sicht ist diese Generalermächtigung für Forschende datenschutzrechtlich höchst bedenklich, und der Gesetzesentwurf hat hier die Eigeninteressen dieses Wirtschaftszweiges zu stark berücksichtigt.





### 1.1.6 Vernehmlassungsverfahren zum Bundesgesetz über die Unternehmensidentifikationsnummer

**Anlässlich der verschiedenen Vernehmlassungsverfahren zum Bundesgesetz über die Unternehmensidentifikationsnummer haben wir auf die Möglichkeiten der Überwachung und Persönlichkeitsverletzungen in Verbindung mit der Verwendung einer solchen Nummer (UID) im Bereich Business to Business hingewiesen. Zudem haben wir empfohlen, einerseits ihre Verwendung in diesem Bereich zu verbieten oder zumindest einzuschränken. Andererseits sollte das BFS die UID nur mit der Einwilligung der betroffenen Person im Internet veröffentlichen.**

Wie wir in unserem 16. Tätigkeitsbericht 2008/2009 (Ziff. 1.1.4) bereits erwähnt haben, entspricht die Verwendung der Unternehmensidentifikationsnummer (UID) zur Erleichterung des Informationsaustausches zwischen den Unternehmen und der Verwaltung

(Business to Government – B2G) und innerhalb der Verwaltung (Government to Government – G2G) dem Verhältnismässigkeitsprinzip. Das hat die Prüfung des Entwurfs zum Bundesgesetz über die Unternehmensidentifikationsnummer (UIDG) gezeigt. Hingegen entstehen bei der ergänzenden Verwendung zwischen den verschiedenen Unternehmen (Business to Business – B2B) bedeutend grössere Möglichkeiten für eine Überwachung und Verletzung der Privatsphäre, da die Nummer insbesondere zur Profilierung eingesetzt werden kann. Diesen Risiken wird im Gesetzesentwurf jedoch nicht genügend Rechnung getragen. Unseres Erachtens sollte daher der Einsatz der UID für Anwendungen zwischen den Unternehmen verboten oder zumindest eingeschränkt werden.

Im Hinblick auf die Verwendung der UID nicht nur in den Bereichen B2G und G2G, sondern auch im Bereich B2B, müsste im Gesetz vorgesehen werden, dass der Bundesrat die Grenzen für eine Benutzung in diesem Gebiet festlegt. Überdies sollten die im Bericht über die Ergebnisse des Vernehmlassungsverfahrens erwähnten Einschränkungen (Verbot der missbräuchlichen Verwendung der UID und der Verwendung zu Werbe- oder Marketingzwecken oder Verbot der Übermittlung der UID ins Ausland) auf Ebene der Verordnung wieder aufgegriffen werden.

Die erste Fassung des Entwurfs sah die Veröffentlichung der UID durch das Bundesamt für Statistik (BFS) im Internet vor, mit Ausnahme der Fälle, in denen sich die betroffene Person einer Veröffentlichung widersetzt hat (Opt-out-Prinzip). Im Anschluss an unsere Bemerkungen zu den Veröffentlichungsmodalitäten hat das BFS seinen Gesetzesentwurf in dem Sinne geändert, dass die UID nun nur noch im Internet veröffentlicht werden darf, wenn die betroffene Person ihre Einwilligung dazu erteilt hat (Opt-in-Prinzip). Im Übrigen sind wir der Ansicht, dass die Tragweite der Einwilligung im Sinne von Art. 13 Abs. 1 des vorliegenden Gesetzesentwurfs zu allgemein ist. Unseres Erachtens sollte diese Bestimmung so geändert werden, dass die Einwilligung nur für den konkreten Einzelfall gilt.

## 1.2 Datenschutzfragen allgemein

### 1.2.1 Videoaufnahmen mittels Drohnen

**Auch bei Videoaufnahmen aus Drohnen oder aus anderen Luftfahrzeugen ist der Datenschutz zu beachten, wenn damit bestimmbare Personen aufgenommen werden. Wir haben dazu verschiedene Kriterien aufgestellt, die jeweils im Einzelfall zu überprüfen sind.**

Das Bundesamt für Zivilluftfahrt (BAZL) wollte von uns wissen, welche Datenschutzkriterien bei Videoaufnahmen aus Luftfahrzeugen inklusive Drohnen zu beachten sind. Es ist schwierig, abschliessende allgemeine Kriterien aufzustellen, da jeweils der konkrete Fall zu beurteilen ist. Grundsätzlich konnten wir, in Anlehnung an unser bereits bestehendes Merkblatt «Videoüberwachung durch private Personen» (siehe unsere Webseite www.derbeauftragte.ch, Themen – Datenschutz – Videoüberwachung), folgende Punkte festhalten:

Werden erkennbare Personen aufgenommen, fragt sich zunächst, ob die Bilder durch eine natürliche Person ausschliesslich zum persönlichen Gebrauch bearbeitet und nicht an Aussenstehende (Personen, die nicht zum engeren Privat- und Familienkreis gehören) bekannt gegeben oder irgendwo publiziert werden. Dann ist das DSG nicht anwendbar. Werden die Aufnahmen aber über den eng auszulegenden persönlichen Gebrauch hinaus bearbeitet (bspw. im Internet publiziert), müssen die Personen mit technischen Massnahmen unkenntlich gemacht werden.

Macht also ein Privater Aufnahmen von einer Drohne aus, die nicht ausschliesslich zu seinem persönlichen Gebrauch bestimmt sind, gilt Folgendes: Private Personen, die Personendaten bearbeiten, dürfen die Persönlichkeit der Betroffenen nicht widerrechtlich verletzen. Eine Persönlichkeitsverletzung ist widerrechtlich, wenn sie nicht durch Einwilligung des Verletzten, durch ein überwiegendes privates oder öffentliches Interesse oder durch ein Gesetz gerechtfertigt ist. Es ist kaum davon auszugehen, dass sich Private zur Legitimierung von Aufnahmen aus Luftfahrzeugen auf ein Gesetz stützen können. Sie müssen also die Einwilligung der betroffenen Personen oder ein überwiegendes privates oder öffentliches Interesse aufweisen können.

Weiter hat die private Person die allgemeinen Datenschutzgrundsätze einzuhalten: So dürfen Personendaten nur rechtmässig beschafft werden. Ihre Bearbeitung hat nach Treu und Glauben zu erfolgen und muss verhältnismässig sein. Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist. Die Beschaffung von Personendaten und insbesondere der Zweck ihrer Bearbeitung müssen für

die betroffene Person ersichtlich sein. Ist für die Bearbeitung von Personendaten die Einwilligung der betroffenen Person erforderlich, so ist diese Einwilligung erst gültig, wenn sie nach angemessener Information freiwillig (und bei besonders schützenswerten Personendaten ausdrücklich) erfolgt. Personendaten dürfen 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 gewährleistet. Liegt ein Rechtfertigungsgrund vor und ist keine mildere Massnahme möglich, so sind die Daten so rasch als möglich zu löschen resp. zu anonymisieren.

Wie bereits erwähnt müssen diese Voraussetzungen jeweils im Einzelfall beurteilt werden. Wir verweisen an dieser Stelle auf unser Merkblatt «Videoüberwachung durch private Personen». Es wurde zwar für den Einsatz der Videoüberwachung zu Sicherheitszwecken konzipiert, kann aber hier als Auslegungshilfe beigezogen werden.

Beim Einsatz von Drohnen verbunden mit Videoüberwachung ist zudem datenschutzrechtlich folgendes zu beachten:

- Die Videoüberwachung – mit oder ohne Aufzeichnung – von bestimmbaren Personen darf nur erfolgen, wenn ein Rechtfertigungsgrund vorliegt. In casu kommt, wie erwähnt, als Rechtfertigungsgrund vor allem die Einwilligung der betroffenen Person oder allenfalls ein überwiegendes privates oder öffentliches Interesse in Frage.

  Beispiel 1: Einsatz der Drohnen für Aufnahmen einer archäologischen Ausgrabungsstätte.

  Beispiel 2: Einsatz der Drohnen zu nicht personenbezogenen Zwecken, z.B. in der Planung, und Veröffentlichung der Ergebnisse in einer Form, in der betroffene Personen nicht bestimmbar sind.

- In der BAZL-Bewilligung für solche Aufnahmen sollte möglichst genau aufgeführt werden, für welche Zwecke Videoüberwachung mit oder ohne Aufzeichnung gemacht werden darf. Die Aufnahmen dürfen nur für diese Zwecke benutzt werden (Zweckbindungsprinzip). Dabei versteht es sich von selbst, dass Aufnahmen nur gemacht werden dürfen, wenn diese für die Erreichung der Zwecke nötig und geeignet sind. Kann mit anderen, weniger in die Persönlichkeit eingreifenden Mitteln der gleiche Zweck erreicht werden, ist auf die Aufnahmen zu verzichten (Verhältnismässigkeitsprinzip).

  Beispiel: Bei der Aufnahme einer Baustelle oder einer archäologischen Ausgrabungsstätte darf die Videoüberwachung nur dann bestimmbare Personen

erfassen, wenn diese damit einverstanden sind oder wenn der Einsatz der Drohnen zu nicht personenbezogenen Zwecken erfolgt und die Ergebnisse anonymisiert veröffentlicht werden.

- Videoüberwachung muss generell für die betroffenen Personen erkennbar sein, sei es durch ein Hinweisschild oder durch eine gut sichtbare Kamera (Transparenzprinzip).

  Beispiel: Bei einem Gebäude, das von einer privaten Überwachungsfirma bewacht wird, weist ein Piktogramm auf die Videoüberwachung mittels Drohnen hin.

- Falls die aufgenommenen Bilder mit einer Datensammlung verbunden sind, muss für die betroffene Person ersichtlich sein, bei wem sie das Auskunftsrecht geltend machen kann (Auskunftsrecht).

  Beispiel: Neben einem Piktogramm wird aufgeführt, wer für die Behandlung der Auskunftsgesuche zuständig ist, unter Angabe der Adresse oder einer Telefonnummer.

- Die Personendaten sind durch angemessene technische und organisatorische Massnahmen vor jeglichem unbefugtem Zugriff und Bearbeiten zu schützen (Datensicherheit).

  Beispiel: Der Datenträger mit den Bildern wird in einem verschlossenen Schrank aufbewahrt, der nur befugten Personen zugänglich ist.

- Die Drohnen müssen so eingesetzt werden, dass im Aufnahmefeld der Kamera nur die für den verfolgten Zweck absolut notwendigen Bilder erscheinen (Verhältnismässigkeitsprinzip).

  Beispiel: Bei der Aufnahme einer Baustelle nimmt die Drohne nur Bilder der Baustelle selbst und nicht noch von benachbarten Gebäuden auf.

- Die Aufnahmen mit Personendaten (erkennbaren Personen) dürfen nicht an Dritte bekannt gegeben werden, ausser in durch das Gesetz vorgesehenen oder erlaubten Fällen wie bspw. richterlichen Anfragen (Zweckbindungsprinzip).

  Beispiel: Ein Richter verlangt die Herausgabe von Bildern in einem hängigen Strafverfahren.

- Die Aufnahmen müssen innert kürzester Frist gelöscht oder anonymisiert werden. Die Aufbewahrungsdauer ist dabei vom verfolgten Zweck abhängig; wir gehen jedoch davon aus, dass eine Dauer von höchstens einer Woche in den meisten Fällen genügen sollte.

  Beispiel: Die Aufnahmen der Baustelle werden innerhalb von 24 Stunden anonymisiert.

- Allenfalls sollten die Gesuchssteller auch auf mögliche strafrechtliche Folgen (wie bspw. Hausfriedensbruch) hingewiesen werden.





### 1.2.2 Biometrische Zugangssysteme beim Sportzentrum KSS: Weitere Entwicklung

**Das Bundesverwaltungsgericht erachtet die zentralisierte Speicherung biometrischer Daten im Rahmen der Zutrittskontrolle zu einem Sport- und Freizeitzentrum für die betroffenen Personen als eine unverhältnismässige Persönlichkeitsverletzung.**

Nachdem sich das Sportzentrum KSS in Schaffhausen geweigert hatte, unsere Empfehlungen betreffend die Dezentralisierung der biometrischen Daten (match on card) zu befolgen (vgl. unseren 16. Tätigkeitsbericht 2008/2009, Ziff. 1.2.4), zogen wir den Fall vor das Bundesverwaltungsgericht (BVGer).

In seinem Urteil vom 4. August 2009 (A-3908/2008) hat das BVGer unsere Klage gutgeheissen und mehrere Klarstellungen betreffend die Fragen des Datenschutzes beim Einsatz von biometrischen Erkennungssystemen vorgenommen. Es machte insbesondere deutlich, dass extrahierte Daten (Templates), in diesem Fall digitalisierte Rohdaten des Fingerabdrucks, Personendaten im Sinne des DSG darstellen und dass die betroffenen Personen, wenn ihre Daten in einer zentralen Datenbank gespeichert werden, die Kontrolle über deren mögliche Verwendung völlig verlieren.

Demgemäss gelangt das BVGer zum Schluss, dass die Speicherung der biometrischen Daten in einer zentralisierten Datenbank im Rahmen der Zugangskontrolle zu einem Sport- und Freizeitzentrum für die betroffenen Personen eine unverhältnismässige Persönlichkeitsverletzung bedeutet. Zudem betont das Gericht, dass die Persönlichkeitsverletzung weder durch die Einwilligung der betroffenen Personen (da diese nicht angemessen informiert sind und ihre Einwilligung nicht Ausdruck ihres freien Willens ist), noch durch ein überwiegendes privates Interesse gerechtfertigt sei. Im Übrigen erachtet das BVGer die von uns vorgeschlagene technische Lösung, also ein dezentrales

Match-on-card-System, als geeignet, wobei es die Möglichkeit anderer technischer Lösungen offen lässt, soweit diese den Datenschutzanforderungen gerecht werden. Schliesslich erinnert das Gericht daran, dass es dem Sportzentrum KSS frei stehe, selber von der Verwendung eines biometrischen Systems abzusehen.

Der Weiterzug befindet sich im Anhang Ziff. 4.1.8 und kann auf unserer Webseite www.derbeauftragte.ch, unter Dokumentation – Datenschutz – Weiterzüge, abgerufen werden.

### 1.2.3 Augenschein zur Einrichtung eines Systems der Zugangskontrolle in einem Skigebiet

**Zugangskontrollsysteme in Skigebieten müssen DSG-konform sein. Dem Verhältnismässigkeitsprinzip entsprechend darf der Bildschirm, auf dem die Personendaten der Abonnenten zu sehen sind, für die anderen Wintersportler nicht sichtbar sein. Nur das Personal, das die Gültigkeit der Fahrkarten kontrolliert, soll das Gerät im Blick haben. Aufgrund der Beschwerde einer betroffenen Person haben wir beim Betreiber einer Wintersportanlage interveniert. Er hat unsere Anregung, den Monitor entsprechend zu drehen, akzeptiert.**





Wir haben an dieser Stelle bereits früher (vgl. unseren 14. Tätigkeitsbericht 2006/2007, Ziff. 1.2.8) aufgezeigt, dass die Zutrittskontrollsysteme in den Skigebieten die Anforderungen des Datenschutzgesetzes genügen müssen. Gemäss dem Verhältnismässigkeitsprinzip dürfen nur diejenigen Personen, die mit der Überprüfung der Abonnemente betraut sind, von den darin enthaltenen Personendaten Kenntnis nehmen. Die öffentliche Anzeige der Fotografie, des Namens und Vornamens oder auch des Geburtsdatums der Abonnementsinhaber widerspricht den Grundsätzen des Datenschutzes. Der Bildschirm, auf dem die Daten erscheinen, darf sich daher nicht im Blickfeld von Drittpersonen, in diesem Fall der übrigen Wintersportler, befinden.

Auf die Beschwerde einer Privatperson hin haben wir im Rahmen unserer Aufsichtspflichten Kontakt mit den Betreibern des betreffenden Skigebiets aufgenommen. Wir erklärten ihnen die Rechtslage in dem Bereich und ersuchten sie, Stellung zu nehmen und uns die für die nächste Skisaison getroffenen Massnahmen mitzuteilen. Die Verantwortlichen nahmen unsere Aufforderung positiv auf und erklärten, sie würden die notwendigen Massnahmen treffen, um die Privatsphäre ihrer Kunden zu achten. Zu Beginn der Wintersaison liessen uns die Verantwortlichen des Skigebiets indes wissen, dass sie darauf verzichtet hätten, den Monitor in Betrieb zu nehmen, und luden uns zu einer Prüfung des Systems vor Ort ein. Im Februar 2009 kamen wir dieser Einla-

dung nach. Bei der Besichtigung konnten wir feststellen, dass der (ausgeschaltete) Monitor zur Warteschlange hin ausgerichtet und daher für die übrigen Personen direkt einsehbar war. Wir stimmten dem Vorschlag zu, den Monitor in Richtung der Seilbahnkabinen zu drehen, so dass die bei den Kabinen befindlichen Mitarbeiter die Identität der Abonnementsinhaber überprüfen können (namentlich wenn sich niemand in der Kontrollkabine aufhält). Die übrigen Benutzer hätten dann zwar die Möglichkeit, den Kontrollbildschirm im Vorübergehen wahrzunehmen, was aber nur eine minimale Persönlichkeitsverletzung darstellt und daher vertretbar erscheint.

Im Anschluss an unseren Augenschein wandten wir uns mit einem Schreiben an die Firma Skidata AG, die Lieferantin des Zugangssystems, um sie auf diese Problematik aufmerksam zu machen. Sie teilte uns mit, dass sie im Rahmen ihrer Beratertätigkeiten ihre Kunden über die Rechtslage in diesem Bereich informieren werde.

### 1.2.4 Überwachungstätigkeiten der Gesellschaft Securitas AG

**Zu den Überwachungstätigkeiten der Gesellschaft Securitas AG haben wir im Rahmen unserer Kontrollkompetenzen Ermittlungen durchgeführt, insbesondere im Zusammenhang mit der im Auftrag der Firma Nestlé AG erfolgten Überwachung der Gruppe Attac und den angeblich auf die Lausanner «Groupe anti-répression» ausgerichteten Tätigkeiten. Da wir nicht über Zwangsmittel verfügen, wie Zivil- oder Strafrichter sie einsetzen können, konzentrierten wir uns auf die im Datenschutzgesetz verankerte Verpflichtung zur Anmeldung von Datensammlungen. Es hat sich überdies gezeigt, dass es für diese Art der Informationsbeschaffung Gesetzesnormen braucht.**

Im Juni 2008 ersuchte uns der Anwalt der Gruppe Attac, im Falle der im Auftrag der Firma Nestlé AG durchgeführten Überwachung der Gruppe durch die Gesellschaft Securitas AG einzuschreiten. Zur Ermittlung des Sachverhalts richteten wir Fragen an die Gesellschaften Securitas und Nestlé bezüglich der im Rahmen dieser Überwachung erfolgten Bearbeitung von Personendaten. Unsere Anfrage betraf namentlich die Rechtfertigungsgründe, die Beschaffung von Daten betreffend die Mitglieder von Attac, die Bearbeitung dieser Daten bei den Firmen Securitas und Nestlé, und die Aufbewahrung und die Bekanntgabe der fraglichen Daten. Nachdem wir festgestellt hatten, dass die beiden Gesellschaften keine Datensammlung bei unserer Behörde angemeldet hatten, forderten wir sie zudem auf, dies gegebenenfalls nachzuholen. Der Anwalt von Attac behauptete, Securitas und Nestlé hätten die Informationspflicht gegenüber den betroffenen Personen beim Beschaffen von sensiblen Personendaten oder Persönlichkeitsprofilen und die Pflicht zur Anmeldung der Datensammlungen

verletzt. Den von Nestlé und Securitas vorgelegten Schriftstücken zufolge wurde die Beschaffung von Personendaten betreffend Attac Ende des Jahres 2004 eingestellt. Aus den Schlussfolgerungen des waadtländischen kantonalen Untersuchungsrichters geht hervor, dass diese Datenbeschaffung Ende 2005 eingestellt wurde. Da die Informationspflicht gegenüber den betroffenen Personen im Falle einer Beschaffung von besonders schützenswerten Personendaten oder von Persönlichkeitsprofilen erst seit dem 1. Januar 2008 in Kraft ist, konnten Nestlé und Securitas bei der Datenbeschaffung betreffend Attac gar nicht gegen diese Pflicht verstossen haben.

Im August 2008 ersuchte uns die Lausanner «Groupe anti-répression» (AntiRep), zu überprüfen, ob die Datenbearbeitungen im Zusammenhang mit der Überwachung durch die Securitas im Einklang mit der eidgenössischen Datenschutzgesetzgebung seien. In Beantwortung unserer Anfragen teilte uns die Securitas mit, dass sie keine Daten betreffend die AntiRep bearbeitet habe. Wir haben diese Behauptungen zur Kenntnis genommen, da wir nicht wie Zivil- und Strafrichter Zwangsmittel einsetzen können (zum Beispiel die Beschlagnahme). Das DSG begrenzt nämlich die Ermittlungsbefugnis des EDÖB klar. Damit hat sich der Gesetzgeber dafür entschieden, ein zivil- oder strafrechtliches Vorgehen vor allem den betroffenen Personen zu überlassen.

Was die Pflicht zur Anmeldung der Datensammlungen bei unserer Behörde anbelangt, so teilte uns die Firma Nestlé mit, dass sie einen Datenschutzberater eingesetzt habe; damit hat sie sich der Meldepflicht betreffend ihre Datensammlungen entledigt. Securitas liess uns wissen, dass sie über keine gemäss dem DSG anmeldepflichtige Datensammlung verfüge. Diese Angabe muss noch überprüft werden.

Die Untersuchung der Fälle Attac und AntiRep hat darüber hinaus die Notwendigkeit aufgezeigt, Normen zur Regelung von Tätigkeiten auszuarbeiten, die von Privatunternehmen zum Zwecke der Informationsbeschaffung verfolgt werden (z. B. Auskunfteien und Überwachungsgesellschaften, Detektivagenturen).

### 1.2.5 Stellungnahme zum geplanten Strassenverkehrsunfallregister (Via sicura)

**Zum neu geplanten Strassenverkehrsunfallregister, bestehend aus einem Erfassungs- sowie einem Auswertungsregister, haben wir Stellung genommen. Da darin auch besonders schützenswerte Personendaten bearbeitet werden sollen, muss ein formelles Gesetz die Datenbearbeitung vorsehen.**

Im Rahmen der Ämterkonsultation nahmen wir zur neuen Verordnung über das Strassenverkehrsunfallregister Stellung. Sie soll eine einheitlichere Erfassung (mittels Erfas-

sungsregister) und die zentrale Auswertung (mittels Auswertungsregister) von Strassenverkehrsunfällen ermöglichen. Zudem soll das Auswertungsregister mit anderen Informationssystemen des Bundesamtes für Strassen (ASTRA) verknüpft werden. In unserer Stellungnahme wiesen wir insbesondere darauf hin, dass eine Regelung des Strassenverkehrsunfallregisters auf Verordnungsstufe nicht genüge, da in seinem Rahmen auch besonders schützenswerte Personendaten bearbeitet werden sollen. Aus diesem Grund müsse ein Gesetz im formellen Sinn die Datenbearbeitung vorsehen.

Weiter wiesen wir darauf hin, dass in der Verordnung Pseudonymisierung und Anonymisierung durcheinander gebracht worden waren. Dazu hielten wir fest, dass auch pseudonymisierte Daten – im Gegensatz zu anonymisierten Daten – Personendaten im Sinn des Datenschutzgesetzes sind. Eine Möglichkeit, pseudonymisierte Daten zu anonymisieren, ist die Verwendung der so genannten Hashfunktion. Da dieser Prozess nicht (oder nur mit unverhältnismässigem Aufwand) umkehrbar ist, ist ein Rückschluss auf das Pseudonym und somit auf die betroffene Person praktisch ausgeschlossen.

Wir nahmen an einer Sitzung des ASTRA zur Besprechung der fehlenden gesetzlichen Grundlage teil. Da die formellgesetzlichen Grundlagen für das Strassenverkehrsunfallregister im Rahmen der geplanten Revision des Strassenverkehrsgesetzes (Via-sicura-Vorlage) eingeführt werden sollen, musste vor allem eine Übergangslösung für rund drei Jahre resp. bis zur Inkraftsetzung der Revision gefunden werden. Anlässlich der erwähnten Sitzung wurden verschiedene Lösungsmöglichkeiten besprochen. Erfreulich war es für uns zu sehen, dass es dem ASTRA ein Anliegen ist, eine datenschutzkonforme Lösung zu finden.





### 1.2.6 Pranger für Raser?

**Mit Bestimmtheit ist es nicht das Anliegen des Datenschutzes, verantwortungslose Raser zu schützen. Wir bezweifeln jedoch, dass der Pranger ein taugliches Mittel zur Abschreckung darstellt. Die Polizeihoheit in Sachen Ahndung von Verkehrsdelikten liegt bei den Kantonen. Mithin sind daher auch die kantonalen Datenschützer zu gemeinsam abgestimmtem Handeln aufgerufen.**

Wiederholt wurde in den letzten Jahren der Ruf laut, die Veröffentlichung von persönlichen Daten unverbesserlicher Raser zwecks Abschreckung (Prävention) solle erlaubt werden. Es war selbstredend nie unser Ziel, Raser aus datenschutzrechtlichen Gründen schonen zu wollen. Es ist verständlich, dass man sich von solch gewissenlosen Verkehrsteilnehmern bedroht fühlt und dass nach tragischen Unfällen Unmut aufkommt. Es gilt allerdings unseres Erachtens zu bedenken, dass oberstes Ziel von

Massnahmen gegen die Raserei die Verhinderung solcher Unfälle und der Gefährdung von Unbeteiligten sein muss. Dabei muss das Prinzip der Zweck- und Verhältnismässigkeit gewahrt bleiben. Wie wir in den Medien eingehend erörtert haben, ist es zwar legitim, die Daten von Rasern (beispielsweise im Internet) zu Fahndungszwecken zu veröffentlichen. Das Gleiche gilt für Hooligans und Schläger. Der Pranger als Mittel zur Abschreckung ist aber eigentlich ein mittelalterliches Konzept und seine Wiedereinführung im 21. Jahrhundert bestenfalls heikel. Zunächst geht es bei Veröffentlichungen stets um die Frage der Rechtsgleichheit. Stellt man nämlich Raser an den Pranger, so muss man sich umgehend fragen, wieso man dasselbe nicht auch mit allen andern Straftätern tut. Wieso sollten bspw. nicht auch persönliche Daten von allen Autofahrerinnen und -fahrern veröffentlicht werden, die schon einmal wegen Trunkenheit am Steuer belangt wurden und ebenfalls Menschen gefährdet oder auf dem Gewissen haben?

Wir bezweifeln aber auch, ob der Pranger überhaupt präventive Wirkung entfaltet. Unter Umständen kann er sein Ziel verfehlen, ja sogar genau das Gegenteil bewirken, wenn Raser eine allfällige Publikation im Internet als Trophäe herumreichen. Wir verweisen in diesem Zusammenhang auf den Umstand, dass nicht wenige Raser ihre Taten selber aufs Internet stellen und auf diese Weise sogar schon als Übeltäter identifiziert werden konnten. Solche Beispiele zeigen deutlich, dass ein Pranger tatsächlich zur Rangliste mutieren kann. Bedeutend wirksamer wäre demgegenüber, lernunfähigen Rasern ihr Auto definitiv und den Führerausweis für sehr lange Zeit wegzunehmen. Ebenso sollten Dritte hart bestraft werden können, wenn sie wissentlich einem Raser ihr Fahrzeug zur Verfügung stellen. Die Polizeihoheit in Sachen Ahndung von Verkehrsdelikten liegt aber bei den Kantonen. Die kantonalen Datenschützer sind daher zum gemeinsamen Handeln aufgerufen.



### 1.2.7 Revision des Sportgesetzes

**Im Rahmen der Totalrevision des Bundesgesetzes über die Förderung von Turnen und Sport haben wir zwei gesetzliche Grundlagen angeregt, die eine Basis für Dopingkontrollen schaffen und den Datenaustausch zwischen verschiedenen Dopingbekämpfungsstellen erleichtern sollen. Unsere Vorschläge wurden gutgeheissen und in das Gesetz integriert. Das revidierte Gesetz erhöht die Rechtssicherheit für Sportlerinnen und Sportler im Bereich der Dopingbekämpfung.**

Bis jetzt erfolgten Dopingkontrollen bei Sportlern auf einer mehr oder weniger freiwilligen Basis. Sportveranstalter und Dopingbekämpfungsstellen konnten nur Kontrollen durchführen, wenn der Athlet vorgängig zugestimmt hatte. Da allerdings ein Sportler

von einem Wettbewerb ausgeschlossen werden kann, wenn er vorab keine Antidopingerklärung abgibt, konnte in diesem Zusammenhang kaum von einer freiwilligen Einwilligung im Sinne des DSG die Rede sein. Aus diesem Grund haben wir die Schaffung einer gesetzlichen Grundlage angeregt, welche es anerkannten Antidopingstellen erlaubt, Dopingkontrollen durchzuführen.

Da Dopingkontrollen im Spitzensport international koordiniert und, insbesondere im Falle von Missbräuchen, Daten international ausgetauscht werden müssen, bedurfte es einer gesetzlichen Regelung, die auch einen solchen Datentransfer reguliert. Vor diesem Hintergrund haben wir ein Gesetz vorgeschlagen, das einen internationalen Datenaustausch mit anerkannten Dopingbekämpfungsstellen (wie z.B. der World Anti-Doping Agency) unter Berücksichtigung der Bestimmungen des DSG ermöglicht.

### 1.2.8 Datenschutz und Doping

Die World Anti-Doping Agency (WADA) hat 2009 einen «International Standard for the Protection of Privacy» verabschiedet. Damit wird das Datenschutzniveau innerhalb der WADA und den angeschlossenen Verbänden erhöht. Allerdings sind diese Bestimmungen nicht darauf ausgelegt, ein angemessenes Datenschutzniveau gemäss DSG zu etablieren. Wir haben die WADA darauf hingewiesen, dass aus diesem Grund nach DSG weiterhin Massnahmen zu treffen sind, bevor Personendaten aus der Schweiz an die WADA weitergegeben werden.

### 1.2.9 Befreiung von der Gebührenpflicht für Radio und Fernsehen

**Gemäss Radio- und Fernsehverordnung können AHV- und IV-Bezüger unter gewissen Voraussetzungen eine Befreiung von der Gebührenpflicht verlangen. In diesem Rahmen sind sie verpflichtet, der Billag einen entsprechenden Nachweis zu erbringen. Im Rahmen unserer Aufsichtstätigkeit haben wir festgestellt, dass die Praxis der Firma und insbesondere das Anmeldeformular missverständlich waren. Betroffene Personen übermittelten der Billag tendenziell Daten, welche diese gar nicht benötigte. Wir haben daraufhin mit der Firma eine datenschutzkonforme Lösung erarbeitet.**

Die Radio- und Fernsehverordnung (RTVV) erlaubt der Billag, zur Beurteilung, ob eine Person von der Gebührenpflicht befreit werden kann, die notwendigen Informationen von dieser anzufordern. Weitergehende Auskünfte (insbesondere Informationen über die Höhe der bezogenen AHV-Zahlungen) dürfen von der Billag nicht eingefordert werden. Daher reicht es in der Regel aus, wenn die Bezüger von der AHV-Kasse eine

entsprechende Bescheinigung verlangen und diese der Billag einreichen. Uns wurde allerdings ein Fall bekannt, in welchem eine Billag-Mitarbeiterin eine Kopie des rechtskräftigen Entscheids über den Anspruch auf Ergänzungsleistungen verlangt hat. Darauf haben wir bei der Billag interveniert. Nach deren Aussagen handelte es sich um das einmalige Versehen einer Mitarbeiterin. Doch mussten wir feststellen, dass das Anmeldeformular dahingehend missverständlich war, als es die Antragsteller dazu aufforderte, den rechtskräftigen Entscheid anstatt einer einfachen Bescheinigung einzureichen. Die Billag hat uns gegenüber zugesagt, das Formular entsprechend anzupassen.





### 1.2.10 Grenzüberschreitende Amtshilfe und Art. 6 DSG

**Das Datenschutzgesetz ist auch bei der grenzüberschreitenden Amtshilfe zu beachten. Zuerst ist jeweils zu prüfen, ob die Amtshilfe in einem Spezialgesetz geregelt ist. Sodann darf bei der Bekanntgabe der Daten in ein anderes Land die Persönlichkeit der betroffenen Personen nicht schwerwiegend gefährdet werden, namentlich weil eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet. In einem solchen Fall ist für ausreichende Garantien zu sorgen. Dies kann mittels Datenschutzklausel in einem Abkommen oder allenfalls in einer Erklärung geschehen.**

Wir haben an der interdepartementalen Arbeitsgruppe zum Thema «grenzüberschreitende Amtshilfe» teilgenommen. Datenschutzrechtlich stellte sich dabei vor allem die Frage, wie sich Art. 6 DSG zur grenzüberschreitenden Datenbekanntgabe auf die internationale Amtshilfe auswirkt. Aus diesem Grund haben wir für die Arbeitsgruppe das Thema «Sonderfall DSG – Art. 6 DSG und grenzüberschreitende Amtshilfe» näher ausgeleuchtet. Dabei hielten wir Folgendes fest:

Als Querschnittgesetz ist das DSG auch bei der grenzüberschreitenden Amtshilfe zu beachten. Allgemein gilt, dass Bundesorgane Personendaten grundsätzlich nur bekannt geben dürfen, wenn dafür hinreichende Rechtsgrundlagen bestehen. Die Bekanntgabe von besonders schützenswerten Personendaten setzt eine formellgesetzliche Grundlage voraus. Somit ist für den jeweiligen Bereich als erstes zu prüfen, ob spezialgesetzliche Amtshilfebestimmungen vorliegen. Der Vollständigkeit halber ist darauf hinzuweisen, dass das Abrufverfahren kein Fall von Amtshilfe darstellt. Dafür braucht es immer eine Rechtsgrundlage.

Wird die Amtshilfe in einem Spezialgesetz geregelt, ist von Fall zu Fall zu prüfen, in welchem Verhältnis diese Bestimmungen zu den Anordnungen des DSG stehen. Das

Bundesgericht selbst hat in einem Fall betreffend das Börsengesetz festgehalten, es könne nicht generell gesagt werden, das DSG sei auf die Amtshilfe – analog der Ausnahme für die Rechtshilfe nach Art. 2 Abs. 2 DSG – zum Vornherein nicht anwendbar. Würde dieser Ausnahmekatalog über seinen Wortlaut hinaus nach den Grundsätzen «lex specialis derogat legi generali» bzw. «lex posterior derogat legi priori» leichthin ausgedehnt, verlöre der Datenschutz relativ schnell seine Natur als Querschnittmaterie mit einheitlichen Grundsätzen und allgemeinen Prinzipien. Der Gesetzgeber könne aber gewissen im DSG vorgesehenen Prinzipien, Grundsätzen oder Ansprüchen bereits beim Erlass der spezialgesetzlichen Regelung derart Rechnung tragen, dass einzelnen Bestimmungen des DSG daneben (materiell) keine eigenständige Bedeutung mehr zukomme. Falls dies zutreffen würde, könne das DSG allgemein subsidiär als Massstab für die Handhabung des bei der spezialgesetzlichen Amtshilfebestimmung zustehenden Ermessens dienen. Das gelte insbesondere für die allgemeinen Datenschutzgrundsätze. Spezialgesetzliche Bestimmungen sind somit grundsätzlich parallel zum DSG zu beachten (vgl. BGE 126 II 126, resp. 2A.355/1999). Mit anderen Worten gilt das DSG grundsätzlich auch, wenn spezialgesetzliche Amtshilfebestimmungen vorliegen.

Fehlen dagegen spezialgesetzliche Amtshilfebestimmungen, ist zu prüfen, ob die im DSG vorgesehenen Voraussetzungen für eine ausnahmsweise Datenbekanntgabe ohne Vorliegen einer spezialgesetzlichen Grundlage erfüllt sind. Bei dieser Prüfung ist aber ein strenger Massstab anzulegen. In jedem Fall gelten auch hier im Weiteren die allgemeinen Datenschutzgrundsätze (wie bspw. das Rechtsmässigkeits-, das Verhältnismässigkeits- oder das Zweckbindungsprinzip).

Unabhängig davon, ob die Amtshilfe spezialgesetzlich geregelt ist oder nicht, ist bei der grenzüberschreitenden Amtshilfe Art. 6 DSG wie folgt zu beachten: Das DSG hält fest, dass Personendaten nicht ins Ausland bekannt gegeben werden dürfen, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, namentlich weil eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet. Mit anderen Worten hat der Inhaber einer Datensammlung zu prüfen, ob die im Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung von Personendaten (STE 108) und im Zusatzprotokoll zu diesem Übereinkommen bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung aufgestellten Grundsätze beachtet werden. Im Weiteren muss der Inhaber der Datensammlung auch sicherstellen, dass die Grundsätze des DSG eingehalten werden (dass also die betroffene Person bei Nichteinhaltung dieser Grundsätze ihre Interessen wahren kann, dass das Auskunftsrecht gewährleistet wird, und dass ein unabhängiges Aufsichtsorgan besteht). Die ganze vorgenannte Prüfung der Angemessenheit kann aber auch aufgrund der (nicht abschliessenden) Staatenliste auf unserer Webseite geprüft werden. Werden Daten in ein Land bekannt gegeben, das gemäss der Staaten-

liste über einen angemessenen Datenschutz verfügt, gilt Art. 6 DSG grundsätzlich als erfüllt (selbstverständlich ausser wenn im konkreten Fall ernsthafte Hinweise auf eine Verletzung des Datenschutzes hindeuten). Weiter ist zu beachten, dass in bestimmten Staaten die Datenschutzgesetzgebung – im Gegensatz zum schweizerischen DSG – für juristische Personen nicht gilt, weshalb bei der Bekanntgabe von Daten betreffend juristische Personen Art. 6 DSG ebenfalls nicht erfüllt wäre.

Falls eine angemessene Datenschutzgesetzgebung fehlt, ist auf anderem Weg für ausreichende Garantien zu sorgen. Bei der grenzüberschreitenden Amtshilfe können diese Garantien mittels Datenschutzklausel in einem Abkommen oder allenfalls in einer separaten Erklärung vereinbart werden. Bei der Bekanntgabe von besonders schützenswerten Personendaten muss der Staatsvertrag von der Bundesversammlung genehmigt werden (formelle Rechtsgrundlage). Die Datenschutzklausel muss jeweils an das Spezialgebiet angepasst werden und bestimmte Punkte enthalten. Auf unserer Website finden sich als Beispiele die Standardvertragsklauseln der EU und der Mustervertrag des Europarats.

Falls weder eine angemessene Datenschutzgesetzgebung noch eine Datenschutzklausel vorliegen, kann zuletzt geprüft werden, ob nicht eine weitere gesetzlich vorgesehene Ausnahme vorliegt. Allerdings sind diese Ausnahmen sehr restriktiv zu handhaben.



### 1.2.11 Datenschutz und RFID

**Die meisten Bürger kennen die RFID-Technologie (Radio Frequency Identification) aus den Geschäften, in denen Schreib- und Lesegeräte bei der Kasse aufgestellt sind. Befindet sich ein nicht deaktivierter RFID-Chip noch an oder in einem Produkt, löst das Lesegerät beim Vorbeigehen einen Alarm aus. Solche Chips befinden sich zunehmend an Waren, aber auch in Bahnbilletten, in Bibliotheksbüchern, in Wegfahrsperren von Autos und bei der Fluggepäcksteuerung. Bei der RFID-Technologie besteht insbesondere das Risiko, dass Daten bearbeitet werden können, ohne dass die Betroffenen dies erkennen.**

Wir haben in einem Referat an der ETH in Zürich das Thema «Datenschutz und RFID» erläutert. Anfang des Jahrzehnts wurde vermehrt von dieser neuen Technologie gesprochen. Wir waren damals nicht sicher, inwiefern sie durch das DSG abgedeckt ist, und beschlossen deshalb, sie zu analysieren. Die Analyse brachte folgende Erkenntnisse: Die RFID-Technologie ist nicht so neu, wie man dies eigentlich aufgrund der

ersten Informationen erwartet hätte. Sie wurde bereits Ende des zweiten Weltkriegs zur Freund-/Feind-Erkennung eingesetzt. RFID kann organisatorisch gesehen als ein «neues» Sachmittel mit speziellen Eigenschaften in einem System, bspw. einer Anwendung, betrachtet werden. Es hat besondere Eigenschaften, welche den Datenschutz beeinträchtigen können.

Ein grundsätzliches Risiko besteht darin, dass die Daten in einem Transponder oder «tag» (RFID-Chip) innert einer gewissen Distanz mit Funkwellen bearbeitet werden können. Dabei ist weder eine Sichtverbindung notwendig, noch müssen die Betroffenen aktiv in den Prozess eingreifen. Mit anderen Worten heisst dies, dass die Datenbearbeitung ohne Wissen der Betroffenen stattfinden kann. Alle Daten, die auf RFID-tags gespeichert sind und nicht zerstört, gelöscht oder speziell geschützt werden, lassen sich durch (versteckte) Lese- und Schreibgeräte lesen oder manipulieren. Werden diese mit Daten aus anderen Quellen vernetzt, besteht das Risiko, dass Einkaufs- oder Bewegungsprofile erstellt werden.

Die RFID-tags sind meist in einem System verknüpft mit Netzwerken, Arbeitsplatzgeräten, Servern und weiteren Elementen, so dass man bei der Planung einer datenschutzkonformen RFID-Anwendung (von der Erhebung der Daten bis zu deren Anonymisierung oder Löschung) auch diese betrachten muss. Dabei gilt es, die folgenden wichtigen Vorgaben des Datenschutzes in das zu konstruierende System einfliessen zu lassen:

- Transparenz: Der Einsatz von RFID-Technologie muss für die betroffene Person erkennbar sein. So kann jede Person bei letzterem ihr Auskunftsrecht geltend machen, und wer ein schutzwürdiges Interesse hat, kann verlangen, dass er die Daten korrigiert, sperrt oder löscht oder einen Vermerk anbringt. Der Inhaber der Datensammlung muss das System angemessen dokumentieren. Je sensitiver die bearbeiteten Personendaten oder der Zweck der Datenbearbeitung, umso detaillierter sollte die Dokumentation sein. Ohne sie besteht keine Transparenz und ist – neben mangelnder Steuerbarkeit solcher Systeme – die Datenschutzkonformität nicht gegeben.
- Zweckbindung: Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist.
- Verhältnismässigkeit: Die Systeme sind so zu gestalten, dass man für die Aufgabenerfüllung möglichst wenige Personendaten benötigt. Wenn möglich sollen anonymisierte Daten verwendet werden; wenn kein Personenbezug mehr

vorhanden ist, ist das DSG nicht mehr anwendbar. Sofern es in einzelnen Fällen eine Identifikation der Personen braucht, sind die Systeme so zu gestalten, dass man mit Pseudonymen arbeiten kann. Im Weiteren sind all jene Daten zu löschen, die für den Zweck der Datenbearbeitung nicht mehr notwendig sind.

- Rechtmässigkeit: Die Datenbearbeitung darf kein Recht verletzen, also weder das DSG noch andere Gesetze oder Verordnungen. Private Personen dürfen Personendaten bearbeiten, wenn sie einen Rechtfertigungsgrund haben. Dies kann eine Rechtsgrundlage, eine Einwilligung des Betroffenen oder ein überwiegendes öffentliches oder privates Interesse sein.
- Einwilligung: Ist für die Bearbeitung von Personendaten die Einwilligung der betroffenen Personen erforderlich, so ist diese erst gültig, wenn sie nach angemessener Information freiwillig erfolgt. Dies bedeutet unter anderem, dass man dem Betroffenen mitteilen muss, welche Daten man wo und wie bearbeitet und wann sie gelöscht werden. Im Weiteren muss bei der Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen die Einwilligung ausdrücklich erfolgen. Dies kann mündlich oder schriftlich geschehen. Weil eine mündliche Zustimmung meist schwierig zu beweisen ist, empfehlen wir normalerweise, die ausdrückliche Einwilligung schriftlich einzuholen. Im Weiteren hat der Betroffene das Recht, seine Einwilligung für die Datenbearbeitung jederzeit zu widerrufen.
- Datensicherheit: Personendaten sind insbesondere gegen unbefugte Datenbearbeitung und technische Fehler mit Hilfe angemessener technischer und organisatorischer Massnahmen zu schützen. Insbesondere Systeme, welche besonders schützenswerte Personendaten oder Persönlichkeitsprofile bearbeiten oder sensitiven Zwecken dienen, gilt es, dem Stand der Technik entsprechend zu schützen. Es ist dafür zu sorgen, dass insbesondere die Vertraulichkeit, Verfügbarkeit und Integrität der Daten gewährleistet ist.
- Kontrolle: Kontrollen schaffen Vertrauen. Diese Kontrollen können sowohl durch interne Mitarbeiter als auch durch externe Auftragnehmer wahrgenommen werden. Um den Datenschutz und die Daten- oder Informationssicherheit zu verbessern, sind künftig unabhängige Zertifizierungsorgane vorgesehen, welche die jeweiligen Systeme beurteilen werden.

### 1.2.12 Schutz von sensitiven Daten auf Speichersystemen

**Verschlüsselungsverfahren sind gute Vorkehrungen, um sensitive Daten auf Speichersystemen wie Festplatten oder USB-Sticks zu schützen. Es ist dabei aber zu berücksichtigen, dass Betriebssysteme bzw. Anwendungen die sensitiven Daten (oder Teile davon) auch in anderen Dateien wie etwa Swap- und Temporärdateien ablegen. Diese müssen ebenfalls geschützt werden. Der Zugriff auf verschlüsselte Daten erfolgt meist nur über ein Passwort, weshalb es möglichst sicher sein muss. Auf dem Markt sind heute einige Verschlüsselungstools erhältlich. Wir haben die beiden Programme Rohos Mini Drive und TrueCrypt auf ihre Anwendbarkeit hin untersucht.**

Sensitive Daten auf elektronischen Speichersystemen sollten verschlüsselt werden. Verliert oder vergisst man bspw. einen Laptop, der ausgeschaltet oder gesperrt ist, so wird es für einen nicht Zugriffsberechtigten schwierig oder gar unmöglich, die Daten zu entschlüsseln. Dasselbe gilt auch für verloren gegangene USB-Speicher-Sticks.

Die heute teilweise für den persönlichen Gebrauch gratis verfügbaren und aus dem Internet herunterladbaren Verschlüsselungstools verwenden Chiffrieralgorithmen wie bspw. den AES256, welcher dem Stand der Technik entspricht. Dieser und viele andere Algorithmen wurden veröffentlicht, so dass sie unter anderem auch von unabhängigen Stellen auf ihre Sicherheit überprüft werden konnten. Bei Verschlüsselungssystemen ist aber das gesamte Verfahren zu betrachten, von der Verschlüsselung der ursprünglich im Klartext vorhandenen Daten bis zu ihrer Entschlüsselung (gesamthafte Implementierung der Sicherheitsvorkehrungen ins System). Im Weiteren gilt es zu beachten, dass Betriebssysteme und Anwendungen Daten bspw. in Auslagerungsdateien wie swapfile bzw. pagefile.sys ablegen, die von einem möglichen Angreifer bei unzureichendem Schutz eingesehen werden können. Aufgrund unserer heutigen Kenntnisse gibt es die folgenden Möglichkeiten, diese Auslagerungsdateien zu «sichern»:

- Man löscht die Datei und sorgt dafür, dass der Arbeitsspeicher (RAM) entsprechend gross ausgelegt ist, so dass ein Auslagern (swapping) gar nicht mehr notwendig ist; oder
- man löscht den Inhalt der Auslagerungsdatei beim Herunterfahren des Computers physisch.

Weiter ist es wichtig, den Offlinedateien-Cache (Offline-Datenbank) zu verschlüsseln, da sonst alle vom Netzwerk zwischengespeicherten Daten auf dem Computer unkodiert vorhanden sind. Der Computer erstellt aufgrund der eingesetzten Anwendungen

noch andere Dateien, die allenfalls sensitive Informationen beinhalten können, wie bspw. temporäre (Internet-)Dateien. Diese sollten nach der Bearbeitung gelöscht werden, insbesondere in einem Internetcafé. Hier könnten auch auf einfache Weise Keylogger eingesetzt werden, mit denen sich Passwörter ausspähen lassen, ohne dass dies der Benutzer bemerkt. Beim eigenen Computer ist es ratsam, die Löschung sensitiver Informationen beim Ausschalten des Geräts automatisiert durchzuführen, so dass beim Neustart keine «alten» Daten mehr vorhanden sind. Eine andere Lösungsmöglichkeit besteht darin, die gesamte Systempartition zu verschlüsseln, so dass alle Dateien wie bspw. Swap- und Tempdateien kodiert gespeichert sind und von Unberechtigten nicht eingesehen werden können. Zwar belastet dies den Rechner stärker, dafür erübrigt sich aber die Löschung der diversen (Temp-)Dateien.

In vielen Fällen erfolgt der Zugriff auf die verschlüsselten Daten bzw. auf das Verschlüsselungstool mit Hilfe eines Passworts. Dieses muss so konstruiert sein, dass es sich nur schwer knacken lässt. Dazu sollte es möglichst komplex sein, also mindestens über acht Zeichen verfügen, die sich aus Gross- und Kleinbuchstaben, Nummern und Sonderzeichen zusammensetzen. Ein solches Passwort kann man konstruieren, indem man einen Satz schreibt und z.B. jeweils den Anfangsbuchstaben der einzelnen Wörter sowie die darin enthaltenen Satzzeichen und Zahlen für das Passwort verwendet («Ein schöner, knackiger Apfel kostet ein Pfund.» ergäbe als Passwort Es,kAk1£.). Passwörter im Klartext sollen nicht an unsicheren Orten aufbewahrt werden. Als zusätzlicher Schutz kann neben dem Passwort (Wissen) auch noch eine Chipkarte oder ein USB-Stick (Besitz) oder sogar ein biometrisches Datum (spezifische Eigenschaft einer Person, wie bspw. der Fingerabdruck) verwendet werden. Dies erhöht die Sicherheit der Daten.

Wir haben als Beispiele die beiden Verschlüsselungsprogramme Rohos Mini Drive und TrueCrypt auf ihre Anwendbarkeit hin analysiert. Rohos Mini Drive wird auf USB-Speicher-Sticks eingesetzt. Mit TrueCrypt kann man Daten namentlich auf Festplatten und, mit Hilfe von Administratorenrechten, auch auf USB-Speicher-Sticks in verschlüsselter Form bearbeiten.

Rohos Mini Drive, Version 1.6.0.0, benötigt folgende Minimalausstattung: Windows 2000 / XP / 2003 / Vista; USB 1.1/2.0 Anschluss; USB-Flash-Laufwerk oder U3 Smart Flash Drive mit 1 MB oder mehr Speicherplatz; die max. Grösse der verschlüsselten Partition beträgt 2GB. Das Verschlüsselungsprogramm Rohos Mini Drive kann für die Verschlüsselung von Daten auf USB-Speicher-Sticks eingesetzt werden. Sobald das Programm auf einem solchen Stick installiert wurde, ist es auf jedem Computer ohne Administratorenrechte einsetzbar. Die Entschlüsselung geht so vor sich, dass das Dokument in einem «versteckten» Ordner dekodiert und mit der jeweiligen Anwendung

geöffnet wird. Der Ordner und die sich darin befindenden bearbeiteten (entschlüsselten) Dokumente bleiben bestehen, wenn man den Rohos Disk Browser verlässt. Es ist deshalb wichtig, dass man diese Zwischendateien löscht, damit diese nicht von anderen Personen eingesehen werden können. Wir haben die Zwischendateien bei unserem Versuch gelöscht und festgestellt, dass diese Löschung logisch und nicht physisch erfolgt. Mit Recovery-Werkzeugen gelang es uns, die Dateien wieder herzustellen. Der Benutzer muss sich also bewusst sein, dass er sie noch mit einem separaten Tool physisch löschen muss, damit sie nicht mehr rekonstruierbar sind (Wipe-Tools). Rohos stellt eine neue Version des Produkts in Aussicht, welche es erlauben wird, die Entschlüsselung direkt in der entsprechenden Anwendung vorzunehmen, so dass keine temporären Dateien mehr auf der Disk zwischengespeichert werden.

TrueCrypt (Version 6.2.a) ist ein freies Open-Source-Programm für die Verschlüsselung von Datenträgern. Es ist auf den folgenden Betriebssystemen einsetzbar: Windows 2000, XP, 2003, Vista, 7; Linux, Mac OS X, Mac OS X/Intel. Benutzer, welche keine Administratorenrechte besitzen, haben die Möglichkeit, TrueCrypt in einer etwas eingeschränkten Form zu verwenden. Sie können namentlich Volumen (FAT), nicht aber Partitionen erstellen, in denen sich die sensitiven Daten mit Hilfe von Verschlüsselungsverfahren sicher bearbeiten lassen. Im Weiteren ist es auch nicht möglich, NTFS-Volumen zu erstellen und TrueCrypt im «portable» bzw. «traveler Mode» einzusetzen. Das Programm TrueCrypt traveler Mode, welches bspw. auf einem USB-Speicher-Stick installiert werden kann, ist nur auf Systemen einsetzbar, auf denen man Administratorenrechte besitzt.

Die Ver- bzw. Entschlüsselung erfolgt «on the fly», d.h. in Echtzeit (real time Encryption). Bei diesem Verfahren erfolgt eine «direkte» Ver- bzw. Entschlüsselung im Hauptspeicher (RAM), ohne dass temporäre Dateien erstellt werden. Für diese Echtzeitverschlüsselung benötigt TrueCrypt Gerätetreiber (device driver). Benutzer, die keine Administratorenrechte besitzen, können die Gerätetreiber im Windows weder installieren noch starten.

## 1.3 Internet und Telekommunikation

### 1.3.1 E-Government und der digitale Bürger

**Die neue AHV-Nummer findet immer mehr Verbreitung als Personenidentifikator in verschiedenen E-Governmentprojekten. Dabei wird die Tatsache, dass die Verwendung der Nummer für diese Zwecke vorher gesetzlich geregelt werden muss, gerne übersehen.**

Die E-Governmentprojekte des Bundes werden mit grossem Elan vorangetrieben. Dabei stellen wir fest, dass die an den Projekten Beteiligten oft nur am Rand und sehr spät mit datenschutzrechtlichen Problemen an uns gelangen. Ein allgemeines Problem in der Welt des E-Government stellt sich beim Authentifizierungsprozess der Bürgerinnen und Bürger. Wie kann der Staat beispielsweise feststellen, dass der stimmberechtigte Bürger X seine Stimme elektronisch abgegeben hat, oder ist es wirklich die Bürgerin Y, die der Gemeinde ihren Wegzug elektronisch meldet?

In den Augen vieler wäre die einfache Lösung, als digitale Authentifizierung die neue 13-stellige AHV-Versichertennummer zu verwenden. Wir haben jedoch auch in früheren Tätigkeitsberichten schon betont, dass die Ausbreitung der AHV-Nummer als Personenidentifikator hohe Risiken für die Bürgerinnen und Bürger birgt, da sie unvorhersehbare Verknüpfungen ermöglicht. Damit die allgemeine Verwendung der AHV-Nummer als Personenidentifikator zumindest durch den Volkswillen legitimiert und die dazu notwendige politische Debatte geführt wird, muss sie gesetzgeberisch ausreichend geregelt werden. Eine Bedingung, die bei der Planung der verschiedenen Projekte gerne vergessen und in der Zeitplanung ungenügend berücksichtigt wird. In unserer Stellungnahme zum e-CH Standard 0045, der ein Glossar im Bereich der elektronischen Stimmregister enthält, haben wir uns erneut in entsprechender Weise geäussert.

### 1.3.2 Strassenansichten im Internet: Google Street View

**Nach eingehender Prüfung des Dienstes Street View kamen wir zum Schluss, dass er aus datenschutzrechtlicher Sicht erhebliche Mängel aufweist. Zudem gingen bei uns zahlreiche Beschwerden von betroffenen Personen ein. Daher haben wir eine entsprechende Empfehlung erlassen und beim Bundesverwaltungsgericht Klage gegen Google eingereicht.**

Seit der Aufschaltung des Online-Dienstes Google Street View Mitte August sind sowohl beim EDÖB als auch bei Google Switzerland GmbH selber zahlreiche Hinweise aus

der Bevölkerung auf mangelhafte oder fehlende Unkenntlichmachung von Gesichtern oder Nummernschildern eingegangen. Unsere Recherchen bestätigten diesen Befund. Wir haben überdies festgestellt, dass Google lückenhaft und geografisch zu unpräzis über bevorstehende Kamerafahrten informierte. Diese Erkenntnisse wurden Google mitgeteilt, worauf die Verantwortlichen des Unternehmens Massnahmen zur Ausbesserung der Mängel vorschlugen, die jedoch noch nicht überzeugten. Unserer Ansicht nach braucht es zum Schutz der Privatsphäre eine vollständige Anonymisierung von Gesichtern und Autokennzeichen. Daher forderten wir in unserer Empfehlung vom 11. September 2009, dass Google

- eine verbesserte Lösung zur vollständigen Unkenntlichmachung von Gesichtern und Autokennzeichen erarbeitet,
- der Anonymisierung im Umfeld heikler Einrichtungen wie z.B. Spitäler, Schulen oder Gefängnissen besondere Beachtung schenkt,
- Aufnahmen aus Privatstrassen löscht, wenn keine Einwilligung dafür vorliegt,
- Aufnahmen von umfriedeten Orten (Höfe, Gärten) entfernt und künftig die Kamera entsprechend niedriger montiert,
- sowohl eine Woche vor den Aufnahmen als auch eine Woche vor deren Aufschaltung informiert, welche Städte und Dörfer betroffen sind, und dass Google
- keine neuen Bilder von Schweizer Strassen aufschaltet, bis die Rechtsfragen geklärt sind.

Da Google der Empfehlung in den meisten Bereichen nicht nachkam, haben wir beim Bundesverwaltungsgericht Klage gegen Google, Inc. und die Google Switzerland GmbH eingereicht. Im Rahmen von vorsorglichen Massnahmen verlangten wir, dass keine weiteren in der Schweiz aufgenommenen Bilder aufgeschaltet und hierzulande keine weiteren Kamerafahrten durchgeführt werden. Im Dezember haben wir mit Google eine Vereinbarung getroffen. Mit dieser wurden unsere mit den vorsorglichen Massnahmen beabsichtigten Ziele vollumfänglich erfüllt: Für die Dauer des Gerichtsverfahrens werden keine neuen Bilder aus der Schweiz aufgeschaltet. Bei Kamerafahrten werden allfällig betroffene Personen rechtzeitig informiert.

Google verpflichtet sich weiter, ein rechtskräftiges schweizerisches Gerichtsurteil zu akzeptieren und auch auf die sich bereits im Ausland befindlichen Bilder aus der Schweiz anzuwenden. Die getroffene Vereinbarung wurde in der Folge vom Bundesverwaltungsgericht geprüft und nicht beanstandet.

Empfehlung und Klageschrift befinden sich im Anhang Ziff. 4.1.6 respektive 4.1.7 und können auf unserer Webseite www.derbeauftragte.ch, Dokumentation – Datenschutz – Empfehlungen resp. Weiterzüge, abgerufen werden.

### 1.3.3 Strassenansichten im Internet: «Touchtown»

**Auf der Webseite www.touchtown.ch betreibt eine Firma ein Konkurrenzprodukt zu Google Street View mit ganz ähnlichen Funktionen. Im Vergleich zu Google verfolgt die Annularspace GmbH jedoch einen anderen Ansatz bei der Datenerhebung, der von uns als datenschutzkonform erachtet wird.**

Obwohl in einigen Fällen die betroffenen Personen ohne weiteres erkennbar sind und Gesichter nicht unkenntlich gemacht wurden, stufen wir den Dienst «Touchtown», gestützt auf unsere bisherigen Abklärungen, nicht als datenschutzwidrig ein. Anders als Google, Inc. macht die Firma Annularspace GmbH ihre Aufnahmen mit tragbaren Aufnahmegeräten und informiert die betroffenen Personen vor der Aufnahme mit Lautsprecherdurchsagen und Flyer. Auf diese Weise haben die Betroffenen jeweils die Möglichkeit, sich aus dem Blickfeld der Kamera zu entfernen, um nicht aufgenommen zu werden. In Fällen, wo dies aufgrund von Menschenmengen oder örtlichen Gegebenheiten nicht möglich ist, werden die abgebildeten Personen nach Angaben der Firma manuell unkenntlich gemacht. Zudem wurden nach unseren bisherigen Kenntnissen keine Bilder der Privatsphäre gemacht, wenn nicht vorher die Zustimmung der betroffenen Personen eingeholt worden war. Bisher sind bei uns jedenfalls keine Beschwerden von betroffenen Personen eingegangen.

### 1.3.4 Auswertungen von Webseiten-Zugriffen

**Google, Inc. bietet zur Auswertung von Zugriffen auf Webseiten einen Dienst mit dem Namen «Google Analytics» an. Dazu werden die notwendigen Informationen in die USA an die Server von Google übermittelt und dort analysiert. Da die Firma Safe-Harbor-zertifiziert ist, kann der Dienst unter gewissen Voraussetzungen sowohl von Bundesorganen als auch von Privaten genutzt werden, ohne dass dafür spezielle Garantien vereinbart werden müssten.**

Mit dem Internetdienst «Google Analytics» können Betreiber von Internetseiten die Zugriffsstatistiken auf ihrer Website ohne Installation und Betrieb von serverseitigen Zusatzprogrammen erfassen und entsprechende Auswertungen vornehmen. Dazu

müssen sie einen von Google, Inc. zur Verfügung gestellten Programmcode in ihre Internetseite integrieren, mittels welchem Google die Zugriffe auf die Internetseite erfassen, die Daten in die USA übermitteln und für den Betreiber der Website aufbereiten kann. Dies stellt eine Datenweitergabe an Dritte in einem Outsourcingverhältnis dar; wer «Google Analytics» einsetzt, muss deshalb die Nutzer seiner Seiten in einem «Disclaimer» darüber informieren, dass ihre Daten von Google in den USA bearbeitet werden. Google stellt einen solchen Disclaimer zur Verfügung. Es obliegt nun den Betreibern, die Benutzerinnen und Benutzer ihrer Webseite über den Einsatz von «Google Analytics» umfassend zu informieren.





### 1.3.5 Internetfernsehen

**Wir haben die Dienstleistungen eines in der Schweiz ansässigen Internetfernseh-Anbieters auf die Vereinbarkeit mit dem Datenschutzgesetz überprüft und für gut befunden. Dies geschah vor dem Hintergrund der im letzten Jahr erstellten Erläuterungen zum digitalen Fernsehen, ITV und IPTV.**

Internetfernsehen erfreut sich einer zunehmenden Beliebtheit. Wie wir bereits in unseren Erläuterungen zum digitalen Fernsehen, ITV und IPTV festgehalten haben, besteht dabei allerdings die Möglichkeit, dass das Fernsehkonsumverhalten der Nutzerinnen und Nutzer aufgezeichnet wird. Wir haben dies zum Anlass genommen, mit den grossen Anbietern von digitalem Fernsehen und einem Anbieter von Internetfernsehen Kontakt aufzunehmen, um zu untersuchen, welche Personendaten sie zu welchen Zwecken bearbeiten. In allen Fällen konnten wir feststellen, dass die Datenbearbeitung in Übereinstimmung mit dem DSG erfolgte. Insbesondere der Anbieter des Internetfernsehdienstes zeichnete sich durch Datensparsamkeit und unterdurchschnittlich lange Aufbewahrungsfristen aus.

Die erwähnten Erläuterungen finden Sie auf unserer Webseite www.derbeauftragte.ch, Themen – Datenschutz – Sonstige Themen.

### 1.3.6 Erläuterungen zur mobilen Datenbearbeitung

Der moderne Mensch ist mobil und möchte überall arbeiten und somit auf seine Dokumente zugreifen können, sei es zu Hause, im Büro oder unterwegs. Es existieren verschiedene Möglichkeiten, dieses Ziel zu erreichen. Beispielsweise kann er seine Daten auf einem Datenträger mit sich führen oder sie im Internet ablegen. Je nach gewählter Lösung ergeben sich unterschiedliche Risiken und entsprechende Gegenmassnahmen.

Wir haben vier grobe Modelle unterschieden, zu denen wir jeweils neben den generellen Vor- und Nachteilen die Datenschutzrisiken aufzeigen. Die Erläuterungen zur mobilen Datenbearbeitung finden sich im Anhang Ziff. 4.1.1 sowie auf unserer Webseite www.derbeauftragte.ch, unter Themen – Datenschutz – Internet.

### 1.3.7 Erläuterungen zum Umgang mit Suchmaschinen

Ohne Suchmaschinen wäre eine sinnvolle und effiziente Nutzung des World Wide Web mit seinen Milliarden von Seiten heute praktisch unmöglich. Um die Auffindbarkeit von Informationen im Internet ständig zu verbessern, müssen Suchmaschinen allerdings gezielt Informationen über das Suchverhalten und die Qualität der Treffer erheben und statistisch auswerten. Damit ist auch ein Eingriff in die Privatsphäre der Internetnutzer verbunden, und zwar sowohl bei der Auswertung der Suchanfragen als auch bei der Bereitstellung von Suchergebnissen. Informationen und Tipps zum Umgang mit Suchmaschinen finden sich im Anhang Ziff. 4.1.2 oder auf unserer Webseite www.derbeauftragte.ch, Themen – Datenschutz – Internet.

### 1.3.8 Einführung der gesicherten Nachrichtenübermittlung (secure messaging)





**Der EDÖB verwendet zur gesicherten Nachrichtenübermittlung seit kurzem statt PGP die offizielle Lösung «Secure Messaging». Die bisherigen Zertifikate der Klasse C bringen im Vergleich zu denen der Klasse B, die als sicherer gelten, gewisse Nachteile bei Nutzerkontrolle und Passwortschutz mit sich, aber auch Vorteile bezüglich der einfachen Benutzung und der kryptographischen Sicherheit.**

Seit dem 1. Januar 2000 konnten wir eine inoffizielle Lösung für eine gesicherte elektronische Nachrichtenübermittlung nutzen, bei der jeder Arbeitsplatz über die Software PGP (Pretty Good Privacy) verfügte. So waren wir in der Lage, verschlüsselte und/oder signierte Nachrichten mit allen Angehörigen der weltweiten PGP-Gemeinschaft auszutauschen, die eine vereinfachte Form der Public Key Infrastruktur (PKI) darstellt.

Mit der Einführung der offiziellen Lösung «Secure Messaging» in unserer Dienststelle verfügt nunmehr jeder Mitarbeiter über ein elektronisches Zertifikat der Klasse C für die Signatur und die Chiffrierung der E-Mails. Diese letztere Operation ist nur mit Empfängern möglich, die ebenfalls eine gesicherte Nachrichtenübermittlung vom Typ

S/MIME nutzen. Zertifikate der Klasse C begünstigen eindeutig eine einfache Nutzung, da sie im Nutzerprofil gespeichert sind und kein Passwort für die Signatur durch den Absender oder die Entschlüsselung durch den Empfänger der Nachricht erfordern. Anders ist die Situation bei den Zertifikaten der Klasse B (oder A), da diese auf einer individuellen Chipkarte gespeichert sind und ein Passwort für jede Unterschrift oder Dechiffrierung einer Nachricht benötigen. Es ist hier hervorzuheben, dass die Zertifikate der Klasse B in dieser Hinsicht sicherer sind als diejenigen der Klasse C, dass letztere aber mit RSA-Schlüsseln in doppelter Länge, nämlich 2048 Bit, kryptographisch sicherer sind. Vergessen wir nicht, dass erst kürzlich eine ganze RSA-Zahl von 768 Bit (232 Dezimalziffern) mit Hilfe «angemessener Mittel» faktorisiert worden ist, was die Prognose bestätigt, der zufolge RSA-Schlüssel von 1024 Bit (darunter die Zertifikate der Klasse B) nur noch während einiger Jahre sicher sind.

## 1.4 Justiz/Polizei/Sicherheit

### 1.4.1 Umsetzung Schengen: Kontrolle des EDÖB bei der diplomatischen Vertretung der Schweiz in Kairo

**Als Aufsichtsbehörde der Bundesorgane im Bereich des Datenschutzes sind wir mit der Kontrolle der Bearbeitungen von Personendaten im Schengener Informationssystem betraut. Daher haben wir eine Überprüfung bei der diplomatischen Vertretung der Schweiz in Kairo (Ägypten) vorgenommen. Unsere Schlussfolgerungen und Verbesserungsvorschläge haben wir an das Eidgenössische Departement für auswärtige Angelegenheiten gerichtet.**

Als Aufsichtsbehörde der Bundesorgane im Bereich des Datenschutzes kontrollieren wir die Personendatenbearbeitungen durch Bundesorgane im Schengener Informationssystem (SIS), und dies entsprechend den aufgrund der Schengen-Zusammenarbeit bestehenden Anforderungen. Unter anderem führen wir diese Überprüfungen bei den diplomatischen und konsularischen Vertretungen der Schweiz im Ausland durch.

In diesem Zusammenhang haben wir eine Kontrolle bei der diplomatischen Vertretung der Schweiz in Kairo in Ägypten vorgenommen. Gestützt auf unsere Feststellungen haben wir einen Bericht und Verbesserungsvorschläge vorgelegt, die das EDA akzeptiert und umgesetzt hat. Das EDA legte insbesondere in einer internen Weisung die Verantwortungsbereiche und Aufgaben der mit der Sicherheit und dem Datenschutz betrauten Personen bei den schweizerischen Auslandsvertretungen fest. Zudem änderte es die Passwortverwaltung entsprechend den Weisungen betreffend die Informatiksicherheit in der Bundesverwaltung. Es beschränkte den Zugang zu den Serverräumen des Informatiknetzwerkes der schweizerischen Vertretung in Kairo ausschliesslich auf die berechtigten Personen (Verantwortliche der Informatikdienste) und stellte klare Vorschriften betreffend die Aufbewahrung der Personendaten auf. Überdies setzt das EDA seine Tätigkeiten zur Anweisung und Sensibilisierung seiner Mitarbeiter auf dem Gebiet des Datenschutzes fort.

Das Fehlen von sicheren Kommunikationssystemen für die Datenübermittlung per E-Mail zwischen den schweizerischen Vertretungen im Ausland und den übrigen Dienststellen der Bundesverwaltung ist jedoch weiterhin problematisch. Mit dieser Schwierigkeit, auf die wir hingewiesen haben, befasst sich derzeit das Bundesamt für Informatik und Telekommunikation (BIT), das Massnahmen für die Sicherung und den Schutz solcher Daten für die Bundesämter einführt.

Weitere Berichte zu Schengen befinden sich in diesem Kapitel und in Ziff. 1.10.

### 1.4.2 Umsetzung Schengen: Logfiles SIS

**Die Zugriffe auf den nationalen Teil des Schengener Informationssystems (N-SIS) werden in Besucherdateien (Logfiles) registriert. Im Rahmen der Wahrnehmung ihrer Aufgaben müssen die Datenschutzbehörden diese analysieren. In Zusammenarbeit mit dem Bundesamt für Polizei haben wir die Struktur der N-SIS-Logfiles und ihre Nutzung untersucht.**

Gemäss den Schengen-Abkommen verfügt die Schweiz über eine nationale Kopie der SIS-Datenbank (N-SIS). Die darin enthaltenen Informationen sind sensible Daten, auf die nur eine begrenzte Personengruppe zugreifen darf. Sämtliche Zugriffe auf die Datenbank N-SIS werden in Besucherdateien (Logfiles) registriert. Aus ihnen ist zu erfahren, wer was wann und warum getan hat. Im Rahmen ihrer jeweiligen Zuständigkeiten müssen die nationalen und die kantonalen Datenschutzbehörden die Logfiles der Endnutzer analysieren können. In Zusammenarbeit mit dem Bundesamt für Polizei (fedpol) konnten wir die Struktur dieser Logfiles untersuchen. Dies ermöglicht uns, unsere Gesuche um Einsicht in Auszüge aus den Logfiles gezielter zu stellen und den Kantonen bei ihren Gesuchen wirksamer zu helfen. Wir haben diese Aufschlüsse der Schengen-Koordinationsgruppe der Datenschutzbehörden bei unserer Tagung vom 12. November 2009 vorgelegt und unseren kantonalen Kollegen das Verfahren für die Nutzung der Zugriffsprotokolle erläutert.

Weitere Berichte zu Schengen befinden sich in diesem Kapitel und in Ziff. 1.10.

### 1.4.3 Umsetzung Schengen: Kontrolle des EDÖB bei der Bundeskriminalpolizei

**Die erste Kontrolle der im Schengener Informationssystem vorgenommenen Datenbearbeitungen hat gezeigt, dass die Bundeskriminalpolizei als Endnutzerin die gesetzlichen Sicherheits- und Datenschutzanforderungen einhält.**

Aufgrund der Bedeutung und des Umfangs der in der Schweiz seit Juni 2008 im Schengener Informationssystem (SIS) erfolgten Bearbeitungen von Personendaten planten wir für 2009 eine erste Überprüfung der Datenbearbeitungen im SIS und der Nutzung dieses Systems. Wir beschlossen, die Rechtmässigkeit des Zugriffs der Mitarbeiter (Einzelnutzer) der Bundeskriminalpolizei (BKP) sowie die Einhaltung der gesetzlichen Sicherheits- und Datenschutzanforderungen bei der Nutzung des SIS durch eben diese Mitarbeiter zu überprüfen. Einige kantonale Datenschutzbehörden haben bei den kantonalen Nutzern des SIS ebenfalls Kontrollen durchgeführt.

Wir ersuchten das Bundesamt für Polizei (fedpol), die verschiedenen Dokumentationen bezüglich der Datenbearbeitungen im SIS bereitzustellen. Diese Dokumentationen unterzogen wir einer Analyse, um unseren bei der Überprüfung vor Ort eingesetzten Fragebogen gezielter auszuformulieren. Die Kontrolle fand im Juni 2009 statt und betraf verschiedene Punkte. Sie ermöglichte uns festzustellen, auf welche Weise die Mitarbeiter der BKP Zugriff zu den Daten des SIS erhalten, und welche Verfahren zur Anwendung kommen, wenn Daten widerrechtlich bearbeitet werden oder wenn sich herausstellt, dass sich im SIS unrichtige Daten befinden.

Wir überprüften auch die Profile der BKP-Mitarbeiter, die zum Zugriff auf das SIS berechtigt sind, und analysierten die technischen und organisatorischen Sicherheitsmassnahmen. Die Räumlichkeiten der BKP sind gesichert (Loge beim Gebäudeeingang und Zutritt zu den verschiedenen Räumen ausschliesslich mit persönlichen Badges). Der Zugriff auf das SIS ist nur von einem Computer mit einer zugelassenen IP-Adresse unter ausschliesslicher Verwendung einer kryptographischen Karte und dem entsprechenden Passwort möglich. Auf eine Analyse der Logfiles wurde bei dieser Überprüfung verzichtet. Dafür wären zusätzliche Informationen von fedpol erforderlich gewesen, die uns erst nach Abschluss der Kontrolle geliefert wurden. So konnten wir der Datenschutzbehörde des Kantons Bern im Rahmen ihrer eigenen Aufsichtstätigkeiten nützliche Informationen über die Verwendung der Logfiles geben. Unsere nächsten Überprüfungen bei anderen Nutzern beim Bund werden auch die Analyse der Logfiles einbeziehen. Abschliessend konnten wir bei dieser Kontrolle feststellen, dass die BKP als Endnutzerin des SIS die gesetzlichen Sicherheits- und Datenschutzanforderungen einhält. Somit hatten wir keine Bemerkungen oder Empfehlungen anzubringen.

Weitere Berichte zu Schengen befinden sich in diesem Kapitel und in Ziff. 1.10.





### 1.4.4 Umsetzung Schengen: Koordinationsgruppe Schengen der Schweizerischen Datenschutzbehörden

**Auf der Grundlage der entsprechenden Verordnung haben wir die Initiative zur Bildung einer Koordinationsgruppe der Schweizerischen Datenschutzbehörden im Rahmen der Umsetzung der Schengen-Assoziierungsabkommen ergriffen. 2009 haben wir diese Koordinationsgruppe zweimal einberufen.**

Artikel 54 der Verordnung über den nationalen Teil des Schengener Informationssystems (N-SIS) und das SIRENE-Büro sieht vor, dass die kantonalen Datenschutzbehörden und der EDÖB im Rahmen ihrer jeweiligen Zuständigkeiten aktiv zusammenarbeiten und für eine koordinierte Aufsicht über die Bearbeitung von Personendaten sorgen.

Auf der Grundlage dieser Gesetzesbestimmung haben wir die Bildung einer Koordinationsgruppe der Schweizerischen Datenschutzbehörden im Rahmen der Umsetzung der Schengen-Assoziierungsabkommen (nachfolgend: Koordinationsgruppe) in die Wege geleitet. Die Koordinationsgruppe ermöglicht den Datenschutzbehörden der kantonalen und der eidgenössischen Ebene eine aktive Zusammenarbeit im Rahmen ihrer Zuständigkeiten für die Beaufsichtigung der Datenbearbeitungen, die in Anwendung der Schengen-Assoziierungsabkommen vorgenommen werden. Unter Beachtung der Zuständigkeiten jedes ihrer Mitglieder widmet sich die Koordinationsgruppe namentlich folgenden Aufgaben: Austausch von Informationen, die für die wirksame Beaufsichtigung der oben genannten Datenbearbeitungen notwendig sind; Prüfung der Schwierigkeiten bei der Auslegung oder Anwendung der Gesetzesbestimmungen; Untersuchung der Probleme, die sich bei den Aufsichtstätigkeiten oder der Ausübung der Rechte der betroffenen Personen ergeben können; Formulierung von harmonisierten Vorschlägen und Stellungnahmen im Hinblick auf gemeinsame Lösungen; Unterstützung und Koordinierung der Aufsichtstätigkeiten der einzelnen Mitglieder. Die Koordinationsgruppe setzt sich aus einem Vertreter pro kantonale Datenschutzbehörde sowie einem Vertreter des EDÖB zusammen, der ihr Sekretariat besorgt.

Im Laufe des Jahres 2009 haben wir die Koordinationsgruppe zweimal einberufen. An der Sitzung vom 3. April 2009 konzentrierten sich die Bemühungen darauf, ein für die reibungslose Abwicklung der Tätigkeiten der Koordinationsgruppe notwendiges Reglement auszuarbeiten. Wir stellten auch den Rahmen und die Ziele der bei den Endnutzern des SIS durchzuführenden Kontrollen vor. Insbesondere erläuterten wir das geplante Vorgehen im Hinblick auf unsere angekündigte Kontrolle bei der Bundeskriminalpolizei. Des Weiteren legten wir die Ergebnisse unserer bei der diplomatischen und konsularischen Vertretung der Schweiz in Kiew (Ukraine) durchgeführten Kontrolle vor.

An der Sitzung vom 12. November 2009 verabschiedete die Koordinationsgruppe ihre Geschäftsordnung. Bei dieser Gelegenheit vermittelten wir den Teilnehmern aus den Kantonen Informationen über die laufenden Arbeiten bei der gemeinsamen Kontrollinstanz Schengen, der Arbeitsgruppe Justiz und Polizei der europäischen Konferenz der Datenschutzbeauftragten und der Koordinationsgruppe Eurodac. Wir erläuterten die Verfahren betreffend die Kontrollen der Logfiles des SIS beim Inhaber der Datensammlung fedpol. Des Weiteren stellten wir die Resultate unserer Kontrollen bei der Bundeskriminalpolizei und bei der diplomatischen und konsularischen Vertretung der Schweiz in Kairo (Ägypten) vor. Die Datenschutzbehörden der Kantone Bern und Freiburg berichteten über den Fortschritt ihrer Kontrollen bei den jeweiligen kantonalen Polizeibehörden. Schliesslich erhielt eine Arbeitsgruppe den Auftrag, allen Mitgliedern

der Koordinationsgruppe ein Dokument zur Methodologie der Aufsichtstätigkeiten zur Verfügung zu stellen; dieses Dokument greift auf unsere internen Kontrollverfahren, auf die Empfehlungen und vorbildlichen Datenschutzpraktiken des vom europäischen Rat verabschiedeten Schengen-Katalogs sowie auf den Datenschutzkatalog zum Zweck der Entwicklung gemeinsamer Kontrollstandards zurück, der von der Arbeitsgruppe Justiz und Polizei der europäischen Datenschutzbeauftragten ausgearbeitet wurde.

Weitere Berichte zu Schengen befinden sich in diesem Kapitel und in Ziff. 1.10.

### 1.4.5 Auskunftsgesuche betreffend das Informationssystem ISIS

**Im Jahr 2009 war die Anzahl der Auskunftsgesuche betreffend das Informationssystem ISIS nicht so erheblich wie 2008. Im Rahmen der für 2010 geplanten Revision der Gesetzgebung über die innere und äussere Sicherheit ist die Einführung eines direkten Zugriffsrechts geplant, das mit dem für die Dateien JANUS und GEWA geltenden Recht vergleichbar ist.**

Im Jahr 2008 wurden 148 so genannte indirekte Auskunftsgesuche betreffend das Informationssystem ISIS bei unserem Sekretariat eingereicht (vgl. unseren 16. Tätigkeitsbericht 2008/2009, Ziff. 1.4.4). 2009 sind 34 Auskunftsgesuche bei uns eingegangen. Dies bedeutet allerdings immer noch eine Verdoppelung gegenüber den Zahlen aus früheren Jahren (1998 bis 2007). Wie uns der Nachrichtendienst des Bundes mitteilte, ist im Rahmen der 2010 geplanten Revision der Gesetzgebung über die innere und äussere Sicherheit vorgesehen, das System des so genannten indirekten Zugriffsrechts durch ein direktes zu ersetzen, welches auf der Gesetzgebung über den Zugriff auf die Dateien JANUS und GEWA beruht (vgl. unseren 16. Tätigkeitsbericht 2008/2009, Ziff. 1.4.2, und unseren 15. Tätigkeitsbericht 2007/2008, Ziff. 1.4.4).

### 1.4.6 Verbesserung der Sicherheitsvorschriften für Ordonnanzwaffen

**Die Massnahmen zur Aufdeckung der potentiellen Gefahren im Zusammenhang mit Ordonnanzwaffen erfordern besondere Achtsamkeit, wenn diese die Bearbeitung von sensiblen Personendaten einschliessen. Im Besonderen muss der Grundsatz der Verhältnismässigkeit eingehalten werden, namentlich bei einer Sicherheitskontrolle ohne die Einwilligung der betroffenen Person.**

Um jegliche potentielle Gefahr, die ein Inhaber von Ordonnanzwaffen darstellen kann, rechtzeitig zu erkennen, hat der Bundesrat vorgeschlagen, in der Militärgesetzgebung

neue Massnahmen einzuführen. Zwei davon stellen einen erheblichen Eingriff in die Persönlichkeit und die Grundrechte der betroffenen Personen dar. Die erste Massnahme ist mit der Bearbeitung und insbesondere der Bekanntgabe von besonders schützenswerten Daten betreffend die Gesundheit verbunden. Es handelt sich um die für die Bundes-, Kantons- und Gemeindebehörden sowie für Ärzte, Psychiater und Psychologen vorgesehene Meldepflicht, wenn sie Anzeichen dafür erkennen, dass ein Militärangehöriger mit seiner Waffe eine Gefahr für sich selbst oder für Dritte darstellen könnte, oder wenn es sonstige Hinweise auf eine missbräuchliche Verwendung gibt. Die Datenschutzbestimmungen werden peinlich genau einzuhalten sein, insbesondere bei unbegründeten Meldungen. Entsprechend unseren Aufsichtspflichten und gegebenenfalls in Zusammenarbeit mit den kantonalen Datenschutzbehörden werden wir bei den mit der Bearbeitung dieser Meldungen betrauten Militärbehörden Kontrollen durchführen.

Die zweite Massnahme besteht in der Einführung einer zwar begrenzten, aber doch ohne die Einwilligung der betroffenen Person erfolgenden Sicherheitskontrolle. Im Rahmen der Ämterkonsultation haben wir den Standpunkt vertreten, dass die übrigen Massnahmen ausreichend erschienen, um die Gefährlichkeit einer Person zu bestimmen, und dass eine Sicherheitskontrolle nur dann stattfinden sollte, wenn sie als wirklich notwendig erachtet wird. Zudem haben wir in unserer Stellungnahme betont, dass eine Sicherheitskontrolle, auch wenn sie nur teilweise eingesetzt würde, nicht dem Verhältnismässigkeitsprinzip entspräche. Der Bundesrat und das Parlament haben unserem Standpunkt nicht Rechnung getragen; das Parlament hat jedoch den verbindlichen Charakter der Meldepflicht beseitigt.



### 1.4.7 Vorentwurf zur Revision des Bundesgesetzes über die Überwachung des Post- und Fernmeldeverkehrs

**Im Rahmen der Ämterkonsultation zum Vorentwurf der Revision des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs machten wir verschiedene datenschutzrechtliche Anmerkungen. Insbesondere bemängelten wir die ungenügenden Angaben zur Wirksamkeit des Einsatzes von Informatikprogrammen, die unbemerkt auf Informationsverarbeitungssystemen platziert werden sollen. Weiter beanstandeten wir den im Gesetz vage umschriebenen Begriff des Internetanbieters sowie die unklare Handhabung von Aufbewahrungsfristen.**

Im Hinblick auf die Einführung der Bundesstrafprozessordnung bedarf es einer Anpassung des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldever-

kehrs (BÜPF). Im Rahmen der Ämterkonsultation zum Vorentwurf haben wir dazu verschiedene Anmerkungen gemacht. Unklarheiten bestanden im Vorentwurf vor allem bei der Umschreibung des Personenkreises, auf den das Gesetz Anwendung findet. Wir haben hier eine Klarstellung verlangt. Weiter haben wir kritisiert, dass die beim Überwachungsdienst gespeicherten Daten nicht gelöscht werden sollten. Wir sind der Auffassung, dass gesetzliche Löschungsfristen zwingend integriert werden müssen.

Im Rahmen der Notsuche nach Personen kritisierten wir, dass die gesetzliche Formulierung «Dabei dürfen auch Daten unbeteiligter Dritter eingesehen werden» zu allgemein sei und eine erhebliche Missbrauchsgefahr in sich berge. Aus diesem Grund sollten Umstände und Zweck näher umschrieben werden.

Im Zusammenhang mit der Überwachung des Postverkehrs umschrieb der Gesetzesentwurf die Verpflichtung, darüber Auskunft geben zu können, mit wem die überwachte Person via Postverkehr Verbindung hat oder gehabt hat. Zudem seien die Verkehrs- und Rechnungsdaten während mindestens zwölf Monaten aufzubewahren. Unseres Erachtens könnten Anbieter von Postdienstleistungen aufgrund dieser Formulierung dazu verpflichtet werden, sämtliche postalischen Kontakte für zwölf Monate auf Vorrat zu speichern. Wir haben die Vorratsdatenspeicherung bemängelt und entsprechende Anpassungen gefordert.

Dem unbemerkten Einsatz von Informatikprogrammen auf Informationsverarbeitungssystemen stehen wir insgesamt skeptisch gegenüber. Auf der einen Seite ist die Wirksamkeit solcher Programme nicht ausreichend geklärt, und auf der anderen Seite stellt deren unbemerktes Platzieren bspw. auf dem PC Dritter einen schwerwiegenden Eingriff in die Privatsphäre dieser Personen dar.

Ein weiterer Kritikpunkt ist die unklare Umschreibung des Begriffs «Internetanbieter». Darunter könnte auch der Betreiber eines privaten WIFI-Netzwerkes fallen. Wir lehnen eine Ausdehnung der Verpflichtung zur Überwachung von privaten WIFI-Netzwerken (bspw. eines Hotels oder eines Restaurants) ab. Aus diesem Grund haben wir vorgeschlagen, anstelle des Begriffs «Internetanbieter» auf den in der Verordnung zum Fernmeldegesetz klar umschriebenen Begriff des Fernmeldedienstanbieters abzustellen.

## 1.5 Gesundheit

### 1.5.1 Revision des Epidemiengesetzes: Infektionskrankheiten

**Bezüglich der Verordnung des Eidgenössischen Departements des Innern zur Verhinderung der Einschleppung von neu auftretenden Infektionskrankheiten drängt sich die Schaffung einer klaren gesetzlichen Grundlage auf. Dies umso mehr, da auch im Bereich der grenzüberschreitenden Bekanntgabe von Personendaten eine regelungsbedürftige Unklarheit besteht.**

Auch am Datenschutz ging die Schweinegrippe nicht spurlos vorbei. Bereits in einem frühen Stadium wurden wir in die Ämterkonsultation zur «Änderung der Verordnung des EDI zur Verhinderung der Einschleppung von neu auftretenden Infektionskrankheiten» mit einbezogen. Besonders im Flugverkehr stellte sich auf den Inlandflugplätzen das Problem, inwieweit im grenzüberschreitenden Bereich die Bekanntgabe von Personendaten erlaubt sei. Wir haben zwar unvermittelt die Notwendigkeit anerkannt, die uns unterbreiteten Änderungen in besagter Verordnung so schnell wie möglich in Kraft zu setzen. Zugleich haben wir zuhanden des Bundesamts für Gesundheit (BAG) aber auch die Frage aufgeworfen, ob für diesen heiklen Bereich im Dienste der öffentlichen Gesundheit nicht die Gelegenheit genutzt werden sollte, im Rahmen der laufenden Revision des Epidemiengesetzes für eine ausreichende gesetzliche Grundlage zu sorgen. Mit diesem Anliegen wurden wir gleichzeitig auch aus dem Bereich des Flugverkehrs kontaktiert.

Gemäss Bundesgesetz über den Datenschutz dürfen Organe des Bundes bekanntlich besonders schützenswerte Personendaten und Persönlichkeitsprofile nur bearbeiten, wenn dies in einem Bundesgesetz im formellen Sinn ausdrücklich vorgesehen ist. Eine konkrete gesetzliche Grundlage für die geplante Datenbearbeitung durch das BAG findet sich nun aber im Epidemiengesetz nicht. Eine Ausnahme besteht lediglich, wenn ausserordentliche Umstände es erfordern; dann kann der Bundesrat für das ganze Land oder einzelne Landesteile die notwendigen Massnahmen treffen. Im Übrigen geht das Epidemiengesetz davon aus, dass die Massnahmen zur Bekämpfung von übertragbaren Krankheiten durch die Kantone getroffen werden müssen. Da bezüglich des Datenschutzes im Bereich der grenzüberschreitenden Bekanntgabe von Personendaten eine regelungsbedürftige Unklarheit besteht und es sich bei den mittels der Verordnung abzusichernden Daten (Gesundheitsfragebogen) um besonders schützenswerte Personendaten handelt, drängt sich unseres Erachtens eine klare gesetzliche Grundlage auf. Wir werden die weitere Entwicklung mit Spannung verfolgen.

### 1.5.2 eHealth: Beurteilung der empfohlenen Architektur

**Die für eHealth empfohlene Architektur kann als datenschutzfreundlich qualifiziert werden. Wir haben uns insbesondere in der Kerngruppe des Teilprojekts Standards und Architekturen dafür eingesetzt, dass grundsätzliche Anforderungen wie die informationelle Selbstbestimmung, die dezentrale Struktur und die Zweckbindung die Architektur prägen.**

Im August 2009 wurden erste Empfehlungen zu den Standards und der Architektur für eHealth Schweiz verabschiedet. Sie sollen dazu beitragen, dass sich elektronische Gesundheitsdienste in eine koordinierte Richtung entwickeln. Dem Datenschutz soll dabei, so verlangt es der Bundesrat, eine hohe Priorität zugestanden werden (vgl. unseren 16. Tätigkeitsbericht 2008/2009, Ziff. 1.5.3). Nun stellt sich die Frage, ob diese Forderung im Teilprojekt Standards und Architektur beachtet wurde und, noch wichtiger, wie sich diese Forderung in der eHealth-Architektur niederschlägt.

Die erste Frage kann mit ja beantwortet werden. Die Sensibilität gegenüber datenschutzrechtlichen Problemen ist im Teilprojekt vorhanden, was in Projekten dieser Dimension nicht selbstverständlich ist.

Die Antwort zur zweiten Frage lässt sich im Dokument «Empfehlungen Teilprojekt Standards und Architektur» des Koordinationsorgans Bund-Kantone (www.e-health-suisse.ch, Umsetzung – Standards und Architektur). In diesem Dokument werden die wesentlichen Bausteine der Architektur vorgestellt, ebenso wie die Grundsätze und Richtlinien, die den Bausteinen zugrunde liegen. Besonderen Wert haben wir auf die informationelle Selbstbestimmung, die dezentrale Struktur und die Zweckbindung die Architektur gelegt. Die Kerngruppe des Projekts, in der wir regelmässig mitarbeiten, hat eine Architektur erarbeitet, welche die Grundsätze berücksichtigt. In den nächsten Schritten werden wir insbesondere bei der Definition der Rollen, welche die Behandelnden in eHealth einnehmen können, und der Identifikationsverfahren aktiv mitwirken.

### 1.5.3 Mindeststandards bei Eintrittsformularen von Spitälern

**Wer in ein Spital eintritt, hat in der Regel ein Eintrittsformular auszufüllen. Es besteht jedoch keine Pflicht, ein solches integral zu unterzeichnen. Sämtliche Fragen sind gewissen Kriterien unterworfen, anhand derer Patientin und Patient die Rechtmässigkeit überprüfen können. Wir haben zwei Punkte auf solchen Formularen gesondert betrachtet.**

Beim Eintritt in ein Spital haben Patientinnen und Patienten in der Regel ein Eintrittsformular auszufüllen. Wiederholt wurden wir in diesem Zusammenhang gebeten, zur

Rechtmässigkeit der diversen Fragen auf solchen Formularen Stellung zu nehmen. Denn gemäss DSG sind alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen, Personendaten – also auch Personalien bzw. administrative Daten wie Name, Vorname und Adresse. Daten über die Gesundheit sind besonders schützenswerte Personendaten. Selbstredend haben nicht alle Spitäler dieselben Eintrittsformulare; sie müssen somit separat geprüft werden. Im Folgenden beleuchten wir zwei Punkte detailliert.

Teil von Eintrittsformularen kann die Frage nach der Teilnahme an einem Forschungsprojekt oder einer Studie sein. Patientinnen und Patienten müssen wissen, dass eine solche Teilnahme immer auf freiwilliger Basis erfolgt. Die Einwilligung, die schriftlich erfolgen muss, ist nur gültig, wenn Teilnehmerinnen und Teilnehmer vorgängig über Ziel und Zweck des Projektes und die damit verbundene Datenbearbeitung genügend aufgeklärt worden sind. In der Praxis werden dazu Informationsblätter abgegeben und Gespräche geführt. Damit die Einwilligung gültig ist, müssen Betroffene deren Tragweite (Umfang und Zweck) erkennen können; nur dann handelt es sich um eine aufgeklärte Einwilligung («informed consent»). Ausschlaggebend ist dabei die Einhaltung des Transparenzprinzips bei der Formulierung von Klauseln und Informationsformularen.

Die an einer Studie teilnehmende Person muss zudem ausführlich über Zweck und Ablauf der Studie sowie über sämtliche Datenbearbeitungen und Datenschutzvorkehren (Übermittlung, Speicherung, Vernichtung der Daten, Schutz vor unbefugtem Zugriff Dritter, allenfalls vorgesehene Pseudonymisierungs- und Anonymisierungsmassnahmen usw.) informiert werden. Stets muss ausdrücklich auf die Freiwilligkeit der Einwilligung und die jederzeitige Widerrufsmöglichkeit hingewiesen werden. Widerruft jemand seine Einwilligung, so muss er davon ausgehen können, dass sämtliche seiner Daten vernichtet werden; es empfiehlt sich, zur Sicherheit eine Bestätigung dieser Löschung zu verlangen. Selbstverständlich können sich Teilnehmerinnen und Teilnehmer jederzeit damit einverstanden erklären, dass ihre bis zum Zeitpunkt des Widerrufs im Rahmen der Studie bearbeiteten Daten weiterverwendet werden dürfen. Ein entsprechender Passus sollte in der Einwilligungserklärung figurieren. Auch dieses Einverständnis kann jede Person dank des Rechts auf informationelle Selbstbestimmung jederzeit widerrufen.

Ist die Weiterverwendung nicht geregelt, so darf nicht einfach angenommen werden, dass die Daten weiter verwendet werden dürfen, es sei denn, sie seien anonymisiert worden. Wenn also alle Merkmale entfernt wurden, welche die Identifizierung einer betroffenen Person ermöglichen, bedarf die Weiterverwendung keiner Einwilligung, da es sich nicht mehr um Personendaten handelt.

Ein zweiter Punkt ist das Outsourcing. Es ist heute üblich, dass Spitäler für gewisse administrative Arbeiten praxisfremde, professionelle Institutionen heranziehen. Soweit solche Dritte keine Patientendaten erhalten (wie beispielsweise für Buchhaltungsabschlüsse), ist dies datenschutzrechtlich unproblematisch. Verrechnungsstellen wie die Ärztekasse hingegen erhalten bei ihrer Tätigkeit Einblick in detaillierte Leistungsblätter und damit in medizinische Daten und Zusammenhänge. Arbeiten Spitäler mit einer solchen Institution zusammen, müssen sie deshalb die Patientinnen und Patienten darüber informieren und ihre Einwilligung einholen.

Diese so genannte Patientenerklärung sollte auf einem separaten Formular erfolgen. Eine Ablehnung der Einwilligung darf nicht mit Nachteilen oder Bedingungen verknüpft sein. Zwar benötigt die Krankenkasse eine Abrechnung der Leistungen, um die Vergütung berechnen zu können. Diese Abrechnung muss aber nicht unbedingt durch die Ärztekasse (Abrechnungsinstitut) erfolgen, sondern kann auch vom Spital vorgenommen werden. Patientinnen und Patienten können der Weitergabe ihrer persönlichen Gesundheitsdaten je nach Situation ausdrücklich (d.h. mündlich oder schriftlich) oder stillschweigend zustimmen. Sie müssen aber freiwillig und ohne Druck entscheiden und gegebenenfalls auch gewisse Passagen der Einwilligungserklärung durchstreichen können.





Wiederum gilt auch hier: Die Einwilligung ist nur gültig, wenn sich die Patientin oder der Patient über das Ausmass der ganzen Datenbearbeitung, den Zweck und den oder die Empfänger der Daten im Klaren ist. Nichtig sind daher alle pauschalen Einwilligungserklärungen, welche immer wieder auf Formularen für Versicherungsverträge oder in den allgemeinen Geschäftsbedingungen zu finden sind.

### 1.5.4 Outsourcing von medizinischen Daten

Das Merkblatt «Auslagerung der Rechnungsstellung durch einen Arzt» wird zurzeit von uns überarbeitet. Dies wird noch einige Zeit in Anspruch nehmen, da grundlegende Fragen in Zusammenhang mit der Zulässigkeit einer Datenbearbeitung durch einen Dritten (Outsourcing) geklärt werden müssen. Mit der letzten Revision des DSG wurde ein neuer Artikel 10a eingeführt. Er hält fest, dass die Datenbearbeitung durch einen Dritten grundsätzlich zulässig ist, wenn keine gesetzliche oder vertragliche Geheimhaltungspflicht es verbietet. Für Ärztinnen und Ärzte besteht aber eine ausdrückliche gesetzliche Geheimhaltungspflicht (Patientengeheimnis nach Artikel 321 StGB). Das datenschutzrechtliche Verbot eines Outsourcings würde hier klarerweise die Ausla-

gerung der Rechnungsstellung durch einen Arzt ohne ausdrückliche Zustimmung der Patientin oder des Patienten verbieten. Die auftretenden Fragestellungen, unter anderem in Bezug auf die Qualifikation von Hilfspersonen, deren Beantwortung weitgreifende Konsequenzen für alle Formen des Outsourcings im Bereich von vertraglichen oder gesetzlichen Geheimhaltungspflichten haben wird, hat uns dazu veranlasst, eine schriftliche Stellungnahme des Bundesamtes für Justiz einzuholen. Entsprechend dieser Stellungnahme werden wir, auch in Zusammenarbeit mit den kantonalen Datenschutzbehörden, das Thema Outsourcing weiter bearbeiten.

### 1.5.5 Merkblatt über Austritts- und Operationsberichte

Wir mussten das «Merkblatt über Austritts- und Operationsberichte» leicht anpassen, weil das Bundesgericht in einem neuen Entscheid die Rechte der Versicherungen an den Austritts- und Operationsberichten konkretisiert hat. Grundsätzlich halten wir aber an einer graduellen Bekanntgabe der Informationen an den Versicherer fest. Das Merkblatt kann auf unserer Webseite www.derbeauftragte.ch, Dokumentation – Datenschutz – Merkblätter, abgerufen werden.

### 1.5.6 Versand von Blutproben ins Ausland

**Schickt eine Firma aus der Schweiz Blutproben zur Analyse in ein Labor nach Südafrika, so muss sie durch einen Vertrag mit dem südafrikanischen Labor einen angemessenen Datenschutz gewährleisten.**

Eine Firma aus der Schweiz kontaktierte uns hinsichtlich eines Forschungsprojekts, das den Versand von Blutproben zu Analysezwecken nach Südafrika vorsieht. Die Blutproben werden mit den Initialen (Vorname und Name) und einer Identifikationsnummer versehen an das Labor in Südafrika geschickt. Die Firma wollte von uns wissen, ob sie mit dem Labor zwingend einen Vertrag abschliessen müsse.

In diesem Zusammenhang musste vorweg die Frage geklärt werden, ob eine Blutprobe mit den genannten Identifikatoren noch ein Personendatum darstellt. Blut oder allgemein zellhaltige Körperproben enthalten die DNA der Probandin oder des Probanden. Die DNA wiederum enthält Informationen über eine bestimmbare Person. Somit sind wir zum Schluss gekommen, dass eine Blutprobe in Kombination mit den genannten Identifikatoren ein Personendatum darstellt. Die Firma sendet also regelmässig Personendaten in ein Land, das keinen angemessenen Datenschutz gewährleistet.

Entsprechend haben wir die schweizerische Firma darauf hingewiesen, dass sie mit dem Labor in Südafrika eine vertragliche Vereinbarung treffen muss, welche den betroffenen Personen einen angemessenen Schutz ihrer Personendaten gewährleistet.

### 1.5.7 Einkommensstatistik frei praktizierender Ärzte

**Die nachträgliche Verfeinerung einer Statistik kann dazu führen, dass eine Verbindung zwischen Daten und betroffener Person wieder hergestellt werden könnte. Dadurch würden sich die datenschutzrechtlichen Anforderungen ändern. Im Zusammenhang einer Anfrage betreffend die regelmässige Statistik über das Einkommen frei praktizierender Ärzte galt es, das Problem der kleinen Menge zu erkennen und zu umgehen.**

Die FMH lässt seit den Siebzigerjahren eine Statistik über die Einkommensverhältnisse frei praktizierender Ärzte erstellen und hat sich nun entschieden, die Auswertung zu verfeinern. Die Auftragnehmerin gelangte mit der Bitte an uns, abzuklären, ob dadurch datenschutzrechtliche Probleme aufträten. Die Verfeinerung der Auswertung bringt einen datenschutzrechtlich problematischen Effekt mit sich: das Problem der kleinen Menge. Durch kreuztabellarische Datenverknüpfungen entstehen zum Teil Mengen von weniger als 20 Datensätzen (N < 20). Das hätte bei der zu beurteilenden Statistik dazu geführt, dass manche Datensätze betroffenen Personen hätten zugeordnet werden können. Somit hätte es sich nicht mehr um unpersönliche statistische Daten gehandelt, was zu komplett veränderten Datenschutzanforderungen geführt hätte. Die Auftragnehmerin schlug vor, für die Auswertung den Grenzwert auf N > 20 zu setzen, was aus unserer Sicht im vorliegenden Fall ausreicht.

### 1.5.8 Medizinisches Forschungsprojekt in einem Spital

**In vielen medizinischen Forschungsprojekten müssen wir leider feststellen, dass die Auflagen nicht vollständig umgesetzt werden. Meist entsprechen die Sicherheitsmassnahmen nicht dem Stand der Technik. Im Weiteren ist die Information der Patientinnen und Patienten bzgl. Sperr- und Vetorecht sowie das Einholen der Einwilligungen verbesserungswürdig.**

Teil unserer Aufgaben ist es, die Einhaltung der Auflagen zu kontrollieren, welche die Expertenkommission für das Berufsgeheimnis in der medizinischen Forschung für die Erteilung von generellen oder Sonderbewilligungen auferlegt. Wir haben für die Kon-

trolle ein Spital ausgewählt, welches im Besitze einer generellen Bewilligung ist. Sie erlaubt dem Spital, mit internen Patientendaten Forschungsprojekte durchzuführen, ohne dafür immer eine Sonderbewilligung bei der Expertenkommission einholen zu müssen. Dabei gelten folgende Auflagen:

- Personendaten müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden. Dabei wird der Forschungsprozess betrachtet, von der Erhebung der Personendaten bis zu deren Anonymisierung oder Löschung.

  Im vorliegenden Fall werden die Daten der Patienten in zwei Papierarchiven gelagert. Im Kurzzeitarchiv befinden sich diejenigen Dossiers, mit denen bis vor zwei Jahren noch gearbeitet wurde, danach gelangen sie ins Langzeitarchiv im Keller. Nun befindet sich im Kurzzeitarchiv auch ein Kopierer. Die Türe zum Kurzzeitarchiv war zudem mit einem Keil unterlegt und stand somit offen. Die meisten Leute, welche auf diesem Stockwerk arbeiten, benutzen sehr wahrscheinlich besagtes Kopiergerät für ihre tägliche Aufgabenerfüllung, ohne die Informationen im Archiv zu bearbeiten. Wir haben dies beanstandet und darauf aufmerksam gemacht, dass der Kopierer aus Vertraulichkeitsgründen ausserhalb des Archivs aufzustellen sei, so dass nur die Berechtigten Zugriff auf die archivierten Patientendossiers haben. Zusätzlich haben wir auch darauf aufmerksam gemacht, dass der Kopierer in Brand geraten könnte, was mit grosser Wahrscheinlichkeit eine Vernichtung der archivierten Patientendossiers zur Folge hätte. Im Weiteren haben wir auch festgestellt, dass die Archivräume bei den Eingangstüren als solche gekennzeichnet sind. Wir erachten dies als gefährlich, weil ein Unbefugter damit sofort weiss, wo sich die archivierten Patientendaten in einem Spital befinden.

  Die Identifizierung der jeweils für ein Forschungsprojekt notwendigen Patientendossiers erfolgt über die Diagnosecodes (ICD-10) oder über den Operationscode (CHOP). Diese sind EDV-gestützt mit Hilfe einer Drittperson abrufbar und erlauben die Identifikation der gesuchten Dossiers. Der Forscher kann somit die notwendigen Daten aus den Krankenakten erheben. Damit die Identifikation der Patienten mittels Name, Vorname und Adresse im Forschungsprojekt nicht mehr direkt möglich ist, werden die notwendigen Daten mit Hilfe eines Pseudonyms in eine Excel-Datei übernommen. Das Pseudonym setzt sich aus den Anfangsbuchstaben des Namens und des Vornamens sowie dem Geburtstag zusammen. Wir haben darauf hingewiesen, dass ein so sprechendes Pseudonym nicht als datenschutzkonform betrachtet wer-

den kann. Umfassende Lösungen im Bereich der Pseudonymisierung können der Publikation «Generische Lösungen zum Datenschutz für Forschungsnetze in der Medizin» der Autoren Reng, Debold, Specker und Pommerening (März 2006, siehe bspw. unter www.tmf-net.de, Produkte und Services) entnommen werden.

Die Durchführung der Forschungsarbeit erfolgt mit Hilfe der pseudonymisierten Daten, welche in der Excel-Datei in einem PC festgehalten sind. Der Zugriff auf den PC ist mit Hilfe von User-ID und Passwort möglich. Wir erachten dies als genügend, wenn die Identifikation der Person nur über ein Pseudonym möglich ist. Befindet sich die Tabelle, welche das Pseudonym mit den jeweiligen Identifikationen beinhaltet, ebenfalls auf dem PC, ist diese Tabelle dem Stand der Technik entsprechend zu schützen. Dies bedeutet im vorliegenden Fall, dass bei einem nicht vernetzten (stand-alone) PC die Tabelle namentlich mit guten Chiffrierverfahren zu schützen ist. Ist der PC aber vernetzt, genügen User-ID und Passwort nicht mehr. Dann ist zusätzlich zum Passwort bspw. noch eine Chipkarte einzusetzen, deren Passwort- oder PIN-Eingabe aber nicht durch einen Keylogger aufgezeichnet werden kann.

- Eine weitere Auflage war, dass das Spital aufgrund der Bewilligung kein Forschungsprojekt ohne die Einwilligung der kantonalen Ethikkommission durchführen darf, und dass gewisse Informationen über die Forschungsprojekte gesammelt und einmal pro Jahr dem Sekretariat der Expertenkommission für das Berufsgeheimnis in der medizinischen Forschung zugestellt werden.

  Gemäss den Angaben aus dem Spital wurde kein Forschungsprojekt ohne die Zustimmung der kantonalen Ethikkommission durchgeführt. Es ist uns aber aufgefallen, dass gewisse Daten nicht erhoben wurden, die dem Sekretariat der Expertenkommission einmal jährlich zuzustellen sind.

- Ein weitere Auflage war auch, dass das Spital seine Patientinnen und Patienten systematisch darüber aufklärt, dass Personendaten für Forschungszwecke verwendet werden können und dass diese Verwendung untersagt werden kann (Vetorecht).

  Wir haben die Verantwortlichen darauf aufmerksam gemacht, dass in der Informationsbroschüre für die Patientinnen und Patienten im Bereich Forschung noch der Hinweis fehlt, dass sie ein Sperr- bzw. Vetorecht haben, wenn sie ihre Daten nicht für Forschungszwecke zur Verfügung stellen wollen.

### 1.5.9 Sammlung von Patientendaten für die medizinische Forschung

**Wir haben festgestellt, dass die Spitäler, welche im Besitze einer generellen Bewilligung der Expertenkommission für die Offenbarung des Berufsgeheimnisses in der medizinischen Forschung sind, in vielen Fällen fälschlicherweise davon ausgehen, bei den betroffenen Patientinnen oder Patienten keine Einwilligung für die Forschungsarbeiten einholen zu müssen. Die Einwilligung muss bei einer generellen Bewilligung jedoch nur dann nicht eingeholt werden, wenn es unverhältnismässig schwierig, unmöglich oder unzumutbar wäre.**

Mehrere Kontrollen haben gezeigt, dass die Forscher in den Spitälern davon ausgehen, es müsse keine Einwilligung bei den betroffenen Patientinnen und Patienten eingeholt werden, wenn mit Daten geforscht wird, die im Spital gespeichert bzw. archiviert sind, sofern das Spital im Besitz einer generellen Bewilligung der Expertenkommission in der medizinischen Forschung ist. Diese Interpretation entspricht aber nicht den normativen Vorgaben. Nur wenn es für die Forschenden unverhältnismässig schwierig, unmöglich oder unzumutbar ist, die Einwilligung der betroffenen Personen (bzw. der gesetzlichen Vertreter oder der nächsten Angehörigen) einzuholen, darf aufgrund der generellen Bewilligung auch mit solchen Personendaten geforscht werden.

Unmöglich oder unverhältnismässig schwierig bedeutet etwa, dass die betroffene Person, deren gesetzliche Vertreter oder die nächsten Angehörigen nicht aufgefunden werden können. Im Weiteren gilt es auch zu berücksichtigen, dass die Einholung von Einwilligungen bei den Betroffenen unzumutbar sein kann. Dies kann dann der Fall sein, wenn eine erneute Konfrontation der Betroffenen mit einer schwierigen Situation eine starke emotionale Belastung mit sich bringen würde, etwa durch die Erinnerung an eine vergangene schwere Krankheit oder einen Suizid in der Familie. Nur in solchen Fällen darf ohne Einwilligung der Betroffenen aufgrund der generellen Bewilligung der Expertenkommission Forschung betrieben werden.

Vermehrt ist in letzter Zeit behauptet worden, dass Daten für die Forschung nicht gelöscht werden dürfen, weil man zu einem späteren Zeitpunkt noch Erkenntnisse erlangen könnte, die für die Nachkommen wichtig sein könnten. Es wird auch immer wieder darauf hingewiesen, dass man bei vorhandenen Daten keine Einwilligungen mehr für neue Forschungszwecke einholen könne (solle), insbesondere weil der Aufwand dafür viel zu gross sei. Ein solches Vorgehen ist aber nicht datenschutzkonform. Je sensibler die zu bearbeitenden Personendaten sind, umso detaillierter sind die Betroffenen über die Datenbearbeitung zu informieren, damit sie verstehen können, wozu genau sie

ihre Einwilligung geben (Zweck, Umfang der Datenbearbeitung, Löschung etc.). Macht sich der Betroffene aufgrund der Informationen ein falsches Bild über die Einwilligung, so ist diese ungültig. Ein anderer Lösungsansatz besteht darin, Systeme aufzubauen, die den Forschenden anonyme Daten zur Verfügung stellen. Dies geschieht in vielen Fällen mit dem Einsatz von Pseudonymen. Werden die Pseudonyme und die dazugehörenden identifizierenden Informationen bei einer vertrauenswürdigen dritten Partei (Trusted Third Party, TTP) sicher verwaltet, so kann man davon ausgehen, dass der Forscher mit anonymisierten Daten arbeitet. In solchen Fällen wäre keine Einwilligung notwendig. Erst für eine allfällige Identifizierung der Personen für das Forschungsprojekt bräuchte es eine Einwilligung. Lösungsansätze dazu findet man in der Schriftenreihe der Telematikplattform für Medizinische Forschungsnetze mit der Bezeichnung «Generische Lösungen zum Datenschutz für Forschungsnetze in der Medizin / Generische Datenschutzkonzepte» der Autoren Reng, Debold, Specker und Pommerening vom März 2006 (siehe bspw. unter www.tmf-net.de, Produkte und Services).

## 1.6 Versicherungen

### 1.6.1 Case Management

**Im Rahmen eines Case Managements werden besonders schützenswerte Personendaten bearbeitet. Da Case Manager sowohl im Interesse des Auftraggebers als auch der betroffenen Person handeln und sich dabei Interessenskonflikte ergeben können, müssen die Grundsätze der Zweckbindung und der Transparenz besonders gewissenhaft beachtet werden.**

Case Management wird durch verschiedene Stellen betrieben. Speziell dabei ist, dass Case Manager einerseits von Versicherungen oder Arbeitgebern eingesetzt werden, um die durch einen Unfall oder Krankheit entstehenden Kosten möglichst gering zu halten, und andererseits die betroffene Person so betreuen sollen, dass sie wieder in den Arbeitsprozess integriert werden können. Dass dabei zwischen den Zielen der Versicherung oder des Arbeitgebers und den Zielen der betroffenen Person ein Interessenskonflikt entstehen kann, liegt auf der Hand.

Damit der Case Manager die Datenbearbeitung legal vornehmen kann, ist es besonders wichtig, dass er die betroffene Person über seine Rolle, seine Ziele, den Zweck der Datenbearbeitung und seinen Auftraggeber informiert. Zudem dürfen die Personendaten nur für die Zwecke verwendet werden, welche für die betroffene Person erkennbar sind. Case Manager dürfen sich somit gegenüber der betroffenen Person nicht als «Wohltäter» in einer schwierigen Situation präsentieren, sondern müssen für Transparenz sorgen – auch darüber, dass sich ihre Tätigkeit unter Umständen zum Nachteil des oder der Betroffenen auswirken kann.

### 1.6.2 Registrierung der Datensammlungen von Krankenkassen

**Die obligatorischen Krankenversicherungen gelten als Bundesbehörden und müssen ihre Datensammlungen bei uns anmelden oder einen Datenschutzverantwortlichen bezeichnen. Offenbar bestehen diesbezüglich gerade bei kleineren Krankenkassen noch Unklarheiten.**

Die anerkannten sozialen Krankenversicherer gelten gemäss DSG als Bundesorgane und müssen als solche sämtliche Datensammlungen bei uns registrieren. Von dieser Pflicht können sie sich befreien, indem sie einen Datenschutzverantwortlichen benennen, der unabhängig die betriebsinterne Einhaltung der Datenschutzvorschriften

überwacht und ein Verzeichnis der Datensammlungen führt. Eine in Zusammenarbeit mit dem Bundesamt für Gesundheit (BAG) durchgeführte Untersuchung hat gezeigt, dass einige Krankenversicherer ihrer gesetzlichen Verpflichtung nicht nachgekommen sind. Wir haben sie säumigen Versicherer kontaktiert und auf ihre gesetzliche Verpflichtung hingewiesen.

Unsere Intervention zeigte, dass die interne Benennung eines Datenschutzverantwortlichen, der das Kriterium der Unabhängigkeit erfüllt, gerade bei kleineren Krankenkassen schwierig sein kann. Trotzdem scheute ein Teil dieser Krankenversicherungen vorerst die Registrierung der Datensammlungen. Offenbar bestanden unbegründete Befürchtungen bezüglich der Offenlegung von Versicherungsdaten. Nach persönlichen Aufklärungsgesprächen entschieden sich einige Versicherungen dann doch dafür. In wenigen Fällen sind wir mit den Versicherern noch im Gespräch, weil sich bei ihnen die Situation aufgrund von Übernahmen oder anderen Sachverhalten noch unklar präsentiert.





### 1.6.3 Umfang des Akteneinsichtsrechts im UVG-Verfahren

**Auch im Fall der Überprüfung eines Rentenanspruchs kann der Versicherer Einsicht in Akten verlangen, welche aus dem Zeitraum vor der Rentenzusprechung stammen. Die Voraussetzungen der Verhältnismässigkeit müssen dabei gewahrt bleiben.**

Aufgrund der Anfrage eines Anwaltes befassten wir uns mit der Frage, ob es zulässig ist, dass ein Unfallversicherer im Fall einer Rentenüberprüfung Einsicht in medizinische Akten erhält, welche aus dem Zeitraum vor der Rentenzusprechung stammen. Der Anwalt war der Ansicht, dass der Unfallversicherer nach der Zusprechung einer Rente nur noch Anspruch auf Einsicht in Akten hat, welche nach dem Zeitpunkt der Rentensprechung entstanden sind.

Wir kamen zum Schluss, dass auch im Fall der Überprüfung eines Rentenanspruchs die Einsichtnahme in Akten, welche aus dem Zeitraum vor der Rentenzusprechung stammen, verhältnismässig ist, insofern die Akten für den konkreten Fall tatsächlich von Bedeutung sind. Wir mussten dabei berücksichtigen, dass der Unfallversicherer im UVG eine gesetzliche Grundlage für die Datenbearbeitung findet und dass die Person, welche einen Rentenanspruch geltend macht, ohnehin verpflichtet gewesen wäre, alle Informationen herauszugeben, welche für die Beurteilung des Rentenanspruchs relevant sind.

### 1.6.4 Merkblatt zum Einholen von Gutachten durch Haftpflichtversicherer

Das Merkblatt «Einholen von Gutachten durch Haftpflichtversicherer» haben wir an die aktuelle Rechtsprechung angepasst. Das Einholen eines Gutachtens durch einen Haftpflichtversicherer zur Klärung des Leistungsanspruchs ist auch ohne Zustimmung der betroffenen Person zulässig. Die Grundsätze der Zweckmässigkeit und der Transparenz müssen jedoch gewahrt bleiben. Der Versicherer hat die betroffene Person also über das Einholen eines Gutachtens und über den Zweck der damit verbundenen Datenbearbeitung zu informieren.

Das Merkblatt kann auf unserer Internetseite www.derbeauftragte.ch, Dokumentation – Datenschutz – Merkblätter, abgerufen werden.

### 1.6.5 Elektronische Datenbekanntgabe im AHV-/IV-Bereich

**Das Bundesamt für Sozialversicherung will die Datenbank eRegress für die kantonalen Ausgleichskassen bzw. IV-Stellen zugänglich machen, damit diese die an sie delegierten Aufgaben im Rahmen des Regresses in der AHV und IV elektronisch bearbeiten können. Obwohl wir das Bedürfnis verstehen, diese Daten im Abrufverfahren zur Verfügung zu stellen, konnten wir kein grünes Licht geben, da für Bundesorgane das Legalitätsprinzip gilt. Im geltenden Sozialversicherungsrecht sind die notwendigen gesetzlichen Grundlagen klar nicht vorhanden. Auch konnten wir die Kriterien für einen Pilotversuch nicht bejahen. Es muss also für die Öffnung der Bundesdatenbank eine genügende gesetzliche Grundlage im formellen Sinn geschaffen werden.**

Das Bundesamt für Sozialversicherung (BSV) hat Regressaufgaben in der AHV und IV an die kantonalen Ausgleichskassen bzw. IV-Stellen delegiert. Der erforderliche Datenaustausch erfolgt in Papierform. Nun will das BSV den kantonalen Stellen die elektronische Bearbeitung dieser Daten ermöglichen. Zu diesem Zweck soll ihnen die bestehende und beim EDÖB angemeldete Datenbank eRegress, welche das BIT entwickelt hat, zugänglich gemacht werden. Das BIT hat uns das Resultat der BSV-internen Datenschutzabklärungen zur Stellungnahme unterbreitet.

Wir haben in unserer Stellungnahme zwar bejaht, dass eine gesetzliche Grundlage für die Datenbearbeitung und -bekanntgabe in Papierform für den Regress im Bereich der AHV/IV besteht. Für die elektronische Zugänglichmachung, also die Datenbekannt-

gabe mittels Abrufverfahren hingegen haben wir festgestellt, dass eine gesetzliche Grundlage fehlt.

Der Gesetzgeber verlangt für Bundesorgane höhere gesetzliche Anforderungen für das Zugänglichmachen von Daten im Abrufverfahren, weil bei diesen das Gefährdungspotential für das Persönlichkeitsrecht der Betroffenen höher ist. Gemäss Art. 19 Abs. 3 DSG ist eine gesetzliche Grundlage, in welcher das Abrufverfahren ausdrücklich verankert ist, notwendig; für Gesundheitsdaten ist sogar ein Gesetz im formellen Sinn erforderlich. Es müssen die Organe, welche Zugang haben, bezeichnet werden, die Kategorien der abrufbaren Daten, die Zugangs- und Bearbeitungsberechtigung und der Zweck. Wir haben zwar in Art. 14 der Verordnung über den Allgemeinen Teil des Sozialversicherungsrechts (ATSV) eine gesetzliche Grundlage für das Outsourcing erkannt, nicht aber eine solche für die Bekanntgabe von Daten im Abrufverfahren.

Eine gemeinsame Führung der Datenbank im Sinne von Art. 16 Abs. 2 DSG haben wir als denkbar erachtet, hielten jedoch fest, dass sich eine entsprechende Bundesratsverordnung auch im Sozialversicherungsgesetz abstützen müsste, das die gemeinsame Führung der automatisierten Datenbank in den Grundzügen zu regeln hätte, während die Einzelheiten in der bundesrätlichen Verordnung festgehalten werden könnten. Ausserdem haben wir ausgeführt, dass auch für eine gemeinsam geführte Datenbank eine gesetzliche Grundlage im formellen Sinn vorhanden sein muss und eine Verordnung nicht genügt. Aus unserer Sicht konnten wir schliesslich auch die Kriterien für einen Pilotversuch nicht als erfüllt betrachten.



### 1.6.6 Sozialmissbrauchshotline

**Eine politische Partei hat eine Telefonnummer bekannt gegeben, auf der Bürgerinnen und Bürger angeblichen Sozialmissbrauch melden können. In diesem Zusammenhang tauchten verschiedene rechtliche Fragen auf. Wir haben festgehalten, dass zwar ein öffentliches Interesse an der Bekämpfung des Sozialmissbrauchs besteht, es aber ausschliesslich eine Aufgabe der zuständigen Behörden ist, solche Informationen zu bearbeiten.**

Nachdem durch die Medien bekannt geworden war, dass eine politische Partei eine Telefonnummer eingerichtet hat, über die Bürgerinnen und Bürger vermeintlichen Sozialmissbrauch melden können, haben wir zu dieser Problematik Stellung genommen. Dabei geht es um die Frage, ob Staatsaufgaben ohne ausdrücklichen gesetzlichen Auftrag auch von privaten Personen wahrgenommen werden dürfen. Eine ausdrück-

liche Ermächtigung für private Personen besteht, wenn sie gestützt auf das öffentliche Interesse am Kampf gegen den Sozialmissbrauch die zuständigen Behörden direkt benachrichtigen. Anders ist es hingegen, wenn die Anzeige an eine private Institution ergeht.

Wir haben festgestellt, dass im Bereich der Sozialversicherungsgesetzgebung des Bundes keine gesetzliche Grundlage besteht für die Delegation solcher sozialpolizeilicher Aufgaben an Private. Gleichzeitig und unabhängig von der Frage der Rechtsgrundlage kann gegen eine solche private Stelle von einer betroffenen Person Klage wegen widerrechtlicher Verletzung der Persönlichkeit eingereicht und die Löschung der gespeicherten Daten verlangt werden.

## 1.7 Arbeitsbereich

### 1.7.1 Datenschutz im Rahmen der Verwendung der elektronischen Infrastruktur in der Bundesverwaltung

**Die Bundesverwaltung verfügt über keine Rechtsgrundlage für die Bearbeitung der mit ihrer elektronischen Infrastruktur verbundenen Daten. Eine departementsübergreifende Arbeitsgruppe hat einen Entwurf für die Schaffung einer solchen Rechtsgrundlage ausgearbeitet.**

Für die Wahrnehmung ihrer Aufgaben hat die Bundesverwaltung in den letzten Jahren eine elektronische Infrastruktur eingerichtet (Computer, Netzwerke, Website, elektronische Post, usw.). Die Informationen werden elektronisch bearbeitet (zum Beispiel E-Mails) und die Nutzung dieser Infrastruktur erzeugt eine ganze Reihe elektronischer Spuren (zum Beispiel Logfiles).

Die mit der Verwendung der elektronischen Infrastruktur verbundene Datenmenge, einschliesslich der Sicherungskopien, ist gewaltig und hängt sehr häufig mit einer identifizierten oder identifizierbaren Person zusammen (persönliche E-Mail-Adresse, IP-Adresse, usw.). Ausserdem kann es sich bei den bearbeiteten Personendaten um besonders schützenswerte Daten handeln (zum Beispiel um den Inhalt privater E-Mails oder die Liste der besuchten Websites).

Für die Bearbeitung von Daten dieses Typs muss die Bundesverwaltung über eine formelle Gesetzesgrundlage verfügen, doch hat diese bisher gefehlt. Unter dem Gesichtspunkt des Datenschutzes ist diese Situation nicht vertretbar. Um diese Lücke zu beheben, wurde unter der Leitung des Bundesamtes für Justiz (BJ) eine Arbeitsgruppe geschaffen, an der das Bundesamt für Informatik und Telekommunikation (BIT), das Eidgenössische Justiz- und Polizeidepartement (EJPD), das Informatikstrategieorgan Bund (ISB), die Bundeskanzlei (BK), das eidgenössische Personalamt (EPA) und der EDÖB beteiligt sind.

Der erste Entwurf zur Abänderung des Regierungs- und Verwaltungsorganisationsgesetzes (RVOG) sah vor, dass die Bundesverwaltung befugt sein sollte, nach Belieben sämtliche mit der elektronischen Infrastruktur verbundenen Daten zu bearbeiten, sofern gewisse Voraussetzungen erfüllt sind. In der Vernehmlassung stiess der Entwurf auf heftige Kritik. Die Arbeitsgruppe änderte darauf hin ihre Sichtweise. Die zweite

Änderungsvorlage zum RVOG führt ein generelles Verbot der Bearbeitung der mit der elektronischen Infrastruktur verbundenen Daten ein, mit Ausnahmen. Unter dem Aspekt des Datenschutzes ist dieser zweite Vorschlag besser, denn er verpflichtet die Verantwortlichen der elektronischen Infrastruktur, zu bestimmen, welche Datenbearbeitungen notwendig sind.

### 1.7.2 Anwesenheitskontrolle mittels Fingerabdrücken

**Ein Unternehmen hat uns angefragt, wie ein System zur Kontrolle der Anwesenheit und zur Arbeitszeiterfassung von Mitarbeitenden mittels Fingerabdruck aufgebaut werden kann. Wir haben dem Unternehmen, um die Risiken bei der Bearbeitung von biometrischen Daten einzuschränken, empfohlen, nicht den Fingerabdruck selbst, sondern nur einen Extrakt daraus zu verwenden.**

Bei den Fingerabdrücken und den daraus extrahierten Merkmalen handelt es sich um biometrische Daten. Sie sind in aller Regel unverwechselbare Wesensmerkmale einer Person und lassen eine Verwendung durch unberechtigte Dritte nicht zu. Somit schränken biometrische Authentifizierungssysteme die Risiken der klassischen Stempelkarten (wie Verlust, Kopieren oder Diebstahl) stark ein.

Allerdings sollte anstelle des Fingerabdrucks nur ein Extrakt daraus verwendet werden, um die mit der Bearbeitung von biometrischen Daten verbundenen Sicherheitsrisiken gering zu halten. Dabei filtert man bestimmte Merkmale des Fingerabdrucks heraus, die sich eindeutig einer Person zuordnen lassen. So wird das Risiko einer Zweckentfremdung der Daten minimiert, während eine sichere Kontrolle der Anwesenheit und die Zeiterfassung der Mitarbeitenden gewährleistet bleibt. Die extrahierten Merkmale des Fingerabdrucks des Mitarbeiters sollten darüber hinaus auf einer Chipkarte lokal gespeichert werden. Der Aufbau einer zentralen Datenbank mit biometrischen Merkmalen, welche diversen Sicherheitsrisiken ausgesetzt ist, ist nicht nötig.

Mehrere Unternehmen haben ähnliche Anfragen zum Einsatz von biometrischen Merkmalen gestellt, was uns dazu veranlasst hat, einen Leitfaden zu biometrischen Erkennungssystemen zu verfassen, zu finden unter www.derbeauftragte.ch, Dokumentation – Datenschutz – Leitfäden.

### 1.7.3 Spionagesoftware am Arbeitsplatz

**Während des letzten Geschäftsjahres haben wir immer wieder Beschwerden über den Einsatz von diversen Computerprogrammen erhalten, die eine zeitlich lückenlose Überwachung von Arbeitnehmern am Arbeitsplatz erlauben. In allen Fällen konnten wir bewirken, dass die betroffenen Unternehmen ihre Praxis schliesslich datenschutzkonform gestalteten.**

Ein Grossteil der Beschwerden betrafen die heimliche Installation einer Software, welche eine rund-um-die-Uhr-Überwachung des Arbeitnehmers am Arbeitsplatz ermöglicht. Solche Programme verletzen die Privatsphäre des Betroffenen. Der Arbeitgeber ist zwar durchaus berechtigt, die Arbeitsleistung seiner Angestellten sowie den Gebrauch der dafür zur Verfügung gestellten Informatikmittel (PC, Email, Internet etc.) zu kontrollieren. Er hat jedoch kein Recht, seine Mitarbeiter auf Schritt und Tritt zu überwachen, sondern muss gewisse Regeln einhalten. So muss er einerseits klar kommunizieren, wie die Informatikmittel am Arbeitsplatz zu verwenden sind (Nutzungsreglement). Er muss transparent erklären, dass die Einhaltung des Reglements kontrolliert und ein Verstoss dagegen sanktioniert werden kann, wobei er auszuführen hat, was genau kontrolliert wird und mit welchen Mitteln.





Abgesehen von den Vorgaben des Datenschutzgesetzes sind auch die arbeitsrechtlichen Bestimmungen einzuhalten, welche eine permanente und heimliche Überwachung am Arbeitsplatz nicht erlauben oder sogar unter Strafe stellen.

Wir haben die Unternehmen angewiesen, ihre Praxis den datenschutz- und arbeitsrechtlichen Bestimmungen anzupassen.

### 1.7.4 Familienzulagen und Anmeldeformular

**Bereits im vergangenen Jahr haben wir die gesetzliche Einführung des Familienregisters begrüsst und zur entsprechenden Rechtsgrundlage keine Einwände vorgebracht. In der Folge haben wir aus der Bevölkerung mehrere Anfragen im Zusammenhang mit den verschiedenen Anmeldeformularen und den damit erhobenen Personendaten erhalten. Daher haben wir vorgeschlagen, die Anmeldeformulare einheitlich zu gestalten.**

Nachdem wir die gesetzliche Grundlage über die Familienzulagen gutgeheissen haben (vgl. unseren 16. Tätigkeitsbericht 2008/2009, Ziff. 1.7.1) und das Gesetz am 01.01.2009 in Kraft getreten ist, erhielten wir aus der Bevölkerung diverse Anfragen über die Sen-

sibilität der Personendaten, die mittels Familienzulagenformularen erhoben werden. In der Folge stellten wir fest, dass sich die Formulare zur Datenerhebung zwecks Beantragung solcher Zulagen inhaltlich sehr unterschieden. Weil mit diesen Formularen auch besonders schützenswerte Personendaten erhoben werden und die Praxis der verschiedenen Familienausgleichkassen unterschiedlich war, regten wir an, die Formulare schweizweit zu vereinheitlichen. Wir schlugen vor, den materiellen Inhalt der Antragsformulare auf gesetzlicher Ebene, im Familienzulagengesetz, zu regeln. Die Umsetzung und Anwendung dieses Gesetzes liegt zwar in der Verantwortung der kantonalen Ausführungsorgane. Unserer Ansicht nach tangiert aber die Vereinheitlichung des Inhalts der Formulare diese kantonale Aufsichtskompetenz nicht.

### 1.7.5 Gesundheitscheck für die Mitarbeiter der Post

**Die Post stellte uns ein Gesundheitsmanagementprojekt vor. Es bezweckt im Wesentlichen gesundheitliche Prävention, Absenzenmanagement und auch Case Management für Unfall- oder Krankheitsfälle. Dabei fallen Gesundheitsdaten der Arbeitnehmer an, die vom Arbeitgeber bearbeitet werden. Wir haben das Projekt analysiert und nichts dagegen einzuwenden, sofern aus datenschutzrechtlicher Sicht bestimmte Bedingungen eingehalten werden.**

Das Gesundheitsmanagementprojekt der Post dient der Gesundheitsvorsorge der Mitarbeiter, der Handhabung von Unfall- und Krankheitsfällen und der Verwaltung von Abwesenheiten. Die Post als Arbeitgeberin wird in diesem Zusammenhang Gesundheitsdaten der Mitarbeitenden und damit auch besonders schützenswerte Personendaten bearbeiten. Wir erklärten den Verantwortlichen, dass ein solches Projekt mit gesundheitspräventiven Massnahmen, abgesehen von der in der Invalidenversicherung vorgesehenen Früherfassung, nur im Rahmen der üblichen arbeitsrechtlichen Bestimmungen erfolgen darf. Denn eine gesetzliche Delegation der in der IV vorgesehenen Massnahmen an den Arbeitgeber ist nicht vorgesehen. Der Arbeitgeber braucht somit für ein solches Gesundheitsmanagementprojekt die Einwilligung der Arbeitnehmenden; und da es dabei nicht um die Erfüllung des Arbeitsvertrags geht, ist beiderseitige Freiwilligkeit Voraussetzung. Zwar obliegt dem Arbeitgeber eine Fürsorgepflicht, die auch Gesundheitsschutz und Gesundheitsprävention beinhaltet, jedoch beschränkt sich diese Pflicht auf arbeitstechnische Gegebenheiten und Probleme. Abweichungen sind denkbar, gehören jedoch in den Bereich der Ausnahmen (z.B. offensichtliche sich wiederholende gesundheitsbedingte Abwesenheiten). Andere Unterstützungsmassnahmen des Arbeitsgebers setzen grundsätzlich immer die Einwilligung der betroffenen Personen voraus.

Das bedeutet, dass das Gesundheitsmanagementsystem eines Unternehmens sowohl auf Arbeitgeberseite als auch auf Arbeitnehmerseite auf Freiwilligkeit basiert. Dabei sind die Arbeitnehmer explizit auf die Freiwilligkeit der Teilnahme hinzuweisen. Die Post hat das Konzept aufgrund unserer Bemerkungen angepasst.

### 1.7.6 Personal- und Videoreglement von Lidl

**Aufgrund von Medienberichten haben wir während des letzten Jahres die Praxis der Firma Lidl in Sachen Videoüberwachung und Durchsuchungen von Mitarbeitenden am Arbeitsplatz näher untersucht. Dabei stellten wir fest, dass die erforderliche Information an die Arbeitnehmer ungenügend war, während die Bearbeitung der Arbeitnehmerdaten datenschutzkonform erfolgte.**

In den Medien wurde berichtet, dass sich Lidl in Sachen Videoüberwachung und Durchsuchung von Mitarbeitenden am Arbeitsplatz nicht datenschutzkonform verhält. Daher haben wir von der Firma mehr Informationen zur Bearbeitung von Arbeitnehmerdaten verlangt. In der Folge haben wir Datenschutzkonzept, Personalreglement und Videoüberwachungserklärung der Firma analysiert. Es hat sich herausgestellt, dass die erforderlichen Informationen an die Mitarbeitenden für die Videoüberwachung und die Durchsuchungen präzisiert werden müssen. Die Firma Lidl hat die von uns vorgeschlagenen erforderlichen Änderungen vorgenommen.

### 1.7.7 «Mitarbeiter-Check» im Internet

**Auf dem Markt für Kredit- und Wirtschaftsinformationen herrscht ein starker Wettbewerb, der Unternehmen ständig zu neuen Innovationen zwingt. So bot eine Kreditauskunftei Personalverantwortlichen Bonitätsdaten über mögliche neue oder bereits angestellte Mitarbeitende zum Kauf an. Das Bundesverwaltungsgericht hat unseren Antrag auf vorsorgliche Massnahmen gegen diesen Dienst gutgeheissen.**

Mit dem Dienst «Mitarbeiter-Check» plante eine in der Schweiz ansässige Kreditauskunftei, bonitätsrelevante Informationen über Mitarbeitende an Personalverantwortliche zu verkaufen, um auf diese Weise ihre Kundenbasis auszuweiten. Noch während der Vorbereitungszeit zum Start des Dienstes erhielten wir aufgrund zahlreicher Werbemails der Kreditauskunftei davon Kenntnis. Da Mitarbeiterdaten durch Art. 328b OR besonders geschützt sind, haben wir sofort beim Bundesverwaltungsgericht interveniert und in Form einer provisorischen Massnahme beantragt, das Anbieten von

«Mitarbeiter-Check» sofort zu untersagen. Das Bundesverwaltungsgericht hat unser Begehren gutgeheissen, das Anbieten des Dienstes für drei Monate untersagt und uns aufgefordert, innerhalb dieser Frist eine Empfehlung zu erlassen. In der Folge teilte die Kreditauskunftei mit, sie werde den besagten Dienst definitiv nicht anbieten.

### 1.7.8 Zustellung von Pensionskassenausweisen

**Die Zustellungspraxis von Vorsorgeeinrichtungen, welche die persönlichen Pensionskassenausweise statt direkt ihren Versicherten deren Arbeitgeber zustellen, verletzt das Legalitätsprinzip und die sozialversicherungsrechtliche Schweigepflicht. Nachdem eine Vorsorgeeinrichtung unsere Empfehlung abgelehnt hat, haben wir einen Antrag auf Entscheid gestellt, über den nun das Departement des Innern entscheiden muss.**

Uns kam zu Ohren, dass eine Pensionskasse die persönlichen Pensionskassenausweise der Arbeitnehmer an eine vom Arbeitgeber angegebene Adresse sendet. Anschliessend verteilt der Arbeitgeber die nicht persönlich adressierten Ausweise an die Arbeitnehmer, wobei er die Möglichkeit erhält, vom Inhalt Kenntnis zu nehmen.

Wir sind der Meinung, dass diese indirekte Zustellungspraxis widerrechtlich ist. Die private Vorsorgeeinrichtung ist hier als Bundesorgan tätig und also bei der Bearbeitung von Daten an das Legalitätsprinzip gebunden. Demzufolge darf sie Daten nur bekannt geben, wenn dafür eine gesetzliche Grundlage vorhanden ist. Eine solche existiert jedoch nicht; kein Gesetz rechtfertigt die Bekanntgabe von Daten der versicherten Arbeitnehmer an deren Arbeitgeber. Zudem regelt das Bundesgesetz über die berufliche Alters-, Hinterlassenen- und Invalidenvorsorge (BVG) klar, wie die Datenbekanntgabe zu erfolgen hat, damit die Schweigepflichten eingehalten werden.

Da trotz mehrfachem Schriftwechsel keine einvernehmliche Lösung gefunden werden konnte, haben wir eine Empfehlung erlassen. Die Vorsorgeeinrichtung soll erstens die Zusendung der Pensionskassenausweise ihrer Versicherten an deren Arbeitgeber unverzüglich einstellen. Zweitens soll sie beim Versand der Ausweise gewährleisten, dass die Dokumente direkt und ausschliesslich an die versicherte Person gelangen. Die Vorsorgeeinrichtung hat die Empfehlung abgelehnt. Da sie als Bundesorgan tätig ist, haben wir am 27. August 2009 gemäss aufsichtsrechtlichem Verfahren betreffend Bundesorgane beim Eidgenössischen Departement des Innern (EDI) einen Antrag auf Entscheid in dieser Angelegenheit gestellt.

Wir sind der Meinung, dass sich die Vorsorgeeinrichtung weder auf Art. 86b BVG, noch Art. 331 Abs. 4 OR und auch nicht auf Art. 89bis Abs. 2 ZGB als gesetzliche Grundlage

berufen kann. Zudem ist nicht ersichtlich, zu welchem vorsorgerechtlichen Zweck der Arbeitgeber die persönlichen Vorsorgedaten und allenfalls die Gesundheitsdaten der Arbeitnehmer benötigt, weshalb die Datenbekanntgabe auch nach Art. 86a Abs. 5 BVG zweckwidrig ist. Schliesslich darf der Arbeitgeber auch unter dem Blickwinkel von Art. 328b OR keine Kenntnis von den persönlichen Vermögensverhältnissen und den Gesundheitsdaten seines Arbeitnehmers haben.

Folglich ist davon auszugehen, dass die Pensionskasse das Legalitätsprinzip verletzt, da sie einem Dritten ohne gesetzliche Grundlage Daten bekannt gibt. Da sich die Vorsorgeeinrichtung für die Datenbekanntgabe auf keine gesetzliche Ausnahme stützen kann, ist zudem von einer Verletzung der Schweigepflicht auszugehen. Der Entscheid des EDI liegt noch nicht vor. Er könnte sowohl von uns als auch von der betroffenen Vorsorgeeinrichtung an das Bundesverwaltungsgericht weiter gezogen werden.

Im Anhang Ziff. 4.1.5. ist der Antrag zum Entscheid an das EDI vom 27. August 2009 abgedruckt.

### 1.7.9 Personalreglement Publica

**Die Pensionskasse des Bundes hat für ihr Personal im Personalreglement eigene Datenschutzbestimmungen formuliert. Unsere im Rahmen der Ämterkonsultation geäusserten Einwände sind von der Publica übernommen worden.**

Die Pensionskasse des Bundes, Publica, hat sich entschieden, für ihr Personal eigene Datenschutzbestimmungen ins Personalreglement aufzunehmen. Im Rahmen der Ämterkonsultation haben wir festgestellt, dass das Reglement auf einer ungenügenden gesetzlichen Grundlage beruht. Weiter bemerkten wir, dass im Entwurf für Persönlichkeits- und Abklärungstests keine Informationspflicht enthalten war und eine Bestimmung über die Aufbewahrungsfrist dieser Testresultate fehlte.

Ausserdem war eine zeitlich unbeschränkte Frist für die Aufbewahrung der Daten vorgesehen. Auch war keine Frist für die Rücksendung von Bewerbungsunterlagen bestimmt worden. Zudem war ein Abrufverfahren vorgesehen, welches nicht klar regelte, welche Datensammlungen gemeint sind, was für Daten in welcher Sammlung und in welcher Form vorhanden sind, welchem Zweck sie dienen, wer Zugriff hat und wer verantwortlich ist. Schliesslich erkannten wir Unklarheiten bei der Bearbeitung von Gesundheits- bzw. medizinischen Daten.

Die Publica hat unsere Einwände aufgenommen und die Regelungen angepasst.

## 1.8 Handel und Wirtschaft

### 1.8.1 Anmeldepflicht für ausländische Inhaber einer Datensammlung

**Die Pflicht zur Anmeldung einer Datensammlung beim EDÖB ist eine öffentlich-rechtliche Bestimmung, auf welche das Territorialitätsprinzip Anwendung findet. Diese Pflicht entsteht für Privatpersonen, die regelmässig besonders schützenswerte Personendaten oder Persönlichkeitsprofile bearbeiten oder Personendaten an Dritte bekannt geben.**

Im Auftrag einer in Zürich ansässigen Anwaltskanzlei haben wir ein Gutachten zur Anmeldepflicht von Datensammlungen, welche sich im Ausland befinden, erstellt. Die Anfrage der Anwaltskanzlei erklärt sich aus dem Umstand, dass ein Teil der Datenbearbeitung in Spitälern in der Schweiz erfolgt und die Daten auf einen Server geschickt werden, der sich in den Niederlanden befindet und im Eigentum einer belgischen Firma steht. Die Pflicht zur Anmeldung einer Datensammlung gemäss Artikel 11a DSG ist eine öffentlich-rechtliche Bestimmung, auf welche das Territorialitätsprinzip anwendbar ist. Die Anmeldepflicht beschränkt sich somit auf Sachverhalte, die in der Schweiz stattfinden. Da im vorliegenden Fall keine regelmässige Bearbeitung von besonders schützenswerten Personendaten oder von Persönlichkeitsprofilen in der Schweiz erfolgt und keine regelmässige Datenbekanntgabe an einen Dritten stattfindet, sind wir zum Schluss gekommen, dass keine Pflicht zur Anmeldung der sich in den Niederlanden befindlichen Datensammlung besteht, obwohl ein Teil der Datenbearbeitung in der Schweiz erfolgt.



### 1.8.2 Erläuterungen zur Datenweitergabe bei Unternehmensfusionen

Unternehmensfusionen sind in der Wirtschaft an der Tagesordnung. Es liegt auf der Hand, dass dabei immer auch mit personenbezogenen Daten gearbeitet wird. In den verschiedenen Reorganisations- und Zusammenlegungsprozessen werden Personendaten übertragen und mannigfach bearbeitet. Dabei besteht vor allem das Risiko, dass Unberechtigte Zugriff auf personenbezogene Informationen erhalten, dass zu viele Daten (zu früh oder den falschen Personen) bekannt gegeben werden, oder dass die Personendaten plötzlich zweckentfremdet zum Einsatz kommen. Dabei gilt das Datenschutzgesetz selbstverständlich auch während Fusionen in allen Phasen. Wir haben diese Risiken umrissen und empfehlen Massnahmen zur Vermeidung allfälliger Per-

sönlichkeitsverletzungen. Die Erläuterungen dazu befinden sich im Anhang Ziff. 4.1.4 und können auf unserer Webseite www.derbeauftragte.ch, Themen – Datenschutz – Unternehmen, abgerufen werden.

### 1.8.3 Erläuterungen zum betrieblichen Datenschutzverantwortlichen

Die Revision des Datenschutzgesetzes, in Kraft seit 2008, ermöglicht den Unternehmen die Selbstregulierung. Wenn sie einen Datenschutzverantwortlichen ernennen und den EDÖB darüber informieren, dürfen sie künftig darauf verzichten, ihre Datensammlungen bei uns anzumelden. Position und Person des Datenschutzverantwortlichen müssen jedoch gewissen Kriterien genügen. Seine zentralen Aufgaben sind es, die Bearbeitung von Personendaten im Betrieb zu prüfen und wenn nötig zu korrigieren, und eine Liste aller vorhandenen Datensammlungen zu führen. Für diese Aufsichtsfunktion muss der Datenschutzverantwortliche unabhängig sein – er darf keine anderen Tätigkeiten ausüben, muss die notwendige fachliche Eignung aufweisen (und zwar im Bereich Datenschutz ebenso wie betriebsspezifische Fachkenntnisse), und er muss weisungsunabhängig arbeiten können sowie Schutz vor Sanktionen geniessen. Zudem muss er natürlich Zugang zu allen Datensammlungen, Datenbearbeitungen und notwendigen Informationen haben. Die Erläuterungen dazu befinden sich im Anhang Ziff. 4.1.3 und können auf unserer Website www.derbeauftragte.ch, Themen – Datenschutz – Unternehmen, abgerufen werden.





### 1.8.4 Bekanntgabe von Personendaten an Dritte durch Vereine zu Marketingzwecken

**Ein Schweizer Sportverband hat von seinen Mitgliedervereinen eine Liste sämtlicher Vereinsmitglieder angefordert. Die Daten sollten zu Marketingzwecken verkauft werden. Mehrere Vereine haben uns gefragt, ob das entsprechende Vorgehen korrekt sei und ob sie die Personendaten weiterleiten dürften. Wir erklärten ihnen, dass sie für eine Weitergabe die Einwilligung der betroffenen Personen benötigen, und forderten den Verband auf, die Vereine auf diese Rechtslage hinzuweisen und allfällige bereits gelieferte Daten keinesfalls zu verwenden. Die Aufgabe, die Einwilligung der einzelnen Mitglieder einzuholen, könnte der Verein im Rahmen eines Outsourcings aber an den Verband übertragen.**

Nicht zum ersten Mal haben wir uns mit der Weitergabe von Adressen und weiteren Personendaten von Vereinsmitgliedern an Dritte zu Marketingzwecken (z.B. an Spon-

soren) befasst (vgl. unseren 16. Tätigkeitsbericht 2008/2009, Ziff. 1.8.5). Vereine dürfen personenbezogene Daten nur an Dritte weitergeben, wenn diese Bekanntgabe für die Betroffenen erkennbar ist und sie eingewilligt oder sich nicht dagegen ausgesprochen haben. Die Vereine können eine solche Bekanntgabe in ihren Statuten festhalten oder im Einzelfall die Einwilligung einholen. Zudem müssen die Betroffenen darüber informiert werden, dass sie sich jederzeit einer derartigen Verwendung ihrer Personendaten zu Marketingzwecken widersetzen können.

Im Frühjahr 2009 hat ein Schweizer Sportverband seine Mitgliedervereine angeschrieben und, gestützt auf seine Statuten, eine Liste sämtlicher Vereinsmitglieder (inklusive Post- und Email-Adressen) angefordert. Diese Daten sollten zu Marketingzwecken genutzt werden. Zudem hat der Verband ausgeführt, dass die Weitergabe der Daten an Dritte (durch den Verband) in jedem Fall im Einklang mit dem DSG sei.

In der Folge haben mehrere regionale Vereine angefragt, ob das entsprechende Vorgehen korrekt sei. Insbesondere wollten sie wissen, ob sie die vom Verband gewünschten Personendaten weiterleiten durften oder sogar mussten. Wir haben die Vereine darauf aufmerksam gemacht, dass sie ihre Mitgliederdaten nur dann weitergeben dürfen, wenn dafür die Einwilligung der einzelnen Mitglieder vorliegt. Für nicht besonders schützenswerte Daten genügt eine implizite Einwilligung, welche mit einer Opt-out-Möglichkeit umgesetzt werden kann. Auf jeden Fall ist den Betroffenen der Empfänger und der Zweck der Datenbekanntgabe mitzuteilen sowie ein Widerspruchsrecht einzuräumen. Zudem haben wir betont, dass die Verwendung der Email-Adressen bei Massenwerbung dem Bundesgesetz gegen den unlauteren Wettbewerb (UWG) untersteht und unter anderem eine explizite Einwilligung (Opt-in) voraussetzt.

Wir haben zudem bei dem Verband interveniert und ihn aufgefordert, seine Vereine auf die korrekte Rechtslage hinzuweisen und allfällige bereits von den regionalen Clubs gelieferte Daten keinesfalls zu verwenden. Insbesondere darf er diese Daten nicht an weitere Dritte bekannt geben, solange nicht sichergestellt ist, dass die Weitergabe durch die Vereine an den Verband rechtmässig (also insbesondere mit Vorliegen der Einwilligung der einzelnen Mitglieder) erfolgt ist. Nur dann ist der Verband nämlich zur Bearbeitung und Weitergabe der Daten an Dritte berechtigt.

Anlässlich einer Sitzung hat uns der Verband mitgeteilt, dass bei der praktischen Umsetzung oftmals Probleme bestehen, da die Vereine meist weder über Kapazitäten noch den Willen verfügten, bei den Vereinsmitgliedern entsprechend um Einwilligung anzufragen. Wir haben ein mit dem DSG in Einklang stehendes Vorgehen vorgeschlagen: Die Vereine könnten die Aufgabe, die Einwilligung der einzelnen Mitglieder einzuholen, im Rahmen eines Outsourcings an den Verband übertragen. Der Verband kann aber die Adressdaten nur einmalig dazu verwenden, um im Namen des Vereins die

Einwilligung zur Datenverwendung durch den Verband zu erfragen. Nach der Anfrage darf der Verband nur noch diejenigen Personendaten bearbeiten, für welche er die Einwilligung der betroffenen Personen erhalten hat.

### 1.8.5 Informationsservice über Mieterbonität

**Nach unserer Empfehlung vom Dezember 2008 in Sachen «Mieter Check» haben wir mit der Firma Deltavista AG intensive Gespräche über die Umsetzung geführt. Anlässlich der Nachkontrolle im Herbst 2009 hat uns die Firma ein System vorgestellt und Unterlagen ausgehändigt, welche wir in der vorgezeigten Form als datenschutzrechtlich ausreichend und als den Empfehlungen entsprechend betrachtet haben. Demzufolge haben wir das aufsichtsrechtliche Verfahren beendet.**

Die Firma Deltavista AG bietet über die Internetplattform «Mieter Check» zugangsberechtigten Personen Bonitäts- und Wirtschaftsdaten von potenziellen Mieterinnen und Mietern an. So sollen Vermieter die Angaben von Interessenten prüfen können, um das Risiko von Mietzinsausfällen zu minimieren.

In der ursprünglichen Version hatte der «Mieter Check» zur Berechnung der Bonität eines betroffenen potentiellen Mieters einen Score verwendet – zwischen 250 und 700 Punkten und graphisch auf einer horizontalen Achse dreifarbig dargestellt (rot, gelb, grün) – der nicht nur die Zahlungserfahrungen und die Mobilität des Mieters, sondern auch die Zahlungserfahrungen des Umfeldes sowie soziodemographische Daten auswertete. Zusätzlich zu diesem Score wurden verschiedene weitere Elemente mit einer Einzelampel (rot, gelb, grün) bewertet, so beispielsweise die Bonität der Familienmitglieder, negative Firmenbeziehungen oder die durchschnittliche Wohndauer an einer Adresse. Diese Einzelampeln wurden in einer Gesamtampel zu einem Bonitätsrating des potentiellen Mieters verdichtet. Je nach Farbe dieser Entscheidungsampel empfahl der «Mieter Check» den Vertragsabschluss (grün), die Vornahme von Zusatzabklärungen (gelb) oder den Nichtabschluss (rot).

Unsere Sachverhaltsabklärung im Juni 2008 zeigte, dass die Deltavista AG gegenüber der ursprüngliche Version des «Mieter Checks» Anpassungen vorgenommen und insbesondere problematische Datenverknüpfungen entfernt hatte. So waren der Score mit den soziodemographischen Daten sowie die Blacklistenprüfung nicht mehr Teil der Bonitätsbeurteilung der betroffenen Person. Neben der Gesamtampel wurde ein Erläuterungstext eingeblendet und die Zahlungserfahrungen mit den Buchstaben A, B, C und D erläutert. Die Gesamtampel zeigte nur noch rot an, wenn negative Zahlungs-

erfahrungen der nachgefragten Person vorhanden waren oder wenn der Status dieser Person (minderjährig, bevormundet, verstorben) einem gültigen Vertragsabschluss entgegenstand.

Wir stellten in der überarbeiteten Version aber immer noch Mängel bei der Bonitätsrelevanz der angebotenen Daten (insbesondere die Bonitätsbewertung der Haushaltsmitglieder und ihre Verknüpfung mit der Bonität der betroffenen Person) sowie bei der Gewährung des Auskunfts- und Löschungsrechts fest. Deshalb haben wir am 16. Dezember 2008 eine Empfehlung erlassen (vgl. unseren 16. Tätigkeitsbericht 2008/2009, Ziff. 1.8.4). Nach intensiven Gesprächen mit der Deltavista AG über die Umsetzung dieser Empfehlung führten wir im Herbst 2009 bei der Firma eine Nachkontrolle durch. Im System, welches uns vorgeführt wurde, fliessen nur noch Daten der betroffenen Person in die Bonitätsbewertung ein. Es wird nun Kunden und betroffenen Personen gleichwertig mitgeteilt, welche Elemente in die Ampelbewertung einfliessen. Zudem wird erläutert, wie die Zahlungserfahrungen gewichtet werden und dass der Bonitätsbericht ein tagesaktueller Report ist, der stetigen Veränderungen unterworfen sein kann, weshalb eine Entscheidung allgemein nicht nur auf der Ampelbewertung basieren sollte. Wer das Auskunftsrecht geltend macht, erhält die selben Informationen wie der Kunde, der die Bonitätsdaten des potentiellen Mieters abfragt. Die Einzelampeln und die Gesamtampel sowie die übrigen Informationen sind für die betroffene Person transparent und sie kann erkennen, welche Daten die Firma im «Mieter Check» bearbeitet, weshalb sie von ihrem Recht auf Datenberichtigung und Datenlöschung Gebrauch machen kann. Aufgrund der vorgeführten Version und der ausgehändigten Unterlagen haben wir das Verfahren beendet.



### 1.8.6 Abklärungen bei einem Gentestanbieter

**Im Rahmen einer Kontrolle vor Ort haben wir bei einem Anbieter von Vaterschaftsanalysen und Genealogietests kleinere Mängel in Bezug auf die Transparenz festgestellt. Da die Firma in Zürich diese Mängel umgehend behoben hat, haben wir von einer Empfehlung abgesehen.**

Aufgrund zweier Hinweise haben wir bei einer Firma in Zürich, welche Vaterschaftstests und Herkunftsanalysen (Genealogietests) anbietet, eine Sachverhaltsabklärung durchgeführt. Der Firma wurde vorgeworfen, dass sie erstens die Resultate dieser Genealogietests trotz Löschungsantrag der betroffenen Personen weiter speichert, und dass sie zweitens die DNA-Proben ohne Zustimmung der betroffenen Personen für die Durchführung der Tests an ein Unternehmen in die USA schickt. Die Sachverhaltsabklärung konzentrierte sich somit auf die Bereiche Datenspeicherung in der Zürcher

Firma und Weitergabe von Speichelproben an eine US-Firma für DNA-Analysen im Rahmen der Genealogietests. Das Verfahren rund um die Vaterschaftsanalysen haben wir ebenfalls untersucht und konnten keine Verstösse gegen das DSG feststellen. Die Sachverhaltsabklärung in den Büroräumlichkeiten in Zürich hat ergeben, dass die Firma wenn möglich den Löschungsanträgen der betroffenen Personen nachkommt. Es werden lediglich die administrativen Daten der Kundinnen und Kunden weiterhin aufbewahrt, soweit dies für die Buchhaltung notwendig ist.

In Bezug auf die Weitergabe von DNA-Proben für Genealogietests an das Unternehmen in den USA haben wir festgestellt, dass die Information an die Kundinnen und Kunden mangelhaft gewesen ist. Wohl war auf der Internetseite der Firma erkennbar, dass es zum besagten Datenaustausch kommt; die Kundinnen und Kunden wurden aber in der Vereinbarung nicht ausdrücklich darauf hingewiesen. Aufgrund unserer Intervention hat die Firma diesen Mangel behoben und sowohl die Internetseite als auch die Analysevereinbarung entsprechend angepasst.

Die Sachverhaltsabklärung hatte zudem ergeben, dass die Firma in Zürich mit dem Unternehmen in den USA keinen schriftlichen Vertrag für die Analyse der DNA-Proben abgeschlossen hatte. Die Datensicherheit war somit nur ungenügend gewährleistet. Auch dieser Mangel wurde aufgrund unserer Intervention umgehend behoben. Unsere Abklärungen haben zudem gezeigt, dass die Partnerfirma in den USA Safe-Harbor-zertifiziert ist, wovon die Zürcher Firma aber keine Kenntnis hatte.

Zusammenfassend kann festgehalten werden, dass sich der Vorwurf der Datenbearbeitung trotz Löschungsantrag nicht erhärtet hat. In Bezug auf den Datenaustausch mit dem Unternehmen in den USA haben wir kleinere Mängel festgestellt, welche von der Firma in Zürich aber umgehend behoben wurden. Somit erübrigten sich weitere Schritte unsererseits.

## 1.9 Finanzen

### 1.9.1 Datenschutz im internationalen Zahlungsverkehr (SWIFT)

**Im Rahmen des Streits um den Zugriff auf Finanztransaktionsdaten durch die USA, welche auf den Servern des Finanzdienstleisters SWIFT gespeichert wurden, hat dieser zwei neue Rechenzentren in der Schweiz eröffnet. Auf diese Weise soll den Bedenken der europäischen Datenschutzbehörden und des EDÖB Rechnung getragen werden. Zudem verhandelten die USA mit der EU über ein Abkommen, welches ihnen im Rahmen der Bekämpfung des internationalen Terrorismus den Zugriff auf die in der EU gespeicherten SWIFT-Daten ermöglichen sollte.**

Über SWIFT wird der Grossteil der internationalen Finanz- und Wertschriftentransaktionen abgewickelt. Hierfür betrieb das Unternehmen bislang zwei Rechenzentren, welche identische Datensätze speichern und verarbeiten. Das eine liegt in Belgien, das andere in den USA. Auf dieses können die US-Behörden bei laufenden Verfahren im Rahmen der Terrorismusbekämpfung zugreifen. Da dort sämtliche Daten der SWIFT gespeichert werden, gelangen also auch Daten an die US-Behörden, die in keinem direkten Zusammenhang mit den USA stehen (beispielsweise rein innereuropäische oder, in wenigen Fällen, selbst innerschweizerische Überweisungen, die über SWIFT abgewickelt werden).

Vor diesem Hintergrund hat die SWIFT beschlossen, die Daten von rein europäischen Transaktionen künftig nur noch in Europa zu speichern, nämlich in Belgien und der Schweiz. Zu diesem Zweck hat sie zwei weitere Rechenzentren in der Schweiz aufgebaut. Das Ziel der SWIFT ist es, den USA den Zugriff auf den rein innereuropäischen bzw. innerschweizerischen Zahlungsverkehr zu entziehen. Wir begrüssen den Aufbau dieser Zentren in der Schweiz.

Die USA haben als Reaktion auf diese Entwicklung mit der EU ein Abkommen ausgehandelt, welches US-Terrorfahndern den Zugriff auf Daten der Europäischen Zone ermöglichen soll. Dieses Abkommen wurde jedoch vom Europäischen Parlament im Februar 2010 abgelehnt. Offen bleibt, ob sich die EU und die USA zu einem späteren Zeitpunkt auf eine Vereinbarung einigen können.

### 1.9.2 Doppelbesteuerungsabkommen

**Die Schweizer Banken sind aufgrund des Bankgeheimnisses und des Vorwurfs der angeblichen Beihilfe zur Steuerhinterziehung international in die Kritik geraten. Im Kampf gegen Steueroasen wurde die Schweiz von der OECD auf eine «graue Liste» gesetzt. Vor diesem Hintergrund hat der Bundesrat beschlossen, in Steuerhinterziehungsfällen von der heutigen Position abzurücken und mit ausgewählten Staaten bilaterale Verträge zu schliessen, welche eine verstärkte Zusammenarbeit in Steuerstrafsachen gewährleisten.**

Die Schweizer Gesetzgebung unterscheidet zwischen Steuerhinterziehung und Steuerbetrug. Weil bei Steuerhinterziehung in der Regel keine internationale Rechtshilfe gewährt wird, wurde die Schweiz als so genannte «Steueroase» bezeichnet und von der OECD auf eine «graue Liste» gesetzt. Daher hat der Bundesrat beschlossen, mit einer Reihe von Staaten bilaterale Verträge auszuhandeln, welche im Wesentlichen auch die internationale Rechtshilfe bei Steuerhinterziehungsfällen ermöglichen. Die notwendigen Voraussetzungen dazu sind, dass der ersuchende Staat den Rechtsweg im Inland ausgeschöpft hat und dass er konkrete Anhaltspunkte für eine Steuerhinterziehung vorweisen kann. So genannte «fishing expeditions» (wie z.B. Rasterfahndungen) werden aber explizit ausgeschlossen.

Wir haben die ausgehandelten Verträge geprüft und kommen zum Schluss, dass sie eine ausreichende gesetzliche Grundlage darstellen, um eine Zusammenarbeit mit den ausländischen Steuerbehörden zu ermöglichen. Allerdings geben wir zu bedenken, dass es dadurch natürlich vermehrt zu Anfragen von ausländischen Staaten kommen wird und mehr Personendaten zwischen den Behörden ausgetauscht werden.

### 1.9.3 Datenschutz im grenzüberschreitenden Forderungsverkauf

**Ein Start-Up-Unternehmen ist mit mehreren datenschutzrechtlichen Fragen zum grenzüberschreitenden Forderungsverkauf an uns gelangt. Aus Sicht des Datenschutzes ist dabei grundsätzlich zwischen der Forderungsabtretung, oder Zession, und dem Inkasso zu unterscheiden, da in diesen beiden Fällen unterschiedliche Anforderungen des DSG gelten.**

Bei der Anwendung des Datenschutzgesetzes (DSG) wird grundsätzlich zwischen der Datenbekanntgabe an Dritte (Art. 3 lit. f DSG) und der Datenbearbeitung durch Dritte (Art. 10a DSG; Outsourcing) unterschieden. Beim reinen Inkasso beauftragt der Gläubiger einen Dritten mit der Eintreibung seiner Forderung. Das Inkassounternehmen ist in

der Regel an die Weisungen des Gläubigers gebunden, der aber die Verfügungsmacht über die Forderung behält. Aus diesem Grund handelt es sich hier um ein Outsourcing gemäss Art. 10a DSG; der Gläubiger muss sich die Tätigkeiten des Inkassounternehmens zurechnen lassen und kann für dessen Datenschutzverletzungen zur Verantwortung gezogen werden.

Bei der Forderungsabtretung (Zession) geht die Forderung vom Vermögen des ursprünglichen Gläubigers (Zedent) auf dasjenige des neuen Gläubigers (Zessionar) über. Der Zedent verliert damit die Verfügungsmacht über die Forderung, er kann also die abgetretene Forderung weder geltend machen noch ein weiteres Mal abtreten. Der Zessionar steht aber nicht in einem Auftragsverhältnis zum Zedenten, sondern hat die Forderung erworben und kann daher selbst entscheiden, was damit weiter geschieht. Da er im eigenen Interesse die Forderung geltend machen, aufschieben oder erlassen kann, handelt es sich bei der damit verbundenen Datenbearbeitung nicht mehr um eine Datenbearbeitung durch Dritte (Outsourcing), sondern um eine Datenbekanntgabe an Dritte (gemäss Art. 3 lit. f DSG) durch den Zedenten. Vor diesem Hintergrund kann nach der Forderungsabtretung der Zedent nicht mehr für Datenschutzverletzungen des Zessionars zur Verantwortung gezogen werden.

Im Hinblick auf einen grenzüberschreitenden Datentransfer in ein Land, welches über kein angemessenes Datenschutzniveau gemäss Art. 6 Abs. 1 DSG verfügt, kann sich der Zedent auf Art. 6 Abs. 2 lit. c DSG berufen. Zwischen dem Zedenten und dem Schuldner besteht eine vertragliche Beziehung, wonach der Schuldner dem Gläubiger den geschuldeten Betrag leisten muss. Falls im Vertrag nichts anderes vereinbart wurde, steht es dem Zedenten frei, diese Forderung an einen Dritten (den Zessionar) zu verkaufen; er muss dies dem Schuldner (aufgrund des Erkennbarkeitsprinzips von Art. 4 Abs. 4 DSG) aber grundsätzlich anzeigen. Da der Schuldner zu Leistung des geschuldeten Entgelts verpflichtet ist, wird die Forderungsabtretung als unmittelbar im Zusammenhang mit dem Abschluss oder der Abwicklung des Vertrages stehend angesehen.



### 1.9.4 Totalrevision der Verordnung zum neuen Mehrwertsteuergesetz

**Die Verordnung zum neuen Mehrwertsteuergesetz (MWSTV) sieht ein Abrufverfahren vor. Im Bereich der Steuergesetzgebung gilt das Legalitätsprinzip und darüber hinaus das Steuergeheimnis. Unsere Bemerkung bezüglich des Abrufverfahrens bzw. unser Vorschlag einer separaten Datenschutzverordnung sind im Entwurf zur MWSTV völlig ausser Acht gelassen worden. Deshalb fehlt nun eine genügende gesetzliche Grundlage für das Abrufverfahren.**

Das neue Mehrwertsteuergesetz (MWSTG), welches vom Parlament am 12. Juni 2009 beschlossen wurde, trat am 1. Januar 2010 in Kraft. Der Entwurf zur Verordnung wurde Ende September 2009 in die Anhörung gegeben. Wir haben bereits bei der ersten internen Ämterkonsultation Ende August 2009 Stellung nehmen können. Dabei konstatierten wir eine Verletzung des Legalitätsprinzips. Wir bemängelten, dass weder im MWSTG noch in der Verordnung eine genügende gesetzliche Grundlage für das Abrufverfahren gegeben ist, und unterstrichen, dass ein solches Verfahren keineswegs in einer Departementsverordnung geregelt werden darf. Eine derartige Subdelegation widerspricht klar dem Legalitätsprinzip in Art. 19 Abs. 3 DSG und ist somit verfassungswidrig.

Wir haben empfohlen, wenigstens in der Verordnung die Datenbearbeitung, die Datenbekanntgabe und das Abrufverfahren genügend präzise zu regeln. Zudem haben wir, um die geplante Inkraftsetzung der Verordnung nicht zu gefährden, vorgeschlagen, die Einzelheiten der Datenbearbeitung und insbesondere das Abrufverfahren in einer separaten Verordnung zu regeln und in einem Anhang zu präzisieren (analog der Datenbearbeitungsverordnung der Eidgenössischen Zollverwaltung). Bei diesem Vorgehen würde die geplante Inkraftsetzung der Mehrwertsteuerverordnung aus unserer Sicht einerseits nicht verzögert, andererseits hätte man genügend Zeit für die Ausarbeitung der datenschutzrechtlich erforderlichen Normen.





In der zweiten Ämterkonsultation wurden unsere Einwände und unser Vorschlag einer separaten Datenschutzverordnung nicht berücksichtigt. Es ist weder aus dem Gesetz noch aus der Verordnung ersichtlich, welche und wie viele Informationssysteme bestehen, welche Daten genau diese Systeme beinhalten, welchem Zweck sie dienen, wer genau zuständig ist und wer auf welche Daten bzw. Informationssysteme Zugriff hat. Das Legalitätsprinzip soll nach dem Willen des Gesetzgebers dazu beitragen, dass der Bürger sein Verhalten nach dem Gesetz richten und die Folgen seines Tuns mit einem den Umständen entsprechenden Grad an Bestimmtheit erkennen kann. Zudem ist das Erfordernis der Transparenz seit der Revision des DSG im Jahr 2008 mit der Aufnahme des Grundsatzes der Erkennbarkeit in Art. 4 Abs. 4 DSG umso höher zu gewichten.

Wir haben an unserer Position hinsichtlich des Abrufverfahrens festgehalten. Es erstaunt, dass das EFD dem Bundesrat nun eine Verordnung unterbreitet, deren datenschutzrechtliche Normen verfassungswidrig sind. Sie verletzen den allgemeinen Grundsatz der Erkennbarkeit, womit von einer widerrechtlichen Persönlichkeitsverletzung auszugehen ist. Aus unserer Sicht ist die fehlende Kooperationsbereitschaft gegenüber dem EDÖB umso unverständlicher, als im Bereich der Steuergesetzgebung ausserdem das Steuergeheimnis gilt und datenschutzkonforme Normen, insbeson-

dere für die Datenbekanntgabe, eigentlich im ureigenen Interesse der Steuerverwaltung selbst liegen müssten. Die übrigen Anregungen sind grundsätzlich berücksichtigt worden. Besonders hervorzuheben und aus unserer Sicht begrüssenswert ist der Vorschlag, wonach ein eigener Datenschutzberater im Bereich Mehrwertsteuer eingesetzt werden soll.

### 1.9.5 Verhältnismässigkeit von Bonitätsdatenbearbeitungen

**Kreditauskunfteien entnehmen betreibungsrechtliche Informationen aus Betreibungsregisterauszügen. Das Bundesgesetz über Schuldbetreibung und Konkurs (SchKG) legt keine Pflichten gegenüber Datenempfängern wie Auskunfteien fest. Trotzdem dürfen diese betreibungsrechtlichen Daten nicht beliebig lange in privaten Registern bearbeitet und weitergegeben werden. Wir haben nun die Frage der Verhältnismässigkeit der Bearbeitungsdauer durch Kreditauskunfteien in einem Gutachten klären lassen. Es hält fest, dass das SchKG bei der datenschutzrechtlichen Verhältnismässigkeitsprüfung der klare Schranken setzt.**

Auskunfteien erhalten Informationen über betreibungsrechtliche Vorgänge aus den Betreibungsregisterauszügen, welche durch die kantonalen Ämter gestützt auf Art. 8a des Bundesgesetzes über Schuldbetreibung und Konkurs (SchKG) erstellt werden. Die Schranken, an welche sich diese Ämter bei der Datenbekanntgabe halten müssen, finden sich in den Artikeln 8a und 149a SchKG.

Die Bearbeitung betreibungsrechtlicher Daten in privaten Registern der Kreditauskunfteien spielt im heutigen Wirtschaftsleben eine immer grössere Rolle, da viele Vertragspartner Einsicht in private Datenbanken von Auskunfteien nehmen, statt einen aktuellen öffentlich-rechtlichen Betreibungsregisterauszug zu konsultieren. Wir wollten die Frage der Verhältnismässigkeit in der Bearbeitung betreibungsrechtlicher Daten durch private Weiterbearbeiter (wie Auskunfteien) klären lassen und beauftragten einen externen Gutachter. Er untersuchte und bewertete anhand der Praxis eines Unternehmens, das sich zur Zusammenarbeit bereit erklärt hatte, die Verhältnismässigkeit der Bonitätsdatenbearbeitung.

Um es vorweg zu nehmen: Der Gutachter hat die Datenbearbeitung des untersuchten Unternehmens als verhältnismässig beurteilt und ihm empfohlen, bei den Vorgängen, welche nach Art. 8a Abs. 3 SchKG nicht bekannt geben werden dürfen bzw. nach Art. 149a Abs. 3 SchKG zu löschen sind, entweder die Bewertung zu löschen oder sie auf den Wert 0 zu setzen. Das Unternehmen hat die Empfehlung akzeptiert und wird sie umsetzen. Im Rahmen der Abklärungen stellte der Gutachter fest, dass die Datenbe-

kanntgabe durch die Betreibungsämter nicht einheitlich erfolge und auch Daten unzulässig an Dritte bekannt gegeben werden. Weiter empfahl uns der Gutachter, darauf hinzuwirken, dass die Umsetzung des SchKG durch die verschiedenen Betreibungsämter vereinheitlicht werde und dass es auf Bundesebene zu einer verstärkten Inspektionstätigkeit komme.

Der Gutacher führte weiter aus, dass die unbefriedigende Umsetzung der SchKG-Vorgaben zwar nicht den Datenempfängern, also den Auskunfteien, angelastet werden könne, da das SchKG für sie keine Pflichten festlegt. Das heisse aber nicht, dass sie die betreibungsrechtlichen Daten beliebig lang bearbeiten könnten. Das SchKG markiere klare Schranken für die Datenbekanntgabe und lege auch die Richtung fest, in welcher die Verhältnismässigkeit der Datenbearbeitung nach DSG geprüft werden sollte.

Wir haben in der Folge zum Ersten die zuständige Dienststelle für die Oberaufsicht SchKG und Konkurs im Bundesamt für Justiz über die Ergebnisse des Gutachtens informiert. Wie bereits bei den Ämterkonsultationen zur Revision des SchKG (vgl. unseren 16. Tätigkeitsbericht 2008/2009, Ziff. 1.8.1) wiesen wir auch jetzt darauf hin, dass Betreibungsdaten und deren Weitergabe durch Auskunfteien an Dritte im heutigen Wirtschaftsleben zunehmend bedeutsamer werden. Da diese Daten vermehrt privat nachgefragt werden, gibt es einen engen Zusammenhang zwischen ihrer staatlichen Bearbeitung durch die Betreibungsämter, ihrer Weitergabe an Privatpersonen und ihrer privatrechtlichen Bearbeitung durch die Auskunfteien. Die gesetzlichen Rahmenbedingungen und die Umsetzung des SchKG beeinflussen die Aufsichtstätigkeit des EDÖB über Auskunfteien erheblich, weshalb wir die Oberaufsichtsbehörde baten, geeignete Massnahmen zu prüfen, damit die Betreibungsämter das SchKG korrekt anwenden und bei der Weitergabe von Betreibungsdaten an Dritte nicht nur eine einheitliche Terminologie benutzen, sondern auch eine einheitliche Praxis verfolgen. Dadurch würde auch das kostenintensive Korrekturverfahren der Privatpersonen, die ihre Daten bei jeder einzelnen Kreditauskunftei korrigieren lassen wollen, reduziert.

Zum Zweiten verfassten wir ein Rundschreiben an die Auskunfteien, um sie über die Ergebnisse des Gutachtens und unser Schreiben an die Oberaufsichtsbehörde zu informieren. Ausserdem teilten wir mit, dass wir in der Frage, wie lange die Bearbeitung betreibungsrechtlicher Daten durch die Auskunfteien verhältnismässig sei, die gesetzlichen Schranken nach SchKG als Richtmass betrachten werden. Wir forderten zudem die Auskunfteien auf, uns mitzuteilen, ob ihre Datenbearbeitung in dieser Hinsicht unseren Vorgaben entspricht. Die Reaktionen auf das Rundschreiben fielen sehr unterschiedlich aus. Der EDÖB prüft nun das weitere Vorgehen.

## 1.10 International

### 1.10.1 Internationale Zusammenarbeit

Ein wirksamer Datenschutz setzt auch die Zusammenarbeit der Datenschutzbehörden auf internationaler Ebene und die Entwicklung von grenzüberschreitenden Normen voraus. Es muss nämlich möglich sein, im Falle von transnationalen Datenbearbeitungen, mit denen wir zunehmend konfrontiert sind, abgestimmte Antworten zu erteilen und allen Personen, unabhängig von ihrem Wohnsitz, die gleichen Rechte zu gewährleisten. Zu diesem Zweck beteiligt sich der eidgenössische Datenschutzbeauftragte an den Arbeiten des Europarates, der europäischen Konferenz und der internationalen Konferenz der Datenschutzbeauftragten, der gemeinsamen Kontrollinstanzen Schengen und Eurodac sowie an der frankophonen Vereinigung der Datenschutzbehörden.

#### Europarat

Aktiv beteiligt haben wir uns an den Arbeiten des beratenden Ausschusses für das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (T-PD, Übereinkommen 108) und seines Büros. Der beratende Ausschuss prüfte in erster Lesung den Entwurf einer Empfehlung über den Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten im Rahmen der Profilierung.

Mit dieser Empfehlung soll ein angemessener und kohärenter rechtlicher Rahmen abgesteckt werden, der ein ausgewogenes Verhältnis zwischen dem Datenschutz und den legitimen Interessen gewährleistet, welche die Erstellung von Personenprofilen rechtfertigen können. Der T-PD hat auch sein Arbeitsprogramm für die kommenden Jahre verabschiedet. Geplant ist insbesondere die Prüfung einer Ergänzung des Übereinkommens 108, namentlich um zum Einen die Herausforderungen anzugehen, die durch die technologischen Entwicklungen in Verbindung mit dem Internet entstehen, und zum Anderen um die Mechanismen für die Umsetzung des Übereinkommens zu verbessern. Der Ausschuss könnte auch eine verbindliche Rechtsurkunde im Bereich der polizeilichen und gerichtlichen Zusammenarbeit in strafrechtlichen Angelegenheiten vorbereiten.

#### Europäische Konferenz der Datenschutzbeauftragten

Die Jahreskonferenz der europäischen Datenschutzbeauftragten, zu der die Datenschutzbehörden der Mitgliedstaaten der EU und des Europarates sowie der europä-

ische Datenschutzbeauftragte und die gemeinsamen Kontrollinstanzen im Bereich der Polizei und Justiz zusammenkommen, fand auf Einladung des britischen Datenschutzbeauftragten in Edinburgh statt. Unter dem Thema «Verbesserung des Datenschutzes unter Berücksichtigung der Vorteile und Schwächen der europäischen Datenschutzgesetzgebung» debattierten die bei der Konferenz vertretenen Behörden über die Zweckmässigkeit einer Änderung der bestehenden Texte und namentlich der europäischen Richtlinie. Sie gelangten zu dem Schluss, dass das Schwergewicht auf eine verbesserte Anwendung der geltenden Bestimmungen gelegt werden müsse.

Die Konferenz verabschiedete eine Erklärung, in der die Rolle hervorgehoben wird, welche Europa bei der Förderung des Datenschutzes weltweit weiterhin wahrnehmen muss, und die an das Engagement der Datenschutzbehörden für die Weiterentwicklung eines hohen Schutzniveaus erinnert. Des Weiteren nahm die Konferenz eine Resolution an, in der die europäischen Staaten aufgefordert werden, die Einhaltung des vollen Ausmasses des Datenschutzes beim Datenaustausch mit Drittstaaten zu gewährleisten, namentlich durch die Aufnahme ausreichender Garantien in die internationalen Abkommen. Die Konferenz beauftragte die Arbeitsgruppe Justiz und Polizei mit der Ausarbeitung einer Musternorm für den Datenschutz.





### Koordinationsgruppe für die Eurodac-Kontrolle

Die Koordinationsgruppe für die Eurodac-Kontrolle, welcher der europäische Datenschutzbeauftragte und die nationalen Datenschutzbeauftragten angehören, hat ihre zweite gemeinsame Überprüfung der Eurodac-Datenbank abgeschlossen. Diese enthält die Fingerabdrücke der Asylbewerber zur Erleichterung des Asylverfahrens in der Europäischen Union, den Ländern des Europäischen Wirtschaftsraums und der Schweiz. Die Inspektion bezog sich auf das Auskunftsrecht der betroffenen Personen und auf die Methoden zur Ermittlung des Alters der jungen Asylsuchenden im Hinblick auf ihre Registrierung in der Datenbank.

Der von der Koordinationsgruppe veröffentlichte Bericht präsentiert die Ergebnisse der Überprüfung (http://www.edps.europa.eu, unter Aufsicht – Eurodac). Die Gruppe richtet Empfehlungen an die Mitgliedstaaten und die europäischen Behörden. Sie ist insbesondere der Ansicht, dass die den Asylbewerbern erteilten Auskünfte über ihre Rechte und die Verwendung ihrer Daten relativ unvollständig sind. Die Qualität der erteilten Auskünfte ist je nach Staat unterschiedlich. Überdies werden in der Regel die Asylbewerber besser informiert als die illegalen Einwanderer. Die Gruppe empfiehlt daher eine Verbesserung der Qualität der erteilten Auskünfte und der Art der Informationsvermittlung. Die Datenschutzbehörden müssen für entsprechende Weisungen an

die zuständigen Behörden sorgen, damit der Auskunftspflicht Genüge getan wird. So ist die Einschätzung des Alters junger Asylbewerber für die zuständigen Behörden oft schwierig. Gemäss dem Eurodac-Reglement müssen die Fingerabdrücke von Asylbewerbern ab dem Alter von 14 Jahren abgenommen werden. Die für die Ermittlung des Alters angewendeten Methoden sind nicht genügend harmonisiert, transparent und verlässlich. Eine Gesamtbeurteilung der Verlässlichkeit der verschiedenen eingesetzten Methoden wäre angebracht. Die Gruppe empfiehlt auch, das Alter für die Abnahme von Fingerabdrücken auf 18 Jahre anzuheben. Die Koordinationsgruppe hat eine dritte Überprüfung des gesicherten Systems für den Informationsaustausch Dublinet begonnen, deren Resultate 2010 veröffentlicht werden sollen.





### Gemeinsame Kontrollinstanz Schengen

Die gemeinsame Kontrollinstanz Schengen (GK) besteht aus zwei Vertretern der nationalen Datenschutzbehörden aller Staaten, die das Durchführungsübereinkommen zum Schengener Abkommen unterzeichnet haben. Die Schweiz ist durch den EDÖB und durch die kantonalen Datenschutzbehörden vertreten. Die GK konzentriert ihre Tätigkeit auf die korrekte Auslegung des Schengener Abkommens. Auf der Grundlage koordinierter Inspektionen prüft sie, ob die Schengen-Staaten die für den Datenschutz geltenden Bestimmungen einhalten. Die GK hat weiter die Aufgabe, sich zu den Entwicklungen im Bereich der Einwanderungskontrolle und der Bekämpfung neuer Formen der Kriminalität zu äussern. Sie ist auch mit der Behandlung von Beschwerden von Privatpersonen betraut. Die GK hat ihren 8. Tätigkeitsbericht für den Zeitraum Dezember 2005 bis Dezember 2008 veröffentlicht (siehe unsere Webseite www.derbeauftragte.ch, Themen – Datenschutz – Schengen/Dublin).

Die GK hat zwei Überprüfungen betreffend die Anwendung von Artikel 97 (Ausschreibung von vermissten Personen und von Personen, die im Interesse ihres eigenen Schutzes oder zur Gefahrenabwehr in Gewahrsam genommen werden müssen) und von Artikel 98 (Bearbeitung der Daten von Zeugen oder von Personen, die im Rahmen eines Strafverfahrens vor Gericht erscheinen müssen) des Schengen-Abkommens abgeschlossen.Die Berichte und die aus diesen Überprüfungen hervorgegangenen Empfehlungen sind veröffentlicht worden (siehe unsere Webseite www.derbeauftragte.ch, Themen – Datenschutz – Schengen/Dublin). Die an die Schengen-Staaten gerichteten Empfehlungen zielen auf eine Verbesserung des Ausschreibungsverfahrens ab.

Die GK empfiehlt namentlich:

- in den Schengen-Staaten formelle, schriftlich festgelegte Verfahren für alle Behörden einzuführen, die an der Eingabe von Ausschreibungen beteiligt sind;

- in allen Fällen, in denen verschiedene Behörden an der Eingabe von Ausschreibungen beteiligt sind, die Kohärenz der Verfahren und ihre einheitliche Anwendung sicherzustellen;
- für die Übermittlung von Daten zu einer ausgeschriebenen Person im Sinne von Art. 97 deren schriftliche Einwilligung oder zumindest die Existenz eines urkundlichen Nachweises darüber vorauszusetzen;
- sicherzustellen, dass eine Verweigerung der Einwilligung schriftlich erfolgt und amtlich protokolliert wird;
- Daten zu Minderjährigen automatisch zu kontrollieren und offizielle Verfahren einzurichten, um zu verhindern, dass Minderjährige nach Eintritt der Volljährigkeit weiter ausgeschrieben bleiben;
- die Einhaltung der Bestimmungen betreffend die Überprüfung und Erfassungsdauern zu verbessern (Art. 98);
- zu prüfen, ob die nationalen Behörden, die Zugriff auf Ausschreibungen haben, tatsächlich dazu befähigt sind.

Die GK hat auch einen Leitfaden zu den Rechten der betroffenen Personen aufgearbeitet, der demnächst veröffentlicht wird.

Weitere Berichte zu Schengen befinden sich in Ziff. 1.4.





### Internationale Konferenz der Datenschutzbeauftragten

Die 31. Internationale Konferenz der Datenschutzbeauftragten fand vom 3. bis 5. November 2009 in Madrid statt (www.privacyconference2009.org), auf Einladung der spanischen Datenschutzbehörde. Rund 1500 Teilnehmer aus der ganzen Welt, die Datenschutzbehörden, internationale Organisationen, verschiedene Sektoren der Wirtschaft und akademische und wissenschaftliche Kreise vertraten, beteiligten sich an den Arbeiten.

Die Konferenz bietet die Möglichkeit, mit den zuständigen Behörden der fünf Kontinente aktuelle, im gemeinsamen Interesse liegende Themen oder auch Fragen betreffend die Modalitäten der Zusammenarbeit anzugehen. Die Konferenzteilnehmer befassten sich mit den aktuellen Herausforderungen, die sich für den Datenschutz im Bereich der Sicherheitspolitiken, der sozialen Netzwerke und der Informations- und Kommunikationstechnologien in einer vernetzten und globalisierten Welt stellen. Die Datenschutzbehörden, die Vertreter der Zivilgesellschaft, der Wirtschaft und der In-

dustrie sind sich einig bezüglich der Notwendigkeit, einen harmonisierten Rahmen für den Datenschutz ungeachtet jeglicher Grenzen zu schaffen. So haben die Datenschutzbeauftragten von rund 50 Staaten einstimmig eine Resolution verabschiedet, in der ein internationaler Normenentwurf für den Datenschutz und den Schutz der Privatsphäre begrüsst wird, zu dessen Ausarbeitung wir aktiv beigetragen haben (siehe unsere Webseite www.derbeauftragte.ch, Themen – Datenschutz – Internationale Zusammenarbeit).

Dieser Entwurf ist eine wichtige Etappe in der Ausgestaltung der Zielsetzungen der anlässlich der 27. internationalen Konferenz im September 2005 angenommenen Erklärung von Montreux, die namentlich die Annahme eines universellen verbindlichen Rechtsinstruments vorsieht. Der Text soll dazu beitragen, unter all den Herangehensweisen im Datenschutz einen gemeinsamen Nenner zu bestimmen. Er führt die Grundprinzipien des Datenschutzes auf, die den verschiedenen Regionen der Welt und den unterschiedlichen Rechtssystemen gemeinsam sind. Er umschreibt die Rechte der betroffenen Personen. Auch legt er die Betonung auf die Umsetzung der Datenschutzanforderungen und befürwortet namentlich aktive Massnahmen und die Einrichtung von unparteiischen und unabhängigen Aufsichtsbehörden, die insbesondere über ausreichende Kompetenzen, über Eingriffs- und Untersuchungsbefugnisse und über angemessene Ressourcen verfügen.





Nun ist es Aufgabe der Regierungen und der internationalen Organisationen, in einer Rechtsurkunde die im internationale Normenentwurf aufgeführten Grundsätze zu verankern und zu konkretisieren. Dieser Entwurf bildet auch einen Referenztext für Staaten, die am Anfang ihrer gesetzgeberischen Verfahren im Bereich des Datenschutzes stehen. Die internationale Konferenz wird ihre Arbeiten im Hinblick auf den Abschluss einer solchen Urkunde fortführen. Unter diesem Gesichtspunkt erscheint es uns dringlich, die Förderung des Übereinkommens des Europarates und seines Zusatzprotokolls noch aktiver zu unterstützen und Staaten, die nicht Mitglied des Rates sind, zu einem Beitritt zu diesen beiden Urkunden aufzufordern.

Die Konferenz nahm auch einstimmig eine von uns eingebrachte Resolution an, die auf die Verstärkung der internationalen Zusammenarbeit auf weltweiter Ebene im Bereich Datenschutz und des Schutzes der Privatsphäre abzielt (siehe Anhang Ziff. 4.1.9). Es geht insbesondere um eine Intensivierung der Zusammenarbeit zwischen den Datenschutzbehörden, die in Anbetracht der technologischen Entwicklungen, welche keine Grenzen kennen, als Regulatoren unerlässlich sind. Die Datenschutzbehörden stehen vor einer zweifachen Herausforderung: Zunächst müssen sie darauf achten, dass der bestehende Datenschutz in Ländern, die über eine Gesetzgebung in diesem Bereich

verfügen, nicht geschwächt wird. Sodann müssen sie zu dem Bemühen beitragen, sämtliche Länder der Welt zur Anerkennung und Anwendung dieses Schutzniveaus zu veranlassen, damit allen Personen die gleichen Rechte in Sachen Bearbeitung von Personendaten gewährleistet werden.

Die Globalisierung der Beziehungen, die Entwicklung der Informations- und Kommunikationstechnologien oder die Online-Schaltung von Diensten mit universeller Reichweite, wie die verschiedenen Dienste von Google oder die sozialen Netzwerke, oder auch das Aufkommen einer Überwachungsgesellschaft und die Entwicklung der damit einhergehenden Informationssysteme erfordern koordinierte und einheitliche Antworten und Lösungen zur Festlegung der Bedingungen, die unter dem Gesichtspunkt des Datenschutzes und des Rechts auf Achtung der Privatsphäre einzuhalten sind. Zur Erreichung dieser Ziele wird die Konferenz ihre Strukturen und ihre Arbeitsweise überdenken. Sie könnte sich mit einem ständigen Sekretariat ausstatten.





### Frankophone Vereinigung der Datenschutzbehörden

Wir sind auch in der frankophonen Vereinigung der Datenschutzbehörden (Association francophone des autorités de protection des données, AFAPDP) aktiv, in der wir einen der drei stellvertretenden Vorsitze innehaben. Die AFAPDP hielt ihre 3. Generalversammlung am Rande der 31. Internationalen Konferenz in Madrid ab. Dieser Versammlung ging eine frankophone Konferenz und ein Treffen mit dem ibero-amerikanischen Netzwerk der Datenschutzbehörden voraus.

Diese beiden Netzwerke verabschiedeten eine gemeinsame Erklärung, in der sie namentlich ihren Willen zum Ausdruck bringen, aktiv zur Verstärkung der internationalen Zusammenarbeit im Bereich des Datenschutzes beizutragen. Ausserdem unterstützen sie die Entwicklung internationaler Instrumente, um vorhandene Divergenzen unter den verschiedenen nationalen und regionalen Rechtsstrukturen im Datenschutz abzubauen und weltweit ein hohes Schutzniveau zu gewährleisten, unter gleichzeitiger Mitwirkung an der Beseitigung von Hindernissen für einen flüssigen und sicheren Informationsaustausch auf internationaler Ebene. Die beiden Netzwerke werden ihre Zusammenarbeit künftig fortsetzen und weiter entwickeln.

Die frankophone Konferenz legte das Schwergewicht auf die in der Bearbeitung von Personendaten liegenden Herausforderungen für die Grundrechte und -freiheiten. Dabei wurde die Bedeutung eines soliden gesetzgeberischen Rahmens und der Schaffung unabhängiger und leistungsfähiger Aufsichtsbehörden hervorgehoben. Die Konferenz unterstrich das stetig wachsende Interesse der Schwellenländer an der Einfüh-

rung einer rechtlichen Datenschutzregelung und begrüsste die Einsetzung neuer Datenschutzbehörden, namentlich in Tunesien und Marokko. Des Weiteren befasste sich die Konferenz mit der entscheidenden Frage nach den Massnahmen, um Daten von Kindern im Zeitalter des Internet und der sozialen Netzwerke besser zu schützen.

Es wurde darauf hingewiesen, dass sich die Datenschutzbehörden nicht genügend für den Schutz der Rechte von Kindern einsetzten, die eines der schwächeren Glieder der Informationsgesellschaft darstellen. So wird die AFAPDP in Zusammenarbeit mit der internationalen Organisation der Frankophonie ihre Bemühungen zur Förderung des Schutzes von Kindern bei der Bearbeitung sie betreffender Daten fortsetzen. Dazu wird sie Ausbildungs- und Sensibilisierungsinstrumente erarbeiten. Sie wird sich auch weiterhin um die Entwicklung verbindlicher Rechtsurkunden und um die Unterstützung der neuen Staaten bei der Einrichtung ihrer Gesetzgebung und ihrer Behörden im Bereich des Datenschutzes bemühen.

# 2. Öffentlichkeitsprinzip: Jahresbilanz 2009

## 2.1 Zugangsgesuche

### 2.1.1 Departemente und Bundesämter

**Die Anzahl der eingereichten Zugangsgesuche ist im Vergleich zum Vorjahr etwa gleich geblieben. Über die Jahre hinweg zeigt sich, dass prozentual immer weniger vollständige Verweigerungen ausgesprochen werden, dafür werden mehr teilweise Zugänge gewährt. Schlichtungsanträge wurden im vergangenen Jahr deutlich mehr gestellt.**

Gemäss den uns mitgeteilten Zahlen sind im Jahr 2009 bei den Bundesbehörden 232 Zugangsgesuche eingereicht worden. In 124 Fällen gewährten die Behörden einen vollständigen, bei 40 Gesuchen einen teilweisen Zugang. 68 Zugangsgesuche wurden komplett abgelehnt. Gegenüber dem Vorjahr haben sich diese Zahlen nicht grundlegend verändert (vgl. Statistik Ziff. 3.5).

Es kann positiv festgehalten werden, dass seit Inkrafttreten des Öffentlichkeitsgesetzes der Prozentsatz der vollständigen Verweigerungen kontinuierlich gesunken ist: Von 43% (2006) über 33% (2007) resp. 32% (2008) auf 29 % im Jahr 2009. Im Gegenzug ist der Anteil der teilweise gewährten Zugänge von 3% (2006) auf immerhin 17% (2009) gestiegen. Der Anteil der vollständig gewährten Zugänge im Jahr 2009 entspricht mit 54 % genau dem Durchschnitt der letzten dreieinhalb Jahre.

Einmal mehr muss unterstrichen werden, dass diesen Zahlen nur eine beschränkte Aussagekraft zukommt. So geben einzelne Bundesbehörden unumwunden zu, dass sie Anfragen aus der Öffentlichkeit, die ohne weiteres zum Zugang führen, «formlos» erledigen und nicht in die Statistik aufnehmen. Weiter muss angesichts der Tatsache, dass einzelne Verwaltungsstellen in den dreieinhalb Jahren seit Inkrafttreten des Gesetzes überhaupt keine Zugangsgesuche gemeldet haben, der Schluss gezogen werden, dass zahlreiche Gesuche gar nicht als solche erkannt werden. Wie schon in früheren Jahren gehen wir also davon aus, dass in der Bundesverwaltung tatsächlich mehr als die in der Statistik ausgewiesenen Zugangsgesuche gestellt und wohl auch positiv beurteilt werden.

In Bezug auf die Gebühren kann erneut festgehalten werden, dass die Bundesämter in der Regel kein Entgelt für die Beurteilung der Zugangsgesuche verlangen. Gemäss Meldung der Bundesämter wurde im Berichtsjahr nur in 6 Fällen den Gesuchstellern

eine Gebühr in Rechnung gestellt. Dabei ist der uns gemeldete Gesamtbetrag im Umfang von SFr. 3850.- im Vergleich zu den Vorjahren markant höher (2008: SFr. 1280.-; 2007: SFr. 1730.-). Weiterhin keine verlässlichen Angaben lassen sich über den bei den Ämtern und Departementen entstandenen 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 hat der gemeldete Zeitaufwand erneut zugenommen (2007: 273 Stunden; 2008: 509 Stunden; 2009: 748 Stunden).

Losgelöst von konkreten Zugangsgesuchen haben uns einzelne Öffentlichkeitsberater mitgeteilt, dass der Aufwand im Zusammenhang mit der Anwendung des Öffentlichkeitsgesetzes tendenziell zugenommen hat. Dabei wird insbesondere darauf verwiesen, dass die Einbindung in ein Schlichtungsverfahren (und in ein allfälliges Gerichtsverfahren) für ein Amt mit einem sehr grossen Aufwand einhergehen kann. Das BAKOM publiziert seit letztem Jahr grundlegende Entscheide aus dem Rundfunk- und Telekommunikationsbereich in einer Datenbank im Internet. Auch wenn es sich dabei nicht wie beim Öffentlichkeitsgesetz um so genannte passive, sondern um aktive Information handelt, trägt die Entscheiddatenbank des BAKOM – nebst anderen damit verfolgten Zwecken – auch wesentlich zum transparenten Verwaltungshandeln bei.





### 2.1.2 Parlamentsdienste

Gemäss Angaben der Parlamentsdienste wurde im Jahr 2009 ein Gesuch eingereicht, bei dem der Zugang vollständig gewährt wurde.

## 2.2 Schlichtungsanträge

Im 2009 wurden insgesamt 41 Schlichtungsanträge eingereicht (vgl. Statistik Ziff. 3.7). Im Vorjahr waren es 25. Insgesamt konnten 29 Schlichtungsanträge abgeschlossen werden. In 9 Fällen konnte zwischen den Beteiligten eine Schlichtung erzielt werden. In 18 Fällen erliessen wir – da keine einvernehmliche Lösung möglich oder von vornherein ersichtlich war – Empfehlungen. Zum Teil wurden mehrere Schlichtungsanträge mit einer Empfehlung erledigt. Ein Antrag wurde zurückgezogen und in einem Fall wurde er nicht fristgerecht eingereicht.

Diese Zahlen lassen folgende Schlüsse und Bemerkungen zu:

- In 108 Fällen wurde der Zugang vollständig (68) respektive teilweise (40) verweigert. Dem stehen 41 beim Beauftragten eingereichte Schlichtungsanträge

gegenüber. Mit anderen Worten wird im Berichtsjahr in 38 % aller Fälle von ganz oder teilweise abgelehnten Zugangsgesuchen ein Schlichtungsantrag eingereicht. Im Vorjahr betrug diese Zahl knapp 25%.

- Insgesamt führten knapp zwei Drittel der abgeschlossenen Schlichtungsverfahren (Schlichtungen und Empfehlungen) zu einer für den Gesuchsteller günstigeren Lösung (d.h. Schlichtung, respektive ein weitergehender Zugang als ursprünglich vom Bundesamt zugestanden).

Weiterhin unbefriedigend bleibt die Tatsache, dass die Antragstellerinnen und Antragsteller zu lange auf die Durchführung eines Schlichtungsverfahrens warten müssen. Die grosse Anzahl der im Berichtsjahr eingereichten Schlichtungsanträge wirkt sich zusätzlich negativ auf die Behandlungsdauer der einzelnen Verfahren aus. Das Bundesverwaltungsgericht hat den Beauftragten im Berichtsjahr zweimal wegen Rechtsverzögerung gerügt (Urteil vom 16.04.2009, A-75/2009; sowie Urteil vom 16.12.2009, A-6032/2009).





## 2.3 Abgeschlossene Schlichtungsverfahren

### 2.3.1 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, Dokumentation – Öffentlichkeitsprinzip – Empfehlungen, zu finden. Vier wichtige Empfehlungen werden im Anhang Ziff. 4.2. integral veröffentlicht.

#### Empfehlung EJPD / Auflösungsvereinbarungen Generalsekretär und Stellvertreter (09. Februar 2009)

Der Antragsteller ersuchte beim Generalsekretariat des Eidgenössischen Justiz- und Polizeidepartements (EJPD) um Zugang zu den jeweiligen Vereinbarungen betreffend die Auflösung der Arbeitsverhältnisse mit dem ehemaligen Generalsekretär sowie dessen Stellvertreter. Das EJPD verweigerte die Herausgabe mit dem Argument, dass dadurch die Privatsphäre der Beteiligten beeinträchtigt würde. Der Beauftragte gelangte in seiner Empfehlung zum Schluss, dass das besondere Informationsinteresse der Öffentlichkeit an der Bekanntgabe der Vereinbarungen das Interesse am Schutz der Privatsphäre im konkreten Fall überwiegt.

Nachtrag: Das EDJP war mit der Empfehlung nicht einverstanden und erliess eine Verfügung, die der Antragsteller beim Bundesverwaltungsgericht anfocht. Dieses qualifizierte den Bundesratsantrag des EJPD mit den Auflösungsvereinbarungen als Mitberichtsverfahren. Für Dokumente dieser Art besteht gemäss dem Öffentlichkeitsgesetz kein Recht auf Zugang. Der Antragsteller hat gegen das Urteil Rekurs beim Bundesgericht erhoben.

### Empfehlung Generalsekretariat VBS – armasuisse / Berichte Benchmarking, armasuisse, Helvetisierung (19. Februar 2009)

Der Antragsteller ersuchte bei armasuisse respektive dem Generalsekretariat des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport (VBS) um Zugang zu den Berichten «Benchmarking (Vergleich armasuisse mit ausländischen Beschaffungsstellen)», «Die armasuisse der Zukunft» und «Helvetisierung». Die Behörden führten bei allen Berichten an, dass sie nicht fertig gestellt seien. Zudem wurde der Zugang aufgrund diverser Ausnahmegründe verweigert. Der Beauftragte kam zum Schluss, dass alle Dokumente als fertig gestellt zu betrachten sind. In Bezug auf die Ausnahmegründe vertrat er die Meinung, dass einzig die aussenpolitischen oder internationalen Beziehungen beeinträchtigt werden könnten, im Übrigen der Zugang zu den Berichten jedoch gewährt werden muss.





### Empfehlung BFM / Anonymisierte Rohdaten ZEMIS (05. März 2009)

Der Antragsteller verlangte beim Bundesamt für Migration (BFM) eine Auflistung aller Einreisesperren für das Jahr 2007 als Auszug aus ZEMIS, dem Zentralen Migrationsinformationssystem. Das BFM vertrat die Ansicht, das Öffentlichkeitsgesetz gelange vorliegend nicht zur Anwendung, und bezweifelte darüber hinaus, dass Personendaten aus ZEMIS amtliche Dokumente seien. Der Beauftragte bejahte die Anwendbarkeit des Öffentlichkeitsgesetzes und hielt dem BFM entgegen, dass nicht nur Einzeldaten, sondern die Gesamtheit aller Daten aus einem Informationssystem als virtuelle Dokumente grundsätzlich zugänglich sind. Die vollständige Empfehlung befindet sich im Anhang unter Ziff. 4.2.2.

### Empfehlung BLW / Milchmehrmengen (30. März 2009)

Der Antragsteller ersuchte um die Herausgabe aller vom Bundesamt für Landwirtschaft (BLW) bewilligten Milchmehrmengengesuche an die Produzentenorganisationen und Produzenten-Milchverwerter-Organisationen seit dem 1. Mai 2008. Das BLW verweigerte zum Schutz von Personendaten den Zugang zu den gewünschten Dokumenten.

Der Beauftragte konnte nicht auf die inhaltliche Argumentation des BLW eingehen, da die betreffenden Dokumente zum Zeitpunkt der Durchführung des Schlichtungsverfahrens Teil eines Verfahrens vor Bundesverwaltungsgericht waren. Damit gelangt das Öffentlichkeitsgesetz nicht zur Anwendung.

### Empfehlung ESTV / Cockpits und Amtsreportings (03. April 2009)

Der Antragsteller beantragte bei der Eidgenössischen Steuerverwaltung (ESTV) Zugang zu den Cockpits und den Amtsreportings der Jahre 2006–2008. Die ESTV verweigerte den Zugang mit dem Argument, dass die besagten Berichte eine Controlling-, Steuerungs- und Leitungsfunktion erfüllten und daher zum persönlichen Gebrauch des Direktors bestimmt seien. Folglich gelange das Öffentlichkeitsgesetz gar nicht zur Anwendung. Der Beauftragte teilte diese Ansicht nicht und hielt in seiner Empfehlung fest, dass auch Controlling- und Führungsdokumente der Geschäftsleitung dem Öffentlichkeitsprinzip unterliegen und demnach grundsätzlich zugänglich sind.

Nachtrag: Die ESTV war mit der Empfehlung des Beauftragten nicht einverstanden und erliess eine Verfügung. Dagegen führte der Antragsteller Beschwerde beim Bundesverwaltungsgericht. Dieses kam zum Schluss, dass der Zugang zu den Cockpits nach der Anonymisierung der Personendaten und der Abdeckung der Informationen aufgrund von Ausnahmebestimmungen des Öffentlichkeitsgesetzes und unter Wahrung des Steuergeheimnisses in geeigneter Form zu gewährleisten sei. Die vollständige Empfehlung befindet sich im Anhang unter Ziff. 4.2.3.

### Empfehlung BAG / RoKA-Studien, Kalkulationsbasis, Spezialitätenliste, Tarifverträge (22. April 2009)

Die Antragsteller verlangten beim Bundesamt für Gesundheit (BAG) Zugang zu diversen Dokumenten im Zusammenhang mit dem Tarifvertrag LOA III (Leistungsorientierte Abgeltung zwischen pharmaSuisse und santésuisse). Der Tarifvertrag muss vom Gesamtbundesrat genehmigt werden. Weil der Bundesrat als Kollegialbehörde nicht dem Öffentlichkeitsgesetz unterstehe, lehnte das BAG den Zugang zu allen Zusatzdokumenten ab, die im Zusammenhang mit dem Vertrag zuhanden des Bundesrates eingereicht wurden.

Dieser Argumentation schloss sich der Beauftragte nicht an. Es trifft zwar zu, dass der Bundesrat bei seinen Entscheiden als Kollegialbehörde vom Geltungsbereich des Öffentlichkeitsprinzips ausgenommen ist. Dies gilt nach Ansicht des Beauftragten jedoch nicht für das in die Sache involvierte Bundesamt, welches im Zusammenhang mit der

Genehmigung des Tarifvertrages die administrativen Arbeiten für den Bundesrat erledigt. Die Dokumente wurden vom Beauftragten folglich überprüft und aufgrund ihres Inhalts (allgemeine Information) als zugänglich beurteilt.

### Zwei Empfehlungen EFD / Unterlagen Bundesratstreffen mit einer AG (11. Mai 2009 und 23. Dezember 2009)

Zwei Antragstellerinnen ersuchten beim Generalsekretariat des Eidgenössischen Finanzdepartements (EFD) um Zugang zu allen Dokumenten, welche einen Zusammenhang zu einem Treffen zwischen dem Vertreter einer AG und dem Vorsteher des EFD aufwiesen. Das EFD erklärte, dass dem Bundesrat im Rahmen des Treffens ein einziges Dokument übergeben worden war. Es verweigerte den Zugang aufgrund darin enthaltener Geschäftsgeheimnisse und wegen der vom Bundesrat zugesicherten Geheimhaltung. Der Beauftragte überprüfte die Geschäftsverwaltungstabellen des EFD, woraus ersichtlich wurde, dass nur das besagte Dokument darin aufgeführt war. Er stützte das Departement in seiner Argumentation, empfahl jedoch die Herausgabe zweier E-Mails, welche die Anhörung betreffend des Zugänglichmachens des übergebenen Dokuments zum Gegenstand hatten.

### Empfehlung EDA / Rückerstattungsübereinkommen (15. Juni 2009)

Die Gesuchstellerin verlangte vom Eidgenössischen Departement für auswärtige Angelegenheiten (EDA) Zugang zu einem Rückerstattungsübereinkommen vom November 2005. Ungefähr 10 Monate nach der ablehnenden Stellungnahme reichte die Gesuchstellerin einen Schlichtungsantrag beim Beauftragten ein. Der Beauftragte hielt in seiner Empfehlung fest, dass einerseits die gesetzliche Frist für die Einreichung eines Schlichtungsantrags nicht eingehalten wurde und andererseits das Öffentlichkeitsgesetz nicht zur Anwendung gelange, da das besagte Dokument vor Inkrafttreten des Gesetzes erstellt worden war.

### Empfehlung UVEK / Zusatzdokumente zur Staatsrechnung (19. Juni 2009)

Der Antragsteller beantragte beim Eidgenössischen Departement für Umwelt, Verkehr, Energie und Kommunikation (UVEK) Zugang zu den Zusatzdokumenten zur Staatsrechnung 2008. Das UVEK verweigerte den Zugang mit der Begründung, es habe die Dokumente im Auftrag einer parlamentarischen Kommission erstellt. Das Öffentlichkeitsgesetz gelte nicht für Beratungen und Sitzungsunterlagen der parlamentarischen Kommissionen und Delegationen. Der Beauftragte vertrat die Ansicht, dass dieser Vor-

behalt nur dann gelten kann, wenn die Dokumente aufgrund eines unmittelbaren und besonderen Auftrags einer parlamentarischen Kommission erstellt worden sind. Hat die Behörde die Dokumente – wie vorliegend der Fall – vorgängig bereits für sich selber (oder Dritte) erstellt, gelangt der Vorbehalt nicht zur Anwendung. Daher empfahl der Beauftragte, die Dokumente herauszugeben. Das UVEK akzeptierte die Empfehlung und informierte über die Herausgabe der Dokumente an den Antragsteller. Die vollständige Empfehlung befindet sich im Anhang unter Ziff. 4.2.4.

### Empfehlung BAZL / Safety Case Document (Sicherheitsbericht) (03. Juli 2009)

Die Antragstellerin ersuchte beim Bundesamt für Zivilluftfahrt (BAZL) um Zugang zum Sicherheitsbericht von Skyguide bezüglich des Instrumentenlandesystems ILS RWY 28 Zürich. Das BAZL lehnte den Zugang ab, da nicht mit der Materie vertraute Personen aufgrund der Komplexität der Unterlagen falsche Schlussfolgerungen ziehen könnten und zudem Geschäftsgeheimnisse von Skyguide tangiert würden. Das Bundesverwaltungsgericht hatte in einem bereits abgeschlossenen Beschwerdeverfahren das Akteneinsichtsrecht in Bezug auf die gleichen, nun vom Beauftragten begutachteten Dokumente beurteilt. Es verwehrte das Einsichtsrecht mit der Argumentation, dass allgemein die Sicherheit der Luftfahrt aufgrund falscher Interpretationen gefährdet sei und darüber hinaus Geschäftsgeheimnisse von Skyguide betroffen seien. Da sich das Bundesverwaltungsgericht also zu den fraglichen Dokumenten bereits abschlägig geäussert hatte, war der Beauftragte an die Beurteilung der Nichtzugänglichkeit gebunden.

### Empfehlung Suva / Kontrollunterlagen (14. Juli 2009)

Die Antragstellerin beantragte Zugang zu den Akten, welche die Suva als Kontrollorgan in Zusammenhang mit der Überprüfung einer Maschine erstellt hatte. Die Suva verweigerte den Zugang aufgrund ihrer Schweigepflicht, der Beeinträchtigung der Privatsphäre der Inverkehrbringerin der Maschine und wegen der Unmöglichkeit der Anonymisierung der betroffenen Personendaten. Der Beauftragte empfahl aus diesem Grund und weil ein überwiegendes öffentliches Interesse fehlt, den Zugang zu verweigern.

### Empfehlung BAFU und ARE / Vergleichende Studie Abbaustandorte Hartgestein (16. Juli 2009)

Umwelt- und Naturschutzorganisationen verlangten Zugang zu einer vergleichenden Studie betreffend die Abbaustandorte für Hartgestein. In Absprache mit dem Bun-

desamt für Raumentwicklung (ARE) gewährte das Bundesamt für Umwelt (BAFU) den Zugang zu einer anonymisierten Version der Studie, verweigerte jedoch aus verschiedenen Gründen, so unter anderem wegen der Geschäfts- und Fabrikationsgeheimnisse der darin erwähnten Unternehmen, einen uneingeschränkten Zugang. In seiner Empfehlung stellte der Beauftragte fest, dass es vorliegend insbesondere an einem überwiegenden öffentlichen Interesse für die Bekanntgabe der Daten der betroffenen Unternehmen fehlt.

### Empfehlung AHV-Ausgleichsfonds / Expertisen zum Verkehrswert einer Immobilie (08. September 2009)

Der Antragsteller wollte Zugang zu zwei Expertenberichten betreffend den Verkehrswert einer Immobilie, die vom AHV-Ausgleichsfonds für den Eigengebrauch erworben worden war. Der Ausgleichsfonds lehnte den Zugang zu den Expertisen ab, weil es sich dabei um interne Arbeitsdokumente handle. Darüber hinaus vertrat er die Ansicht, dass das Öffentlichkeitsgesetz für den Fonds nicht gelte. Die relevante Gesetzgebung qualifiziert den Fonds nicht eindeutig als Einheit der Bundesverwaltung. Organisationen und Private ausserhalb der Bundesverwaltung sind nur in jenen Tätigkeitsbereichen dem Öffentlichkeitsgesetz unterstellt, in denen sie Erlasse oder Verfügungen erlassen. Der Beauftragte kam zum Schluss, dass das Öffentlichkeitsgesetz nicht zur Anwendung gelange. Der Fonds konnte daher nicht verpflichtet werden, die Expertisen zugänglich zu machen. Aus Transparenzgründen, so der Beauftragte in seiner Empfehlung, wäre es wünschenswert, dass eine Institution mit einer derart wichtigen öffentlichen Aufgabe zur Offenlegung seiner Dokumente verpflichtet wird.

### Empfehlung BFE / Kleinwasserkraftanlagen (15. September 2009)

Der Antragsteller ersuchte um Zugang zu einer Auflistung der Koordinaten der Kleinwasserkraftanlagen. Das Bundesamt für Energie (BFE) verweigerte den Zugang aus datenschutzrechtlichen Überlegungen. Aufgrund der Koordinaten hätten die Projektanten ermittelt werden können. Der Beauftragte erachtete diese Zugangsverweigerung als rechtmässig und angemessen. Insbesondere erkannte er kein überwiegendes öffentliches Interesse an der Bekanntgabe der Personendaten der Projektanten.

### Sechs Empfehlungen EDI, EJPD, VBS, EFD, EVD, UVEK / Zusatzdokumentation Voranschlag 2010 (02. November 2009)

Der Antragsteller beantragte bei den Generalsekretariaten von EDI, EJPD, VBS, EFD, EVD und UVEK Zugang zu den Zusatzdokumenten zum Voranschlag 2010. Die Departemente schoben den Zugang bis zur Verabschiedung des Geschäfts durch die Bundes-

versammlung auf. Der Beauftragte verwies vorweg auf seine Empfehlung vom 19. Juni 2009 betreffend die Zusatzdokumentation zur Staatsrechnung 2008.

Bezüglich der Zusatzdokumentation zum Voranschlag anerkannte er, dass ihre vorzeitige Bekanntgabe tatsächlich zu einer wesentlichen Beeinträchtigung der Meinungs- und Willensbildung des zuständigen legislativen Organs führen würde. Er vertrat allerdings die Ansicht, dass diese Meinungs- und Willensbildung nicht in der Bundesversammlung, sondern in den Finanzkommissionen der Räte stattfinde. Darum empfahl er den Aufschub des Zugangs bis nach der Behandlung des Geschäfts in den Finanzkommissionen. Alle betroffenen Departemente waren mit der Empfehlung nicht einverstanden und erliessen eine Verfügung. Darin teilten sie dem Antragsteller mit, dass die Zusatzdokumentationen nicht in den Anwendungsbereich des Öffentlichkeitsgesetzes fielen. Zuständig für deren Herausgabe seien daher die Finanzkommissionen der Räte. Die vollständige Empfehlung befindet sich im Anhang unter Ziff. 4.2.5.



### 2.3.2 Schlichtungen

In folgenden Fällen konnte eine Schlichtung erzielt werden:

#### Schlichtung VBS / Zeitmilitär



Der Antragsteller ersuchte das VBS um Zustellung diverser Unterlagen betreffend Zeitmilitärs (Zeitmilitärs stehen als Angestellte in Uniform für eine zeitlich befristete Tätigkeit im Dienst der Schweizer Armee). Nach der Vermittlung durch den Beauftragten wurden dem Antragsteller alle gewünschten Dokumente, welche in den Geltungsbereich des Öffentlichkeitsgesetzes fielen, zugestellt.

#### Schlichtung Swissmedic / Medikamentenunterlagen (zwei Schlichtungsanträge)

Swissmedic verweigerte den Antragstellerinnen den Zugang zu medikamentenspezifischen Unterlagen, weil das Gesuch aufgrund der Vielzahl der Dokumente nicht bearbeitet werden könne. Nach zwei Schlichtungsverhandlungen einigten sich die Beteiligten auf ein zeitlich gestaffeltes Vorgehen. Zudem legten sie den zu entrichtenden Gebührenbetrag fest. Die Umsetzung der Angelegenheit ist noch nicht definitiv abgeschlossen.

#### Schlichtung BLW / Milchmehrmengen

Der Antragsteller verlangte vom Bundesamt für Landwirtschaft (BLW) Einsicht in Unterlagen betreffend die Milchmehrmengenverteilung. Im Rahmen der Schlichtung ei-

nigten sich die Beteiligten darauf, dass das BLW weitere Abklärungen in Bezug auf die Zugänglichkeit der Dokumente, den Aufwand für die Anonymisierung sowie die zu erwartenden Gebühren vornimmt. Weiter verständigten sie sich darauf, welche Angaben auf dem Controllingformular aus Datenschutzgründen abgedeckt werden. Die Angelegenheit ist noch nicht definitiv abgeschlossen.

### Schlichtung BAG / In Vitro

Die Antragsteller verlangten Einsicht in die Akten der Eidgenössischen Kommission für allgemeine Leistungen und Grundsatzfragen (ELGK) zum Thema In-Vitro-Fertilisation / Embryotransfer (IVF-ET). Das Gesuch erfolgt im Hinblick auf ein Beschwerdeverfahren im Zusammenhang mit der Nichtübernahme einer IVF durch den Krankenversicherer. Das BAG verweigerte den Zugang mit Verweis auf die laufenden Verhandlungen. Im Schlichtungsverfahren widerrief das BAG seine Begründung und führte an, dass die ELGK nicht in den Anwendungsbereich des Öffentlichkeitsgesetzes falle. Im Gespräch mit beiden Seiten konnte folgende Einigung gefunden werden: Das BAG stellte den Antragstellern jene anonymisierten Dokumente zu, welche die Position der ELGK zum besagten Themenbereich festhalten.

### Schlichtung IVI / Unterlagen zu Viren

Der Antragsteller ersuchte das Institut für Viruskrankheiten und Immunprophylaxe (IVI) um Einsicht in zahlreiche Dokumente. Weil aufgrund des Umfangs der nachgefragten Dokumente eine hohe Gebühr zu erwarten war, informierte die Behörde den Gesuchsteller und setzte ihm eine 10-tägige Frist zur Aufrechterhaltung des Gesuchs. Nach Verstreichen dieser Frist reichte der Antragsteller ein zweites, gekürztes Zugangsgesuch ein. Das IVI informierte ihn abermals über die zu erwartenden hohen Kosten. Nun wollte der Antragsteller die Gebührenhöhe durch den Beauftragten beurteilt wissen. Nach Vermittlung durch den Beauftragten erklärte sich das IVI zu einem kostenlosen Zugang zu einem Grossteil der Dokumente bereit.

### Schlichtung FINMA

Der Antragsteller gelangte an den Beauftragten, weil ihm die Eidgenössische Finanzmarktaufsicht (FINMA) den Zugang zu Erhebungen betreffend Versicherungsvermittler aus Gründen des Datenschutzes verweigerte. Die Dokumente stammten noch vom ehemaligen Bundesamt für Privatversicherungen, das 2009 in die FINMA überführt worden war. Nach Einleitung des Schlichtungsverfahrens durch den Beauftragten lud die FINMA den Antragsteller zu einem Gespräch ein, bei dem er die gewünschten Informationen erhielt.

### Bundeskanzlei / Richtlinien für Bundesratsgeschäfte (Roter Ordner)

Der Antragsteller reichte bei der Schweizerischen Bundeskanzlei (BK) ein Zugangsgesuch ein und verlangte eine elektronische Kopie der Richtlinien für Bundesratsgeschäfte. Diese Richtlinien, auch bekannt als «Roter Ordner», regeln die Vorbereitung und Erledigung der Bundesratsgeschäfte und enthalten Verfahrensvorschriften sowie Vorlagen für die Gestaltung von Bundesratsanträgen.

Die BK sah bei einer Gewährung des Zugangs die freie Willensbildung des Bundesrates beeinträchtigt und machte darüber hinaus geltend, die Dokumente seien als intern klassifiziert und dürften somit aufgrund der Informationsschutzverordnung nicht zugänglich gemacht werden. Im Rahmen des Schlichtungsverfahrens anerkannte die BK, dass diese Argumente vor dem Öffentlichkeitsgesetz nicht standhielten. Sie zeigte sich schliesslich bereit, dem Antragsteller die gewünschte elektronische Kopie des Roten Ordners zuzustellen.

### Schlichtung BAG / Virennachweise

Der Antragsteller reichte einen Schlichtungsantrag ein, weil das BAG ihm die gewünschten Dokumente über den Nachweis bestimmter Viren nicht zugestellt habe. Im Gespräch wurde eine für den Antragsteller zufrieden stellende Lösung gefunden: Einerseits stellte das Amt ein aus Versehen nicht ausgehändigtes Dokument umgehend zu, andererseits konnte mit dem Antragsteller geklärt werden, dass gestützt auf das Öffentlichkeitsgesetz von einem Amt nicht die Erstellung eines bestimmten Dokuments verlangt werden kann.

## 2.4 Evaluation

**Drei Jahre nach Inkrafttreten des Öffentlichkeitsgesetzes hat der Beauftragte den Evaluationsbericht zu diesem Gesetz präsentiert. Er zeigt auf, dass in dieser Zeit insgesamt eine positive Entwicklung zugunsten einer grösseren Transparenz in der Bundesverwaltung stattgefunden hat, auch wenn es immer noch Anzeichen für das Festhalten am Geheimhaltungsprinzip gibt. Gestützt auf die Evaluation benennt der Beauftragte in seinem Begleitbericht jene Bereiche, in denen er Handlungsbedarf sieht.**

Das Öffentlichkeitsgesetz schreibt dem Beauftragten vor, dem Bundesrat über Vollzug, Wirksamkeit und Umsetzungskosten Bericht zu erstatten. Der von einem externen Institut erstellte Evaluationsbericht wurde – zusammen mit einem Begleitbericht des

Beauftragten – fristgerecht drei Jahre nach Inkrafttreten des Gesetzes beim Bundesrat eingereicht und auch der Öffentlichkeit vorgestellt. Das Gesetz verlangt, dass sich der erste Bericht zu den Umsetzungskosten des Öffentlichkeitsprinzips in der Verwaltung äussern muss.

### Evaluationsbericht des IDHEAP

Aus Gründen der Objektivität entschied sich der Beauftragte, eine externe Stelle, das Institut de hautes études en administration publique (IDHEAP), mit der Durchführung der Evaluation zu beauftragen. Das IDHEAP-Team baute seine Untersuchung auf Dokumentenanalysen und qualitativen Interviews auf. Es konsultierte eine grosse Anzahl der Öffentlichkeitsberater der Bundesverwaltung sowie eine Expertengruppe bestehend aus Personen aus dem Journalismus, dem universitären Umfeld und einigen hohen Departementsvertretern.

Bei der Frage, welche Kosten die Einführung des Öffentlichkeitsgesetzes verursacht hat, kam das Evaluationsteam zum Schluss, dass sowohl die für die Umsetzung getätigten Investitionen als auch die jährlichen Kosten für die Gesuchsbehandlung sehr bescheiden seien.

Gemäss Evaluationsbericht deuten mehrere Elemente auf eine positive Entwicklung in Bezug auf die Zugänglichkeit amtlicher Dokumente hin. So werten die Befragten das Öffentlichkeitsgesetz insgesamt als positiv, weil es das Bewusstsein der Verwaltung für ihre Informationspflichten schärfe sowie die Rechte und Pflichten bei der Informationsweitergabe kläre. Als eine direkte Folge der Einführung des Öffentlichkeitsgesetzes sieht der Bericht eine aktivere Informationspolitik (insbesondere die Veröffentlichung von Berichten und Dokumenten im Internet), die ihrerseits zu einer transparenten Verwaltung beiträgt. Dieser positiven Entwicklung steht in einigen Verwaltungseinheiten noch immer ein Festhalten am Geheimhaltungsprinzip gegenüber. So wird beispielsweise von der gesuchstellenden Person verlangt, sie müsse ihre Identität und die Beweggründe für die Einreichung eines Zugangsgesuchs offen legen – beides steht im Widerspruch zum Öffentlichkeitsgesetz.

Weiter zeigt der Bericht auf, dass spezifische Praktiken zur Einschränkung des Dokumentenzugangs entwickelt worden sind. So hat ein Bundesamt beschlossen, kein Online-Gesuchsformular einzuführen, um die Nachfrage nach Dokumenten gering zu halten. Eine Analyse der Websites zeigte, dass gewisse Bundesämter sogar gesetzeswidrige Informationen präsentieren und den Eindruck erwecken, der Zugang zu Dokumenten sei allgemein gebührenpflichtig, oder ein Zugangsgesuch müsse per Post eingereicht werden, obwohl das Gesetz jede Form von Gesuchen, mündliche und schriftliche, gestattet.

Basierend auf den Ergebnissen ihrer Beurteilung formulierten die Evaluatoren eine Reihe von Empfehlungen für eine transparente Bundesverwaltung. Sie schlagen unter anderem eine stärkere Promotion des Öffentlichkeitsgesetzes bei der Bevölkerung sowie eine konstante Sensibilisierung der Mitarbeitenden der Bundesverwaltung vor.

Der Evaluationsbericht des IDHEAP ist auf unserer Webseite www.derbeauftragte.ch, unter Dokumentation – Öffentlichkeitsprinzip – Evaluation 2009, zu finden.

### Begleitbericht des Beauftragten

Ergänzend zum Evaluationsbericht verfasste der Beauftragte einen Begleitbericht zuhanden des Bundesrates. Nach drei Jahren Erfahrung mit dem Gesetz zieht er den Schluss, dass die Umsetzung des Öffentlichkeitsprinzips in der Bundesverwaltung grundsätzlich den Erwartungen entspricht, die Bundesrat und Parlament während des Gesetzgebungsprozesses geäussert haben. Er hebt insbesondere die Tatsache hervor, dass die Bundesverwaltung – entgegen aller Befürchtungen im Vorfeld der Einführung des Öffentlichkeitsprinzips – nicht von Zugangsgesuchen überflutet wurde.

Beim Vollzug des Öffentlichkeitsgesetzes gibt aus es Sicht des Beauftragten verwaltungsintern noch zahlreiche Schwachstellen. So besteht unter anderem in folgenden Bereichen Handlungsbedarf:

- Verlängerung der Frist für die Durchführung des Schlichtungsverfahrens: Die meisten bisher durchgeführten Schlichtungsverfahren können aus verschiedenen praktischen Gründen (Komplexität der Fälle, Personalressourcen, Disponibilität – bei allen Beteiligten – für sofortige Durchführung von Sitzungen etc.) nicht innerhalb der gesetzlich vorgeschriebenen Frist von 30 Tagen abgeschlossenen werden. Ein Vergleich mit anderen Ländern zeigt, dass sich auch dort ein erheblicher Teil der Schlichtungsverfahren über mehrere Monate oder gar Jahre hinzieht (siehe Evaluationsbericht IDHEAP, S. 39).
- Stärkung der Kompetenzen des Beauftragten im Schlichtungsverfahren: Die Evaluation hat gezeigt, dass der Handlungs- und Entscheidungsdruck zu sehr zu Lasten der Gesuchstellenden geht. So kann die Verwaltung die Herausgabe von Dokumenten an den Beauftragten hinauszögern und/oder ihre Zugangsverweigerung ungenügend begründen und auf diese Weise das Schlichtungsverfahren in die Länge ziehen. Die Evaluatoren und der Beauftragte erachten daher eine Stärkung seiner Kompetenzen während des Verfahrens als sinnvoll; beispielsweise durch ein Weisungsrecht des Beauftragten gegenüber der

Verwaltung, sowie ein Beschwerderecht des Beauftragten gegenüber ihren Verfügungen, die von seinen Empfehlungen abweichen.

- Anhebung der minimalen Aufwandgrenze für die Gebührenerhebung: In den ersten drei Jahren wurden – nicht zuletzt aus Effizienzgründen – nur wenig Gebühren (ausgewiesene Einnahmen von gut SFr. 3000) erhoben. Mit der Anhebung der minimalen Aufwandgrenze für die Erhebung von Gebühren, von SFr. 100 beispielsweise auf SFr. 500, könnte man den Geboten der Vereinfachung und der Vereinheitlichung des Verwaltungshandelns Rechnung tragen.

Der Begleitbericht des Beauftragten ist auf unserer Webseite www.derbeauftragte.ch, unter Dokumentation – Öffentlichkeitsprinzip – Evaluation 2009, zu finden.

# 3. Der EDÖB

## 3.1 Erneuerung unseres Geschäftsverwaltungssystems (GEVER)

**Der EDÖB arbeitet seit zehn Jahren mit seinem eigenen Geschäftsverwaltungssystem (EDÖB-Office), welches der Vertraulichkeit der Daten einen hohen Stellenwert einräumt. Diese ist namentlich gegenüber allen internen und externen Administratoren der Anwendung gewährleistet. Somit entspricht das System vollumfänglich den im Revisionsentwurf zur Verordnung über den Schutz von Informationen des Bundes vorgesehenen Anforderungen. Bei der demnächst anstehenden Migration des EDÖB-Office zu einer der standardisierten Lösungen des Bundes arbeiten wir daran, dass das neue System diesen Anforderungen in organisatorischer und technischer Hinsicht Rechnung tragen wird.**

Seit dem 1. Januar 2000 verfügen wir mit EDÖB-Office über ein höchst vertrauliches Geschäftsverwaltungssystem. Das Konzept beruht auf einer End-to-end-Chiffrierung (von den Kunden bis zum Datenbankserver und zu den Druckservern) der potentiell sensiblen Inhalte. Diese Aufgabe wurde ohne Verzögerungen und praktisch ohne Erschwerung der redaktionellen Arbeiten mit herkömmlicher Büroinformatik und darüber hinaus unter Integration der elektronischen Nachrichtenübermittlung bewältigt. Der so erzielte wesentliche Vorteil liegt in der absoluten Vertraulichkeit der Dokumente, insbesondere gegenüber den (internen) Verwaltern der Anwendung und den (externen) Verwaltern der Datenbank, da sie nicht über die für die Dechiffrierung der Inhalte erforderlichen Schlüssel verfügen. Das Ablagesystem und die Schnittstelle für die Überführung der Akten ins Bundesarchiv können noch verbessert werden. Das ist einer der Gründe für unseren Entschluss, zu einer der standardisierten Lösungen des Bundes, nämlich Fabasoft oder GEVER-Office, zu migrieren.

Unsere ersten Evaluationen liessen indes rasch deutlich werden, dass keines dieser beiden Produkte ein gleichwertiges Niveau der Datenvertraulichkeit bietet, wie wir es seit zehn Jahren kennen. Wir begrüssen in diesem Zusammenhang die Revisionsvorlage zur Verordnung über den Schutz von Informationen des Bundes (ISchV), die auf eine Erweiterung der in der Verordnung aufgestellten Bearbeitungsvorschriften auf alle Informatiksysteme (einschliesslich GEVER), mit einer Umsetzungsfrist bis Ende 2013, abzielt. Ohne diesen Zeitpunkt abzuwarten, arbeiten wir aktiv an der Migration von EDÖB-Office in ein Geschäftsverwaltungssystem, das den Anforderungen sowohl des Programms GEVER-Bund als auch des Regierungs- und Verwaltungsorganisationsgesetzes (RVOG) entspricht.

## 3.2 4. Europäischer Datenschutztag

**Beleidigungen und Verleumdungen, sexuelle Belästigung oder Mobbing über das Internet sind Phänomene, mit denen zahlreiche Jugendliche in ihrem Leben bereits konfrontiert worden sind. Diese Phänomene illustrieren, wie wichtig es ist, gerade auch im Netz Personendaten nur sehr sparsam preiszugeben. Im Rahmen des 4. Europäischen Datenschutztags haben wir an mehreren Veranstaltungen über die Risiken für Jugendliche im Web informiert.**

Absicht des diesjährigen Datenschutztags war es, den Umgang von Jugendlichen mit den neuen Medien zu beleuchten und sie selber, aber auch Eltern und Lehrer, für den Schutz der Privatsphäre zu sensibilisieren. Obwohl sie die modernen Kommunikationsmittel häufig und intensiv nutzen, sind sich viele jugendliche User nämlich wenig bewusst, welche Gefahren im Web lauern und wie man sich vor ihnen schützen kann. Und die Erwachsenen sind angesichts der rasanten technischen Entwicklungen bei der Begleitung des Nachwuchses manchmal schlicht überfordert.

Zu diesem Zweck waren wir sowohl in der Deutschschweiz wie auch in der Romandie an verschiedenen Veranstaltungen präsent. Radiosender beider Landesteile griffen das Thema «Jugendliche und der Datenschutz im Internet» in ihren Sendungen auf. Die Hörerinnen und Hörer erhielten die Gelegenheit, ihre Fragen und Anliegen an unsere Experten zu richten.

In der Stadt Bern ermunterte der Beauftragte Hanspeter Thür am Gymnasium Kirchenfeld die Schülerinnen und Schüler zu einer verantwortungsvollen Nutzung des Internets und seiner vielfältigen Anwendungen. Die vielen Spuren, die wir im Netz freiwillig und unfreiwillig hinterlassen, machten uns und unsere Privatsphäre angreifbar. Um unliebsamen Überraschungen vorzubeugen, riet Thür den Jugendlichen schliesslich, die Online-Welt mit offenen Augen und wachem Verstand zu erkunden. Dazu zählt auch das Lesen der Datenschutzbestimmungen oder die Regelung der Privacy-Einstellungen des eigenen Netzwerk-Profils (z.B. Facebook oder myspace).

Anlässlich des Datenschutztages schalteten wir auf unserer Website auch Informationen zum sicheren Umgang mit dem Web auf, die sich an Jugendliche, Eltern und Lehrer richten (www.derbeauftragte.ch, Themen – Datenschutz – Internet). Darunter befindet sich auch eine umfangreiche Linksammlung, welche auf schweizerische und ausländische Webseiten zum Thema Internet und Jugendliche hinweist.

## 3.3 Publikationen des EDÖB – Neuerscheinungen

**Die Website dient uns als Plattform, auf der wir über unsere Tätigkeiten in den Bereichen Datenschutz und Öffentlichkeitsprinzip informieren. So haben wir auch im vergangenen Jahr weitere Texte und Beobachtungen zu verschiedenen Themen aufgeschaltet. Zu den neuen Publikationen zählen die Erläuterungen zum betrieblichen Datenschutzverantwortlichen, zur mobilen Datenbearbeitung und zu Unternehmenszusammenschlüssen, sowie Informationen und Tipps zu den Datenschutzrisiken, denen Jugendliche im Internet ausgesetzt sind.**

Kinder und Jugendliche finden heutzutage bereits sehr früh Einstieg in die modernen Kommunikationstechnologien und erkunden diese mit grossem Interesse. Diese an und für sich positive Entwicklung birgt aber gewisse datenschutzrechtliche Risiken. Viele jugendliche User sind sich nämlich zu wenig bewusst, wie wichtig ein behutsamer Umgang mit ihren Personendaten für den Schutz ihrer Privatsphäre ist. Und die Erwachsenen sind angesichts der rasanten technischen Entwicklungen bei der Begleitung des Nachwuchses manchmal schlicht überfordert. Vor diesem Hintergrund haben wir auf unserer Webseite www.derbeauftragte.ch Informationen, Ratschläge und Links zum Thema «Kinder, Jugendliche und die Tücken des Internets» aufgeschaltet. Sie finden die Seite unter Themen – Datenschutz – Internet.

Heute bestehen durch die Möglichkeiten der Informatik und des Internets zahlreiche Varianten der mobilen Datenbearbeitung, die einerseits bequem und effizient sind, anderseits insbesondere bei sensiblen Informationen Fragen der Datensicherheit aufwerfen. Unter Themen – Datenschutz – Internet haben wir Erläuterungen dazu aufgeschaltet.

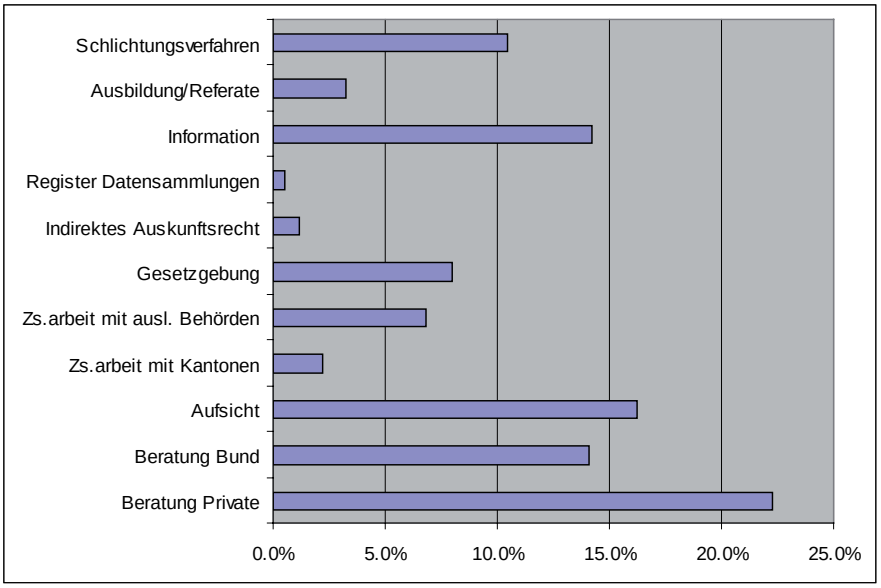
Das revidierte Bundesgesetz über den Datenschutz vom 01. Januar 2008 ermöglicht Unternehmen durch verschiedene Gesetzesänderungen die Selbstregulierung. So müssen beispielsweise Inhaber von Datensammlungen diese nicht anmelden, wenn sie einen Datenschutzverantwortlichen bezeichnet haben, der unabhängig die betriebsinterne Einhaltung der Datenschutzvorschriften überwacht und Verzeichnisse der Datensammlungen führt.

Wir haben nun Erläuterungen verfasst, welche die Aufgaben eines solchen betrieblichen Datenschutzbeauftragten skizzieren. Sie befinden sich unter Themen – Datenschutz – Unternehmen. Am selben Ort gehen wir auf die datenschutzrechtlichen Gefahren im Rahmen von Unternehmenszusammenschlüssen ein und erläutern die Massnahmen, die erforderlich sind, um den Datenschutz bei Fusionen zu gewährleisten.

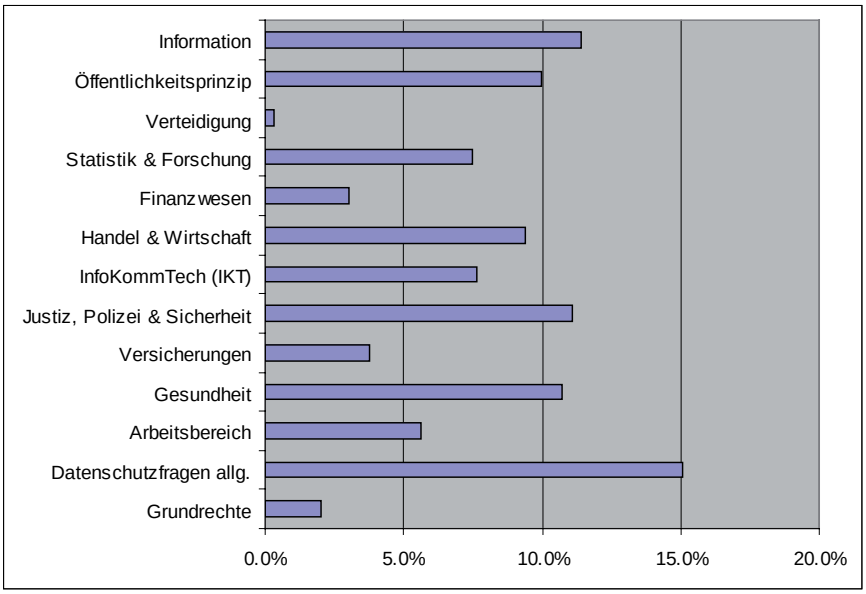
Um ihre Leistungspflicht abzuklären, holen Haftpflichtversicherer regelmässig bei externen Experten (Ärztinnen, Ingenieuren etc.) Aktengutachten ein. In unserem Merkblatt erläutern wir, welche datenschutzrechtlichen Aspekte dabei zu berücksichtigen sind. Auch mit der Herausgabe von Austritts- und Operationsberichten an Krankenversicherer hatten wir uns zu befassen. Das entsprechende Merkblatt nennt die Voraussetzungen, unter denen Spitäler und Heime Personendaten aus solchen Berichten an die Versicherer weitergeben dürfen. Beide Texte finden Sie unter Dokumentation – Datenschutz – Merkblätter.

## 3.4 Statistik über die Tätigkeit des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (Zeitraum: 1. April 2009 bis 31. März 2010)

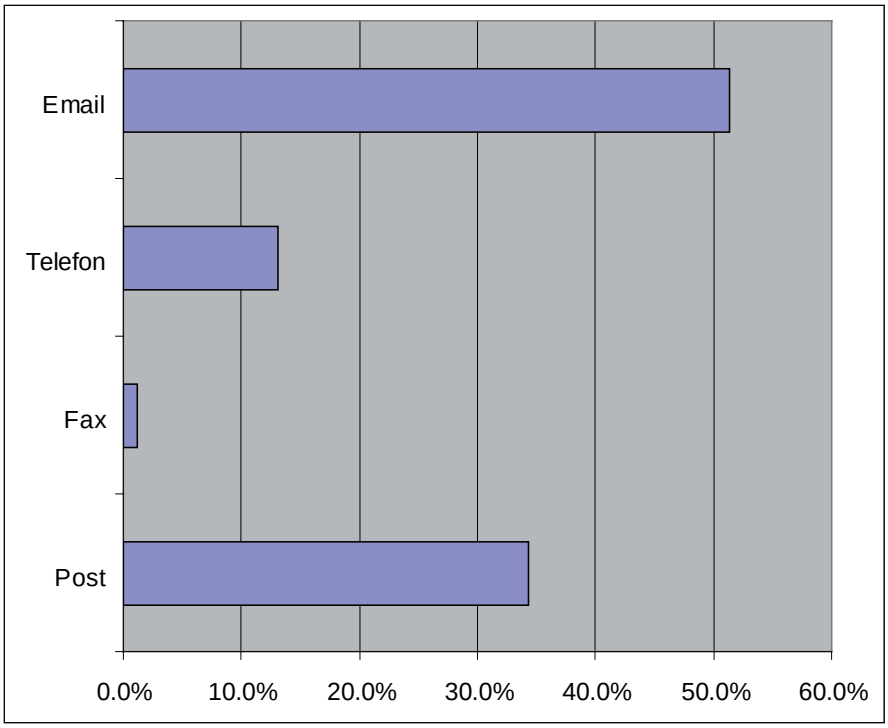
### Aufwand nach Aufgabengebiet



## Aufwand nach Sachgebiet



**Herkunft der Anfragen**



## 3.5 Statistik über die bei den Departementen eingereichten Zugangsgesuche nach Art. 6 des Öffentlichkeitsgesetzes (Zeitraum: 1. Januar 2009 bis 31. Dezember 2009)

| Departement | Anzahl Gesuche | Zugang vollständig gewährt | Zugang vollständig verweigert | Zugang teilweise gewährt / aufgeschoben |
|---|---|---|---|---|
| BK | 27 | 17 | 6 | 4 |
| EDA | 13 | 7 | 3 | 3 |
| EDI | 48 | 22 | 17 | 9 |
| EJPD | 30 | 19 | 8 | 3 |
| VBS | 20 | 12 | 6 | 2 |
| EFD | 11 | 3 | 6 | 2 |
| EVD | 28 | 13 | 8 | 7 |
| UVEK | 55 | 31 | 14 | 10 |
| **Total 2009 (in %)** | **232 (100%)** | **124 (54%)** | **68 (29%)** | **40 (17%)** |
| | | | | |
| TOTAL 2008 (in %) | 221 (100%) | 115 (52%) | 71 (32%) | 35 (16%) |
| TOTAL 2007 (in %) | 249 (100%) | 147 (59%) | 82 (33%) | 20 (8%) |
| TOTAL 2006 (in %) | 95 (100%) | 51 (54%) | 41 (43%) | 3 (3%) |

### Schweizerische Bundeskanzlei BK

| Betroffener Fachbereich | Anzahl | Zugang vollständig gewährt | Zugang vollständig verweigert | Zugang teilweise gewährt / aufgeschoben |
|---|---|---|---|---|
| BK | 12 | 6 | 6 | 0 |
| EDÖB | 15 | 11 | 0 | 4 |
| **TOTAL** | **27** | **17** | **6** | **4** |

### Eidgenössisches Departement für auswärtige Angelegenheiten EDA

| Betroffener Fachbereich | Anzahl | Zugang vollständig gewährt | Zugang vollständig verweigert | Zugang teilweise gewährt / aufgeschoben |
|---|---|---|---|---|
| EDA | 13 | 7 | 3 | 3 |
| **TOTAL** | **13** | **7** | **3** | **3** |

**Eidgenössisches Departement des Innern EDI**

| Betroffener Fachbereich | Anzahl | Zugang vollständig gewährt | Zugang vollständig verweigert | Zugang teilweise gewährt / aufgeschoben |
|---|---|---|---|---|
| GS EDI | 6 | 2 | 3 | 1 |
| EBG | 0 | 0 | 0 | 0 |
| BAK | 6 | 3 | 3 | 0 |
| BAR | 1 | 1 | 0 | 0 |
| METEO CH | 0 | 0 | 0 | 0 |
| BAG | 16 | 7 | 4 | 5 |
| BFS | 1 | 1 | 0 | 0 |
| BSV | 9 | 5 | 3 | 1 |
| SBF | 0 | 0 | 0 | 0 |
| ETH Rat | 0 | 0 | 0 | 0 |
| SWISSMEDIC | 8 | 3 | 3 | 2 |
| SNF | 0 | 0 | 0 | 0 |
| SUVA | 1 | 0 | 1 | 0 |
| **TOTAL** | **48** | **22** | **17** | **9** |

**Eidgenössisches Justiz- und Polizeidepartement EJPD**

| Betroffener Fachbereich | Anzahl | Zugang vollständig gewährt | Zugang vollständig verweigert | Zugang teilweise gewährt / aufgeschoben |
|---|---|---|---|---|
| GS EJPD | 3 | 1 | 2 | 0 |
| BJ | 5 | 4 | 1 | 0 |
| FEDPOL | 3 | 2 | 0 | 1 |
| METAS | 0 | 0 | 0 | 0 |
| BFM | 13 | 10 | 2 | 1 |
| BA | 2 | 0 | 1 | 1 |
| SIR | 0 | 0 | 0 | 0 |
| IGE | 1 | 0 | 1 | 0 |
| ESBK | 3 | 2 | 1 | 0 |
| ESchK | 0 | 0 | 0 | 0 |
| RAB | 0 | 0 | 0 | 0 |
| ISC | 0 | 0 | 0 | 0 |
| **TOTAL** | **30** | **19** | **8** | **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 | 5 | 4 | 2 |
| Verteidigung/ Armee | 5 | 4 | 1 | 0 |
| armasuisse | 0 | 0 | 0 | 0 |
| BABS | 1 | 0 | 1 | 0 |
| BASPO | 3 | 3 | 0 | 0 |
| **TOTAL** | **20** | **12** | **6** | **2** |

**Eidgenössisches Finanzdepartement EFD**

| Betroffener Fachbereich | Anzahl | Zugang vollständig gewährt | Zugang vollständig verweigert | Zugang teilweise gewährt / aufgeschoben |
|---|---|---|---|---|
| GS | 2 | 0 | 2 | 0 |
| EFV | 0 | 0 | 0 | 0 |
| EPA | 1 | 0 | 1 | 0 |
| ESTV | 7 | 3 | 3 | 1 |
| EZV | 0 | 0 | 0 | 0 |
| EAV | 0 | 0 | 0 | 0 |
| BBL | 1 | 0 | 0 | 1 |
| BIT | 0 | 0 | 0 | 0 |
| EFK | 0 | 0 | 0 | 0 |
| PUBLICA | 0 | 0 | 0 | 0 |
| ZAS | 0 | 0 | 0 | 0 |
| **TOTAL** | **11** | **3** | **6** | **2** |

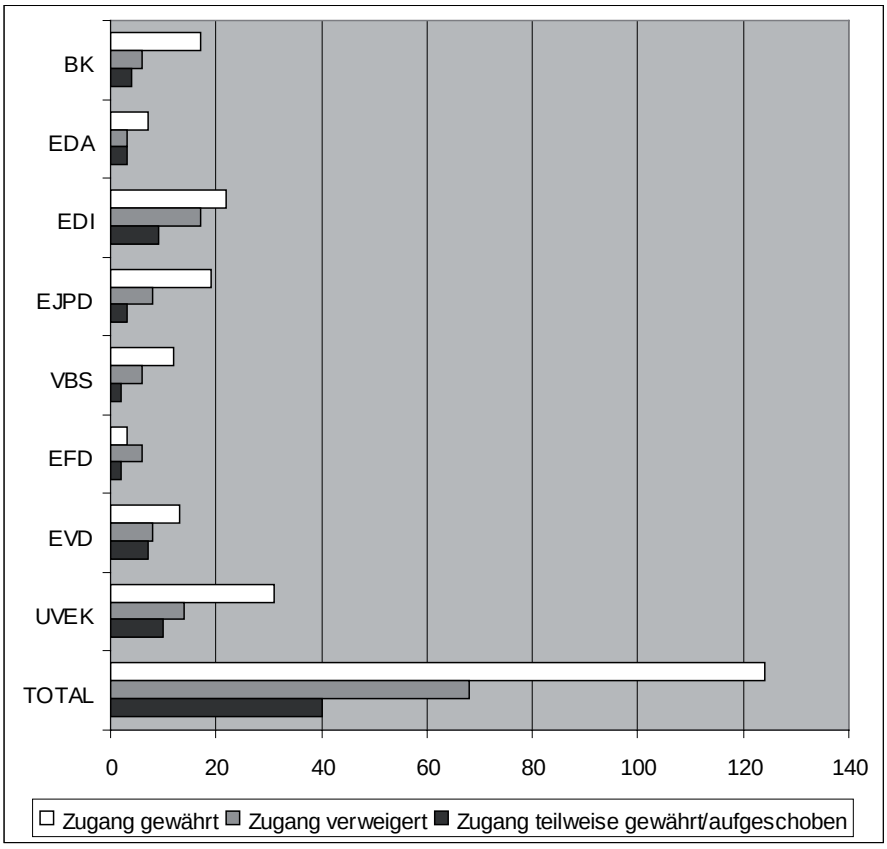
**Eidgenössisches Volkswirtschaftsdepartement EVD**

| Betroffener Fachbereich | Anzahl | Zugang vollständig gewährt | Zugang vollständig verweigert | Zugang teilweise gewährt / aufgeschoben |
|---|---|---|---|---|
| GS | 4 | 0 | 2 | 2 |
| SECO | 7 | 4 | 2 | 1 |
| BBT | 3 | 2 | 1 | 0 |
| BLW | 5 | 0 | 3 | 2 |
| BVET | 6 | 4 | 0 | 2 |
| BWL | 0 | 0 | 0 | 0 |
| BWO | 0 | 0 | 0 | 0 |
| PUE | 0 | 0 | 0 | 0 |
| WEKO | 1 | 1 | 0 | 0 |
| ZIVI | 2 | 2 | 0 | 0 |
| BFK | 0 | 0 | 0 | 0 |
| **TOTAL** | **28** | **13** | **8** | **7** |

**Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK**

| Betroffener Fachbereich | Anzahl | Zugang vollständig gewährt | Zugang vollständig verweigert | Zugang teilweise gewährt / aufgeschoben |
|---|---|---|---|---|
| GS | 1 | 0 | 1 | 0 |
| BAV | 5 | 3 | 1 | 1 |
| BAZL | 6 | 5 | 1 | 0 |
| BFE | 9 | 3 | 5 | 1 |
| ASTRA | 1 | 0 | 0 | 1 |
| BAKOM | 5 | 3 | 1 | 1 |
| BAFU | 17 | 8 | 3 | 6 |
| ARE | 0 | 0 | 0 | 0 |
| COMCOM | 1 | 1 | 0 | 0 |
| ENSI | 3 | 1 | 2 | 0 |
| PostReg | 3 | 3 | 0 | 0 |
| UBI | 4 | 4 | 0 | 0 |
| **TOTAL** | **55** | **31** | **14** | **10** |

**Behandlung der Zugangsgesuche**



## 3.6 Statistik über die bei den Parlamentsdiensten eingereichten Zugangsgesuche nach Art. 6 des Öffentlichkeitsgesetzes (Zeitraum: 1. Januar 2009 bis 31. Dezember 2009)

**Parlamentsdienste PD**

| Betroffener Fachbereich | Anzahl | Zugang vollständig gewährt | Zugang vollständig verweigert | Zugang teilweise gewährt / aufgeschoben |
|---|---|---|---|---|
| PD | 1 | 1 | 0 | 0 |
| **TOTAL** | **1** | **1** | **0** | **0** |

## 3.7 Anzahl Schlichtungsgesuche nach Kategorien der Antragsteller (Zeitraum: 1. Januar 2009 bis 31. Dezember 2009)

| Kategorie Antragsteller | 2009 |
|---|---|
| Medien | 18 |
| Privatpersonen (bzw. keine genaue Zuordnung möglich) | 8 |
| Interessenvertreter (Verbände, Organisationen, Vereine usw.) | 7 |
| Unternehmen | 5 |
| Rechtsanwälte | 2 |
| Universitäten | 1 |
| **Total** | **41** |

## 3.8 Das Sekretariat 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:** | 8 Personen |
| **Einheit 2:** | 12 Personen |
| **Einheit 3:** | 2 Personen |
| **Kanzlei:** | 3 Personen |

# 4. Anhänge

## 4.1 Datenschutz

### 4.1.1 Erläuterungen zur mobilen Datenbearbeitung

## Mobile Datenbearbeitung – Überblick





In Zeiten vor der elektronischen Datenverarbeitung brachte man seine Texte handschriftlich oder mit der Schreibmaschine zu Papier und verwahrte Vertrauliches in einem abschliessbaren Schrank vor neugierigen Blicken. Um Verlust z.B. durch Feuer zu begegnen, wurden Kopien angefertigt und diese an einem sicheren Ort gelagert.

Heute bestehen durch die Möglichkeiten der Informatik mannigfache Varianten der Datenbearbeitung, die einerseits bequem und effizient sind, anderseits insbesondere bei sensiblen Informationen Fragen der Datensicherheit aufwerfen. Insbesondere durch die Mobilität des modernen Menschen ergeben sich neue Risiken, denen adäquat begegnet werden muss. Wie dies konkret möglich ist, möchten wir im Folgenden am Beispiel von Herrn Unstet zeigen.

Herr Unstet fühlt sich wohl bei seinem Arbeitgeber. Trotzdem beobachtet er den Stellenmarkt aufmerksam und bewirbt sich von Zeit zu Zeit auf Stellen, die ihm interessant erscheinen. Dazu aktualisiert er sein Curriculum Vitae (CV) regelmässig.

Als moderner mobiler Mensch will Herr Unstet jederzeit und überall an seinem CV arbeiten können. Dabei hat er selbstverständlich den Anspruch, jeweils auf die letzte Version des Dokuments Zugriff zu haben. Da der Lebenslauf sehr persönliche Angaben enthält und zudem ein Persönlichkeitsprofil darstellt, ist es von Bedeutung, dass die Vertraulichkeit des Dokuments stets gewahrt bleibt.

Herr Unstet ist datenschutzsensibilisiert und legt hohen Wert auf die Vertraulichkeit seiner Personendaten. Daher überlegt er sich, welche Kriterien für eine datenschutzfreundliche und sichere Bearbeitung erfüllt sein müssen. Ihm ist bekannt, dass gemäss einer in London 2006 durchgeführten Untersuchung innerhalb eines halben Jahres 55'000 Mobiltelefone, 5000 Handhelds, 3000 Laptops und 900 USB-Sticks in den Taxis

Londons gefunden wurden[1]. Eine weitere Gefahr geht von Schadcodes (Viren, Trojaner, Würmer) aus, die sich über portable Geräte verbreiten. Kriminelle versuchen vermehrt, auf diese Weise an sensible Personendaten zu gelangen.[2]

Im Einzelnen prüft Herr Unstet, inwieweit Vertraulichkeit, Integrität und Verfügbarkeit seiner Daten beim Einsatz der verschiedenen Lösungen gewährleistet sind. Besonderes Augenmerk richtet er auf die in Art. 8 der Verordnung zum Bundesgesetz über den Datenschutz (VDSG) aufgeführten Risiken:

- unbefugte oder zufällige Vernichtung
- zufälliger Verlust
- technische Fehler
- Fälschung, Diebstahl oder widerrechtliche Verwendung
- unbefugtes Ändern, Kopieren, Zugreifen oder andere unbefugte Bearbeitungen.

Welche Lösungen stehen Herrn Unstet nun zur mobilen Bearbeitung seines CVs zur Verfügung?

Folgende vier Grobformen (Modelle) können unterschieden werden:

- Daten lokal, Anwendung lokal
- Daten lokal, Anwendung im Internet
- Daten im Internet, Anwendung lokal
- Daten im Internet, Anwendung im Internet

Für jede dieser Variationen ergeben sich spezifische Anforderungen, welche für die Datenschutzansprüche von Herrn Unstet relevant sind. Diese werden nachfolgend detailliert beschrieben.



[1] http://www.pressebox.de/pressemeldungen/ime-mobile-solutions-gmbh-0/boxid-94946.html
[2] http://www.symantec.com/de/de/about/theme.jsp?themeid=smpr_20090415&depthpath=0

## Modell 1: Daten und Anwendung lokal

Bei diesem Modell gibt es drei Varianten, welche für Herrn Unstet interessant sind:

a) Daten und Anwendung befinden sich auf einem Laptop oder einem ähnlichen Gerät. Herr Unstet benutzt seinen Laptop, auf dem sich sein elektronischer Lebenslauf und die Anwendungen für dessen Bearbeitung befinden. Er kann in diesem Fall die Daten ohne externen oder entnehmbaren Speicher und auch ohne Verbindung zum Internet bearbeiten.

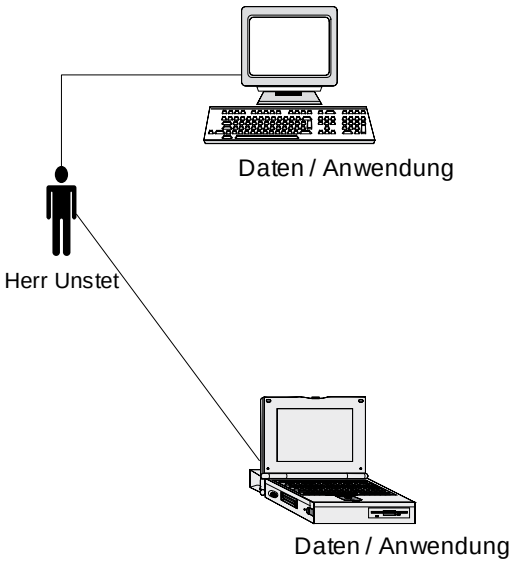
b) Die Daten befinden sich auf einem USB-Stick und die Anwendung auf einem PC (z.B. zu Hause, am Arbeitsplatz oder im Internetcafe). Herr Unstet verfügt über keinen tragbaren Computer. Sein CV befindet sich auf einem mobilen Speicher (z.B. auf einem USB-Stick). Damit er die Daten bearbeiten kann, benötigt er einen Rechner mit einer kompatiblen Anwendung. Er kann z.B. an seinem Heim-PC, am Büroarbeitsplatz, im Internetcafe usw. den USB-Stick mit dem Rechner verbinden. Er bearbeitet die Daten direkt auf dem Stick. In diesem Fall benötigt er ebenfalls keine Internetverbindung. Regelmässiges Kopieren der Daten auf ein sicheres Gerät ist unerlässlich (Backup).

c) Daten und Anwendung befinden sich auf einem mobilen Datenträger wie z.B. einem USB-Stick.





### Eigenschaften und Beispiele



Eine Internetverbindung ist in keiner der beschriebenen Varianten notwendig. Sowohl die Daten als auch die zu deren Bearbeitung erforderliche Anwendung sind bei Variante a und c unter Kontrolle und Verantwortung von Herrn Unstet.

**Beispiel**

Als Textverarbeitung kann beispielsweise AbiWord[3], eine kostenlos erhältliche Anwendung, die für alle gängigen Betriebssysteme verfügbar ist, benutzt werden. AbiWord existiert auch als portable Version[4], die man auf einem USB-Stick überall hin mitnehmen kann. Sie lässt sich ohne Installation auf dem Rechner, auf dem gerade gearbeitet wird, starten. Dies ist sehr nützlich, falls dieser Computer keine geeignete Textverarbeitung enthält.

**Vorteile**

Befinden sich sowohl die Daten als auch die Anwendung auf einem lokalen Speicher, wird die Gefahr von Zugriffen Dritter oder von Malware aus dem Internet eliminiert. Zum anderen ist man unabhängig von externen Anbietern. Bei den Varianten a und c ist die Verfügbarkeit des Nutzers über Daten und Anwendung hoch.

**Nachteile**

Herr Unstet muss seine Speichermedien (mit Daten und Anwendung) aufgrund der Gefahr von Verlust oder Beschädigung stets mit sich führen. Zudem ist das Anfertigen von Sicherungskopien aufwendig und die Mobilität des Nutzers eingeschränkt. Bei Variante b hat Unstet nur Zugriff auf sein CV, wenn er zusätzlich einen PC mit einer kompatiblen Anwendung findet.

**Fazit: Risiken und Empfehlungen**

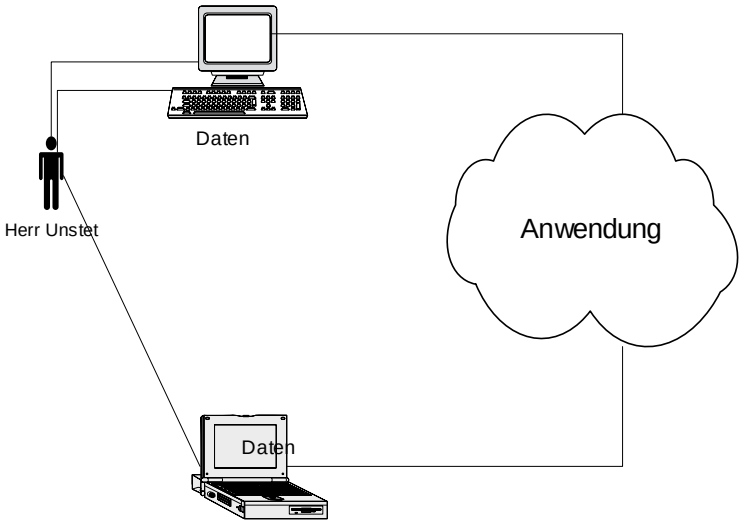
Bei Modell 1 wird die hohe Verfügbarkeit mit einer umständlichen Handhabung erkauft. Dafür ist die Vertraulichkeit hoch. Daten, die sich auf einem USB-Träger befinden, sind gefährdet durch Verlust, Beschädigung oder Vernichtung, sei es durch Diebstahl oder einen technischen Defekt. Wer USB-Sticks verwendet, sollte daran denken, dass diese schnell verloren gehen können. Wenn es die Schutzwürdigkeit der Daten erfordert, sollte man deshalb unter allen Umständen mit chiffrierten Daten arbeiten. Eine einfache und gratis im Netz erhältliche Anwendung für diesen Zweck ist z.B. Truescript.

[3] http://www.abisource.com/ ou http://abiword.org
[4] http://portableapps.com/

## Modell 2: Daten lokal, Anwendung im Internet

Bei diesem Modell befinden sich die Daten entweder auf einem Rechner (z.B. PC oder Laptop) oder auf einem mobilen Speichermedium (z.B. USB-Stick). Dieses Modell ist in der Praxis eher selten. Meistens stellen die Anbieter sowohl die Anwendung als auch den Speicherplatz für die Daten im Paket zur Verfügung. Doch kann man diese Konstellation auch erreichen, indem man die Daten lokal speichert und beim Provider löscht.

### Eigenschaften




Da Herr Unstet nur seinen Lebenslauf auf sich trägt, ist er für dessen Bearbeitung auf die Anwendung eines Anbieters angewiesen. Diese findet er im Internet. Für dieses Modell ist eine Internetverbindung also zwingend notwendig.

### Vorteile

Herr Unstet muss die Anwendung nicht lokal mit sich führen. Seine Daten wären auch dann noch physikalisch vorhanden, wenn der Anbieter ausfallen würde (z.B. den Dienst einstellt). Die meisten Anbieter ermöglichen es ihren Kunden, die Daten in gängigen Formaten abzuspeichern (pdf, doc usw.)

### Nachteile

Für die Bearbeitung der Daten ist eine Internetverbindung erforderlich. Diese birgt die Gefahr von unbefugten Zugriffen sowie einer Infektion durch Malware. Herr Unstet ist darauf angewiesen, dass die angebotene Anwendung zur Verfügung steht und zu seinen Daten kompatibel ist. Die Möglichkeit der Datenbearbeitung kann verloren gehen, wenn der Anbieter einer proprietären Anwendung seinen Dienst einstellt. Das dürfte allerdings selten der Fall sein.

### Fazit: Risiken und Empfehlungen

Es besteht das Risiko, dass der Anbieter der Anwendung Kopien der Daten auch dann noch auf seinen Servern behält, wenn der Nutzer die Daten nach der Bearbeitung gelöscht hat. Dieses Modell ist insbesondere dann mit Vorsicht zu nutzen, wenn mit heiklen Personendaten gearbeitet wird. Es empfiehlt sich, Daten verschlüsselt zu bearbeiten. Wenn Herr Unstet sein CV mit «Google Text & Tabellen» bearbeitet, kann er den Text in der Textverarbeitung direkt verschlüsseln (z.B. mit ClipSecure) und so abspeichern. Seine Daten sind somit geschützt.

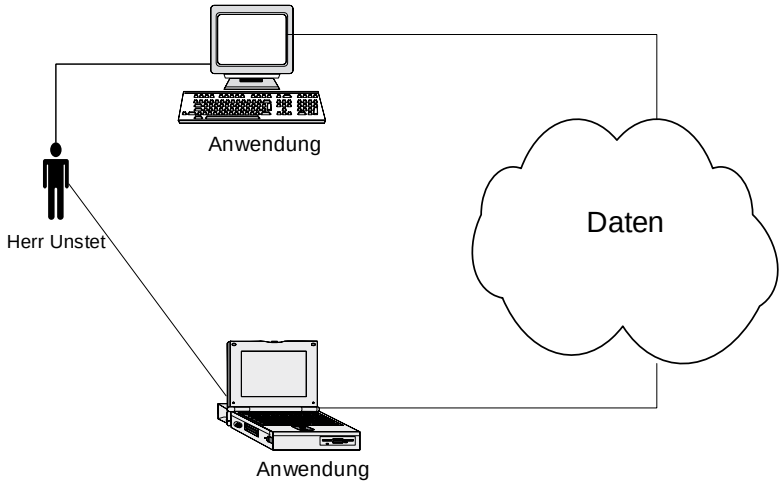




## Modell 3: Daten im Internet – Anwendung lokal

Herr Unstet bearbeitet sein CV bei diesem Model zwar mit einer lokalen Textverarbeitung, speichert sein Dokument jedoch bei einem Anbieter im Internet.

### Eigenschaften und Beispiele




### Beispiel Wuala[5]

Diese kostenlose peer-to-peer basierte Software erlaubt es dem User, seine Dokumente verschlüsselt im Internet abzulegen (die Nutzung grösserer Speicherkapazitäten ist allerdings kostenpflichtig). Der Wuala-Speicherplatz ist als virtuelle Festplatte sichtbar und somit nach gewohnter Manier zu verwenden. Jeder teil-

[5] http://www.wuala.com/de/

nehmende Benutzer kann auch eigenen, nicht genutzten Speicherplatz zur Verfügung stellen. Die Ver- bzw. Entschlüsselung findet auf dem lokalen Rechner statt, so dass die Klartexte diesen nicht verlassen. Auch den Administratoren von Wuala wäre es nicht möglich, die hinterlegten Dokumente zu entschlüsseln.

Als Textverarbeitung kann beispielsweise **AbiWord**[6] benutzt werden (siehe Seite 5).

Bei diesem Modell gibt es drei Varianten, welche für Herrn Unstet interessant sind:

a) Die Anwendung befindet sich auf einem Laptop oder einem ähnlichen Gerät,

b) auf einem PC (z.B. zu Hause, Arbeitsplatz, Internetcafe)

c) oder auf einem USB-Stick.

**Vorteile**

- Zuhause, im Büro, im Internetcafé oder mit dem WLAN-Notebook/Smartphone unterwegs kann Herr Unstet auf sein CV zugreifen und dieses bearbeiten. Er muss keine Dateien auf Datenträgern mit sich führen.
- Da er sein CV-File nicht mit sich führt, kann er es auch nicht verlieren. Beschädigungen von Datenträgern lassen Herrn Unstet kalt.
- Herr Unstet braucht sich nicht selber um das Backup seiner Daten zu kümmern, da dieses in der Regel vom Internetanbieter übernommen wird. Der Verlust der Dokumente ist sehr unwahrscheinlich.
- Bei Bedarf ist ein Anbieter mit Servern in Hochsicherheitsumgebung und geografisch getrennter Ablage möglich (Stichwort: Datenbunker im Internet).
- Meist kostengünstig

**Nachteile**

- Ohne Internetverbindung kann Herr Unstet zwar seine Textapplikation starten, jedoch nicht auf seine Dokumente zugreifen. Das Vorhandensein eines Internetanschlusses ist also Bedingung.
- Auf dem Rechner, auf dem Herr Unstet gerade arbeitet, muss eine geeignete Textverarbeitungsanwendung installiert sein (was in der Regel der Fall ist) oder er muss eine solche mit sich führen.
- Falls der Internetanbieter technisch auf den Klartext Zugriff hat, muss Herr Unstet auf dessen Redlichkeit vertrauen.

[6] http://www.abisource.com/ oder http://abiword.org/, http://portableapps.com/

**Fazit: Risiken und Empfehlungen**

- AGB sollten sorgfältig gelesen werden.
- Es empfiehlt sich, die beim Internetanbieter hinterlegten Daten zu verschlüsseln, wenn möglich auf dem Client-Rechner.
- Auch wenn der Internetanbieter um die Sicherung und Verfügbarkeit der Dokumente besorgt ist, sollte bei wichtigen Dokumenten von Zeit zu Zeit eine Kopie erstellt und an einem sicheren Ort verwahrt werden.

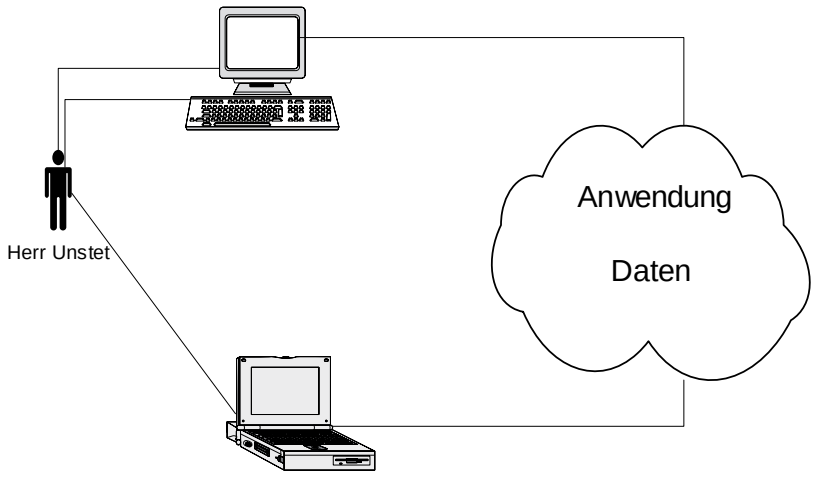




## Modell 4: Daten im Internet – Anwendung im Internet

Bei diesem Modell benutzt Herr Unstet eine Internetanwendung und legt sein CV ebenfalls im Internet ab. Weder Anwendung noch Daten sind also lokal gespeichert.

**Eigenschaften und Beispiele**




**Beispiel: Google Text & Tabellen**[7]

Die von Google kostenlos angebotene Textverarbeitungs- und Tabellenkalkulationsanwendung läuft direkt im Internetbrowser des Benutzers. Es muss keine zusätzliche Software installiert werden. An jedem PC mit Internetzugang ist also das Arbeiten an den Texten problemlos möglich.

Eine lokale Speicherung und das Hochladen von Dokumenten sind möglich, jedoch lässt sich die regelmässige automatische Speicherung im Internet nicht ausschalten.

[7] http://docs.google.com/

Eine Verschlüsselung der Dateien bietet Google nicht an. Vergleichbare Anwendungen sind beispielsweise **Zoho Writer[8] und thinkfree[9].**

### Vorteile

- Herr Unstet kann sich an einen beliebigen, mit dem Internet verbundenen Rechner (zu Hause, am Arbeitsplatz, im Internet-Café etc.) setzen und sein CV bearbeiten. Er muss keinen Datenträger mit sich führen. Somit besteht auch kein Risiko auf Beschädigung, Verlust oder Diebstahl eines USB-Sticks oder eines andern Speichermediums. Auch bei Diebstahl oder Verlust des Rechners bleibt Herr Unstet im Besitz seiner Daten.
- Während der Arbeit am Dokument werden die vorgenommenen Änderungen generell automatisch und in regelmässigen Abständen gespeichert.
- Herr Unstet muss nicht an ein Backup denken.
- Das Risiko eines Datenverlusts durch Brand, Wasser, Diebstahl etc. ist gering.

### Nachteile

- Um auf seine Daten zugreifen und diese bearbeiten zu können, ist immer eine funktionierende Internetverbindung erforderlich.
- Solange die Daten nicht verschlüsselt sind (Google Text & Tabellen bietet keine Verschlüsselungsfunktion), kann die Vertraulichkeit der Daten gefährdet sein. Der Benutzer hat nur eine eingeschränkte Kontrolle über seine Daten.

### Fazit: Risiken und Empfehlungen

- Lesen Sie die AGB der beteiligten Dienstleister sorgfältig, insbesondere die Datenschutzbestimmungen; wer hat in welchem Fall auf welche Daten Zugriff?
- Beim Arbeiten ist darauf zu achten, dass keine Spuren hinterlassen werden bzw. diese nach Beendigung der Arbeit sicher gelöscht werden. Dies gilt vor allem, wenn auf fremden Rechnern (z.B. im Internet-Café) gearbeitet wird.

[8] http://writer.zoho.com/
[9] http://www.thinkfree.com/

- Wählen Sie gute Passwörter.
- Der verwendete Rechner muss frei von Malware sein, namentlich um Angriffe auf ihre Dokumente zu vermeiden. Ebenso ist sicherzustellen, dass keine Keylogger oder ähnliches auf dem Rechner installiert sind, die die Zugangsdaten des Nutzers zum Online-Textsystem abfangen.
- Man muss darauf vertrauen, dass der Internetanbieter die persönlichen Daten korrekt und vertraulich behandelt. Bei wirtschaftlichen Problemen könnte dieser z.B. in Erwägung ziehen, die verwalteten Personendaten zu verkaufen (z.B. im Insolvenzverfahren).

Zur Verschlüsselung der Texte kann beispielsweise **ClipSecure**[10] eingesetzt werden. Dabei handelt es sich um eine einfach zu bedienende Freeware, die zusammen mit jeder textbasierten Anwendung funktioniert, insbesondere mit Google Text & Tabellen, das im Webbrowser läuft. Quasi auf Knopfdruck kann der Text ver- oder entschlüsselt werden. Allerdings ist zu bemerken, dass der Text während des Bearbeitens auf dem Server von Google grundsätzlich eingesehen werden könnte.

## Schlussbetrachtung

Die Wahl der Lösung ist von verschiedenen Faktoren abhängig. Sie wird entscheidend beeinflusst durch die Kosten, die Schutzwürdigkeit der Daten oder von formalen Vorgaben (z.B. Dokumentenformat, Teamarbeit). Ausserdem sind gesetzliche Vorschriften (z.B. staatliche Vorschriften in Bezug auf chiffrierte Daten) und die Verfügbarkeit der Mittel (z.B. Internetzugänge) von grosser Bedeutung. Die oben vorgestellten Modelle können mit mehr oder weniger grossem Aufwand datenschutzkonform gestaltet werden.

Es ist heute technisch machbar, Daten aus der Ferne zu bearbeiten. Allerdings ist die Qualität einer solchen Lösung abhängig von den zu bearbeitenden Daten.

Wenn die Daten keine persönlichen Informationen enthalten, ist aus datenschutzrechtlicher Sicht keine der besprochenen Varianten kritisch. Sobald aber Daten bearbeitet werden, die aus persönlichem Interesse oder aufgrund gesetzlicher Anforderungen nicht für Dritte bestimmt sind, gelten strengere Anforderungen an die Lösungen. Wenn die Information nicht für andere Augen bestimmt ist, sollte man sich an diesen Grund-

[10] http://www.snapfiles.com/get/clipsecure.html

satz halten: Man sollte die Daten stets **chiffrieren**, egal wo und auf welchem Medium sie gespeichert sind und wer sie administriert. Das gilt auch für Daten, die auf einem USB-Stick aufbewahrt werden.

Ein weiterer Entscheidungsfaktor für die Wahl einer Lösung bildet die Anforderung an die Verfügbarkeit der Daten. Wie oben erwähnt, gehen gespeicherte Daten häufig verloren durch den Verlust von Mobiltelefonen, Handhelds, Laptops oder USB-Sticks. Das Risiko eines Datenverlusts ist kleiner, wenn die Daten auf der Infrastruktur professioneller Provider gespeichert und administriert werden. Zudem ist die Stabilität solcher Systeme in der Regel höher. Allerdings muss sich der Anwender merken, wo er welche Daten abgelegt hat. Wenn er die Übersicht darüber verliert, können später wiedererweckte «Datenleichen» für Überraschungen sorgen.

Das gleiche gilt für den Schutz der Daten vor Schadcode. Professionelle Provider haben in der Regel wirksamere Mittel, um Daten vor Viren, Trojanern, Würmern und anderer Malware zu schützen, als der Endbenutzer auf seinen mobilen Geräten.

Die nachfolgende Tabelle soll dabei helfen, für die Minimierung eines Risikos das richtige Modell zu finden. Es handelt sich um eine rudimentäre Qualifizierung der Modelle bezüglich der unter Art. 8 ff VDSG aufgeführten Risiken. Abschliessend muss betont werden, dass es keinen absoluten Schutz für gespeicherte Daten gibt, auch für die höchst persönlichen nicht. Deshalb ist jede Speicherung einer schützenswerten Information riskant – unabhängig vom gewählten System oder Modell.

| Risiken / Modell | Unbefugte oder zufällige Vernichtung | Zufälliger Verlust | Technische Fehler | Fälschung, Diebstahl oder widerrechtliche Verwendung | Unbefugtes Ändern, Kopieren, Zugreifen oder unbefugte Bearbeitung |
|---|---|---|---|---|---|
| Modell 1 | Klein | Gross | Gross | Mittel | Klein |
| Modell 2 | Klein | Gross | Gross | Mittel | Mittel |
| Modell 3 | Klein | Klein | Mittel | Klein/Mittel | Klein/Mittel |
| Modell 4 | Klein | Klein | Mittel | Klein/Mittel | Mittel |

## Weiterführende Dokumente und Links


Praxistipp: Sicherheit von USB-Sticks in Unternehmen. In: Datenschutzberater 4/2009

PC News: «Installationsfreie Programme und USB-Sticks». 2008, in: http://pcnews.at/?Id=14611&Type=Htm

FoeBud e.V.: PrivacyDongle – Anonym im Internet surfen. 2009, in: https://www.foebud.org/datenschutz-buergerrechte/vorratsdatenspeicherung/privacydongle/index

Pressetext Austria: Datenspeicher der Zukunft sind im Web. 2.10.2008, in: http://pressetext.ch/news/081002003/datenspeicher-der-zukunft-sind-im-web/

Fraunhofer Institut: Privatsphärenschutz in Soziale-Netzwerke-Plattformen. 2008, in: http://www.sit.fraunhofer.de/Images/SocNetStudie_Deu_Final_tcm105-132111.pdf

News.ch: Das Internet als Daten-Tresor oder gemeinsame Festplatte. 13.01.2009, in: http://www.news.ch/Das+Internet+als+Daten+Tresor+oder+gemeinsame+Festplatte/330494/detail.htm

Bildung Schweiz: Büro 2.0 – online sein ist alles. 2009, in: http://www.lch.ch/dms-static/e08a9090-8a86-4473-a6a0-8e96778395a4/bildungsnetz37.pdf

PC-Welt: Kostenloser Datenspeicher im Netz. 2008, in: http://content8.wuala.com/contents//Wuala/Blogs%20and%20Press/German/Magazine%20-%20Print%20und%20Online/2008-09-24%20PC%20Welt.pdf

Thomas Söbbing: Cloud Computing – die Zukunftsvisionen von Amazon, Google und Microsoft rechtlich betrachtet. 2009, in: jusletter.ch vom 10.8.09.

World Privacy Forum: Privacy in the Clouds – Risks to Privacy and Confidentiality from Cloud Computing. 2009.

Landesbeauftragter für den Datenschutz Niedersachsen: Mobiles Arbeiten – datenschutzgerecht gestaltet, Orientierungshilfe und Checkliste. 2003.

### 4.1.2 Informationen und Tipps zum Umgang mit Suchmaschinen

#### Einleitung

Aus dem Internet sind Suchmaschinen heute nicht mehr wegzudenken, und ohne sie wäre eine sinnvolle Nutzung des World Wide Web mit seinen Milliarden von Seiten praktisch unmöglich. Um die Auffindbarkeit von Informationen im Internet ständig zu verbessern, müssen Suchmaschinen allerdings gezielt Informationen über das Suchverhalten und die Qualität der Suchtreffer erheben und statistisch auswerten. Nur schon die stetig wachsende Anzahl an Internetseiten macht es für Betreiber von Suchmaschinen erforderlich, eine immer grössere Anzahl an Informationen zu bearbeiten.

Einerseits leisten Suchmaschinen einen Beitrag an die Informations- oder Wissensgesellschaft und steuern damit zum nachhaltigen wirtschaftlichen Wachstum unserer Gesellschaft bei. Andererseits greifen sie durch die Bearbeitung von personenbezogenen Daten **auch in die Privatsphäre von Internetnutzern ein**, und zwar sowohl bei der Auswertung der Suchanfragen als auch bei der Bereitstellung von Suchergebnissen.





#### Datenschutzprobleme mit Suchmaschinen

Aus Datenschutzperspektive lassen sich grundsätzlich zwei verschiedene Problembereiche im Umgang mit Suchmaschinen identifizieren. Der erste betrifft das **Zusammenführen von Informationen, welche sich auf verschiedenen, von einander unabhängigen Internetseiten befinden** und durch die Suchmaschine im Rahmen der Anzeige der Treffer dem User zugänglich gemacht werden. Zum anderen sammeln Suchmaschinen unter Registrierung der IP-Adresse sämtliche Anfragen, Ergebnisse und Trefferabrufe der Benutzer und können so Personenprofile von Suchenden anlegen, auswerten und nutzen.

#### Hintergrundinformationen und Tipps

- Sobald im Internet Daten über eine bestimmte Person verfügbar sind, kann man diese über Suchmaschinen nahezu beliebig finden. Suchmaschinen ermöglichen es, auch noch so verstreute Informationen zusammenzuführen und an einem Ort abzurufen. Vor diesem Hintergrund sollten Internetnutzer sehr sorgfältig abwägen, **welche Informationen** sie über sich ins Internet stellen.
- Zwar können einzelne Daten für sich genommen harmlos sein (z.B. Vereinsinformationen, Informationen über die Arbeitsstelle, über das Studium, etc.). Werden diese allerdings zusammengetragen und analysiert, so kann hieraus schnell ein online abrufbares **Persönlichkeitsprofil** entstehen. Oftmals hat-

ten die Nutzer nie die Absicht, ein solches Profil im Internet verfügbar zu machen. Es ist zudem zu beachten, dass die Daten auch **von dritter Seite** im Internet publiziert werden können.

- Es ist kaum möglich, Suchmaschinen das Zusammentragen von Ergebnissen zu verbieten. Vielmehr müssen die betroffenen Personen die Betreiber der einzelnen Webseiten gezielt angehen, um ihre Löschungs- und Berichtigungsrechte geltend zu machen. Daher sollten User **stets ein wachsames Auge** darauf haben, welche Daten über sie im Internet verfügbar sind und somit über Suchmaschinen gesammelt werden könnten.
- Betreiben Sie selbst eine Website, können Sie den Suchmaschinen im Html-Code **Anweisungen** geben, eine bestimmte Seite nicht auf den Index zu setzen.
- Benutzt eine betroffene Person neben den Suchfunktionen noch **weitere Dienste des Betreibers**, wie z.B. Email-Angebote, so kann der Betreiber nicht nur die IP-Adresse, sondern auch die dahinter stehende Person identifizieren. Über die **Verknüpfung** der Suchanfragen **mit den Identitätsdaten** liesse sich so ebenfalls ein Persönlichkeitsprofil erstellen. Sucht jemand im Internet beispielsweise des Öfteren nach bestimmten Krankheitsbildern, könnte man daraus schliessen, dass dieser User an der betreffenden Krankheit leidet. Würden solche Daten weitergegeben, so könnte die betroffene Person entsprechende Nachteile erleiden.
- Da die Betreiber von Suchmaschinen vorwiegend davon leben, möglichst effektiv und **zielgruppengerichtet** online Werbung zu schalten, haben sie ein nicht unerhebliches Interesse an einer Verknüpfung der Suchanfrage mit den Identitätsdaten. Dies ist solange unproblematisch, als die verknüpften Daten (Persönlichkeitsprofile) nicht zu anderen Zwecken verwendet werden (z.B. für die Weitergabe an eine Versicherung zur Berechnung von Versicherungsprämien).
- Ferner ist zu beachten, dass fast alle Suchmaschinen sämtliche **Anfragen** inkl. IP-Adresse über einen längeren Zeitraum **speichern** (in der Regel mehrere Monate). Mittlerweile sind jedoch auch Suchmaschinen verfügbar, welche die Identifikationsdaten der Nutzer schneller löschen oder gar nicht speichern (z.B. cuil.com oder scroogle.org).
- Als Nutzer von Suchmaschinen sollten Sie sich vor Augen halten, dass solche Möglichkeiten der **Verknüpfung** bestehen, und daher **selbst für sich abwägen**, wie viele und welche Dienstleistungen Sie von einem einzelnen An-

bieter in Anspruch nehmen möchten. Zudem können die Privacy Policies der Anbieter Aufschluss darüber geben, in welchen Ländern die Daten bearbeitet und wie lange sie aufbewahrt werden.

### 4.1.3 Erläuterungen zum betrieblichen Datenschutzverantwortlichen

## Der betriebliche Datenschutzverantwortliche im Gesetz

Das revidierte Bundesgesetz über den Datenschutz vom 01. Januar 2008 (DSG, SR 235.1) ermöglicht Unternehmen durch verschiedene Gesetzesänderungen die Selbstregulierung. So müssen beispielsweise laut Art. 11a Abs. 5 lit. e Inhaber von Datensammlungen diese nicht anmelden, wenn sie einen Datenschutzverantwortlichen bezeichnet haben, der unabhängig die betriebsinterne Einhaltung der Datenschutzvorschriften überwacht und Verzeichnisse der Datensammlungen führt. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) muss darüber informiert werden.

Das DSG spricht in der deutschen Version vom «Datenschutzverantwortlichen», während in der französischen Version vom «conseiller à la protection des données», also dem «Datenschutzberater», gesprochen wird. Da es nicht das Ziel des Gesetzgebers war, die Verantwortung des Inhabers der Datensammlung auf die Person des Datenschutzverantwortlichen abzuwälzen, ist in der Auslegung des DSG der französischen Version zu folgen. Somit liegt die Verantwortung in erster Linie beim Inhaber der Datensammlung (also dem die Daten bearbeitenden Unternehmen). Der Datenschutzverantwortliche haftet nur im Rahmen von Art. 55 des Bundesgesetzes betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht; OR; SR 220).

Die Aufgaben und die organisatorische Stellung des betrieblichen Datenschutzverantwortlichen sind in den Artikeln 12a und 12b der Verordnung zum Bundesgesetz über den Datenschutz (VDSG, SR 235.11) festgehalten.

## Stellung des betrieblichen Datenschutzverantwortlichen

Um seine Aufsichtsfunktion wahrnehmen zu können, muss der Datenschutzverantwortliche die Einhaltung der Datenschutzvorschriften innerhalb des Betriebs unabhängig überwachen (Art. 11a Abs. 5 lit. e DSG). Damit die Selbstregulierung überhaupt effektiv umgesetzt werden kann, muss seine Unabhängigkeit sowohl in organisatorischer und fachlicher Hinsicht als auch im Hinblick auf seine Tätigkeit innerhalb des Betriebs gewährleistet sein.

### Unabhängigkeit in organisatorischer Hinsicht

Um innerhalb des Unternehmens seine Aufgaben wahrnehmen zu können, darf der Datenschutzverantwortliche keine anderen Tätigkeiten ausüben, die mit seinen Aufgaben unvereinbar sind. Ein möglicher Interessenskonflikt muss also bereits durch die organisatorische Stellung des Datenschutzverantwortlichen vermieden werden. In der Praxis bedeutet dies, dass Unternehmen die Funktion des Datenschutzverantwortlichen entweder als Stabstelle oder als Stelle innerhalb der Rechtsabteilung ausgestalten. Gelegentlich ist der Datenschutzverantwortliche auch in der IT-Abteilung oder im Vorstand angesiedelt.

Grundsätzlich sollte in organisatorischer Hinsicht darauf geachtet werden, dass die Stelle des Datenschutzverantwortlichen ausserhalb der Linienverantwortlichkeit steht, da sonst Interessenskonflikte drohen. Einem Unternehmen stehen in diesem Zusammenhang verschiedene Möglichkeiten zur Verfügung, welche von einer Stabstelle bis hin zu einem externen Datenschutzverantwortlichen reichen.

### Unabhängigkeit in fachlicher Hinsicht

Der Datenschutzverantwortliche muss, um seine Aufgaben gehörig und unabhängig durchführen zu können, zudem die notwendige fachliche Eignung aufweisen. Das Recht spricht lediglich davon, dass er über die erforderliche Fachkenntnis verfügen muss (Art. 12a Abs. 2 und Art. 12b Abs. 2 lit. a VDSG), ohne diese aber näher zu präzisieren.

Die Anforderungen umfassen sowohl die Kenntnisse im Bereich Datenschutz als auch die für den Betrieb spezifischen Fachkenntnisse. So sollte der Verantwortliche die wesentlichen Grundzüge des Datenschutzgesetzes kennen und anwenden können. Bringt er nicht bereits juristische Kenntnisse mit, sollte er soweit geschult werden, dass er sich mindestens selbständig ein Bild darüber machen kann, ob, wann und inwiefern eine Datenbearbeitung geeignet ist, die Persönlichkeit einer betroffenen Person zu verletzen. Der EDÖB empfiehlt daher, dass ein (nicht juristisch ausgebildeter) Datenschutzverantwortlicher wenigstens ein halbes Jahr im Bereich Datenschutz gearbeitet bzw. eine Schulung von dieser Dauer erhalten hat.

Weiter muss der Datenschutzverantwortliche aber auch den Betrieb selbst kennen. So muss er aufgrund seiner Fachkenntnisse die angewandten technischen Standards, die Organisation des Inhabers der Datensammlung sowie die einzelnen Bearbeitungen von Personendaten datenschutzrechtlich beurteilen können. Je nach Unternehmen kann dies im Hinblick auf technische Kompetenzen sehr hohe Anforderungen an den Datenschutzverantwortlichen stellen. So sollte der Inhaber dieser Funktion in einem IT-Unternehmen sicherlich über ausreichende technische Erfahrung (bspw. als Program-

mierer) verfügen, um die Datenbearbeitung sowohl technisch als auch datenschutzrechtlich überprüfen zu können.

### Unabhängigkeit im Hinblick auf seine Tätigkeit

Der Datenschutzverantwortliche muss in seiner Tätigkeit soweit unabhängig sein, dass er seine Aufgaben weisungsunabhängig wahrnehmen kann und aufgrund seiner Tätigkeit vom Unternehmen nicht sanktioniert werden darf. Zudem muss er mit ausreichend Ressourcen (meist in Form von Arbeitszeit) ausgestattet sein, um seine innerbetrieblichen Aufgaben erfüllen zu können (Art. 12b Abs. 2 lit. b VDSG). Zwar bestehen je nach Grösse des Unternehmens unterschiedliche Anforderungen; der EDÖB verlangt jedoch, dass die Stelle des Datenschutzverantwortlichen in jedem Fall über genügend Ressourcen verfügt, damit die Funktion nicht zur Alibiübung verkommt.

Weiter muss der Verantwortliche Zugang zu allen Datensammlungen und Datenbearbeitungen sowie zu allen Informationen, die er zur Erfüllung seiner Aufgabe benötigt, haben (Art. 12b Abs. 2 lit. c VDSG). Dies beinhaltet neben dem Zugang auf Anfrage auch, dass er Kenntnis von sämtlichen innerhalb des Unternehmens durchgeführten Datenbearbeitungen erhält.

## Aufgaben des betrieblichen Datenschutzverantwortlichen

Die VDSG sieht für den Datenschutzverantwortlichen im Wesentlichen zwei Aufgabenkategorien vor:

- Auf der einen Seite prüft er die Bearbeitung von Personendaten und empfiehlt Korrekturmassnahmen, wenn er feststellt, dass Datenschutzvorschriften verletzt werden (Art. 12b Abs. 1 lit. a VDSG).
- Auf der anderen Seite führt er intern eine Liste der Datensammlungen nach Art. 11a Abs. 3 DSG (Art. 12b Abs. 1 lit. b VDSG).

Für eine umfassende Wahrnehmung seiner Aufsichtsfunktion muss sich der Datenschutzverantwortliche einen Überblick über sämtliche im Unternehmen bestehenden Datensammlungen und Datenbearbeitungen verschaffen können. Dazu benötigt er ein umfassendes Einsichtsrecht in Dokumente, ein Vorführungsrecht im Hinblick auf Datenverarbeitungssysteme und ein Auskunftsrecht gegenüber sämtlichen für die Datenbearbeitungen verantwortlichen Personen. Dies beinhaltet im Hinblick auf die Auskunftserteilung innerhalb des Unternehmens Weisungsbefugnis; das Unternehmen hat dafür zu sorgen, dass den Weisungen des Verantwortlichen nachgekommen wird.

Der EDÖB empfiehlt daher, innerhalb des Unternehmens eine **Meldepflicht** einzuführen. D.h. sämtliche Datenbearbeitungen und Datensammlungen müssen dem Datenschutzverantwortlichen gemeldet werden (für ein entsprechendes Standardformular siehe Dokumente des EDÖB).

Aufgrund der im Rahmen seiner Aufsichtsfunktion gewonnenen Erkenntnisse hat der betriebliche Datenschutzverantwortliche zu prüfen, ob und inwiefern betriebliche und gesetzliche Datenschutzvorschriften verletzt werden (bzw. verletzt werden könnten). Dazu gehört auch die Durchführung einer Risikoanalyse (z.B. Risiko einer unbeabsichtigten/unberechtigten Datenweitergabe, -löschung oder -bearbeitung, eines Datenverlustes oder technischen Fehlers, etc.). Stellt er im Rahmen seiner Abklärungen fest, dass Vorschriften verletzt werden, muss er Korrekturmassnahmen empfehlen können. Ob sich diese Empfehlungen an die innerhalb des Unternehmens zuständigen Mitarbeitenden oder an die Geschäftsleitung richten, hängt von der internen Organisation des jeweiligen Betriebs ab. In jedem Fall sollte aber der Betrieb dafür sorgen, dass die Empfehlungen umgesetzt werden. Tut er das nicht, muss grundsätzlich davon ausgegangen werden, dass die Datenschutzverletzungen vorsätzlich begangen wurden. Dies kann – falls ein solcher Vorfall publik werden sollte – für den betroffenen Betrieb zu einem nicht unerheblichen Imageschaden führen.





### Befreiung von der Anmeldungspflicht

Gemäss Art. 11a Abs. 5 lit. e DSG ist der Betrieb, welcher gegenüber dem EDÖB einen Datenschutzverantwortlichen benannt hat, von der Registrierungspflicht für seine Datensammlungen befreit. Er muss aber weiterhin intern so organisiert sein, dass Privaten und dem EDÖB auf Anfrage Auskunft über diejenigen Datensammlungen gegeben werden kann, in denen regelmässig besonders schützenswerte Personendaten oder Persönlichkeitsprofile bearbeitet oder aus denen regelmässig Personendaten an Dritte bekannt gegeben werden.

Dies sind die minimalen Anforderungen, welche das DSG zur Befreiung von der Meldepflicht vorsieht. Im Eigeninteresse des Unternehmens empfiehlt der EDÖB allerdings, dass sich der betriebliche Datenschutzverantwortliche darüber hinaus über sämtliche innerhalb des Betriebs vorhandenen Datensammlungen ein Bild macht.

## Massnahmen und Empfehlungen

Nachfolgend werden im Hinblick auf die Selbstregulierung im Datenschutz die gesetzlich vorgeschriebenen Massnahmen erläutert. Weiter listet der EDÖB die für einen datenschutzkonformen Betrieb unabdingbaren organisatorischen Anforderungendar.

### Gesetzlich vorgeschriebene Massnahmen

Aufgrund der gesetzlichen Vorschriften muss die Stelle des Datenschutzverantwortlichen wie folgt ausgestaltet sein:

- Er muss weisungsunabhängig sein.
- Er muss über eine ausreichende fachliche Qualifikation verfügen.
- Er muss die Bearbeitung von Personendaten innerhalb des Betriebs prüfen.
- Er muss Korrekturmassnahmen empfehlen können, wenn er feststellt, dass Datenschutzvorschriften verletzt wurden.
- Er muss Zugang zu allen Datensammlungen und Datenbearbeitungen haben.
- Er muss eine Liste der Datensammlungen nach Art. 11a Abs. 5 lit. e DSG führen und diese auf Anfrage dem EDÖB oder betroffenen Personen zur Verfügung stellen.
- Er darf keine Tätigkeiten ausüben, die mit seinen Aufgaben als Datenschutzverantwortlicher unvereinbar sind.

Damit das Unternehmen von der Befreiung der Anmeldepflicht für seine Datensammlungen Gebrauch machen kann, muss es die oben genannten Anforderungen erfüllen und darüber hinaus dem EDÖB melden, dass es die Stelle eines Datenschutzverantwortlichen bezeichnet hat.





### Organisatorische Vorschläge des EDÖB

Ein Unternehmen sollte in jedem Fall auch über die gesetzlich geforderten Mindeststandards hinaus dem Datenschutz einen hohen Stellenwert einräumen. Verstösse gegen das Datenschutzgesetz rufen – wenn sie in die Öffentlichkeit gelangen – aufgrund der Sensibilität der Bevölkerung oft ein grosses Medienecho hervor, welches dem Ansehen des Unternehmens grossen Schaden zufügen kann. Der EDÖB unterstreicht deshalb, dass es im ureigenen Interesse von Unternehmen liegt, innerhalb ihres Betriebs eine effiziente und wirksame Datenschutzaufsicht zu installieren.

*Hierarchische Datenschutzorganisation innerhalb des Betriebs*

Abgesehen vom unabhängigen Datenschutzverantwortlichen sollte das Unternehmen in unteren Hierarchieebenen so genannte Datenschutzmanager berufen, welche einen Teil ihrer Arbeitszeit für den Datenschutz in ihrem Bereich einsetzen. Ihnen obliegt es, die Kommunikation zwischen dem Unternehmens-Datenschutzverantwortlichen

und den einzelnen Abteilungen oder Bereichen zu gewährleisten, so dass mögliche Probleme frühzeitig erkannt und gemeldet werden können sowie Informationen und Weisungen gezielt in die Abteilungen gelangen.

Eine solche hierarchische Struktur kann durch den unabhängigen Datenschutzverantwortlichen für die nachfolgenden Aufgaben genutzt werden:

1. Zur Schulung der Mitarbeiter durch die Datenschutzmanager (welche vorher entsprechend vom Datenschutzverantwortlichen entsprechend ausgebildet wurden).
2. Für Treffen der Datenschutzmanager der einzelnen Abteilungen bzw. Bereiche, so dass ein Informations- bzw. Wissenstransfer stattfinden kann.
3. Als direkter Kanal für den Datenschutzverantwortlichen, um Sachverhalte innerhalb einer Abteilung oder eines Bereiches abzuklären und Empfehlungen auszusprechen bzw. Weisungen zu erteilen.
4. Zur Meldung von Datensammlungen und Datenbearbeitungen an den Datenschutzmanager für die Weiterleitung an den Datenschutzverantwortlichen; so nimmt ersterer eine Standardisierungs- und Aggregationsfunktion ein.
5. Als Sprachrohr für den unabhängigen Datenschutzverantwortlichen, damit er frühzeitig wahrnehmen kann, welche Datenbearbeitungen innerhalb des Unternehmens geplant, vorbereitet und durchgeführt werden.





Damit die Kommunikation zwischen dem unabhängigen Datenschutzverantwortlichen und den Datenschutzmanagern möglichst effizient verläuft und ersterer einen direkten Zugang zu den Abteilungen und Bereichen erhält, empfiehlt es sich, hierarchisch keine Zwischenstufen zu kreieren. Wenn also die Arbeitsbelastung für den Datenschutzverantwortlichen zu hoch wird, weil zu viele Datenschutzmanager seine Zeit in Anspruch nehmen, empfiehlt der EDÖB, einen weiteren unabhängigen Datenschutzverantwortlichen zu ernennen. Die Datenschutzmanager können dann auf die beiden Verantwortlichen aufgeteilt werden, und die Schaffung neuer Hierarchiestufen wird vermieden.

*Standardisierte Datenschutzprozesse*

Der EDÖB empfiehlt den Unternehmen, einige wenige spezifische Datenschutzprozesse zu implementieren, welche von den Mitarbeitenden im täglichen Geschäft umgesetzt werden sollten:

1. *Meldung und Kontrolle von Datensammlungen*: Der unabhängige Datenschutzverantwortliche sollte nach Möglichkeit über sämtliche innerhalb seines Be-

triebes vorhandenen Datensammlungen Bescheid weissen. Es ist daher ein standardisiertes Formular zu schaffen und im Betrieb zu verteilen, mit welchem die vorhandenen und geplanten Datensammlungen und Datenbearbeitungen erhoben werden. Damit können Bestand, Mutationen und Löschungen der Sammlungen überwacht werden, und der unabhängige Datenschutzverantwortliche kann sich zu jeder Zeit einen Überblick darüber verschaffen, welche Daten wo bearbeitet werden.

2. *Risikobeurteilung*: Aufgrund der Meldungen/Kontrollen von Datensammlungen und Datenbearbeitungen sollte der unabhängige Datenschutzverantwortliche eine Risikoanalyse durchführen. Sie sollte ihm ermöglichen, den potenziellen Schaden eines worst case abzuschätzen. Für heikle Datensammlungen (hohes Potential eines Imageschadens für das Unternehmen, grosser Schaden für die Betroffenen, für welchen das Unternehmen haftbar gemacht werden könnte, etc.) sollte der unabhängige Datenschutzverantwortliche neben ausreichenden Sicherheitsmassnahmen auch Notfallszenarien entwerfen, die im Falle eines worst case zur Anwendung kämen.

3. *Meldung von Datenschutzverletzungen*: Zur Risikominimierung und zur Umsetzung von Notfallszenarien ist im Falle einer Datenschutzverletzung ein schneller Informationsfluss zwischen der betroffenen Abteilung und dem unabhängigen Datenschutzverantwortlichen von höchster Bedeutung. Dies gilt umso mehr, wenn die Gefahr besteht, dass die Datenschutzverletzung bekannt werden könne und der Betrieb Vertrauensverluste befürchten muss. Die Datenschutzmanager müssen also die Bedeutung und Dringlichkeit einer möglichen Datenschutzverletzung grob abschätzen können.





*Interne Informationsseite und Standardformulare*

Der EDÖB empfiehlt darüber hinaus, im Intranet des Unternehmens eine Informationsseite zum Thema Datenschutz zu erstellen, auf welcher sämtliche relevanten Dokumente und Formulare zur Verfügung gestellt werden. Zudem kann so eine aktive Information der Mitarbeitenden erfolgen.

Unternehmen sollten für die Meldung sämtlicher Datensammlungen und Datenbearbeitungen Standardformulare erstellen, mit welchen sich die Datenschutzverantwortlichen einen Überblick über die im Unternehmen durchgeführten Datenbearbeitungen verschaffen können.

### 4.1.4 Erläuterungen zur Datenweitergabe bei Unternehmenszusammenschlüssen

Unternehmenszusammenschlüsse und die Veräusserung von Unternehmensteilen sind in der Wirtschaft alltägliche Vorgänge, die sich grundsätzlich in zwei Phasen unterscheiden lassen. In der Vorbereitungs- und Vertragsabschlussphase finden Verhandlungen zwischen den Fusionspartnern bzw. dem Käufer und dem Veräusserer des Unternehmens oder Unternehmensteils statt, die in einen Fusions- oder Kaufvertrag münden. In der Übernahmephase findet dann der eigentliche Zusammenschluss der Unternehmen oder die Übernahme des Unternehmensbereichs statt.

Da in Unternehmen so gut wie immer personenbezogene Daten bearbeitet werden, sind auch bei Unternehmenszusammenschlüssen die Bestimmungen des Bundesgesetzes über den Datenschutz (DSG, SR 235.1) zu berücksichtigen.

Im Laufe der Vertragsverhandlungen mit potentiellen Käufern führen die Unternehmen in der Regel eine Due Dilligence, also eine sorgfältige Kaufprüfung durch, in welcher den Käufern die Möglichkeit gegeben wird, sich ein Bild von der geschäftlichen Lage und damit dem Wert des Unternehmens zu machen. Hierdurch versucht der Käufer, neben den vorhandenen Aktiven des Unternehmens auch mögliche Synergien und Risiken zu identifizieren, um einschätzen zu können, welchen Nutzen ein Kauf bzw. eine Fusion erbringen würde. Aus diesem Grund ist der Käufer bestrebt, möglichst viele und möglichst umfangreiche Informationen zu erhalten.

Nach abgeschlossenem Fusions- oder Kaufvertrag werden die Unternehmensteile übernommen und integriert. In diesem Zusammenhang werden in der Regel die Geschäftsbereiche neu organisiert und zusammengelegt. Hierbei werden auch Personendaten in andere Geschäftsbereiche übertragen, um im neu strukturierten Unternehmen gewinnbringend eingesetzt zu werden. Aus datenschutzrechtlicher Sicht ist dabei zu beachten, dass die Personendaten auch nach der Fusion noch gemäss den Bestimmungen des DSG bearbeitet werden.

## Risiken

Die datenschutzrechtliche Hauptgefahr im Rahmen von Unternehmenszusammenschlüssen liegt in einer unberechtigten Datenbearbeitung und -weitergabe. In der Vorbereitungs- und Vertragsabschlussphase besteht die Gefahr, dass im Rahmen der Due Dilligence der Umfang der Weitergabe von Personendaten zu weit reicht und die potentiellen Käufer Kenntnis von mehr personenbezogener Information erhalten, als es für den Unternehmenskauf notwendig ist. Im Laufe der Integration der Unternehmen bzw. der Unternehmensteile könnten personenbezogene Daten in andere

Abteilungen transferiert oder zu einem anderen Zweck verwendet werden als bei der Erhebung angegeben. Aus diesen Gründen müssen im Rahmen von Fusionen und Unternehmenskäufen die datenschutzrechtlichen Risiken analysiert und ausreichend berücksichtigt werden.

### Risiken in der Vorbereitungs- und Vertragsabschlussphase

Im Rahmen einer Due Dilligence richten Unternehmen in der Regel einen «Information Room» ein, in dem sämtliche für die Unternehmensbewertung relevanten Informationen bereitgestellt werden. Die potentiellen Käufer bekommen Zugang zu diesem Raum, können die Unterlagen einsehen und sich handschriftliche Notizen machen. Üblicherweise handelt es sich um Informationen über Lieferanten, Kunden, Arbeitnehmer und andere Geschäftspartner.

Eine unberechtigte Datenweitergabe kann folgendermassen zustande kommen:

- Es können Käufer auftreten, die kein eigentliches Kaufinteresse, sondern lediglich ein Interesse an den von der Unternehmung in der Due Dilligence zur Verfügung gestellten Informationen haben.
- Es kann vorkommen, dass das Unternehmen (sei es aus Unachtsamkeit oder um einen höheren Verkaufserlös zu erzielen) mehr personenbezogene Informationen zur Verfügung stellt als unbedingt notwendig.





In beiden Fällen kann es zu Datenschutzverletzungen kommen, weshalb Unternehmen bereits in der Vorbereitungsphase für datenschutzrechtliche Belange sensibilisiert werden sollten.

### Risiken in der Übernahmephase

Während der Übernahme des Unternehmensteils oder des Zusammenschlusses der Unternehmen werden verschiedene Geschäftsbereiche restrukturiert und zusammengelegt, Arbeiten ausgelagert und Datenbestände miteinander abgeglichen und zusammengeführt. Bei solchen Restrukturierungsmassnahmen wird häufig von Grund auf geprüft, wie der Geschäftsbetrieb effizienter und gewinnbringender gestaltet werden kann. Dabei kann es vorkommen, dass Bestände von Personendaten zwischen Geschäftsbereichen transferiert und dort zu anderen Zwecken verwendet werden, als dies bei der Erhebung der Daten den betroffenen Personen kommuniziert worden war. In den meisten Fällen erfolgt eine solche Datenschutzverletzung nicht aus Böswilligkeit der Unternehmen, sondern es wird oft im Rahmen der Restrukturierung schlichtweg vergessen, zu welchem Zweck die Daten ursprünglich gesammelt wurden.

## Massnahmen und Empfehlungen

Bei Unternehmenszusammenschlüssen müssen die Grundsätze der Datenbearbeitung gemäss Art. 4 DSG eingehalten werden. Ist dies der Fall und bestehen entsprechende Rechtfertigungsgründe gemäss Art. 13 DSG, dürfen im Rahmen einer Fusion Personendaten gegen den ausdrücklichen Willen der betroffenen Person bearbeitet und besonders schützenswerte Personendaten oder Persönlichkeitsprofile Dritten bekannt gegeben werden. Ein solcher Grund liegt vor bei Einwilligung des Verletzten, bei einem überwiegenden privaten oder öffentlichen Interesse oder wenn ein Gesetz die Datenbearbeitung vorsieht (Art. 13 Abs. 1 DSG). Das Gesetz nennt beispielsweise ausdrücklich den Abschluss oder die Abwicklung eines Vertrages als Rechtfertigungsgrund zur Bearbeitung von Personendaten (Art. 13 Abs. 2 lit. a DSG).

Zudem existieren im Unternehmensumfeld oft spezifische berufliche oder gesetzliche Schweigepflichten, denen Rechnung getragen werden muss, da ein Verstoss gegen sie meist strafrechtliche Konsequenzen nach sich zieht. Hierunter fallen insbesondere Art. 35 DSG (Verletzung der beruflichen Schweigepflicht) und Art. 47 des Bundesgesetzes über die Banken und Sparkassen (Bankgeheimnis; BankG, SR 952.0). Solche gesetzlichen Geheimhaltungsverpflichtungen müssen auch im Rahmen eines Unternehmenszusammenschlusses in jedem Fall eingehalten werden.





Bei der grenzüberschreitenden Bekanntgabe muss beachtet werden, dass Personendaten nicht ins Ausland übermittelt werden dürfen, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, namentlich weil eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet (Art. 6 Abs. 1 DSG).

### Massnahmen im Rahmen der Vorbereitungs- und Vertragsabschlussphase

Während der Vorbereitungs- und Vertragsabschlussphase kann eine Datenbekanntgabe an Dritte im Rahmen einer Due Dilligence mit Art 13 Abs. 2 lit. a DSG gerechtfertigt werden, da ja der Käufer sämtliche vertraglichen Rechte und Pflichten übernimmt und damit Vertragspartei der Kunden seines Kaufobjekts wird. So muss er diesen Kunden gewährleisten, dass die durch die gekaufte Unternehmung eingegangenen vertraglichen Verpflichtungen erfüllt werden. Um überhaupt abschätzen zu können, welche Risiken in diesen Verpflichtungen stecken und ob er diese Abmachungen gewährleisten kann, werden Käufer im Rahmen einer Due Dilligence entsprechend informiert. Die Datenweitergabe ist hier als «in unmittelbaren Zusammenhang mit […] der Abwicklung eines Vertrages» mit den Kunden des kaufenden Unternehmens zu verstehen (Art. 13. Abs. 2 lit. a DSG). Dies gilt für personenbezogene Daten sowohl von Kunden als auch von Mitarbeiterinnen und Mitarbeitern. Dennoch dürfen diese Informationen in der Regel nicht personenbezogen an den potenziellen Käufer übermittelt werden. Dies

wäre ja auch nicht im Interesse des Verkäufers, da er sonst damit rechnen müsste, dass ihm der potentielle Käufer nach einem Scheitern der Fusionsverhandlungen Kunden bzw. Mitarbeiter abzuwerben versucht. Vor diesem Hintergrund ist vor der Weitergabe von personenbezogenen Daten an den (potentiellen) Käufer eine Information an die betroffenen Personen notwendig, so dass diese eine Möglichkeit haben, sich der Datenweitergabe zu widersetzen. In jedem Fall muss der Verkäufer darauf achten, dass die potentiellen Käufer immer nur in diejenigen personenbezogenen Daten Einblick erhalten, welche sie auch tatsächlich benötigen.

### Massnahmen im Rahmen der Übernahmephase

Im Rahmen der Übernahme der Unternehmensteile ist strikt darauf zu achten, dass die übergebenen Personendaten weiterhin nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen war (Art. 4 Abs. 2 DSG). Daher müssen Unternehmen gewährleisten, dass nur berechtigte Personen Zugriff auf die Daten erhalten und dass die Zweckbestimmung in jedem Moment eingehalten wird. Daher empfiehlt es sich, den Zweck einer jeden internen Datensammlung zu definieren und die zulässigen Bearbeitungsmöglichkeiten festzuhalten, so dass keine Missverständnisse innerhalb des Unternehmens entstehen.





## Empfehlungen

### In der Vorbereitungs- und Vertragsabschlussphase

Um den betroffenen Personen auch im Rahmen einer Due Dilligence einen ausreichenden Datenschutz bieten zu können, empfiehlt der EDÖB die folgenden Massnahmen:

1. Dem potentiellen Käufer und seinen Beratern sollten keine personenbezogenen Daten übergeben werden. Er sollte lediglich die Möglichkeit haben, die für ihn relevanten Daten vor Ort einsehen zu können (Einrichten eines «Information Rooms»).
2. Bei der Auswahl der potentiellen Käufer, denen Zutritt zum Information Room gewährt wird, ist strikt darauf zu achten, dass nur diejenigen Personen zugelassen werden, die ein tatsächliches Interesse an der Übernahme oder der Fusion haben.
3. Nur ein beschränkter Personenkreis darf Zugang zum Informationsraum erhalten. Die Personen müssen sich vertraglich verpflichten, nach einem allfälligen Scheitern der Verhandlungen die Information nicht weiter zu verwenden und sie grundsätzlich zu vernichten.

4. Die offen gelegten Informationen sind immer auf das erforderliche und aufgrund der Interessensabwägung gerechtfertigte Mass zu beschränken und soweit möglich zu anonymisieren oder zu aggregieren, so dass kein Personenbezug hergestellt werden kann.

5. Der Umfang der bereitgestellten Personendaten muss dem Verfahrensstadium angemessen sein, wobei umso mehr Informationen offen gelegt werden dürfen, je näher der Vertragsabschluss rückt und je wahrscheinlicher das Geschäft zustande kommt.

6. Zur zusätzlichen Sicherheit sollten im Rahmen der Due Dilligence so genannte «Non Disclosure Agreements» (NDAs) mit entsprechenden Datenschutzklauseln abgeschlossen werden, mittels welchen sich die potentiellen Käufer und ihre Berater zur Einhaltung des Datenschutzes verpflichten. Diese bieten einen gewissen Schutz, doch bleibt ein Restrisiko bestehen.

7. Spezifische gesetzliche Geheimhaltungsvorschriften (z.B. Art. 35 DSG; Art. 47 BankG, etc.) müssen unbedingt eingehalten werden.





### Im Rahmen der Übernahmephase

Im Rahmen der Übernahmephase empfiehlt der EDÖB die folgenden Massnahmen:

1. Die Datenbestände des gekauften Unternehmens sollten vor ihrer Verwendung im neuen Unternehmen dahingehend geprüft werden, ob der bei der Erhebung angegebene oder ersichtliche Zweck mit der geplanten zukünftigen Datenbearbeitung in Einklang steht.

2. Der Zugriff auf die Datenbestände beider Unternehmen muss so geregelt werden, dass nur diejenigen Mitarbeiter innerhalb des zusammengeschlossenen Unternehmens eine Berechtigung erhalten, die eine solche auch tatsächlich benötigen.

3. Im Zweifelsfall (wenn unklar ist, ob eine geplante Datenbearbeitung rechtlich möglich ist) sollten die betroffenen Personen über die durch die Fusion bedingte neue Datenbearbeitung informiert und gegebenenfalls um ihr Einverständnis gebeten werden.

4. Spezifische gesetzliche Geheimhaltungsvorschriften (z.B. Art. 35 DSG; Art. 47 BankG, etc.) müssen unbedingt eingehalten werden.

### 4.1.5 Antrag auf Entscheid betreffend die Einrichtung der beruflichen Vorsorge X

Bern, 27.08.2009

## Antrag auf Entscheid

des

Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB),
Feldeggweg 1, 3003 Bern, Antragsstellerin

gegen

Einrichtung der beruflichen Vorsorge X (nachfolgend Einrichtung X) Antragsgegnerin

betreffend

**Empfehlung gemäss Art. 27 des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz (DSG) betreffend Zustellung von Pensionskassenausweisen durch die Einrichtung X.**

Sehr geehrter Herr Generalsekretär

Hiermit stellen wir den folgenden

**I. Antrag**

Es sei zu entscheiden mittels einer Verfügung gemäss Art. 27 Abs. 5 DSG der Antragsgegnerin aufzuerlegen,

1. dass sie unverzüglich die von ihr praktizierte Datenbekanntgabe der Pensionskassenausweise von bei ihr versicherten Personen an deren Arbeitgeber einstelle;
2. dass sie den Pensionskassenausweis der versicherten Person in einer Art und Weise versende, die gewährleistet, dass dieser direkt und ausschliesslich an die versicherte Person gelangt.

## Begründung

### I. Sachverhalt

1. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) wurde von betroffenen Bürgern darauf aufmerksam gemacht, dass die Einrichtung der beruflichen Vorsorge X (nachfolgend Einrichtung X) den persönlichen Pensionskassenausweis nicht direkt an die versicherte Person, sondern an die Adresse des Arbeitgebers sendet. Der Arbeitgeber verteilt die nicht persönlich adressierten Pensionskassenausweise anschliessend an seine Arbeitnehmer.

2. Der EDÖB ist grundsätzlich davon ausgegangen, dass eine Verletzung des Datenschutzes vorliegen könnte und hat daher mit der Einrichtung X Kontakt aufgenommen. Aufgrund der uns von der Einrichtung X zur Verfügung gestellten Unterlagen geht hervor, dass diese die persönlichen Pensionskassenausweise nicht an die Privatadresse der versicherten Person, sondern direkt an eine vom Arbeitgeber genannte Couvertadresse mit dem Vermerk «vertraulich» sendet.

3. Inhaltlich enthält der Pensionskassenausweis neben den Stammdaten über die versicherte Person, Daten betreffend Leistungen im Alter, Leistungen bei Invalidität, Leistungen im Todesfall, Entwicklung der Altersguthaben sowie eine Rubrik Freizügigkeit. Unter dieser Rubrik Freizügigkeit wird das Total der eingebrachten Freizügigkeitsleistung, die Freizügigkeitsleistung und der mögliche Betrag für den Vorbezug zugunsten Wohneigentum ausgewiesen. Ausserdem erscheinen auf dem Pensionskassenausweis Informationen über den möglichen Einkauf und die Beiträge sowie Angaben über die Zusammensetzung der Personalvorsorge Kommission.

4. Zusätzlich können, laut Auskunft der Einrichtung X, situations-/systembedingt noch weitere Informationen unter der Rubrik Hinweise auf dem Pensionskassenausweis vermerkt sein, so z. B. die Vormerkung Bezug Alterskapital statt Rente, eingeschränkter Versicherungsschutz, Meldung Erwerbsunfähigkeit, Anspruch auf Invaliditätsleistungen, temporäre Erwerbsunfähigkeit, provisorischer Versicherungsschutz.

### II. Formelles

5. Der EDÖB hat am 8. Juli 2009 gestützt auf Art. 27 Abs. 4 DSG eine Empfehlung erlassen (Beilage 10) und diese der Einrichtung X zugestellt.

6. Gegenstand der Empfehlung ist die Datenbearbeitung der Einrichtung X in ihrer Funktion als Bundesorgan im Bereich der obligatorischen Vorsorgeversicherung (siehe nachfolgend). Aufsichtsorgan über die Berufliche Vorsorge ist das Bundesamt für Sozialversicherung. Das zuständige Departement ist das Departement des Innern, welches mit Schreiben vom 8. Juli 2009 mit einer Kopie über die Empfehlung orientiert worden ist.

7. Der EDÖB behält sich vor, eine Empfehlung für den Bereich der überobligatorischen Vorsorgeversicherung zu erlassen.

8. Die Einrichtung X hat mit ihrem Schreiben vom 10. August 2009 (siehe Beilage 12) die Empfehlung des EDÖB vom 8. Juli 2009 abgelehnt (siehe Beilage 11). Der EDÖB legt daher die Angelegenheit gemäss Art. 27 Abs. 5 DSG dem zuständigen Departement zum Entscheid vor.

## III. Erwägungen

### Personendaten und besonders schützenswerte Personendaten

9. Als Personendaten gelten gemäss Art. 3 lit. a DSG alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen. Somit gelten alle Daten als Personendaten, welche in einem Zusammenhang zu einer betroffenen Person stehen oder mit ihr in Zusammenhang gebracht werden können. Der Pensionskassenausweis, den die Einrichtung X aufgrund von Informationen der versicherten Person und des Arbeitgebers bearbeitet, enthält Daten, die nach Art. 3 lit. a DSG als Personendaten zu qualifizieren sind.

10. Als besonders schützenswerte Personendaten gelten nach Art. 3 Personendaten, die in Art. 3 DSG abschliessend aufgelistet sind. Dazu sind Daten über die Gesundheit gemäss Art. 3 lit. c Ziff. 2 DSG zu zählen. Auf dem Pensionskassenausweis können unter der Rubrik Hinweis auch Gesundheitsdaten aufgelistet werden, wie eingeschränkter Versicherungsschutz, teilweise Erwerbsunfähigkeit. Entgegen der Meinung der Einrichtung X sind solche Daten als Gesundheitsdaten im Sinne von Art. 3 lit. c Ziff. 2 DSG zu qualifizieren und gelten damit als besonders schützenswert. Als Angaben über die Gesundheit gelten alle Informationen, die direkt oder indirekt Rückschlüsse über den physischen oder psychischen Gesundheitszustand einer Person zulassen, Daten also, die im weitesten Sinn einen medizinischen Befund darstellen. Es muss sich nicht um eine den Ansprüchen der Medizin gerecht werdende Diagnose handeln. So kann auch eine Rechnung für ein Medikament als

besonders schützenswertes Datum angesehen werden (URS BELSER, BSK-DSG, Art. 3 DSG N 14) oder auch eine Krankmeldung (DAVID ROSENTHAL, Handkommentar zum Datenschutzgesetz, Schulthess Juristische Medien AG (Zürich, Basel, Genf), 2008, Art. 11a Abs. 3 DSG N 45).

**Bundesorgan**

11. Nach Art. 3 lit. h DSG gelten als Bundesorgane, Behörden und Stellen des Bundes, soweit sie mit Aufgaben des Bundes betraut sind. Private werden nur soweit wie Bundesorgane behandelt, als sie Personendaten für die Erfüllung einer öffentlichen Aufgabe des Bundes bearbeiten. In den anderen Fällen unterstehen sie dem Privatrecht (BSK-DSG, URS MAURER-LAMBROU/SIMON KUNZ, Art. 2 N 15 f.; URS BELSER, BSK-DSG, Art. 3 N 35 f.). Wenn eine Privatperson sowohl private Aufgaben wahrnimmt als auch mit einer öffentliche Aufgabe des Bundes betraut ist, gilt sie im Bereich der öffentlichen Aufgabe als Bundesorgan i. S. v. Art. 2 Abs. 1 lit. b DSG und Art. 3 lit. h DSG (URS MAURER-LAMBROU/SIMON KUNZ, BSK- DSG, Art. 2 N 15 f.; URS BELSER, BSK-DSG, Art. 3 N 35). Die Einrichtung X bietet im Bereich des Bundesgesetzes über die berufliche Alters-, Hinterlassenen- und Invalidenversicherung (BVG, SR 831.40) sowohl im obligatorischen als auch im überobligatorischen Bereich Versicherungen an. Auf dem Pensionskassenausweis können Daten sowohl aus der obligatorischen als auch aus der überobligatorischen Versicherung aufgelistet sein. Zwischen der Vorsorgeeinrichtung und dem Versicherten besteht kein vertragliches, sondern ein gesetzliches Rechtsverhältnis, das mit Antritt des Arbeitsverhältnisses wirksam wird (Art. 10 BVG). Die Vorsorgeeinrichtung ist zur Leistungserbringung in der obligatorischen Vorsorgeversicherung verpflichtet. Die Einrichtung X ist in diesem Bereich als Bundesorgan gemäss Art. 3 lit. h DSG anzusehen, da ihr eine öffentlich-rechtliche Bundesaufgabe übertragen wurde.

**Datenbearbeitung**

12. Unter «Bearbeiten» im Sinne von Art. 3 lit. e DSG wird jeder Umgang mit personenbezogenen Informationen verstanden, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten. Die Einrichtung X beschafft Informationen von Versicherten und Arbeitgebern und erstellt hieraus einen persönlichen Pensionskassenausweis. Daher liegt eine Datenbearbeitung im Sinne von Art. 3 lit. e DSG vor.

## Anwendbarkeit des DSG

13. Das DSG ist anwendbar, da die Einrichtung X als Bundesorgan Personendaten bearbeitet und nach Art. 2 Abs. 2 DSG keine Ausnahmen vom Geltungsbereich vorliegen.

14. Da die Einrichtung X Personendaten in der obligatorischen Vorsorgeversicherung im Sinne von Art. 3 lit. e DSG bearbeitet und als Bundesorgan nach Art. 2 Abs. 1 lit. b DSG i.V. mit Art. 3 lit. h DSG anzusehen ist, kommt das DSG zur Anwendung.

15. Bundesorgane haben neben den allgemeinen Datenschutzbestimmungen nach Art. 4 – 11 DSG grundsätzlich die Bestimmungen von Art. 16 – 25bis DSG zu berücksichtigen.

## Legalitätsprinzip für die Datenbearbeitung durch Bundesorgane

16. Unbestritten ist, dass Arbeitgeber, Arbeitnehmer und Versicherung im Bereich der beruflichen Versicherung eng miteinander verbunden sind. Die verschiedenen Rechte und Pflichten, insbesondere die Rechtslage beim Datenaustausch, ergeben sich jedoch aufgrund der jeweiligen rechtlich relevanten Bestimmungen. Das Datenschutzgesetz bzw. die datenschutzrechtlichen Spezialbestimmungen dienen nicht dazu, dass Vorsorgeeinrichtungen dem Arbeitgeber keine Daten bekannt geben dürften, wie das die Einrichtung X in ihrer Stellungnahme vorbringt. Sie regeln, wie der Datenaustausch rechtskonform erfolgen soll.

    Zu beachten ist, dass die schweizerische Datenschutzgesetzgebung auf zwei unterschiedlichen Konzepten beruht. Es ist klar zu unterscheiden ob die Datenbearbeitung durch Bundesorgane (Art. 17 ff. DSG) oder ob die Datenbearbeitung durch Privatpersonen (Art. 12 ff. DSG) erfolgt. Für die Bearbeitung von Personendaten durch Bundesorgane gilt das Legalitätsprinzip, welches der Gesetzgeber in Art. 17 DSG für den Datenschutz konkretisiert hat. Bundesorgane dürfen demnach Personendaten nur dann bearbeiten, wenn eine gesetzliche Grundlage die Bearbeitung von Personendaten ausdrücklich erlaubt (Grundsatz des Verbots der Datenbearbeitung mit Erlaubnisvorbehalt). Zudem müssen Bundesorgane, soweit nicht besondere gesetzliche Vorschriften bestehen, bei der Datenbearbeitung immer auch die Grundsätze von Art. 4 DSG beachten (BBl 1988 467).

17. Die gesetzliche Grundlage besteht, wenn die Bearbeitung der Daten in einer generell-abstrakten Rechtsnorm geregelt ist, welche genügend bestimmt ist. Die angemessene Bestimmtheit ist dann genügend, wenn sie so präzise formuliert sind,

dass der Bürger sein Verhalten danach richten und die Folgen eines bestimmten Verhaltens mit einem den Umständen entsprechenden Grad an Gewissheit erkennen kann (YVONNE JÖHRI/MARCEL STUDER, BSK-DSG, Art. 17 DSG N 11). Es genügt jedoch, wenn die Informationsbearbeitung in einem einsichtigen sachlichen Zusammenhang mit der Aufgabe des betreffenden Bundesorgans steht und mindestens der Zweck, die beteiligten Organe und das Ausmass der Datenbearbeitung in den Grundzügen festgelegt ist (YVONNE JÖHRI/MARCEL STUDER, BSK-DSG, Art. 17 DSG N 16).

18. Hinsichtlich der Gesetzesform genügt für die Bearbeitung von nicht sensiblen Personendaten ein Gesetz im materiellen Sinn (Art. 17 Abs. 1 DSG). Für die Bearbeitung von besonders schützenwerte Personendaten und Persönlichkeitsprofilen ist ein Gesetz im formellen Sinn erforderlich (Art. 17 Abs. 2 DSG), es sei denn, es kommen die Ausnahmen von Art. 17 Abs. 2 lit. a – c DSG zum Zuge.





### Gesetzliche Grundlage der Datenbekanntgabe nach Art. 19 DSG

19. Nach Art. 19 DSG dürfen Bundesorgane Daten nur bekannt geben, wenn dafür eine Rechtsgrundlage im Sinne von Art. 17 DSG besteht oder die Ausnahmen gemäss Art. 19 DSG vorhanden sind.

20. Das Legalitätsprinzip gilt für jede Bearbeitung von Personendaten durch Bundesorgane, so auch für die Datenbekanntgabe nach Art. 19 Abs. 1 DSG. Die gesetzliche Grundlage für die Datenbekanntgabe muss wie bei Art. 17 DSG nicht nur eine genügende Bestimmtheit aufweisen (siehe vorgehend), sondern sie muss sich ausdrücklich auf den Transfer der Daten als solchen beziehen, d.h. die gesetzliche Grundlage muss eine Ermächtigung oder Verpflichtung für die Datenbekanntgabe enthalten (YVONNE JÖHRI/MARCEL STUDER, BSK-DSG, Art. 17 DSG N 31 und Art. 19 N 25).

    Hingegen spielt es keine Rolle, ob die Datenbekanntgabe ein Recht oder eine Pflicht der bekannt gebenden Behörde oder als Anspruch des Empfängers der Daten umschrieben wird. Der Artikel 19 DSG stellt eine Art allgemeine Amts- und Rechtshilfebestimmung und eine Ausführungsbestimmung zum allgemeinen Amtsgeheimnis dar. Auch wenn die Voraussetzungen nach Art. 19 DSG erfüllt sind, muss das zuständige Organ zusätzlich noch prüfen, ob mit der Bekanntgabe nicht gegen die Grundsätze von Artikel 4 DSG verstossen wird (BBl 1988 469).

### Einschränkung der Datenbekanntgabe

21. Nach Art. 19 Abs. 4 DSG ist die Datenbekanntgabe an Dritte abzulehnen, einzu-schränken oder mit Auflagen zu versehen, wenn gesetzliche Geheimhaltungs- und Schweigepflichten bestehen.

### Datenschutzrechtliche Spezialbestimmungen nach BVG

22. Im Bereich der Sozialversicherung ist klar geregelt wie die Datenbekanntgabe zu erfolgen hat, damit keine Schweigepflicht verletzt ist. Auch im BVG bestehen solche datenschutzrechtlichen Spezialbestimmungen (Art. 85a BVG, Art. 85b BVG, Art. 86 BVG, Art. 86a BVG und Art. 87 BVG), die als lex specialis dem DSG vorgehen (BBl 1988 II 471, 1988 II 444). Die Bestimmungen sind mit dem Bundesgesetz vom 23. Juni 2000 ins BVG eingefügt worden und ersetzen die Verordnung vom 7. Dezember 1987 über die Ausnahmen von der Schweigepflicht in der beruflichen Vorsorge und über die Auskunftspflicht der AHV/IV-Organe (VSABV; SR 831.462.2). Sie dienen als Rechtsgrundlage für die Datenbearbeitung im Bereich des BVG. Nach Art. 86 BVG haben Personen, welche an der Durchführung sowie Kontrolle oder Beaufsichtigung der Durchführung des BVG beteiligt sind, gegenüber Dritten Verschwiegenheit zu bewahren.





23. Die in Art. 86 BVG bestehende Schweigepflicht wird durch die Vorschriften der Datenbekanntgabe in Art. 86a BVG - Art. 87 BVG relativiert.

24. Die Informationspflicht nach Art. 86b BVG ist als Spezialnorm von den übrigen Ausnahmen, welche die Schweigepflicht relativieren (siehe vorgehend) zu unterscheiden. Diese sind einander sachfremd und haben bei Nichtbeachtung unterschiedliche strafrechtliche Folgen (Art. 86 BVG i.V. mit Art. 76 Abs. 4 BVG sowie Art. 86b BVG i.V. mit Art. 75 BVG).

25. Nach Art. 85a BVG wird mit der Überschrift Bearbeiten von Personendaten ein direkter Bezug zum Datenschutz hergestellt. Die mit der Durchführung, der Kontrolle oder der Beaufsichtigung der Durchführung dieses Gesetzes betrauten Organe sind befugt, die Personendaten, einschliesslich besonders schützenswerter Daten und Persönlichkeitsprofile, zu bearbeiten oder bearbeiten zu lassen, die sie benötigen, um die ihnen nach diesem Gesetz übertragenen Aufgaben zu erfüllen. In der Bestimmung steht notgedrungen in allgemeiner Form, welche Organe befugt sind, Personendaten zu bearbeiten

und für welche Zwecke sie es tun dürfen. Die Art der Daten hängt ab vom Zweck für welchen sie bearbeitet werden. Hinsichtlich des Zwecks ist die Bearbeitung von Personendaten auf das beschränkt, was das Organ zur Erfüllung der im BVG vorgesehenen Aufgaben benötigt (Gültigkeit des Grundsatzes der Verhältnismässigkeit). Bei den Organen, die befugt sind, Personendaten zu behandeln, handelt es sich um jene, die im Gesetz bezeichnet sind (BBl 2000 255). Sie haben grundsätzlich die Schweigepflicht einzuhalten.

26. Indem die Einrichtung X auf dem Pensionskassenausweis Daten aus der obligatorischen Vorsorgeversicherung (Sozialversicherung) und der überobligatorischen Vorsorgeversicherung (Privatversicherung) in einem Ausweis zusammenfasst, gibt sie gleichzeitig sowohl Daten aus der Sozialversicherung als auch der Privatversicherung dem Arbeitgeber bekannt. Sofern diese Datenbekanntgabe an den Arbeitgeber keine gesetzliche Grundlage hat und keine Ausnahmen von der Schweigepflicht angerufen werden können, muss von einer Verletzung der Schweigepflicht ausgegangen werden (Art. 86 BVG i.V.mit Art. 76 Abs. 4 BVG).





**Art. 86b BVG, Art. 331 Abs. 4 OR, Art. 89bis Abs. 2 ZGB**

27. Die genügende gesetzliche Grundlage für die Zustellung von Pensionskassenausweisen ist in Art. 86b BVG nur für den Arbeitnehmer als Adressaten vorhanden (Informations-pflicht des Versicherten durch die Versicherung). Diese Bestimmung, die mit dem Bundesgesetz vom 3. Okt. 2003 (1. BVG-Revision) eingefügt wurde, ersetzt die Weisungen des Bundesrates über die Pflicht der registrierten Vorsorgeeinrichtungen zur Auskunftserteilung an Ihre Versicherten vom 11. Mai 1988 (BBl 1988 II 641f.). Diese Weisungen, auf welche sich das BSV in seiner Mitteilung über die berufliche Vorsorge Nr. 10 vom 15. August 1988 bezieht und welche auch die Einrichtung X in ihrer Stellungnahme erwähnt, haben sich an die Aufsichtsbehörden gerichtet und galten für die registrierten Vorsorgeeinrichtungen. Nach diesen Weisungen hatten die Aufsichtsbehörden dafür zu sorgen, dass die Vorsorgeeinrichtungen den Versicherten die mindestens unter Ziffer 2 der Weisungen erwähnten Bereiche Auskünfte erteilen (a) und das die Vorsorgeeinrichtungen die Arbeitgeber anweisen, die Arbeitnehmer über deren Auskunftsrechte nach den Weisungen zu informieren (b). Die Informationspflicht ist aber nicht inhaltlicher Natur.

28. Nach Art. 86b BVG ist die Vorsorgeeinrichtung gesetzlich verpflichtet, den Versicherten jährlich in geeigneter Form zu informieren über a) die Leistungsansprüche, den koordinierten Lohn, den Beitragssatz und das Altersguthaben, b) die Organi-

sation und die Finanzierung und c) die Mitglieder des paritätisch besetzten Organs nach Art. 51 BVG (unaufgeforderte Datenbekanntgabe). Neben diesen Mindestinformationen erteilen die Vorsorgeeinrichtungen nach Art. 86b Abs. 2 BVG auf Anfrage des Versicherten hin weitere Informationen (aufgeforderte Datenbekanntgabe). Aufgrund des Gesetzeswortlautes ist klar ersichtlich, dass die im Pensionskassenausweis festgehaltenen individuellen Informationen über die persönliche Vorsorgesituation der versicherten Person ausschliesslich für diese bestimmt sind. Es war Absicht des Gesetzgebers, einen allgemeinen Informationsgrundsatz zu schaffen, der die Vorsorgeeinrichtungen verpflichtet, ihre Versicherten über deren persönlichen Leistungsansprüche und über die allgemeine Tätigkeit der Vorsorgeeinrichtung jährlich unaufgefordert zu orientieren. Bereits die Weisungen (siehe oben) hatten den Zweck, dass die Vorsorgeeinrichtungen die Versicherten minimal informieren. Gegenüber dem Arbeitgeber hatte die Vorsorgeeinrichtung aber nur die Pflicht, dass der Arbeitnehmer seine Arbeitnehmer über die ihn zustehenden Auskunftsrechte informiert, nicht jedoch über den Inhalt. Die Weisungen sind vom Bundesrat erlassen worden, weil er eine sehr unterschiedliche Informationspraxis der Vorsorgeeinrichtungen festgestellt hatte. Die jährliche Information über die konkrete persönliche Vorsorgesituation versetzt die Versicherten sowohl in den Stand die Entwicklung ihrer individuellen Vorsorgesituation jederzeit nachvollziehen als auch sich ein Bild über die gesamte Tätigkeit der Vorsorgeeinrichtung machen zu können. Die verbesserte Information des Versicherten hat zum Ziel mehr Transparenz zu schaffen und verstärkt damit das Vertrauen der versicherten Person in die Vorsorgeeinrichtung und in die berufliche Vorsorge allgemein (BBl 2000 2678 ff., vgl. dazu auch ISABELLE VETTER-SCHREIBER, Berufliche Vorsorge, Kommentar BVG, Art. 86b N 4) und ist nicht für den Arbeitgeber bestimmt.

29. Die nach Art. 86b BVG erlaubte unaufgeforderte Datenbekanntgabe dient einzig der Information der versicherten Person, damit sich diese über ihre persönliche Vorsorgesituation und Leistungsansprüche ein Bild machen kann. Diese gesetzliche Grundlage ermächtigt und verpflichtet die Vorsorgeeinrichtung explizit dem Arbeitnehmer (und nur diesem) Daten zum Zwecke der vorerwähnten Information bekannt zu geben. Mit der Zustellung des Pensionskassenausweises erfüllt die Einrichtung X eine ihr in Art. 86b BVG gesetzliche vorgegebene Offenlegungs- und Informationspflicht gegenüber dem Versicherten während des Versicherungsverhältnisses. Der Versicherte hat einen rechtlich erzwingbaren Anspruch, dass er jährlich von der Vorsorgeeinrichtung über seine Vorsorgesituation unterrichtet wird (ISABELLE VETTER-SCHREIBER, Berufliche Vorsorge, Kommentar BVG, Art. 86b N 3). Verletzt die Vorsorgeeinrichtung diese Auskunftspflicht, kann dies strafrechtliche Konsequenzen nach sich ziehen (Art. 75 BVG). In Art. 86b BVG wird die Vorsorge-

einrichtung nicht ausdrücklich ermächtigt, Daten über die persönliche Vorsorgesituation der versicherten Person dessen Arbeitgeber bekannt zu geben, weshalb eine genügende gesetzliche Grundlage im Sinne von Art. 19 DSG bzw. Art. 17 DSG bereits für nicht sensible Daten nicht vorhanden ist. Demzufolge ist das Legalitätsprinzip verletzt.

30. Die Einrichtung X ist der Meinung, dass Pensionskassenausweise der Arbeitnehmer auch dem Arbeitgeber bekannt gegeben werden dürfen, da dieser die Informationen aus dem Pensionskassenausweis benötige, damit er als Arbeitgeber seiner Informationspflicht nach Art. 331 Abs. 4 OR nachkommen könne. Der jährliche Pensionskassenausweis gemäss Art. 86b Abs. 1 BVG enthalte genau die erforderlichen Daten, damit sich der Arbeitgeber einen ersten Überblick über die individuellen Pensionskassenansprüche seiner Arbeitnehmenden machen könne.

31. Es trifft zu, wie die Einrichtung X ausführt, dass der Arbeitgeber nach Art. 331 Abs. 4 OR eine Informationspflicht über die Forderungsrechte hat und der Arbeitnehmer Anrecht auf Auskunft über die ihm zustehenden Rechte und Anwartschaften/Forderungsrechte hat. Sofern Art. 331 Abs. 4 OR für die obligatorische Versicherung überhaupt relevant ist, (das BVG und die dazu gehörenden Verordnungen regeln die obligatorische berufliche Vorsorge, während Art. 331-331f OR die berufliche Vorsorge im überobligatorischen Bereich regeln (M. AMSTUTZ, P. BREITSCHMID, A. FURRER, D. GIRSBERGER, C. HUGUENIN, M. MÜLLER-CHEN, V. ROBERTO, A. RUMO-JUNGO, A. K. SCHNYDER; Handkommentar zum Schweizer Privatrecht, Schulthess Juristische Medien AG (Zürich, Basel, Genf), 2007; FRANK EMMEL zu Art. 331 f OR, N 1), verknüpft die Einrichtung X zwei an sich richtige Aussagen, um dadurch zu schliessen, eine gesetzliche Grundlage für die von ihr praktizierte Datenbekanntgabe an den Arbeitgeber sei vorhanden. Diese Schlussfolgerung ist falsch: Die Informationspflicht des Arbeitgebers gegenüber dem Arbeitnehmer gemäss Art. 331 Abs. 4 OR betrifft einzig und allein Forderungsrechte gegenüber diesem. Die Informationen im Pensionskassenausweis beinhaltet hingegen konkrete Daten zur persönlichen Vorsorgesituation des versicherten Arbeitnehmers, einschliesslich Informationen über das frühere Arbeitsverhältnis, wie z.B. die Freizügigkeitsleistung. Ausserdem wird weder in Art. 331 Abs. 4 OR noch in Art. 86b BVG die Versicherung ausdrücklich ermächtigt, Informationen über die persönliche Vorsorgesituation bzw. über Gesundheitsdaten des Arbeitnehmers dem Arbeitgeber bekannt zu machen, weshalb schon jede Norm für sich betrachtet keine genügende gesetzliche Grundlage für die Datenbekanntgabe der Versicherung gegenüber dem Arbeitgeber darstellt, die im Sinne von Art. 19 bzw. 17 DSG genügend präzise bestimmt ist.

32. Die Einrichtung X beruft sich Auf Art 89bis Abs. 2 ZGB. Diese Norm verpflichtet die Stiftungsorgane den Begünstigten über die Organisation, die Tätigkeit und die Vermögenslage der Stiftung den erforderlichen Aufschluss zu erteilen. Auch in dieser Bestimmung wird die Versicherung nicht ausdrücklich ermächtigt, Informationen über die persönliche Vorsorgesituation des Arbeitnehmers dem Arbeitgeber zum Zwecke der Information des Arbeitnehmers bekannt zu machen, weshalb auch diese Norm keine genügende gesetzliche Grundlage für die Datenbekanntgabe der Versicherung gegenüber dem Arbeitgeber im Sinne von Art. 19 bzw. 17 DSG ist.

33. Weder Art. 86b BVG, noch Art. 331 Abs. 4 OR und auch nicht Art. 89 bis Abs. 2 ZGB enthalten eine genügende gesetzliche Grundlage für die Datenbekanntgabe an den Arbeitgeber. Deshalb liegt keine gesetzliche Grundlage vor, die eine solche Datenbekanntgabe erlauben würde, weshalb das Legalitätsprinzip verletzt ist. Sofern die Versicherung sich nicht auf eine Ausnahme der Schweigepflicht stützen kann, ist auch von einer Verletzung der Schweigepflicht auszugehen (Art. 86a BVG i. V. mit Art. 76 Abs.4 BVG).





### Art. 86a BVG

34. Der Begriff Datenbekanntgabe in Art. 86a BVG entspricht demjenigen nach DSG. Unter «Bekanntgeben» definiert Art. 3 lit. f DSG das Zugänglichmachen von Personendaten wie das Einsichtgewähren, Weitergeben und Veröffentlichen. Nach der Lehre ist darunter jede aktive Weitergabe und jedes passive Zugänglichmachen zu verstehen, die es einem Dritten ermöglichen, vom Inhalt der personenbezogenen Daten Kenntnis zu nehmen (URS BELSER, BSK-DSG, Art. 3 N 30). Die Datenbekanntgabe ist datenschutzrechtlich einer der heikelsten Bearbeitungsschritte, weil die Daten den ursprünglichen Herrschaftsbereich verlassen und in den Bereich eines Dritten gelangen, wodurch ein hohes Potential für Persönlichkeitsverletzungen durch nicht bestimmungsgemässen Gebrauch geschaffen wird. Eine Bekanntgabe liegt vor, wenn durch eine Datenbearbeitung eine Person Zugang zu Informationen erhält, die ihr vorher nicht bekannt waren oder wenn der Umfang der Personendaten, die einem bestimmten Personenkreis zugänglich sind, erweitert wird (YVONNE JÖHRI, Handkommentar zum Datenschutzgesetz, Schulthess Juristische Medien AG (Zürich, Basel. Genf), 2008, Art. 3 DSG N 74 f.).

35. Voraussetzung für die Datenbekanntgabe ist, dass die informationserhaltende Person als Dritter qualifiziert wird. Als Dritter wird jede andere Person oder Stelle und jedes andere Bundesorgan betrachtet, das nicht mit dem Datenbearbeiter übereinstimmt. Es sind dies Personen, welche Zugang zu Informationen erhalten,

welche ihnen vorgängig nicht bekannt waren (YVONNE JÖHRI, Handkommentar zum Datenschutzgesetz, Art. 3 DSG N 74). So gelten im Versicherungsbereich alle Personen oder Stellen ausserhalb des Versicherungsträgers des betreffenden Sozialversicherungszweiges, so etwa Arbeitgeber, andere (Privat-) Versicherungen oder sonstige Behörden als Dritte. Nichts anderes gilt, wenn der betreffende Sozialversicherungsträger rechtlich oder faktisch mit einer anderen Versicherung verbunden ist (etwa Zusatzversicherung, berufliche Vorsorge). Ist ein Sozialversicherer gleichzeitig als Privatversicherer tätig, hat er die Schweigepflicht gegenüber den Privatversicherern zu wahren. Die Schweigepflicht ist grundsätzlich auch innerhalb der Behörde zu beachten. Daran ändert nichts, dass diese Personen innerhalb des Versicherungsträgers ihrerseits der Schweigepflicht unterstehen (KIESER UELI, ATSG Kommentar, 2. Auflage, Zürich/Basel/Genf 2009, Art. 33 N 10 f.).

36. Entgegen der Ansicht der Einrichtung X werden dem Arbeitgeber mit dem Pensionskassenausweis nicht ausschliesslich zusammenfassend diejenigen Informationen übermittelt, welche er bereits der Versicherung auf dem Anmeldeformular mitgeteilt hat. Der Pensionskassenausweis ist vom Anmeldeformular klar zu unterscheiden. In beiden Vorgängen werden nicht dieselben Daten bearbeitet und die Empfänger der Daten unterscheiden sich ebenfalls, weshalb eine Datenbekanntgabe vorliegt. Nach Art. 11 BVG hat der Arbeitgeber die Pflicht, sich einer Vorsorgeeinrichtung anzuschliessen oder selbst eine Vorsorgeeinrichtung zu errichten (Mitwirkung bei der Durchführung der Vorsorge). Er hat gegenüber der Vorsorgeeinrichtung beim Anmeldevorgang gemäss Art. 10 der Verordnung über die berufliche Alters-, Hinterlassenen- und Invalidenvorsorge (SR 831.441.1, BVV 2) eine Auskunftspflicht. Demgegenüber entspringt die Zustellung des Pensionskassenausweises hingegen der Informationspflicht der Versicherung gegenüber dem Versicherten gemäss Art. 86b BVG (siehe oben). Auf dem Pensionskassenausweis sind Informationen aufgeführt, welche auf dem Anmeldeformular des Arbeitgebers bzw. Arbeitnehmers noch nicht vorhanden waren, so z. B. die Höhe der Freizügigkeitsleistung und allenfalls Gesundheitsdaten. Wenn der Arbeitgeber letztere hinsichtlich der Anmeldung bei der obligatorischen Versicherung einsehen könnte, dann wäre dies für sich betrachtet bereits nicht datenschutzkonform.

37. Es ist von einer Bekanntgabe von Daten durch die Einrichtung X auszugehen, da Daten erhalten die den ursprünglichen Herrschaftsbereich der Versicherung verlassen und durch die nicht persönlich an die Arbeitnehmer adressierten Pensionskassenausweise in den Herrschaftsbereich des Arbeitgebers gelangen, womit

dieser als Dritter Zugang zu Informationen erhält, die ihm vorher nicht in diesem Umfang bekannt waren. Demzufolge ist von einer Datenbekanntgabe an einen Dritten auszugehen.

38. Bei der Datenbekanntgabe unterscheidet Art. 86a BVG, der sinngemäss Artikel 1 Absatz 1 VSABV entspricht (siehe vorgehend) zwischen einer Datenbekanntgabe im Einzelfall auf schriftliches und begründetes Gesuch hin, sowie Fällen, in denen Daten ohne weiteres oder auf Anfrage hin bekannt gegeben werden dürfen. Ferner ist in Fällen, in denen die Datenbekanntgabe an Dritte nicht ausdrücklich vorgesehen ist, die Zustimmung der betroffenen Person erforderlich.

39. Art. 86a Abs. 1 BVG regelt abschliessend die Datenbekanntgabe im Einzelfall aufgrund eines schriftlichen Gesuches durch eine Stelle, welche im Gesetz ausdrücklich genannt ist. Der Arbeitgeber ist nicht ausdrücklich erwähnt. Zudem ersucht er die Pensionskassenausweise nicht im Einzelfall um eine Datenauskunft, sondern bekommt Daten von der Versicherung unaufgefordert zugestellt, weshalb Art. 86a Abs. 1 BVG von vorneherein nicht anwendbar ist. Die Angabe einer Zustelladresse durch den Arbeitgeber ändert nichts an der unaufgeforderten Zustellung durch die Vorsorgeversicherung (siehe unten zu Art. 328b OR).





40. Nach Art. 86a Abs. 2 BVG dürften Daten auch unaufgefordert und ausserhalb von Einzelfällen bekannt gegeben werden. So dürften nach Art. 86a Abs. 2 lit. a BVG Daten an den Arbeitgeber bekannt gegeben werden, wenn er mit der Durchführung des gleichen Gesetzes betraut ist, für ihn die Daten für die Erfüllung der ihm nach diesem Gesetz

    übertragenen Aufgaben erforderlich sind und keine überwiegenden Privatinteressen entgegenstehen. Weder ist in der obligatorischen Vorsorgeversicherung die Erhebung von Gesundheitsdaten durch den Arbeitgeber erlaubt, noch darf der Arbeitgeber bei der überobligatorischen Versicherung Einblick in Gesundheitsdaten erhalten (KURT PÄRLI, Datenaustausch zwischen Arbeitgeber und Versicherung, 1/2004 HAVE/REAS, S. 32 ff.). Es ist kein Grund ersichtlich, wozu der Arbeitgeber auch andere Versichertendaten des Arbeitnehmers für die Erfüllung seiner BVG-Pflichten benötigt. Der Datenbekanntgabe stehen zudem die überwiegenden Privatinteressen des Versicherten entgegen (BGE vom 25. Juli 2001, 2A 96/2000). Grundsätzlich sind die auf dem Pensionskassenausweis enthaltenen Daten nicht besonders schützenswerte Daten im Sinne von Art. 3 lit. c DSG. Im Kontext des Arbeits- und Versicherungsverhältnisses sind Gesundheitsdaten aber nicht auszuschliessen, weshalb Versicherungsdaten eine spezielle Qualität zukommt. Im

Pensionskassenausweis der Einrichtung X sind Daten des Versicherten über seine konkrete persönliche Vorsorgesituation aufgeführt, so auch Freizügigkeitsleistungen. Es können aber offenbar auch Gesundheitsdaten mitgeteilt werden, wie eingeschränkter Versicherungsschutz und temporäre Erwerbsunfähigkeit. Der Pensionskassenausweis kann also nicht nur Informationen über die finanzielle Situation des Arbeitnehmers, sondern mitunter auch über die gesundheitliche Situation enthalten.

Der Arbeitnehmer hat kein Interesse vermögens- und versicherungsrechtliche und allenfalls Gesundheitsdaten seinem Arbeitgeber bekannt zu geben. Ausserdem hat der Arbeitgeber nach Art. 328b OR keinen Anspruch auf diese Daten (siehe unten). Da der Arbeitnehmer die Versichertendaten des Arbeitnehmers nicht für die Erfüllung der gesetzlichen Pflichten gemäss BVG benötigt und der Arbeitnehmer ein überwiegendes Privatinteresse an der Geheimhaltung seiner persönlichen Daten hat, kann Art. 86a Abs. 2 lit. a BVG als Ausnahmegrund von der Schweigepflicht nicht greifen.

41. Zudem dürfen Daten nur weitergegeben werden, wenn sie für den in Frage stehenden Zweck erforderlich sind (Art. 86a Abs. 5 BVG). Es ist nicht ersichtlich, zu welchem vorsorgerechtlichen Zweck der Arbeitgeber die persönlichen Vorsorgedaten und allenfalls Gesundheitsdaten seiner Arbeitnehmer benötigt. Deshalb ist nach Art. 86a Abs. 5 BVG die Datenbekanntgabe an den Arbeitgeber zweckwidrig.





**Art. 328b OR**

42. Es trifft zu, wie die Einrichtung X ausführt, dass der Arbeitgeber nach Art. 331 Abs. 4 OR eine Informationspflicht über die Forderungsrechte hat und der Arbeitgeber nach Art. 328 OR eine Fürsorgepflicht zukommt. Die Einrichtung X verknüpft aber wiederum zwei an sich richtige Aussagen, um dadurch zu schliessen, eine gesetzliche Grundlage für die von ihr praktizierte Datenbekanntgabe an den Arbeitgeber sei vorhanden. Auch diese Schlussfolgerung ist falsch. Die Informationspflicht des Arbeitgebers gegenüber dem Arbeitnehmer gemäss Art. 331 Abs. 4 OR betrifft Forderungsrechte, während die Fürsorgepflicht nach Art. 328b OR den Arbeitgeber verpflichtet, alles zu unterlassen, was den berechtigten Interessen des Arbeitnehmers schadet (so auch Geheimhaltungsinteressen).

43. Entgegen der Auffassung der Vorsorgeeinrichtung steht die Datenbekanntgabe an den Arbeitgeber nicht im Einklang mit Art. 328b OR und der daraus fliessenden Fürsorgepflicht. Weder benötigt der Arbeitgeber die Kenntnis dieser Daten um seiner Auskunfts- und Fürsorgepflicht nachzukommen, noch benötigt der Arbeitgeber,

entgegen der Auffassung der Einrichtung X, die Versicherungsdaten zur Erfüllung des Arbeitsvertrages. Art. 328b OR hat einen weit reichenden Regelungsgehalt. Er beschränkt die zulässige Datenbearbeitung im Arbeitsverhältnis auf den Bezug zum Arbeitsplatz. Demnach darf der Arbeitnehmer Daten nur dann bearbeiten, wenn sie die Eignung des Arbeitsverhältnisses betreffen oder zur Durchführung des Arbeitsvertrages erforderlich sind. Aufgrund seiner aus Art. 328b OR fliessenden Fürsorgepflicht hat der Arbeitgeber gerade alles zu unterlassen, was den berechtigten Interessen des Arbeitsnehmers schaden könnte. Es kann wohl nicht im Interesse des Arbeitnehmers, dass der Arbeitnehmer automatisch Einblick in seine persönliche Vorsorgesituation und allenfalls Gesundheitssituation nehmen kann. Vielmehr ist ein solcher Datentransfer im ausschliesslich im Interesse des Arbeitgebers. Persönliche Verhältnisse, Eigenschaften, Neigungen, die nicht wesentlich die beruflichen Fähigkeiten bestimmen, gehen den Arbeitgeber nichts an und dürfen von ihm weder erfragt noch gespeichert werden (BSK-DSG, MARTIN WINTERBERGER-YANG, Art. 328b/362 OR N 1 ff.). So stehen nach Art. 328b OR bereits Lohndaten früherer Arbeitgeber in keinen Zusammenhang mit dem aktuellen Arbeitsverhältnis. Zudem dürfte der Arbeitgeber auch keinen Zugang zum Gesundheitsfragenbogen haben (BSK-DSG, MARTIN WINTERBERGER-YANG, Art. 328b OR, N2 ff. N 8 und N 13). Deshalb dürfte der Arbeitnehmer bereits unter dem Blickwinkel des Art. 328b OR keine Kenntnis von den persönlichen Vermögensverhältnissen und den Gesundheitsdaten haben. Auch in Art. 328b OR ist keine ausdrückliche Ermächtigung für den Erhalt der Pensionskassendaten enthalten. Davon abgesehen ist Art. 328b OR keine Ausnahme, welche Art. 86 BVG relativieren würde.

**Hinweise der** Einrichtung X

44. Die Einrichtung X weist in Ihrer Stellungnahme hin auf die branchenübliche Zustellpraxis der grossen Versicherungen, die Marktüblichkeit (teilautonome Stiftungen) und die Marktüblichkeit vor dem Hintergrund der Praxis der Stiftung Auffangrichtung BVG. Branchenübliche Zustellungspraxis und Marktüblichkeit vermögen das Legalitätsprinzip, an welches sich ein Bundesorgan gemäss Art 17 DSG halten muss, nicht zu ersetzen. Ausserdem gibt es grosse Versicherungen, welche die Pensionskassenausweise den bei ihr versicherten Personen direkt persönlich und vertraulich zustellen.

45. Das vom Bundesrat genehmigte Reglement 2005 der Auffangstiftung BVG, auf welches die Einrichtung X verweist, würde den Anforderungen im Sinne von Art. 19 bzw. 17 DSG an eine genügende gesetzliche Grundlage ebenfalls nicht genügen, wenn es als gesetzliche Grundlage für das nicht persönliche Zusenden von

Pensionskassenausweisen dienen sollte. Das Reglement erwähnt im zweiten Teil, Allgemeine Bestimmungen (AB), in Art. 55 Abs. 2, dass der Arbeitnehmer die Vorsorgeausweise an die versicherten Arbeitnehmer auszuhändigen hat. Sofern die Zustellung der Pensionskassenausweise in Gewährleistung der Datensicherheit (Art. 7 DSG, siehe unten) erfolgt, d.h. wenn der Arbeitgeber keinen Einblick in die persönlichen Daten der Arbeitnehmer nehmen kann, was der Fall wäre, wenn eine persönliche, vertrauliche Adressierung bestünde, wäre dies datenschutzkonform. Öffnet der Arbeitgeber eine persönlich und vertraulich an seinen Arbeitnehmer adressierte Sendung, würde er sich nach Art. 179 StGB strafbar machen. Werden hingegen Daten des Arbeitnehmers dem Arbeitgeber bekannt gemacht und ist kein Rechtfertigungsgrund für die Schweigepflichtverletzung vorhanden, würde auch dieser Vorgang vor dem Legalitätsprinzip nicht standhalten, da das Reglement keine generell-abstrakte und genügend bestimmte Rechtsnorm ist, die nach Art. 17 DSG gefordert wird, was aber nicht Gegenstand der aktuellen Sachverhaltsabklärung ist.

46. Entgegen der Meinung der Einrichtung X ist nicht der Arbeitgeber für die Zustellungspraxis der Einrichtung X datenschutzrechtlich verantwortlich, sondern die Einrichtung X. Daran ändert nichts, dass der Arbeitgeber auf Aufforderung der Versicherung hin eine Zustelladresse angibt und die Versicherung die Pensionskassenausweise an diese Adresse, offenbar mit dem Vermerk «vertraulich», zustellt. Bevor die Daten in den Herrschaftsbereich des Arbeitgebers gelangen, verlassen sie zunächst den Herrschaftsbereich der Versicherung. Da der Arbeitgeber ein Dritter ist und er Daten erhält, die ihm vorher in diesem Umfang nicht bekannt waren, findet eine Datenbekanntgabe an einen Dritten statt. Die Versicherung hat technische und organisatorische Massnahmen zu treffen, damit gewährleistet werden kann, dass die Pensionskassenausweise nicht an den Arbeitgeber, sondern vertraulich an die versicherte Person gelangen. Ziel ist es, dass ein allfälliges unbefugtes Bearbeiten von Personendaten verhindert wird. Dieses rein organisatorische Problem kann die Vorsorgeeinrichtung nicht auf die Unternehmen abwälzen (KURT PAULI, Basler Kommentar Datenschutzgesetz, Art. 7 N 7). Für die Datensicherheit bei der Übermittlung von Pensionskassenausweisen ist nach Art. 7 DSG die Vorsorgeeinrichtung zuständig.

### III. Fazit

Da die Einrichtung X den Arbeitgebern Pensionskassenausweise der Arbeitnehmer zustellt, welche nicht persönlich und vertraulich an jeweiligen versicherten Personen adressiert sind, gibt sie einem Dritten ohne gesetzliche Erlaubnis Daten bekannt, wes-

halb das Legalitätsprinzip verletzt ist. Da die Einrichtung X für die Datenbekanntgabe an den Dritten sich auf keine gesetzliche Ausnahme stützen kann, ist von einer Schweigepflichtverletzung auszugehen, da sie einem Dritten Einblick in Daten ermöglicht, an welchen dieser selber ein Interesse haben kann (Art. 86a BVG i.V. m Art. 76 Abs. 4 BVG).

Aus diesen Gründen ersucht Sie der EDÖB den eingangs gestellten Anträgen zu entsprechen.

Mit freundlichen Grüssen

Hanspeter Thür





**Beilagen**:

| | |
|---|---|
| Beilage 1: | Schreiben EDÖB vom 15. Mai 2008 |
| Beilage 2: | Schreiben Einrichtung X vom 27. Mai 2008 |
| Beilage 3: | Schreiben EDÖB vom 3. Juni 2008 |
| Beilage 4: | Schreiben Einrichtung X vom 7. Juli 2008 |
| Beilage 5: | Schreiben EDÖB vom 24. Juli 2008 |
| Beilage 6: | Schreiben Einrichtung X vom 11. September 2008 |
| Beilage 7: | Schreiben EDÖB vom 13. Februar 2009 |
| Beilage 8: | Schreiben Einrichtung X vom 12. März 2009 |
| Beilage 9: | Schreiben EDÖB vom 3. April 2009 |
| Beilage 10: | Empfehlung des EDÖB vom 8. Juli 2009 |
| Beilage 11: | Orientierung EDI Schreiben des EDÖB vom 8. Juli 2009 |
| Beilage 12: | Stellungnahme der Einrichtung X vom 10. August 2009 |

### 4.1.6 Empfehlung betreffend «Google Street View»

Bern, 11.09.2009

**Empfehlung**

**(Art. 29 Abs. 3 DSG)**

**des**

**Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB)**

**Feldeggweg 1, 3003 Bern**

an

**Google, Inc.**

**1600 Amphitheatre Parkway**

**Mountain View, CA 94043**

**USA**

und

**Google Switzerland GmbH**

**Brandschenkestrasse 110**

**8002 Zürich**

in der Sache

**Google Street View**

betreffend

**die Bearbeitung und Veröffentlichung von Bildaufnahmen über Personen und Autokennzeichen im Internet**

## I. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte stellt fest:

1. Google, Inc. hat in der Nacht vom 17. auf den 18. August 2009 seinen Dienst Google Street View in der Schweiz lanciert. Der Dienst erlaubt über das Internet einen virtuellen Rundgang durch Strassenzüge. Um diesen Dienst anbieten zu können, fuhr und fährt Google, Inc. in der Schweiz mit eigens hierfür umgebauten Fahrzeugen öffentlich zugängliche Strassenzüge ab und nimmt diese Strassenzüge mit speziellen, auf diesen Fahrzeugen (in einer Höhe von ca. 2.75m) montierten Bildaufnahmegeräten auf. In diesem Rahmen wurden für die Schweiz von Google, Inc. nach eigenen Angaben bisher mehr als 20 Mio. Bilder veröffentlicht.

2. Da sich auf diesen Strassenzügen Personen bewegen, werden durch die Aufnahmen zwangsläufig Bilder von betroffenen Personen durch Google, Inc. bearbeitet. Nach der Aufnahme der Bilder bereitet Google, Inc. diese auf und stellt sie in seinem Dienst Google Street View im Internet gratis zur Verfügung. Die Aufbereitung der Bilder beinhaltet unter anderem die Erstellung eines virtuellen Raums, welcher eine virtuelle Rundumansicht des Strassenzugs ermöglicht, sowie die automatisierte Unkenntlichmachung der Gesichter von betroffenen Personen sowie der Nummernschilder von Kraftfahrzeugen.

3. Im Rahmen seiner Abklärungen am online geschalteten Dienst Google Street View stellte der EDÖB fest, dass die Anonymisierungssoftware nur einen gewissen Anteil der aufgenommenen Gesichter und Autokennzeichen anonymisiert (nach bisherigen Angaben von Google, Inc., die im Streitfall von unabhängiger Seite überprüft werden müssen, beträgt dieser Anteil ca. 98%). Google, Inc. stellt auf Street View zudem ein einfaches webbasiertes Formular zur Verfügung, mit welchem nicht unkenntlich gemachte Bilder gemeldet werden können, bzw. über welches für bestimmte Bilder Löschungsbegehren gestellt werden können. In der Regel wird diesen Begehren innerhalb von 24 bis 48 Stunden durch Google, Inc. entsprochen. Bei Google, Inc. sind nach deren eigenen Angaben bereits bis zum 2. September 2009 rund x Gesuche zur Entfernung von Häusern, Gesichtern und Autokennzeichen eingegangen und innert weniger als 24 Stunden bearbeitet worden.

4. Zudem musste der EDÖB bei der Aufschaltung des Dienstes Google Street View feststellen, dass weit mehr Städte und Strassenzüge aufgenommen wurden, als auf der Google-Webseite und gegenüber dem EDÖB angekündigt.

5. Google informiert im Schreiben vom 4. September 2009, welches die anlässlich der Verhandlung vom 2. September 2009 unterbreiteten Vorschläge zusammenfasst, bezüglich der Autokennzeichen in Aussicht, dass der Detektor der Blurring-Software für Schweizer Kennzeichen neu trainiert werde und mit Bezug auf das Gesichter-Blurring in der Schweiz als erstes Land eine neue Version der Detektor-Software eingesetzt werde. Die Umsetzung der vorgeschlagenen Massnahmen bedürfe der Organisation und Planung. Die neuen Prozesse würden so rasch als möglich implementiert, es werde aber einige Wochen dauern. Während der nach dem Start des Dienstes Google Street View mit Google, Inc. geführten Gespräche konnte der EDÖB noch nicht feststellen, ob und inwieweit in Zukunft aufgrund der von Google, Inc. gewählten Technologie eine wesentliche Verbesserung der Unkenntlichmachung der Gesichter von betroffenen Personen sowie der Nummernschilder von Kraftfahrzeugen zu erwarten ist. Im Gespräch vom 2. September 2009 wurde indessen von der Verhandlungsdelegation von Google klar gestellt, dass eine vollständige Unkenntlichmachung von Gesichtern und Autokennzeichen auch mit Hilfe der verbesserten Software nicht möglich sei. Google stellt ferner in Aussicht, dass es an Organisationen herantritt, welche mit Blick auf den Datenschutz gegebenenfalls sensitive Institutionen betreiben, um diese zu informieren, wie sie Bilder aus Street View entfernen lassen können. Hinsichtlich besonders kritischer Orte (z.B. Rotlichtbezirke), wo diese Lösung nicht möglich sei, werde Google die notwendigen Vorkehrungen treffen, um allenfalls von der Software nicht erfasste Personen und Kennzeichen zu identifizieren und Fehler zu beheben. Weiter will Google die Informationen darüber, wo die Fahrzeuge unterwegs sind, erweitern und verbessern.

   An der Sitzung vom 2. September 2009 machte Google klar, dass trotz der in Aussicht gestellten Verbesserungen die Software nicht derart verbessert werden könne, dass sämtliche Gesichter und Autokennzeichen zuverlässig unkenntlich sind. Eine manuelle Nachbearbeitung der Bilder schloss Google mit der Begründung aus, der Aufwand wäre erheblich und unverhältnismässig.

## II. Erwägungen des Eidgenössischen Datenschutz und Öffentlichkeitsbeauftragten

6. Auf einer Vielzahl der durch Google, Inc. bearbeiteten Bilder sind Personen abgebildet. Diese Bilder beziehen sich damit auf bestimmte oder bestimmbare Personen gemäss Art. 3 lit. a des Bundesgesetzes über den Datenschutz (DSG; SR 235.1). Damit handelt es sich bei den von Google, Inc. bearbeiteten

Daten um Personendaten gemäss DSG. Unter Bearbeitung wird gemäss Art. 3 lit. e DSG jeder Umgang mit Personendaten, unabhängig von den angewendeten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten verstanden. Durch die Bildaufnahmen, die nachträgliche teilweise Unkenntlichmachung sowie durch die Veröffentlichung bearbeitet Google, Inc. Personendaten im Sinne des DSG.

7. Gemäss Art. 2 Abs. 1 DSG gilt dieses Gesetz für das Bearbeiten von Daten natürlicher und juristischer Personen durch private Personen. Aufgrund des Territorialitätsprinzips ist das DSG auf jede Bearbeitung, welche in der Schweiz stattfindet bzw. stattgefunden hat, anwendbar. Google, Inc. hat die Bilder in der Schweiz aufgenommen. Daher ist das DSG für die Beurteilung des vorliegenden Sachverhalts anwendbar.

8. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte klärt nach Art. 29 Abs. 1 lit. a DSG von sich aus oder auf Meldung Dritter hin den Sachverhalt näher ab, wenn Bearbeitungsmethoden geeignet sind, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen (Systemfehler). Vorliegend behauptet Google, Inc. zwar, mit ca. 98% einen hohen Grad an Unkenntlichmachung der Gesichter und Nummertafeln zu erreichen. Selbst wenn dies zutrifft, gehen aufgrund der schweizweit grossen Abdeckung und der grossen Anzahl von aufgenommenen Personen die Bilder, auf welchen Personen vollkommen erkenntlich sind, in die Zehntausende. Darüber hinaus ist davon auszugehen, dass eine grosse Zahl von betroffenen Personen auf den Bildern für einen beschränkten Personenkreis weiterhin erkennbar bleibt, selbst wenn die Unkenntlichmachung sämtlicher Gesichter der betroffenen Personen oder der Nummertafeln erfolgreich wäre. Aus diesem Grund ist die Bearbeitungsmethode von Google, Inc. geeignet, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen (Systemfehler). Der EDÖB ist daher dazu berechtigt, den Sachverhalt näher abzuklären und gemäss Art. 29 Abs. 3 DSG eine Empfehlung zu erlassen und diese gemäss Art. 29 Abs. 4 DSG – wenn sie abgelehnt wurde – dem Bundesverwaltungsgericht zum Entscheid vorzulegen.

### a. Erwägungen zu den Grundsätzen der Datenbearbeitung

9. Gemäss Art. 12 Abs. 1 DSG darf, wer Personendaten bearbeitet, dabei die Persönlichkeit der betroffenen Person nicht widerrechtlich verletzen. Dies wird in Art. 12 Abs. 2 lit. a DSG dahingehend konkretisiert, als dass der Datenbearbei-

ter insbesondere nicht Personendaten entgegen den Grundsätzen der Art. 4, 5 Abs. 1 und 7 Abs. 1 DSG bearbeiten darf.

10. Nach dem Rechtmässigkeitsprinzip von Art. 4 Abs. 1 DSG dürfen Personendaten nur rechtmässig bearbeitet werden. Inwiefern die Datenbearbeitung durch Google, Inc. rechtmässig ist, lässt sich erst beurteilen, nachdem geprüft wurde, ob die Datenbearbeitung gegen herrschendes Recht, insbesondere auch gegen Art. 28 des Schweizerischen Zivilgesetzbuches (ZGB; SR 210.0) und das DSG verstösst.

11. Zudem hat die Datenbearbeitung nach dem Prinzip von Treu und Glauben zu erfolgen und muss verhältnismässig sein (Art. 4 Abs. 2 DSG). Nach jetzigem Kenntnisstand des Sachverhaltes geht der EDÖB nicht von einem Verstoss gegen das Prinzip von Treu und Glauben durch Google, Inc. aus.

12. Nach dem Verhältnismässigkeitsprinzip muss die Datenbearbeitung im Hinblick auf den zu erreichenden Zweck verhältnismässig sein. Der Zweck der Datenbearbeitung durch Google, Inc. liegt in der kostenfreien Veröffentlichung von Strassenansichten im Internet (wobei auf den Bildern er-scheinende Personen und Autokennzeichen teilweise unkenntlich gemacht werden). So erhofft sich Google, Inc. Werbeeinnahmen durch so genannte Klicks auf dem Produkt Google Street View. Aus diesem Grund wird zu beurteilen sein, inwieweit das Interesse von Google, Inc. an der Veröffentlichung der Bilder und das öffentliche Interesse an der Möglichkeit eines virtuellen Rundgangs durch die aufgenommenen Strassenzüge das schützenswerte Persönlichkeitsinteresse der betroffenen Personen überwiegen (vgl. Erwägungen zur möglichen Persönlichkeitsverletzung).

13. Gemäss dem Zweckmässigkeitsprinzip von Art. 4 Abs. 3 DSG dürfen Personendaten nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist. Zudem muss die Beschaffung von Personendaten gemäss Art. 4 Abs. 4 DSG erkennbar sein. Google, Inc. informiert die betroffenen Personen nur sehr rudimentär über die Kamerafahrten seiner Fahrzeuge. Ausserdem musste der EDÖB feststellen, dass die Liste der im Internet verfügbaren Orte um ein vielfaches grösser war, als die Liste der von Google, Inc. auf seiner Webseite angekündigten Orte, an denen Aufnahmen gemacht werden sollten bzw. gemacht wurden. Zudem dürften sich wohl die betroffenen Personen nur in

wenigen Fällen darüber informiert haben, ob ein entsprechendes Fahrzeug von Google, Inc. zu einem bestimmten Zeitpunkt einen Strassenzug aufnimmt, um zu vermeiden, fotografiert zu werden. Ebenfalls ist nicht davon auszugehen, dass die betroffenen Personen das heranrückende Fahrzeug bereits aus weiter Ferne erblicken konnten, um sich aus dem Aufnahmebereich der Kamera zu entfernen. Aus diesem Grund kann eine Verletzung des Erkennbarkeitsprinzips durch die Datenbearbeitung durch Google, Inc. nicht ausgeschlossen werden.

Da in vielen Fällen die betroffene Person noch nicht einmal weiss, dass Daten über sie bearbeitet werden, kann sie zwangsläufig auch nicht über den Zweck der Datenbearbeitung informiert worden sein. Ob und inwiefern die Datenbearbeitung durch Google, Inc. allerdings aus den Umständen heraus (insbesondere aufgrund der Medienpräsenz) hätte erkannt werden können, ist zumindest fraglich. Aus diesem Grund ist auch eine Verletzung des Zweckmässigkeitsprinzips nicht auszuschliessen. Kommt man zu dem Schluss, dass durch die Datenbearbeitung von Google, Inc. das Zweckmässigkeitsprinzip und das Erkennbarkeitsprinzip verletzt wurden, so geht der Gesetzgeber gemäss Art. 12 Abs. 2 lit. a DSG von einer widerrechtlichen Persönlichkeitsverletzung aus.

14. Art. 13 Abs. 2 lit. e DSG gibt dem Datenbearbeiter einen Rechtfertigungsgrund, wenn dieser Personendaten zu nicht personenbezogenen Zwecken, insbesondere in der Forschung, Planung und Statistik, bearbeitet und die Ergebnisse so veröffentlicht, dass die betroffenen Personen nicht bestimmbar sind. Die Datenbearbeitung von Google, Inc. zielt in der Regel nicht darauf ab, die gesammelten Personendaten zu einem personenbezogenen Zweck zu bearbeiten.

    Vielmehr versucht Google, Inc. durch die Unkenntlichmachung der Gesichter und Autokennzeichen die Bilder so zu veröffentlichen, dass die betroffenen Personen nicht bestimmbar sind. Vor diesem Hintergrund geht der EDÖB davon aus, dass die Aufnahme von Bildern, auf denen Personen bestimmbar sind, legitim ist, solange die Grundsätze der Datenbearbeitung eingehalten werden und die Bilder vor der Veröffentlichung auf eine Weise unkenntlich gemacht werden, dass die betroffenen Personen nicht mehr bestimmbar sind.

### b. Erwägungen zur möglichen Persönlichkeitsverletzung

15. Bei der Datenbearbeitung durch Google, Inc. stellt sich die Frage, ob und inwiefern das Verhältnismässigkeitsprinzip gemäss Art. 4 Abs. 2 DSG eingehalten wurde. Um dies beurteilen zu können, muss eine Interessenabwägung

zwischen den schützenswerten Interessen der betroffenen Personen und den privaten Interessen von Google, Inc. sowie dem öffentlichen Interesse am Dienst Google Street View durchgeführt werden. Hierbei ist auf die sich konkret abzeichnenden Verhältnisse abzustellen.

16. Die Lehre und Rechtssprechung anerkennt ein Recht am eigenen Bild (BGE 129 III 715 E 4.1). Bilder zeigen Tatsachen in besonders eindringlicher Weise, weshalb regelmässig die informationelle Privatheit und/oder Ehre des Betroffenen verletzt wird. Schon alleine die fotografische Aufnahme kann (muss aber nicht) eine Persönlichkeitsverletzung bedeuten, je nachdem, ob schutzwürdige Interessen des Betroffenen beeinträchtigt werden. In der Weiterverbreitung oder Veröffentlichung eines individualisierenden Bildnisses ohne Einwilligung der betroffenen Person liegt demgegenüber immer eine Persönlichkeitsverletzung vor (Handkommentar zum Schweizer Privatrecht; Aebi-Müller zu Art. 28 ZGB; Rz. 25). Eine solche Persönlichkeitsverletzung wirkt umso schwerer, wenn sich die Person in einer kompromittierenden Situation befindet oder aufgrund der Aufnahmen falsche Rückschlüsse auf das Verhalten einer Person gezogen werden können.

17. Der Zweck von Google Street View ist es, interessierten Personen die Möglichkeit zu geben, sich virtuell durch Ortschaften und Städte zu bewegen. Obwohl der Dienst Google Street View kostenlos weltweit zur Verfügung steht, verfolgt Google Inc. hierbei einen wirtschaftlichen Zweck. Das Geschäftsmodell von Google, Inc. sieht vor, dass durch die im Rahmen des Dienstes aufgeschaltete Werbung in Verbindung mit den Klicks der Nutzer Einnahmen generiert werden. Um dies zu erreichen, hat Google, Inc. ein Interesse daran, dass Google Street View für Internetnutzer möglichst interessant gestaltet wird. Daher spielt die Neugier der Internetnutzer bei der Ausgestaltung des Dienstes eine entscheidende Rolle.

18. Google Street View bildet die betroffenen Personen grundsätzlich nicht individualisiert ab, sondern gibt einen Überblick über alle sich in den Strassenzügen befindlichen Personen. Allerdings ist es durch die Zoomfunktion in Google Street View möglich, aufgenommene Passanten individualisiert zu betrachten. Aber gerade eine solche Veröffentlichung von Bildern wird von der herrschenden Lehre und Rechtssprechung als Persönlichkeitsverletzung betrachtet.

19. Google, Inc. unternimmt zwar Anstrengungen, um zumindest Gesichter von betroffenen Personen und Autokennzeichen unkenntlich zu machen. Dieser Dienst funktioniert nach (vom EDÖB bisher nicht überprüften) Angaben seitens Google, Inc. in ca. 98% der Fälle. Dies bedeutet, dass ca. 98% der aufgenommenen Gesichter und Autokennzeichen unkenntlich gemacht werden. Angesichts der grossen Anzahl an aufgenommenen Personen und Autos, nach Schätzung des EDÖB weit über eine Million, auf den über 20 Mio. von Google, Inc. veröffentlichten Bildern, beträgt die Anzahl an Personen, deren Gesichter und Autokennzeichen nicht unkenntlich gemacht wurden und die im Dienst Google Street View individualisiert betrachtet werden können, schätzungsweise mehrere zehntausend. Diese Schätzungen werden alleine schon durch die rund x Anonymisierungsgesuche, welche bei Google, Inc. bis zum 2. September 2009 eingegangen sind, bestätigt. In dieser Grössenordnung kann daher aus Sicht des EDÖB nicht mehr von Einzelfällen gesprochen werden.

20. Da sich das Unkenntlichmachen nur auf die Gesichter der betroffenen Personen bezieht, ist es nach Meinung des EDÖB unter gewissen Umständen dennoch möglich, betroffene Personen anhand ihrer äusserlichen Merkmale zu erkennen und durch die Zoomfunktion individualisiert zu betrachten. Auch in solchen Fällen ist von einer Persönlichkeitsverletzung auszugehen. Dies ist insbesondere dann der Fall, wenn sich die betroffene Person in der Nähe ihres Lebensmittelpunktes aufhält, wo sie in der Regel bekannt ist. Der EDÖB ist der Meinung, dass betroffene Personen eine solche Darstellung ihres Bildnisses im Internet nicht ohne weiteres erdulden müssen.

21. Eine durch die Erkennbarkeit einer betroffenen Person erfolgende mögliche Persönlichkeitsverletzung wiegt weit schwerer, wenn sich der Betroffene in der Nähe eines sensiblen Bereichs (z.B. Spital, Frauenhaus, Sozialbehörden, Vormundschaftsbehörde, Gerichte, Gefängnisse, Schulen, Rotlichtmilieu, etc.) aufhält. Gleiches gilt im Interesse der nationalen Sicherheit für militärische Anlagen und Einrichtungen, Botschaften, Regierungsgebäude, etc. Aus diesem Grund ist der EDÖB der Meinung, dass bei solchen Einrichtungen höhere Anforderungen an die Unkenntlichmachung gestellt werden müssen.

### c. Erwägungen zum Privatbereich von betroffenen Personen

22. Die Aufnahmekameras, welche auf den Fahrzeugen von Google, Inc. montiert sind, befinden sich in einer Höhe von ca. 2.75m. Damit nehmen diese Kameras

Bilder aus einem anderen Blickwinkel auf als derjenige, der für gewöhnliche Passanten ersichtlich ist.

Auf diese Weise werden von Google, Inc. umfriedete Höfe, welche häufig durch einen Sichtschutz (mit einer Höhe von meist etwas über 2m) verdeckt sind, aufgenommen, obwohl sie dem Einblick eines gewöhnlichen Passanten verschlossen sind. Gemäss Art. 179quater StGB ist die Bildaufnahme im Geheim- oder Privatbereich ohne Einwilligung des Betroffenen sogar strafbar.

23. Ein umfriedeter Hof stellt einen Privatbereich dar, welcher – solange er durch einen Sichtschutz (z.B. Hecke) abgegrenzt ist – vor neugierigen Blicken von Passanten schützt. Damit ist dieser Privatbereich nicht ohne weiteres von jedermann einsehbar. Google, Inc. nimmt allerdings gerade auch solche Privatbereiche mit seinen Aufnahmegeräten auf Bildträger auf und veröffentlicht diese im Rahmen seines Dienstes Google Street View.

24. Durch die Montage seiner Aufnahmegeräte in einer Höhe von ca. 2.75m nimmt Google, Inc. daher zumindest billigend in Kauf, dass Privatbereiche, welche nicht von jedermann einsehbar sind, auf Bildträger abgebildet und im Nachhinein im Internet veröffentlicht werden.

Inwieweit dies zudem vorsätzlich geschieht, kann der EDÖB nicht beurteilen, allerdings ist aufgrund des Ge-schäftsmodells von Google, Inc. die Möglichkeit der vorsätzlichen Aufnahme des Privatbereichs zur Erzielung möglichst vieler Klicks auf Google Street View, indem man die Neugier der Internetnutzer anspricht, nicht ohne weiteres von der Hand zu weisen.

25. Der EDÖB hat weiter festgestellt, dass Bildaufnahmen auch auf Privatstrassen gemacht wurden. Hier bedarf es einer Einwilligung, die indessen in den dem EDÖB bekannten Fällen fehlt.

26. Der EDÖB geht daher auch in diesen Fällen von einer Persönlichkeitsverletzung aus.

### d. Rechtfertigungsgründe

27. Eine Verletzung der Persönlichkeit ist gemäss Art. 13 DSG widerrechtlich, wenn sie nicht durch Einwilligung des Verletzten, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt ist. Eine Einwilligung der betroffenen Personen liegt offensichtlich nicht vor.

28. Ein überwiegendes öffentliches Interesse besteht aus Sicht des EDÖB nicht, auch wenn eingeräumt wird, dass die Möglichkeit, virtuell durch Dörfer und Städte spazieren zu können, durchaus auf breites Interesse stösst. Ein solcher Dienst kann der Öffentlichkeit auch unter Respektierung der Persönlichkeitsrechte der betroffenen Passanten zur Verfügung gestellt. Es ist zu bezweifeln, ob die von Google angewandte Technik die einzige Möglichkeit zur zuverlässigen Unkenntlichmachung von Gesichtern und Autokennzeichen darstellt. Will Google an dieser Methode festhalten, müssen die Bilder nach Meinung des EDÖB nachbearbeitet werden. Das Argument, damit sei ein unverhältnismässiger finanzieller Aufwand verbunden, vermag die Verletzung der Persönlichkeitsrechte einer grossen Zahl von Personen nicht zu rechtfertigen. Immerhin ist festzuhalten, dass Art. 13 Abs. 2 lit. e DSG sogar verlangt, dass Personendaten, die zu nicht personenbezogenen Zwecken bearbeitet wurden, nur veröffentlicht werden dürfen, wenn die betroffenen Personen nicht bestimmbar sind. Das beinhaltet die vollständige Anonymisierung der Personen, was klar weiter geht als die vom EDÖB verlangte Unkenntlichmachung von Gesichtern und Autokennzeichen.

29. Die vom EDÖB verlangte Nachbearbeitung der Bilder findet im Übrigen ohnehin statt, allerdings nur in jenen Fällen, wo Betroffene die Löschung von Personen, Autos oder Häuser selber beantragen. Es kann den betroffenen Personen nicht zugemutet werden, selber aktiv werden zu müssen, um eine gegen sie gerichtete Persönlichkeitsverletzung aus der Welt zu schaffen. Umso mehr, als Teile der Bevölkerung nach wie vor über keinen Internet-Anschluss verfügen und damit nicht einmal Kenntnis erhalten, ob ihre Persönlichkeitsrechte verletzt wurden. Auch für jene, die einen Internet-Anschluss haben, ist die Suche nach möglichen Verletzungen nicht zumutbar, umso mehr, als ein Betroffener gar nicht weiss, wann genau Google wo Bildaufnahmen gemacht hat.

30. Ein überwiegendes privates Interesse ist ebenfalls nicht ersichtlich. Jedenfalls kann der Umstand, dass für Google ein möglicher Gewinn aus der Lancierung des Produkts wegfällt oder reduziert wird, nicht als solcher akzeptiert werden.

### e. Vorläufige Massnahme

31. Google führt selber aus, dass die Verbesserung der Software einige Zeit in Anspruch nehmen wird. Deshalb sind vorläufig und bis zur Klärung der hängigen Rechtsfragen keine weiteren Orte im Internet aufzuschalten.

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

a. Google, Inc. verzichtet bis auf weiteres auf die Aufschaltung neuer Bilder über die Schweiz in seinem Dienst Google Street View.

b. Google, Inc. stellt für die bestehenden Aufnahmen eine verbesserte Lösung zur Unkenntlichmachung von Autonummern und Gesichtern zur Verfügung, welche den Anforderungen des DSG genügt. Insbesondere müssen Gesichter und Autokennzeichen vollständig unkenntlich gemacht werden.

c. Google, Inc. gewährleistet eine Anonymisierung von Personen im Bereich von sensiblen Einrichtungen, insbesondere vor Frauenhäusern, Altersheimen, Gefängnissen, Schulen, Sozialbehörden, Vormundschaftsbehörden, Gerichten und Spitälern.

d. Google, Inc. gewährleistet, dass umfriedete Orte wie Höfe, Gärten usw., welche von Passanten von der Strasse aus nicht eingesehen werden können, nicht auf Bildträger aufgenommen oder entsprechend entfernt werden. Künftig postiert Google die Kameras auf einer Höhe, von der aus keine Einblicke in den geschützten Privatbereich möglich sind.

e. Aufnahmen, die von (gekennzeichneten) Privatstrassen aus gemacht wurden, sind zu entfernen, sofern keine Einwilligung vorliegt.

f. Google, Inc. informiert mindestens eine Woche im Voraus, in welchen Städten und Dörfern in der kommenden Woche Aufnahmen gemacht werden.

g. Google, Inc. informiert eine Woche vor der Aufschaltung aufs Netz, welche Dörfer und Städte aufgeschaltet werden.

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

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

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

EIDGENÖSSISCHER DATENSCHUTZ- UND
ÖFFENTLICHKEITSBEAUFTRAGTER

Hanspeter Thür

### 4.1.7 Weiterzug betreffend «Google Street View»

Bern, 11.11.2009

## Klage in öffentlich-rechtlichen Angelegenheiten (Art. 29 Abs. 4 DSG, i.V.m. Art. 35 lit. b. VGG)

des

**Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB)**

**Feldeggweg 1, 3003 Bern**

**(Kläger)**

**gegen**

**Google, Inc.**

**1600 Amphitheatre Parkway**

**Mountain View, CA 94043 USA**

**(Beklagte)**

**und**

**Google Switzerland GmbH**

**Brandschenkestrasse 110, 8002 Zürich**

**(Beklagte)**

**in der Sache**

**Empfehlung des EDÖB vom 11. September 2009**

**betreffend**

**die Bearbeitung und Veröffentlichung von Bildaufnahmen über Personen und Autokennzeichen im Internet**

## I. Begehren

Folgenden Begehren sei stattzugeben:

*Im Form von provisorischen Massnahmen:*

1. Google, Inc. sowie der Google Schweiz GmbH sei im Rahmen einer vorsorglichen Massnahme gemäss Art. 30 Abs. 1 DSG das Aufschalten von in der Schweiz aufgenommener Bilder bis zum definitiven Entscheid zu untersagen.

2. Google, Inc. und der Google Schweiz GmbH seien bis auf weiteres Kamerafahrten in der Schweiz zu untersagen.

*Im Rahmen der Klage:*

1. Google, Inc. sowie die Google Schweiz GmbH stellen sicher, dass die Veröffentlichung der Bilder im Dienst Google Street View nur erfolgt, wenn Gesichter und Autokennzeichen vollständig unkenntlich worden sind.

2. Google, Inc. sowie die Google Schweiz GmbH stellen sicher, dass im Dienst Google Street View die Anonymität von Personen im Bereich von sensiblen Einrichtungen, insbesondere vor Frauenhäusern, Altersheimen, Gefängnissen, Schulen, Sozialbehörden, Vormundschaftsbehörden, Gerichten und Spitälern, gewährleistet ist.

3. Google, Inc. sowie die Google Schweiz GmbH stellen sicher, dass der Privatbereich (umfriedete Höfe, Gärten usw.) nicht auf Bildträger aufgenommen wird und die bereits aufgenommen Bilder aus dem Privatbereich der betroffenen Personen aus dem Dienst Google Street View entfernt werden.

4. Google, Inc. sowie die Google Schweiz GmbH stellen sicher, dass die von Privatstrassen aus ge machten Aufnahmen aus dem Dienst Google Street View entfernt werden, sofern keine Einwilligung für die Aufnahmen vorliegt.

5. Google, Inc. sowie die Google Schweiz GmbH informieren mindestens eine Woche im Voraus, in welchen Städten und Dörfern in der darauf folgenden Woche Aufnahmen getätigt werden.

6. Google, Inc. sowie die Google Schweiz GmbH informiert eine Woche vor Aufschaltung aufs Netz, welche Dörfer und Städte aufgeschaltet werden.

## II. Sachverhalt

1. Am 19. März 2009 hat Google, Inc. (Beklagte) in Zusammenarbeit mit der Google Schweiz GmbH (Beklagte) das Projekt Google Street View in der Schweiz gestartet und damit begonnen, mit speziell hierfür ausgestatteten Fahrzeugen Strassenzüge in der Schweiz zu photographieren.

   **Beweis:** Email vom 18. März; 2009 E2009.03.18-0041
   *(Anhang 3)*

   Zweck dieser Aufnahmen ist es, über das Internet (http://maps.google.ch/maps?hl=de&tab=wl) virtuelle Spaziergänge durch die abgebildeten Strassenzüge zu ermöglichen und letztere dem Internetnutzer im 360°-Winkel anzubieten.

2. Da der Dienst Google Street View in mehreren Ländern eingeführt wurde bzw. eingeführt wird, hat sich auch die Artikel 29 Datenschutzgruppe der Europäischen Union mit Google Street View befasst

   **Beweis:** Schreiben von Türk an Google B2009.06.03-0018
   *(Anhang 4)*

   und von Google, Inc. verlangt, dass die Bevölkerung vor Aufnahme der Bilder ausreichend informiert und eine angemessene Frist zu Löschung der von Google, Inc. aufgenommenen Daten definiert wird. Google, Inc. hat gegenüber dem EDÖB erklärt, dass eine entsprechende Information vor der Aufnahme der Bilder auch in der Schweiz gegeben werde. Bereits im Zeitraum der Kamerafahrten von Google, Inc. war die Bevölkerung geteilter Meinung über den neuen Dienst, und es wurden erste schriftliche Löschungsbegehren an Google, Inc. gestellt.

3. In der Nacht vom 17. auf den 18. August 2009 hat dann Google, Inc. seinen Dienst Google Street View über die Schweiz auf der Webseite (http://maps.google.ch/maps?hl=de&tab=wl) lanciert. Nach Angaben von Google, Inc. wurden in diesem Rahmen für die Schweiz bisher mehr als 20 Mio. Bilder veröffentlicht. Daraufhin gingen beim EDÖB zahlreiche Beschwerden zu nicht ausreichend unkenntlich gemachte Bilder, Aufnahmen von Privatstrassen und Privatgrundstücken, usw. ein.

4. In der Folge fanden zwischen dem EDÖB und Google, Inc. mehrere Gespräche statt, in denen eine Lösung für die Probleme gesucht wurde. Mit Schreiben vom 04. September 2009, welches die anlässlich der Verhandlung vom 02. September

2009 unterbreiteten Vorschläge zusammenfasst, stellte Google, Inc. in Aussicht, eine neue Version der Software zur Unkenntlichmachung für die Bilder der Schweiz einzusetzen. Dies bedürfe allerdings der Organisation und Planung. Zudem sicherte Google, Inc. zu bis auf weitere keine neuen Bilder mehr für die Schweiz aufzuschalten.

**Beweis:** Schreiben der Google Schweiz GmbH vom 4. September 2009 *(Anhang 5)*

5. Am 11. September 2009 hat der EDÖB eine Empfehlung an Google, Inc. erlassen. Google, Inc. hat mit Schreiben vom 14. Oktober 2009 die Empfehlung in weiten Teilen abgelehnt. Zudem hat Google, Inc. nur zugesichert zum Ende des Jahres 2009 keine neuen Bilder auf seinem Dienst Street View aufzuschalten.

**Beweis:** Empfehlung des EDÖB vom 11. September 2009 *(Anhang 1)*
Schreiben der Google Schweiz GmbH vom 14. Oktober 2009 *(Anhang 2)*





## III. Vorsorgliche Massnahme

6. Gemäss Art. 33 Abs. 2 DSG kann der EDÖB beim Präsidenten der auf dem Gebiet des Datenschutzes zuständigen Abteilung des Bundesverwaltungsgerichts vorsorgliche Massnahmen beantragen, wenn er bei einer Sachverhaltsabklärung nach Art. 29 Abs. 1 DSG feststellt, dass den Betroffenen ein nicht leicht wieder gutzumachender Nachteil droht. Die Aufschaltung von Bildern über betroffene Personen, insbesondere aus deren Privatbereich ist geeignet, deren Persönlichkeit in schwerwiegender Weise zu verletzen. Da die Persönlichkeitsverletzung durch die Veröffentlichung der Bilder im Internet stattfindet, ist der hieraus entstandene Schaden nachträglich durch Entfernung der Bilder nicht wieder gut zu machen. Zeitliche Dringlichkeit im Hinblick auf die Massnahme liegt dahingehend vor, dass Google, Inc. bereits angekündigt hat, nur noch bis Ende 2009 auf die Aufschaltung neuer Bilder zu verzichten. Daher müsste mit einer nicht hinnehmbar grossen Anzahl von neuen schwerwiegenden Persönlichkeitsverletzungen gerechnet, wenn der Endentscheid abgewartet werden würde. Daher ist auch die zeitliche Dringlichkeit der geforderten Massnahme gegeben. Die anzuordnende Massnahme ist darüber hinaus verhältnismässig, da sie geeignet ist, weitere Persönlichkeitsverletzungen zu vermeiden. Sie ist zudem das mildeste zur Verfügung stehende Mittel, um weitere Persönlichkeitsverletzungen zu vermeiden. Diese Massnahme bezieht sich auf

jene Bilder, welche Goolge bereits aufgenommen hat. Da die Bilder in die USA zur Weiterbearbeitung übermittelt werden und damit mit Bezug auf die Durchsetzung eines CH-Urteils eine gewisse Unsicherheit besteht sind Google ferner sämtliche Kamerafahrten in der Schweiz bis auf weiteres zu untersagen, um auf diese Weise zu verhindern, dass neue Bilder im Dienst Street View aufgeschaltet werden. Die vom EDÖB geforderte Massnahme ist auch im Hinblick auf die Zweck-Mittel Relation verhältnismässig, da Google, Inc. sämtliche für sie notwendigen Vorbereitungsarbeiten durchführen kann, um neue Bilder auf dem Dienst Street View aufzuschalten, wenn der EDÖB mit seinen Begehren wider Erwarten scheitern sollte. Die vorsorgliche Massnahme wirkt auch nicht präjudiziell oder verunmöglicht die geplante Endvorfügung. Aufgrund der bisherigen Rechtssprechung des Bundesgerichts (insbesondere BGE 118 IV 45) fällt die Prognose in der Hauptsache positiv aus.





## IV. Formelles

### Bearbeitung von Personendaten:

7. Gemäss Art. 3 lit. a des Bundesgesetzes über den Datenschutz (DSG, SR 235.1) werden als Personendaten alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen definiert. Hierunter ist grundsätzlich jede Art von Information zu verstehen, die auf die Vermittlung oder Aufbewahrung von Kenntnissen ausgerichtet ist, unerheblich davon ob eine Aussage als Zeichen, Wort, Bild, Ton oder Kombinationen aus diesen auftritt und aus welcher Art von Medium die Informationen gespeichert sind (Basler Kommentar zum DSG; Urs Belser zu Art. 3 lit. a DSG; Rz. 5). Entscheidend für die Qualifikation als Personendaten ist, dass sich die Angaben einer oder mehrer Personen zuordnen lassen.

8. Im vorliegenden Fall wurden von der Google Switzerland GmbH (Aufnahmefahrzeug ist auf die Google Schweiz GmbH zugelassen) bzw. von Google, Inc. (Google, Inc. behauptet, sie mache die Aufnahmen) Bilder einer grossen Anzahl von Strassenzügen in der Schweiz photographiert.

**Beweis:** Aufnahme eines Kamerafahrzeuges von Google und dazugehöriger Auszug aus dem E-Autoindex des Kantons Zürich
*(Anhang 6)*

Schreiben der Google Switzerland GmbH vom 14. Oktober 2009
*(Anhang 2)*

Dabei wurden auch Photoaufnahmen einer unbestimmten Anzahl von Personen, welche sich im Blickwinkel der Kameras befanden, gemacht. Damit hat entweder die Google Schweiz GmbH oder Google, Inc. in der Schweiz Personendaten bearbeitet und anschliessend zur Weiterbearbeitung in die USA übermittelt. Da zu diesem Zeitpunkt die Bilder noch nicht unkenntlich gemacht worden sind, handelt es sich hierbei um Personendaten, da die darauf abgebildeten Betroffenen ohne weiteres erkennbar sind.

9. Diese Personendaten wurden bzw. werden in der Folge (nach Angaben von Google) durch Google, Inc. in den USA weiterbearbeitet.





**Anwendbarkeit des DSG**

10. Gemäss Art. 2 DSG gilt das Gesetz für das Bearbeiten von Daten natürlicher und juristischer Personen. Wie bereits oben dargelegt, handelt es sich bei den durch die Beklagten bearbeiteten Bildern von Strassenzügen, auf denen sich Personen befinden, um Personendaten im Sinne von Art. 3 lit. a DSG.

11. Der EDÖB stellt fest, dass sowohl Google, Inc. als auch die Google Switzerland GmbH juristische Personen sind.

12. Aufgrund des Territorialitätsprinzips ist das DSG grundsätzlich für diejenige Datenbearbeitung anwendbar, welche in der Schweiz stattfindet. Damit ist das DSG mindestens für die Bearbeitungsschritte des Photographierens der Strassenzüge und der Übermittlung ins Ausland anwendbar.

**Anwendbarkeit des U.S. – Swiss Safe Harbor Framework und DSG**

13. Google, Inc. hat sich im Rahmen des Briefwechsels vom 1. und 9. Dezember 2008 zwischen der Schweiz und den Vereinigten Staaten von Amerika über die Schaffung eines Datenschutzrahmenwerkes zur Übermittlung von personenbezogenen Daten in die Vereinigten Staaten von Amerika (U.S. – Swiss Safe Harbor Framework; SR 0.235.233.6) selbst zertifiziert und den Safe Harbor Principles unterworfen

**Beweis:** Auszug Safe Harbor Zertifizierung von Google, Inc.
*(Anhang 7)*

Vor diesem Hintergrund sind für sämtliche durch Google, Inc. in den USA erfolgten Datenbearbeitungen die Grundsätze des U.S. – Swiss Safe Harbor Frameworks anwendbar.

14. Das U.S. – Swiss Safe Harbor Framework ist ein Staatsvertrag zwischen der Schweiz und den USA, durch den in den USA für die selbstzertifizierten Unternehmen sektoriell ein angemessenes Datenschutzniveau etabliert wird

**Beweis:** Staatenliste der Staaten mit einem angemessenen Datenschutzniveau http://www.edoeb.admin.ch/themen/00794/00827/index.html?lang=de) *(Anhang 8)*

Gemäss diesem, können sich Unternehmen in den USA freiwillig unter das U.S. – Swiss Safe Harbor Framework zertifizieren und die darin enthaltenen Grundsätze einhalten. Insbesondere wurde hierdurch das Zweckmässigkeitsprinzip (Art. 4 Abs. 3 DSG) und das Erkennbarkeitsprinzip (Art. 4 Abs. 4 DSG) in den Grundsätzen NOTICE, CHOICE und DATA INTEGRITY für die weitere Datenbearbeitung in den USA umgesetzt. Damit ist eine weitere Datenbearbeitung in den USA nur dann zulässig, wenn sie sich in dem in der Schweiz zulässigen Rahmen bewegt.

15. Um beurteilen zu können, ob die Datenbearbeitung in der Schweiz (Datenbeschaffung und Übermittlung in die USA) durch Google, Inc. bzw. die Google Schweiz GmbH daher dem DSG entspricht, muss vorgängig geprüft werden, ob die weitere Datenbearbeitung in den USA mit den Grundsätzen der Datenbearbeitung in Einklang stehen und somit die Datenbearbeitung in der Schweiz (Datenbeschaffung und Übermittlung in die USA) gerechtfertigt werden kann. Aus diesem Grund ist es unumgänglich, vorfrageweise zu klären, ob die Datenbearbeitung durch Google, Inc. in den USA selbst im Einklang mit dem DSG steht, um in einem zweiten Schritt feststellen zu können, ob eine solche die von Google, Inc. oder der Google Schweiz GmbH durchgeführte Datenbearbeitung in der Schweiz rechtfertigt (vgl. hierzu auch Rz. 20 ff.).

**Zuständigkeit des EDÖB**

16. Gemäss Art. 29 Abs. 1 lit. a DSG klärt der EDÖB von sich aus oder auf Meldung Dritter hin den Sachverhalt näher ab, wenn Bearbeitungsmethoden geeignet sind, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen (Systemfehler). Da durch Google, Inc. oder durch die Google Schweiz GmbH Bilder von Strassenzügen in der gesamten Schweiz bearbeitet werden, ist die Datenbearbeitung grundsätzlich geeignet, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen. Der EDÖB ist gemäss Art. 29 Abs. 3 DSG dazu berechtigt, aufgrund seiner Abklärungen Empfehlungen zu erlassen. Hiervon hat der EDÖB aufgrund seiner Zuständigkeit am 11. September 2009 Gebrauch gemacht und gegenüber Google, Inc. sowie der Google Schweiz GmbH Empfehlungen erlassen.

17. Der EDÖB kann die Angelegenheit dem Bundesverwaltungsgericht zum Entscheid vorlegen, wenn seine Empfehlung nicht befolgt oder abgelehnt wird (Art. 29 Abs. 4 DSG). Google, Inc. hat mit Schreiben vom 14. Oktober 2009 zum Ausdruck gebracht, dass sie die Empfehlungen des EDÖB nicht bzw. nur teilweise befolgt.

**Beweis:** Schreiben der Google Switzerland GmbH vom 14. Oktober 2009 *(Anhang 2)*

Die Google Schweiz GmbH hat sich in der vom EDÖB angesetzten Frist nicht geäussert (Beweis: Schreiben vom 14. Oktober 2009). Daher ist der EDÖB befugt, gegen Google, Inc. und die Google Schweiz GmbH Klage zu erheben.





## V. Erwägungen

18. Gemäss Art. 12 Abs. 1 DSG darf, wer Personendaten bearbeitet, die Persönlichkeit der betroffenen Person nicht widerrechtlich verletzen. Eine Persönlichkeitsverletzung wird gemäss Art. 12 Abs. 2 DSG angenommen, wenn der Datenbearbeiter Personendaten entgegen den Grundsätzen der Artikel 4, 5 Absatz 1 und 7 Absatz 1 bearbeitet. Der Gesetzgeber geht in diesem Rahmen von der Fiktion einer Persönlichkeitsverletzung aus. Somit stellt der Verstoss gegen diese Bearbeitungsgrundsätze immer eine Persönlichkeitsverletzung dar (Handkommentar zum Datenschutzgesetz; David Rosenthal zu Art. 12 Abs. 2 lit. a DSG; Rz. 15).

19. Aus diesem Grund ist zu prüfen, ob und in wieweit die Datenbearbeitung durch die Google, Inc. oder die Google Schweiz GmbH in der Schweiz gegen die Grundsätze der Datenbearbeitung verstösst.

### Zum Rechtmässigkeitsprinzip gemäss Art. 4 Abs. 1 DSG (1)

20. Gemäss Art. 4 Abs. 1 DSG dürfen Personendaten nur rechtmässig bearbeitet werden. Eine Verletzung gegen diese Norm liegt immer dann vor, wenn eine Bearbeitung auf einem unrechtmässigen Verhalten beruht (Handkommentar zum Datenschutzgesetz; David Rosenthal zur Art. 4 Abs. 1 DSG; Rz. 6). Erfasst sind Verstösse gegen Verhaltensnormen, die direkt oder indirekt auch den Schutz vor einem Eingriff in die Persönlichkeit einer Person bezwecken (Handkommentar zum Datenschutzgesetz; David Rosenthal zur Art. 4 Abs. 1 DSG; Rz. 7).

21. Inwiefern die Datenbearbeitung (Sammlung der Daten und Übermittlung der Daten ins Ausland) durch Google, Inc. oder die Google Schweiz GmbH in der Schweiz

rechtmässig ist, lässt sich erst beurteilen, nachdem geprüft wurde, ob die weitere Datenbearbeitung durch Google, Inc. im Ausland gegen herrschendes Schweizer Recht, insbesondere gegen Art. 28 des Schweizerischen Zivilgesetzbuches (ZGB; SR 210.0) und die datenschutzrechtlichen Bestimmungen, verstösst. Die vorfrageweise Klärung, ob die Datenbearbeitung durch Google, Inc., insbesondere die Veröffentlichung der Bilder im Dienst Street View gegen Schweizer Datenschutzrecht verstösst, ist zur Beurteilung der Rechtmässigkeit der Sammlung der Daten und deren Übermittlung ins Ausland unumgänglich, da eine Sammlung von Daten in der Schweiz und eine Übermittlung ins Ausland zu einem rechtswidrigen Zweck bereits gegen das Rechtmässigkeitsprinzip von Art. 4 Abs. 1 DSG verstösst.

22. Die Anwendbarkeit des Schweizer Rechts im Hinblick auf die vorfrageweise Klärung, ob eine Persönlichkeitsverletzung durch die Datenbearbeitung von Google, Inc. in den USA mit Wirkung auf Betroffene in der Schweiz stattfindet, ergibt sich zudem aus Art. 139 des Bundesgesetzes über das Internationale Privatrecht (IPRG; SR 291). Danach unterstehen Ansprüche aus Verletzung der Persönlichkeit durch Medien, insbesondere durch Presse, Radio, Fernsehen oder durch andere Informationsmittel in der Öffentlichkeit nach Wahl des Geschädigten dem Recht des Staates, in dem der Geschädigte seinen gewöhnlichen Aufenthalt hat, sofern der Schädiger mit dem Eintritt des Erfolges in diesem Staat rechnen musste (Art. 139 Abs. 1 lit. a IPRG). Gemäss Art. 139 Abs. 3 IPRG ist Absatz 1 auch auf Ansprüche aus Verletzung der Persönlichkeit durch das Bearbeiten von Personendaten sowie aus Beeinträchtigung des Rechts auf Auskunft über Personendaten anwendbar.

23. Da die Veröffentlichung der Bilder auf dem Dienst Street View geeignet ist, die Persönlichkeit einer grossen Anzahl von Personen, welche ihren gewöhnlichen Aufenthalt in der Schweiz haben, zu verletzen, Google, Inc. mit dem Eintritt des Erfolges in der Schweiz rechnen musste und diese Verletzung nach Schweizer Recht beurteilt werden kann, ist damit die Anwendbarkeit des Schweizer Rechts auch aufgrund von Art. 139 IPRG auf die vorfrageweise Klärung gegeben.

**Vorfrage: Untersuchung der Datenbearbeitung durch Google, Inc. in den USA im Lichte des DSG**

24. Nach der Übertragung der Bilder an Google, Inc. in die USA werden diese für die Veröffentlichung im Dienst Street View aufbereitet. Hierzu werden sie in einem bestimmten Format gespeichert und einem automatisierten Unkenntlichmachungsprozess unterzogen, bevor ein Nutzer sie über das Internet abrufen kann. Vor diesem Hintergrund stellt sich die Frage, ob die Veröffentlichung der Bilder in der von

Google, Inc. durchgeführten Art und Weise die Persönlichkeitsrechte der betroffenen Personen verletzt.

***Rechtfertigungsgrund gemäss Art. 13 Abs. 2 lit. e DSG***

25. Gemäss Art. 13 Abs. 1 DSG ist eine Verletzung der Persönlichkeit widerrechtlich, wenn sie nicht durch Einwilligung des Verletzten, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt ist. Gemäss Art. 13 Abs. 2 lit. e DSG fällt ein überwiegendes Interesse der bearbeitenden Person insbesondere in Betracht, wenn sie Personendaten zu nicht personenbezogenen Zwecken insbesondere in der Forschung, Planung und Statistik bearbeitet und die Ergebnisse so veröffentlicht, dass die betroffenen Personen nicht bestimmbar sind.

*Umfang der Unkenntlichmachung der Personendaten*

26. Google, Inc. hat einen automatisierten Verwischungsprozess implementiert, welcher Gesichter von betroffenen Personen unkenntlich machen soll. Nach Angaben von Google, Inc. ist die eingesetzte Software die beste am Markt zur «Anonymisierung von Bildern» verfügbare.





**Beweis:** Schreiben der Google Switzerland GmbH vom 14. Oktober 2009 *(Anhang 2)*

Auf diese Weise könne laut Google, Inc. in der Schweiz bei Gesichtern eine Trefferquote von 98.4% und bei Fahrzeugkennzeichen eine Trefferquote von 97.5% erreicht werden.

**Beweis:** Schreiben der Google Switzerland GmbH vom 4. September 2009 *(Anhang 5)*

Im Rahmen einer Publikation von Wissenschaftlern bei Google, in welchem der Unkenntlichmachungsprozess beschrieben und evaluiert wird, gehen die Forscher lediglich von einem Wirkungsgrad von ca. 89% bei der Unkenntlichmachung von Gesichtern und von 94-96% bei der Unkenntlichmachung von KFZ-Kennzeichen aus.

**Beweis:** Fachartikel: Large-scale Privacy Protection in Google Street View (http://research.google.com/archive/papers/cbprivacy_iccv09.pdf; Stand 02.November 2009) *(Anhang 9)*

Diese Angaben konnten vom EDÖB bisher nicht überprüft werden. Einzelne nicht repräsentative Stichproben des EDÖB und zahlreiche Hinweise aus der Bevölkerung deuten allerdings auf eine grosse Anzahl von nicht verwischten Gesichtern und Kennzeichen hin.

**Beweis:** Stichproben von Ansichten in Google Street View
*(Anhang 10)*

Diese Feststellungen des EDÖB decken sich aber durchaus mit den von Google, Inc. präsentierten Zahlen. Google, Inc. hat eigenen Angaben zufolge über 20 Mio. Bilder veröffentlicht. Bei einer Fehlerquote von nur 2% beträgt rein rechnerisch demnach die Anzahl der Bilder, welche nicht unkenntlich gemacht wurden 400'000. Geht man sogar davon aus, dass lediglich ein Wirkungsgrad von 89% bei Gesichtern erreicht wird, so müsste man von 2.2 Mio. nicht unkenntlich gemachten Bildern ausgehen. Zwar hat Google, Inc. gegenüber dem EDÖB geäussert, dass die Software ständig verbessert werde. Aber nach Meinung des EDÖB ist – wenn überhaupt – nur mit schrittweisen Verbesserungen über einen längeren Zeitraum hinweg zu rechnen.

Dies ändert heute und in nächster Zukunft nichts an der grundlegenden Problematik, dass Tausende von Gesichtern und Autokennzeichen nicht unkenntlich gemacht werden. Selbst wenn ein Wirkungsgrad von 99.5% erreicht würde, müsste man nach wie vor mit 100'000 nicht unkenntlich gemachten Bildern rechnen. Auch ist es den betroffenen Personen nicht zuzumuten, dass diese sich auf die Suche nach nicht unkenntlich gemachten Bildern begeben müssen und entsprechende Löschungsbegehren bei Google, Inc. zu stellen haben. Dies ist insbesondere deshalb auch nicht verhältnismässig, da die betroffenen Personen in den meisten Fällen noch nicht einmal wissen, dass sie aufgenommen wurden und ein nicht unerheblicher Anteil der Betroffenen über keinen Internetanschluss verfügt.

27. Die von Google, Inc. zur Verfügung gestellten einfachen Möglichkeiten Löschungsbegehren im Dienst Google Street View zu stellen, sind bei erfolgreicher Unkenntlichmachung ein Mittel, um der betroffenen Person die Anonymisierung zu gewährleisten. Sie kann aber den Prozess der Unkenntlichmachung weder ersetzen noch für diejenigen Fälle ergänzen, wo dieser nicht funktioniert hat. Google, Inc. hat dafür zu sorgen, dass die von ihr durchgeführte Datenbearbeitung die Persönlichkeit der betroffenen Personen von vorne herein nicht verletzt und darf nicht einfach nur abwarten, bis die betroffenen Personen reagieren und bis zu diesem Zeitpunkt deren Persönlichkeitsrechte systematisch verletzen.

28. Gemäss Art. 13 Abs. 2 lit. e DSG können Personendaten zu nicht personenbezogenen Zwecken bearbeitet und die Ergebnisse so veröffentlicht werden, dass die betroffenen Personen nicht bestimmbar sind. Google, Inc. wendet ein technisches Hilfsmittel an, welches nach eigenen Angaben Trefferquoten von 98.4% bei Gesichtern und 97.5% bei Autokennzeichen erreicht. Diese Zahlen sind allerdings auch bei Google, Inc. intern umstritten, da die Wissenschaftler bei Google, Inc. nur einen Wirkungsgrad bei Gesichtern von 89% ermitteln konnten (siehe Rz. 26). Aufgrund der grossen Anzahl der von Google, Inc. bearbeiteten Bilder gehen daher die nicht unkenntlich gemachten in die Tausende. Aus diesem Grund stellt sich die Frage, ob die automatisierte Anonymisierung ausreicht, damit sich Google, Inc. auf Art. 13 Abs. 2 lit. e DSG berufen kann. Bei nicht repräsentativen Stichproben und durch Beschwerden aus der Bevölkerung hat der EDÖB festgestellt, dass eine Vielzahl von Gesichtern und Autokennzeichen nicht unkenntlich gemacht wurden. Der EDÖB ist daher der Meinung, dass die von Google, Inc. angewandte technische Lösung der Unkenntlichmachung aufgrund der zahlenmässig hohen zu erwartenden Fehlerquote nicht ausreicht, dass Art. 13 Abs. 2 lit. e DSG zur Anwendung kommen kann.

*Grad der Unkenntlichmachung*

29. Obwohl mit der von Google, Inc. verwendeten Software in vielen Fällen Gesichter der betroffenen Personen unkenntlich gemacht werden, kann hierbei noch nicht ohne weiteres von einer Anonymisierung gesprochen werden. Selbst wenn das Gesicht einer betroffenen Person unkenntlich gemacht wurde, ist diese unter gewissen Umständen nach wie vor erkennbar. In wieweit trotz der Unkenntlichmachung der Gesichter ein Personenbezug im Sinne von Art. 3 lit. a DSG hergestellt werden kann, beurteilt sich danach, ob der für die Bestimmung einer Person zu betreibende Aufwand noch zu vertreten sei (Basler Kommentar zum DSG, Urs Belser zu Art. 3 lit. a DSG; Rz. 6). Er ist dann nicht mehr vertretbar, wenn nach den allgemeinen Lebenserfahrungen nicht damit gerechnet werden muss, dass ein Interessent diesen auf sich nehmen wird (BBl 1988 II 445). Ob eine Person bestimmbar ist, muss daher anhand objektiver Kriterien im konkreten Fall beurteilt werden, wobei insbesondere die Möglichkeiten der Technik (z.B. Zoomfunktionen, etc.) als auch die Rahmenbedingungen (z.B. Umgebung der getätigten Aufnahme) zu berücksichtigen sind.

30. Es ist unbestritten, dass zum Zeitpunkt der Aufnahme der Bilder und ihrer Übermittlung in die USA sämtliche auf diesen erscheinenden Personen ohne weiteres erkennbar sind und diese Bilder als Personendaten im Sinne von Art. 3 lit. a DSG

zu qualifizieren sind. Hingegen stellt sich nach erfolgreicher Unkenntlichmachung der Gesichter die Frage, ob diese Massnahme ausreicht, dass ein Personenbezug verneint werden und damit Art. 13 Abs. 2 lit. e DSG als Rechtfertigungsgrund zur Anwendung kommen kann.

31. Werden Bilder von öffentlichen Plätzen, welche stark frequentiert werden, aufgenommen, so ist es sehr unwahrscheinlich, dass sich eine interessierte Person die Mühe macht, eine betroffene Person zu suchen, da grundsätzlich zwei Ereignisse zusammen auftreten müssen, damit eine Person erkennbar ist. Zum einen muss sich die betroffene Person zu dem fraglichen Zeitpunkt genau an dem Platz befunden haben, als Google, Inc. die Photoaufnahme getätigt hat. Zum anderen muss die interessierte Person online auf diesem öffentlich zugänglichen Platz nach der betroffenen Person suchen und sie darüber hinaus erkennen können. Dass diese beiden Ereignisse zusammentreffen, ist unwahrscheinlich. Allerdings ist nicht auszuschliessen, dass eine betroffene Person dennoch im Dienst Street View erkannt wird. Der EDÖB ist der Meinung, dass aufgrund der geringen Wahrscheinlichkeit im Bereich von öffentlichen Plätzen, die stark frequentiert werden, nach erfolgreicher Unkenntlichmachung der Gesichter der betroffenen Personen ein Personenbezug grundsätzlich verneint werden und damit Art. 13 Abs. 2 lit. e DSG zur Anwendung kommen kann. Dennoch kann auch in diesen Fällen nicht vollkommen ausgeschlossen werden, dass eine betroffene Person erkannt wird. Bei der Frage der Bestimmbarkeit der betroffenen Person auf belebten Plätzen trotz erfolgreicher Unkenntlichmachung müssen grundsätzlich zwei verschiedene Wege der Identifikation berücksichtigt werden. Eine interessierte Person kann auf der einen Seite nach einer betroffenen Person auf verschiedenen in Google Street View vorhandenen Aufnahmen suchen (Suche 1Person: NPlätze). In einem solchen Fall ist die Wahrscheinlichkeit, dass eine betroffene Person gefunden wird, sehr klein. Eine interessierte Person kann aber auch auf einzelnen Plätzen nach mehreren ihr bekannten Personen suchen (Suche 1Platz: NPersonen). Hierbei ist die Wahrscheinlichkeit, dass eine betroffene Person gefunden wird, erheblich grösser. Gerade letzteres ist bei Nationalrat Noser geschehen, der in Google Street View in weiblicher Begleitung auf dem Bundesplatz erkannt werden konnte. Zudem publizierte der Blick das Bild einer Person, die angeblich gerade dabei war, «Kunden» Drogen zu verkaufen. Die Person wurde daraufhin als Wirt identifiziert, die aber nicht Drogen, sondern Essgutscheine verteilte. Das Beispiel zeigt darüber hinaus, dass ein aus dem Zusammenhang heraus gerissenes herangezoomtes Bild nicht nur zur Identifikation einer Person führen kann, sondern darüber hinaus zu falschen Interpretationen über einen vom Bild erfassten Vorgang.

**Beweis:** Artikel Blick am Abend vom Montag 24. August 2009, NZZ, BZ; 31. August 2009 und 01. September 2009
*(Anhang 11)*

Aus diesen Gründen ist eine vollständige Unkenntlichmachung von Gesichtern und Kennzeichen unabdingbar.

32. Bei einzelnen Datenschützern besteht allerdings die Meinung, dass aufgrund des Restrisikos der Bestimmbarkeit eine vollständige Anonymisierung der Personen (also nicht nur eine Unkenntlichmachung der Gesichter) verlangt werden (Bruno Baeriswyl; 2009; Die Anwendbarkeit des Datenschutzgesetzes; Digma, Zeitschrift für Datenrecht und Informationssicherheit; Jahrgang 9, Heft 9; September 2009) und daher das bisherige Konzept der «Anonymisierung» (Baeriswyl unterscheidet in diesem Kontext nicht zwischen Unkenntlichmachung und Anonymisierung) geändert werden müsse. Nach Meinung des EDÖB entspringt ein solcher Standpunkt einem Datenschutzverständnis, welches bedeutend weiter geht als das, was der Gesetzgeber in Art. 3 lit. a DSG legiferieren wollte. Durch die Wortwahl, dass sich Personendaten auf eine bestimmte oder bestimmbare Person beziehen, geht der Gesetzgeber weniger weit. Er verlangt bewusst nicht in jedem Fall eine vollständige Anonymisierung, sondern lässt hier einen gewissen Spielraum. So wird in der Botschaft explizit festgehalten, dass nicht jede theoretische Möglichkeit der Identifizierung für die Bestimmbarkeit genügt, sondern genau dann keine Bestimmbarkeit vorliegt, wenn der Aufwand derart gross ist, dass nach der allgemeinen Lebenserfahrung nicht damit gerechnet werden muss, dass ein Interessent diesen auf sich nehmen wird. Der Gesetzgeber möchte damit nicht jedes noch so kleine Risiko, dass eine betroffene Person zufällig erkannt werden könnte, ausschliessen. Gerade aber das fordern jene, die in jedem Fall eine vollständige Anonymisierung verlangen. Dies würde auch der Rechtssprechung von Art. 28 ZGB (vgl. Basler Kommentar zum ZGB; Andreas Meili zu Art. 28; Rz. 20) widersprechen, wonach nicht individualisierte Aufnahmen im Gemein- und Öffentlichkeitsbereich von betroffenen Personen, welche in ausreichender Distanz zur Kamera auf öffentlichen Plätzen aufgenommen wurden, zu dulden sind (vgl. hierzu Rz. 37 und 41). Würde man nämlich so weit gehen, eine vollständige Anonymisierung zu verlangen, dann müsste man die Veröffentlichung eines entsprechenden Bildes unter datenschutzrechtlichen Aspekten als Persönlichkeitsverletzung ansehen, während sie sich aufgrund der Rechtssprechung zu Art. 28 ZGB durchaus im rechtlich zulässigen Rahmen bewegen würde. Ein solcher Widerspruch wäre in der Rechtssystematik zum Persönlichkeitsrecht nicht zu vertreten. Daher ist diese Meinung nach Ansicht des EDÖB abzulehnen.

33. Vollkommen anders stellt sich der Sachverhalt dar, wenn die betroffene Person in der Nähe ihres Lebensmittelpunktes (z.B. in einem kleinen Dorf, in der näheren Umgebung ihres gewöhnlichen Aufenthaltsortes, etc.) aufgenommen wurde. Aufgrund der räumlichen Abgrenzung und des zu erwartenden Bewegungsradius einer betroffenen Person ist die Wahrscheinlichkeit, dass ein Interessierter die betroffene Person findet und trotz der Unkenntlichmachung des Gesichtes erkennt, bedeutend grösser. In diesen Bereichen muss daher nach Meinung des EDÖB damit gerechnet werden, dass eine interessierte Person sich die Mühe macht, nach einer betroffenen Person zu suchen.

    Ganz unabhängig davon, ob das Gesicht einer betroffenen Person unkenntlich gemacht wird oder nicht, kann diese Person grundsätzlich bereits an Kleidung und Körperhaltung erkannt werden. Insbesondere durch die im Dienst Street View enthaltene Zoom-Funktion, welche über das Auflösungsvermögen des menschlichen Auges hinausgeht, ist es möglich, einzelne Personen gezielt zu betrachten und zu identifizieren, auch wenn deren Gesichter unkenntlich gemacht wurden. Vor diesem Hintergrund ist der EDÖB der Meinung, dass die Veröffentlichung der Bilder, welche in der näheren Umgebung des Lebensmittelpunktes einer betroffenen Person gemacht wurden, unzulässig ist, da die betroffenen Personen trotz unkenntlich gemachter Gesichter identifiziert werden können.





*Überwiegendes öffentliches Interesse*

34. Zweifelsohne existiert am Dienst Street View von Google, Inc. ein gewisses öffentliches Interesse. Es stellt sich allerdings die Frage, inwiefern dieses Interesse ein überwiegendes öffentliches Interesse darstellt. Im Bereich von öffentlich zugänglichen Plätzen von allgemeinem Interesse (z.B. aufgrund ihres kulturellen oder historischen Werts) könnte unter gewissen Voraussetzungen von einem überwiegenden öffentlichen Interesse ausgegangen werden.

    Diese kann das schützenswerte Interesse an der informationellen Selbstbestimmung der betroffenen Personen überwiegen, wenn Personen nicht individualisiert angezeigt werden können (keine Zoom-Funktion) und zudem zumindest die Gesichter unkenntlich gemacht wurden (da das Blurring von Gesichtern einen zumutbaren Aufwand zur Verbesserung der Privatsphäre darstellt). Besteht das öffentliche Interesse allerdings in der Neugier bestimmter interessierter Personen, wie dies beispielsweise beim virtuellen Zugang zu Wohngebieten der Fall ist, kann der EDÖB kein überwiegendes öffentliches Interesse erkennen.

*Überwiegendes privates Interesse*

35. Für Google, Inc. stellt der Dienst Street View ein Engagement dar, mittels welchem ein wirtschaftlicher Nutzen verfolgt wird. Durch die Klicks auf Street View generiert Google, Inc. nach eigenen Angaben Werbeeinnahmen. Allerdings kann der EDÖB nicht erkennen, dass die kommerziellen Interessen von Google, Inc. das schützenswerte Interesse an der Privatsphäre der betroffenen Personen überwiegt.

***Erwägungen zu einer möglichen Persönlichkeitsverletzung***

36. Gemäss Art. 4 Abs. 2 DSG hat die Datenbearbeitung nach Treu und Glauben zu erfolgen und muss verhältnismässig sein. Um beurteilen zu können, ob das Verhältnismässigkeitsprinzip im Hinblick auf den Persönlichkeitsschutz von Art. 28 ZGB eingehalten wurde, muss eine Interessenabwägung zwischen den schützenswerten Interessen der betroffenen Person und den privaten Interessen von Google, Inc. sowie dem öffentlichen Interesse am Dienst Street View bzw. an den dort veröffentlichten Bildern durchgeführt werden. Hierbei ist auf die sich jeweils konkret abzeichnenden Verhältnisse abzustellen.

*Recht am eigenen Bild*

37. Die Lehre und Rechtssprechung anerkennt ein Recht am eigenen Bild (BGE 129 III 715 E 4.1). Bilder zeigen Tatsachen in besonders eindringlicher Weise, weshalb regelmässig die informationelle Privatheit und/oder Ehre des Betroffenen verletzt wird. Schon alleine die photographische Aufnahme kann (muss aber nicht) eine Persönlichkeitsverletzung bedeuten, je nachdem, ob schutzwürdige Interessen des Betroffenen beeinträchtigt werden. Die Weiterverbreitung oder Veröffentlichung eines individualisierten Bildnisses ohne Einwilligung der betroffenen Person führt in jedem Fall zu einer Persönlichkeitsverletzung (Handkommentar zum Schweizer Privatrecht; Aebi-Müller zu Art. 28 ZGB; Rz. 25; Studer, P., von Baldegg, R. M.: Medienrecht für die Praxis, 3. aktualisierte Auflage, Hubert Printpach AG, Frauenfeld, S. 92 f.). Eine solche Persönlichkeitsverletzung wirkt umso schwerer, wenn sich die Person in einer kompromittierenden Situation befindet oder aufgrund der Aufnahmen falsche Rückschlüsse auf das Verhalten einer Person gezogen werden können.

38. Ziel der Datenbearbeitung durch Google, Inc. ist es nach eigenen Angaben, die betroffenen Personen nicht individualisiert abzubilden, sondern einen Überblick über Strassenzüge inklusive der sich hierauf befindlichen Personen zu geben, wobei deren Gesichter in den meisten Fällen unkenntlich gemacht wurden. Damit

beruft sich Google, Inc. darauf, dass eine Abbildung in der Regel dann zulässig ist, wenn der Abgebildete «sozusagen Teil der Landschaft, der Umgebung oder des Ereignisses» ist (Basler Kommentar zum ZGB; Andreas Meili zu Art. 28; Rz. 20).

39. Unzulässig ist hingegen das Herausisolieren einzelner Personen aus einem in zulässiger Weise aufgenommenen Personenkreis (Basler Kommentar zum ZGB; Andreas Meili zu Art. 28; Rz. 21; Studer, P., von Baldegg, R. M.: Medienrecht für die Praxis, 3. aktualisierte Auflage, Hubert Printpach AG, Frauenfeld, S. 92 f.). Google, Inc. bietet in seinem Service Street View eine Zoom-Funktion an, mittels welcher eine Vergrösserung von Bildausschnitten angezeigt werden kann. Auf diese Weise bietet Google, Inc. die Möglichkeit an, sämtliche Personen auf dem Bildschirm herauszuisolieren, zu verdeutlichen und individualisiert zu betrachten, wie es für den gewöhnlichen Passanten nicht möglich wäre.

**Beweis:** Stichproben von Ansichten in Google Street View
*(Anhang 10)*

40. Betrachtet man die von Google, Inc. getroffenen Massnahmen zur Unkenntlichmachung der Gesichter und Kennzeichen, so könnte die Meinung vertreten werden, dass diese ausreichen würden, um zur Beurteilung zu kommen, dass keine Persönlichkeitsverletzung vorliege. Da allerdings technische Zoom-Möglichkeiten bestehen, welche eine individualisierte Betrachtung einzelner Personen ermöglicht (siehe Rz. 39), geht der EDÖB davon aus, dass eine Verletzung der Persönlichkeit der betroffenen Personen gemäss Art. 28 ZGB zumindest in den Fällen vorliegt, in denen die betroffene Person nicht ausreichend unkenntlich gemacht wurde.

*Recht auf Achtung der Privatsphäre*

41. Gemäss der in Lehre und Rechtssprechung vertretenen Sphärentheorie umfasst der menschliche Lebensbereich insgesamt drei Sphären, nämlich den Geheim- oder Intimbereich, den Privatbereich und den Gemein- oder Öffentlichkeitsbereich (Basler Kommentar zum ZGB; Andreas Meili zu Art. 28 ZGB; Rz. 23). Die Geheim- und Intimsphäre umfasst diejenigen Lebensvorgänge, die eine Person der Wahrnehmung und dem Wissen aller Mitmenschen entziehen bzw. nur mit ganz bestimmten anderen Menschen teilen will (BGE 118 IV 45). Hierbei kommt es für die Abgrenzung einmal auf den ausdrücklich manifestierten oder konkludent erklärten Geheimhaltungswillen an, andererseits auf die Art des in Frage stehenden Vorganges. Die Privatsphäre umfasst hingegen diejenigen Lebensäusserungen, die der Einzelne gemeinhin mit nahe verbundenen Personen, aber nur mit diesen, teilen will (BGE 118 IV 45). «Was sich in diesem Kreis abspielt ist zwar nicht geheim,

da es von einer grösseren Anzahl Personen wahrgenommen werden kann. Im Unterschied zum Geheimbereich handelt es sich jedoch um Lebenserscheinungen, die nicht dazu bestimmt sind, einer breiten Öffentlichkeit zugänglich gemacht zu werden, weil die betreffende Person für sich bleiben und in keiner Weise öffentlich bekannt werden will» (BGE 97 II 101). Nach Andreas Meili (Baslerkommentar zum ZGB; Andreas Meili zu Art. 28 ZGB; Rz. 26) ist eine Umschreibung dieses Bereiches nicht mit Sicherheit zu treffen; jedenfalls gehören seiner Meinung nach das Haus und die Wohnung einer Person genauso wie auch etwa die Mitgliedschaft in einem Verein privaten Charakters zur Privatsphäre (vgl. auch BGE 97 II 97 ff.; 107 II 1; 111 II 209). Demgegenüber steht der Gemein- oder Öffentlichkeitsbereich. «Diesem Lebensbereich gehören Lebensbetätigungen an, durch die sich der Mensch wie jedermann in der Öffentlichkeit benimmt, durch unpersönliches Auftreten an allgemein zugänglichen Orten und Veranstaltungen oder durch sein öffentliches Auftreten als Künstler und Redner» (BGE 118 IV 45). Nur Tatsachen und Lebensvorgänge aus diesem Bereich dürfen ohne weiteres wahrgenommen und grundsätzlich von jedermann weiterverbreitet werden (Basler Kommentar zum DSG; Andreas Meili zu Art. 28 ZGB; Rz. 27).

42. Die Aufnahmen von Google, Inc. werden grundsätzlich von öffentlichen Strassen aus gemacht. Dem EDÖB sind allerdings auch Fälle bekannt, in welchen Google, Inc. auch nicht öffentliche Privatstrassen zwecks photographischer Aufnahmen abgefahren hat. Google, Inc. behauptet, sie hätten in diesen Fällen die Einwilligung der betroffenen Personen.

**Beweis:** Schreiben vom 14. Oktober 2009
*(Anhang 2)*

43. Aufgrund verschiedener Beschwerden seitens betroffener Personen muss diese Aussage von Google, Inc. allerdings grundsätzlich in Frage gestellt werden.

**Beweis:** Beschwerden betroffener Personen
*(Anhang 12)*

Zudem ist uns nicht bekannt, dass Google, Inc. sämtliche Bewohner einer Privatstrasse um deren Einwilligung im konkreten Einzelfall angefragt hätte. Dies ist auch aufgrund des hierfür zu leistenden Aufwands nicht zu erwarten.

44. Ganz unabhängig davon, ob die Aufnahmen von öffentlichen oder von privaten Strassen aus gemacht wurden, hängt eine mögliche Persönlichkeitsverletzung im wesentlichen davon ab, in welchem Bereich Aufnahmen getätigt wurden. Es

stellt sich hierbei die Frage, ob Bildaufnahmen von Wohnquartieren zur Privatsphäre oder zum Gemein- und Öffentlichkeitsbereich zu zählen sind. Der EDÖB geht davon aus, dass gerade ein Wohngebiet nicht dazu bestimmt ist, einer breiten Öffentlichkeit zugänglich gemacht zu werden. Dies gilt umso mehr, wenn Liegenschaftsbesitzer rund um ihr Grundstück einen Sichtschutz anbringen. Aufgrund von Baubestimmungen ist ein solcher Sichtschutz meist auf eine Höhe von 1.80m bis 2m beschränkt. Da allerdings Google, Inc. bzw. die Google Switzerland GmbH aus einer Höhe von 2.75m photographiert, umgehen sie diesen Sichtschutz regelmässig.

Die Privatsphäre hingegen umfasst alle Grundstücksteile, die den räumlichgegenständlichen Lebensmittelpunkt einer Person insgesamt ausmachen. Sofern und sowie dieser Bereich üblicherweise oder durch bauliche oder landschaftliche Gegebenheiten von der Einsichtnahme durch Dritte ausgeschlossen sind, muss niemand hinnehmen, dass seine Privatsphäre unter Überwindung bestehender Hindernisse mit entsprechenden Hilfsmitteln ausgespäht, aufgezeichnet und im Internet veröffentlicht wird (vgl. Rechtssprechung zu Art. 179quarter des Schweizerischen Strafgesetzbuchs; StGB; SR 311). Beim Vorliegen eines Sichtschutzes ha-ben noch nicht einmal alle Personen, die im Vorübergehen oder Vorüberfahren ein Anwesen betrachten, die Möglichkeit, von dem Kenntnis zu nehmen, was sich hinter dem Sichtschutz abspielt. Zudem erlangen interessierte Personen durch die Zoom-Funktion (welche über das Auflösungsvermögen des menschlichen Auges hinausgeht) im Dienst Google Street View Einblicke, welche ihnen von blossem Auge verborgen bleiben. Darüber hinaus kann eine interessierte Person über den Dienst Google Street View einen umfriedeten Garten in aller Ruhe zu Hause am Bildschirm bis ins kleinste Detail analysieren, während ein vorbeigehender Passant allenfalls einen flüchtigen Blick darauf werfen kann.

Da Google, Inc. bzw. die Google Schweiz GmbH mit der Montage der Kameras in einer Höhe von 2.75m die Position, aus der heraus photographiert wird, frei wählt und dadurch den Sichtschutz zur Sicherung der Privatheit der betroffenen Liegenschaften durchbricht und sich damit gegen den Willen des Berechtigten in gewisser Weise Zugang verschafft, liegt eine schwerwiegende Persönlichkeitsverletzung vor. Nach Meinung des EDÖB muss niemand hinnehmen, dass seine Privatsphäre gegen seinen Willen unter Überwindung bestehender Hindernisse oder mit geeigneten Hilfsmitteln (Montage einer Kamera auf 2.75m) ausgespäht und zu kommerziellen Zwecken verwendet wird, indem die so gewonnen Einblicke der Öffentlichkeit zur Verfügung gestellt werden.

45. Der EDÖB ist der Meinung, dass reine Wohngebiete, auch wenn sie nicht geheim sind und grundsätzlich von den Passanten wahrgenommen werden können, als Privatsphäre zu qualifizieren sind. Dies gilt insbesondere für umfriedete Höfe, welche von einem Sichtschutz umgeben sind. Dies wird auch durch die Rechtsprechung des Bundesgerichts so bestätigt, wonach zum Privatbereich i.e.S. nicht nur gehört, was sich im Haus selbst, sondern auch, was sich in dessen unmittelbarer Umgebung abspielt, die von den Hausbewohnern bzw. von Dritten ohne weiteres als faktisch noch zum Haus gehörende Fläche in Anspruch genommen bzw. anerkannt wird (BGE 118 IV 41 S. 50)[1]. «Zu dieser Umgebung gehört insbesondere auch der Bereich unmittelbar vor der Haustüre eines Wohnhauses. Der Hausbewohner, der vor die Haustüre tritt, um beispielsweise einen dort abgestellten Gegenstand oder die Post aus einem vielfach dort angebrachten Briefkasten ins Haus zu holen, begibt sich dadurch nicht in den privatöffentlichen Bereich, sondern verbleibt in der Privatsphäre i.e.S., die durch Art. 179quarter StGB jedenfalls geschützt ist. Dasselbe gilt für den Hausbewohner, der vor seine Haustüre tritt, um jemanden zu begrüssen bzw. zu empfangen» (BGE 118 IV 41 E 4.e S. 50). Damit entfällt nach Rechtsprechung des Bundesgerichts der Schutz der Privatsphäre nicht bereits deshalb, weil Vorbeikommende aufgrund der landschaftlichen Gegebenheiten Grundstücksteile einsehen können, sondern der typisch private Charakter wird bereits durch dessen erkennbaren Nutzungszweck (Wille zur örtlichen Abgeschiedenheit der betroffenen Person) begründet. Indem Google, Inc. bzw. die Google Schweiz GmbH Grundstücke in Wohngebieten aufnimmt, dringt sie regelmässig in die von den betroffenen Personen geschaffene Privatsphäre ein und beeinträchtigt ausserdem das Recht auf Selbstbestimmung bei der Offenbarung ihrer persönlichen Lebensumstände.

46. Zu einem anderen Schluss kann man bei der Aufnahme von öffentlichen Plätzen, kulturell wichtigen Gebäuden bzw. Stadteilen (wie z.B. einer Altstadt) etc. kommen. Solche Orte, an denen auch ein weitgehendes öffentliches Interesse besteht, können nach Meinung des EDÖB durchaus als Gemein- oder Öffentlichkeitsbereich qualifiziert werden.

47. Daher ist der EDÖB der Meinung, dass die Aufnahmen von Google, Inc. und die im Internet öffentlich zugänglichen Bilder ausschliesslich auf den Gemein- und Öffentlichkeitsbereich zu begrenzen sind. Insbesondere dürfen ohne Einwilligung der

[1] Trotz der Eindeutigkeit dieses Bundesgerichtsentscheids ist unverkennbar, dass sich die damals entscheidenden Richter nicht über die heutzutage verfügbaren technischen Möglichkeiten im Klaren waren. Es obliegt daher dem Gericht zu beurteilen, ob die damals festgelegten Grundsätze dieses Leitentscheids vor dem Hintergrund des Internets nach wie vor Bestand haben.

betroffenen Personen keine Bilder von deren Privatbereich aufgenommen oder veröffentlicht werden, da ansonsten deren Privatsphäre verletzt wird.

*Zusammenfassung der Vorprüfung*

48. Nach Meinung des EDÖB verletzt Google, Inc. die Persönlichkeit der betroffenen Personen, wenn Daten aus deren Privatbereich bearbeitet werden. Solange sich die Datenbearbeitung auf den Gemein- und Öffentlichkeitsbereich beschränkt, reichen die von Google, Inc. getroffenen Massnahmen zur Unkenntlichmachung der betroffenen Personen grundsätzlich aus.

**Zum Rechtmässigkeitsprinzip gemäss Art. 4 Abs. 1 DSG (2)**

49. Nach der vorfrageweisen Abklärung kommt der EDÖB zu dem Schluss, dass die Aufnahmen und die Veröffentlichung von Bildern aus dem Privatbereich gegen Art. 28 ZGB verstossen und damit die Datenbearbeitung von Google, Inc., welche eine solche Rechtsverletzung bewirkt, nicht zulässig ist. Hingegen ist der EDÖB der Meinung, dass Aufnahmen aus dem Gemein- und Öffentlichkeitsbereich grundsätzlich als rechtmässig eingestuft werden können, solange die Unkenntlichmachung von Gesichtern und Autokennzeichen ausreicht, um eine Bestimmbarkeit der betroffenen Personen verneinen zu können. Daher ist nachfolgend zu prüfen, ob und in wiefern die Erhebung dieser Daten im Gemein- und Öffentlichkeitsbereich aufgrund der von Google, Inc. getroffenen Massnahmen mit dem DSG in Einklang steht.

**Verhältnismässigkeitsprinzip Art. 4 Abs. 2 DSG**

50. Gemäss Art. 4 Abs. 2 DSG hat die Bearbeitung von Personendaten nach Treu und Glauben zu erfolgen und muss verhältnismässig sein. Die Erhebung der Bilder von Google, Inc. bzw. der Google Schweiz GmbH ist ohne weiteres geeignet, den gewünschten Zweck zu erreichen nämlich die Veröffentlichung in Street View.

51. Bei der Prüfung der Erforderlichkeit stellt sich die Frage, ob Aufnahmen unter einem anderen Blickwinkel den Persönlichkeitsschutz besser gewährleisten. Geht man davon aus (siehe Erwägungen zur Vorfrage), dass Google, Inc. nur Bilder aus dem Gemein- und Öffentlichkeitsbereich aufnehmen und veröffentlichen darf, spielt es in der Regel keine Rolle, in welcher Höhe die Kameras montiert sind. Sollte das Bundesverwaltungsgericht allerdings wider Erwarten zu dem Schluss kommen, dass Aufnahmen von Google, Inc. im Privatbereich möglich sind, dann stellt die Montage

der Aufnahmekameras in durchschnittlicher Kopfhöhe ein milderes Mittel dar, welches weniger in die Persönlichkeit der betroffenen Personen eingreift. Durch eine Montage der Aufnahmekameras auf durchschnittlicher Kopfhöhe könnte in jedem Fall verhindert werden, dass Aufnahmen aus dem Privatbereich der betroffenen Personen, welche durch einen Sichtschutz vor Blicken von Passanten verborgen bleiben, sichtbar gemacht werden. Da der EDÖB davon ausgeht, dass nicht in jedem Fall gewährleistet werden kann, dass sich die Aufnahmen von Google, Inc. bzw. der Google Schweiz GmbH auf den Gemein- und Öffentlichkeitsbereich beschränken, sind die Kameras immer in durchschnittlicher Kopfhöhe anzubringen oder es sind Massnahmen zu treffen, mit welchen gewährleistet wird, dass keine Bilder veröffentlicht werden, welche nicht von gewöhnlichen Passanten ebenfalls wahrgenommen werden könnten. Dies gilt umso mehr, da aufgrund des in der Schweiz geltenden Baurechts die maximal bewilligte Höhe eines Sichtschutzes in Wohngebieten auf 1.80m bis 2 m beschränkt ist, während die Kameras von Google, Inc. bzw. der Google Schweiz GmbH Aufnahmen in einer Höhe von 2.75 m machen.

52. Im Hinblick auf die Angemessenheit der von Google, Inc. bzw. der Google Switzerland GmbH getätigten Aufnahmen kann auf die vorfrageweise Prüfung verwiesen werden. Die Angemessenheit kann für den Gemein- und Öffentlichkeitsbereich durchaus bejaht werden. Der EDÖB ist allerdings der Meinung, dass eine Veröffentlichung von Bildern aus dem Privatbereich die Persönlichkeitsrechte der betroffenen Personen stärker einschränkt, als das öffentliche Interesse an einer solchen Publikation im Dienst Street View und das private Interesse von Google, Inc. bzw. der Google Switzerland GmbH an der Aufnahme solcher Bilder zum Zwecke der Veröffentlichung und kommerziellen Nutzung dieser Bilder, dies rechtfertigen würde.

53. Vor allem im Privatbereich greift auch Art. 13 Abs. 2 lit. e DSG als Rechtfertigungsgrund nicht, da sich die von den Aufnahmen betroffenen Personen in der Nähe ihres gewöhnlichen Aufenthalts befinden und daher in der Regel trotz der von Google, Inc. getroffenen Massnahmen erkennbar sind.

**Zweckmässigkeitsprinzip gemäss Art. 4 Abs. 3 DSG**

54. Personendaten dürfen nach Art. 4 Abs. 3 DSG nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, der aus den Umständen ersichtlich oder gesetzlich vorgesehen ist. Google, Inc. bzw. die Google Switzerland GmbH hat gewisse Anstrengungen unternommen, um die Bevölkerung über mögliche Kamerafahrten zu informieren. Insbesondere wurden auf der Webseite von Google rudimentär Gebiete veröffentlicht, in welchen in den jeweils kommenden beiden

Monaten Kamerafahrten stattfinden sollen. Diese reichen nach Meinung des EDÖB allerdings bei weitem nicht aus, dass sämtlichen betroffenen Personen der Zweck der Datenbearbeitung durch Google, Inc. bekannt sein dürfte.

55. Der Dienst Google Street View hat aber ein erhebliches Medienecho erfahren, so dass breite Schichten der Bevölkerung über den Zweck der Datenbearbeitung durch Google, Inc. bzw. der Google Switzerland GmbH inzwischen informiert sein dürften. Dies war am Anfang der Kamerafahren noch nicht der Fall, so dass zum Zeitpunkt der Erhebung eines grossen Teils der Bilder, den betroffenen Personen der Zweck der weiteren Bearbeitung noch nicht in jedem Fall bekannt gewesen sein dürfte.

56. Auch der Rechtfertigungsgrund von Art. 13 Abs. 2 lit. e DSG greift insoweit nicht, um die möglichen Verletzungen des Zweckmässigkeitsprinzips zu rechtfertigen, da eine grosse Anzahl betroffener Personen nicht unkenntlich gemacht wurden und selbst wenn dies der Fall war aufgrund der Zoom-Funktion teilweise nach wie vor erkennbar sind. Zudem ist eine Erkennbarkeit von Personen trotz der Unkenntlichmachung ihres Gesichtes in der unmittelbaren Nähe ihres gewöhnlichen Aufenthaltsorts ohne weiteres zu bejahen (siehe Abklärung der Vorfrage). Im Gegensatz hierzu geht der EDÖB davon aus, dass Art. 13 Abs. 2 lit. e DSG als Rechtfertigungsgrund die Widerrechtlichkeit der Verletzung des Zweckmässigkeitsprinzips aufhebt, wenn es sich um Aufnahmen aus dem Gemein- oder Öffentlichkeitsbereich handelt und die Gesichter der betroffenen Personen erfolgreich unkenntlich gemacht wurden, da auf diese Weise eine Erkennbarkeit der betroffenen Personen mit grosser Wahrscheinlichkeit ausgeschlossen werden kann.





**Erkennbarkeitsprinzip gemäss Art. 4 Abs. 4 DSG**

57. Gemäss Art. 4 Abs. 4 DSG muss die Beschaffung von Personendaten und insbesondere der Zweck ihrer Bearbeitung für die betroffene Person erkennbar sein. Dies setzt voraus, dass es der betroffenen Person zumindest aus den Umständen heraus möglich sein muss, die Datenbearbeitung im Voraus zu erkennen, so dass sie die Möglichkeit hat, sich einer unerwünschten Datenbearbeitung zu widersetzen (Handkommentar zum DSG; David Rosenthal zu Art. 4 Abs. 4 DSG; < 51).

58. Zwar hat Google, Inc. auf seiner Webseite grob die Regionen aufgeführt, in welchen photographische Aufnahmen getätigt werden. Der Zeitraum in welchem in den betroffenen Regionen Aufnahmen getätigt werden beträgt aber zwei Monate.

**Beweis:** Auszug aus der Ankündigung von Google, Inc. auf deren Webseite *(Anhang 13)*

Daher ist es für die betroffenen Personen quasi unmöglich, im Vornherein zu erkennen, ob Bilder von ihnen aufgenommen werden. Es ist ebenfalls nicht ausreichend dem Erkennbarkeitsprinzip Genüge getan, wenn behauptet wird, die Fahrzeuge seinen gut sichtbar (vgl. hierzu auch Rz. 62).

59. Hält sich eine betroffene Person im Gemein- oder Öffentlichkeitsbereich auf, so muss sie grundsätzlich damit rechnen, dass sie (nicht individualisiert) aufgenommen werden könnte. Eine betroffene Person muss allerdings nicht damit rechnen, dass Aufnahmen aufgearbeitet und anschliessend auf dem Internet veröffentlich werden sowie dass zusätzlich zu den Bilder verschiedene technische Mittel (wie Zoom-Funktionen) angeboten werden, um einzelne Personen individualisiert darzustellen (siehe hierzu auch Urteil des europäischen Gerichtshofs für Menschenrechte in Sachen Peck gegen United Kingdom vom 28. Januar 2003, Referenznummer: 44647/98). Im Privatbereich ist es für Betroffene in der Regel ohne vorgängige Information nicht erkennbar, wenn sie in ihrer Privatsphäre aufgenommen werden.





60. Als möglichen Rechtfertigungsgrund könnte Google, Inc. für den Gemein- und Öffentlichkeitsbereich Art. 13 Abs. 2 lit. e DSG heranziehen, da Google, Inc. die Gesichter der betroffenen Person vor der Veröffentlichung unkenntlich macht. Nach Meinung des EDÖB kann im Gemein- und Öffentlichkeitsbereich aufgrund der Vielzahl der in diesem Bereich befindlichen Menschen und der geographischen Ferne vom gewöhnlichen Aufenthaltsort der betroffenen Person von einer Veröffentlichung gesprochen werden (im Rahmen welcher betroffene Person grundsätzlich nicht bestimmbar sind; vgl. auch Rz. 30).

61. Anders zu beurteilen ist der Sachverhalt, wenn es sich um Aufnahmen aus der Privatsphäre handelt. In diesem Fall ist nach Meinung des EDÖB die Unkenntlichmachung der Gesichter nicht ausreichend, um die Bestimmbarkeit einer betroffenen Person zu verneinen. Aus diesem Grund kann für diesen Bereich der Rechtfertigungsgrund von Art. 13 Abs. 2 lit. e DSG nicht herangezogen werden.

### VI. Zu den Anmerkungen von Google, Inc.

62. Google, Inc. beruft sich darauf, dass der EDÖB den Dienst Google Street View nach vertiefter Auseinandersetzung als mit dem Datenschutz konform bezeichnet habe.

Ein Vorbehalt sei einzig für den Fall gemacht worden, dass der Anonymisierungsprozess erhebliche Mängel aufweisen sollte.

**Beweis:** Schreiben von Google, Inc. vom 14. Oktober 2009
*(Anhang 2)*

Zudem zeigt sich Google überrascht, dass eine vollständige Unkenntlichmachung der Gesichter und Fahrzeugschilder auf dem Bildmaterial verlangt werde. Dies widerspreche auch den eigenen bisherigen Aussagen des EDÖB, die sich im Übrigen heute noch auf seiner Webseite befinden. Demnach äusserte der EDÖB Vorbehalte lediglich für den Fall, dass die Anonymisierung «erhebliche Mängel» aufweise und «eine grössere Anzahl von Personen auf Google Street View erkennbar» seien. Der EDÖB anerkenne, dass eine vollständige Anonymisierung der Bilder weder möglich noch nötig sei. Daher könne Google diese Kehrtwende nicht nachvollziehen und halte die Forderung einer vollständigen Unkenntlichmachung für rechtlich haltlos. Dem nachzukommen sei nie verlangt worden und sei auch nicht möglich.

63. Der EDÖB hat sich mit der für die Schweiz aufgeschalteten Version des Dienstes Google Street View zum frühest möglichen Zeitpunkt befasst und dabei festgestellt, dass der Unkenntlichmachungsprozess erhebliche Mängel aufweist. Zudem wurde festgestellt, dass nicht nur Aufnahmen vom Gemein- und Öffentlichkeitsbereich gemacht und online gestellt wurden, sondern in grossem Umfang auch Aufnahmen aus dem Privatbereich von betroffenen Personen.

64. Google, Inc. hat sich gegenüber dem EDÖB nur rudimentär darüber geäussert, welche Gebiete beim Start des Dienstes Google Street View aufgeschaltet werden. Aus den dem EDÖB zur Verfügung stehenden Informationen konnte der EDÖB in keiner Art und Weise im vornhinein abschätzen, dass und in welchem Umfang der Privatbereich der betroffenen Personen von der Veröffentlichung der Bilder tangiert sein würde. Vergleicht man die Aufschaltung in der Schweiz mit anderen europäischen Ländern (z.B. Portugal), so beschränken sich die dort aufgeschalteten Gebiete auf einzelne grössere Städte.

**Beweis:** Überblickskarten zur Abdeckung von Google Street View in anderen Ländern
*(Anhang 14)*

65. Zudem hat Google den EDÖB vor der Aufschaltung des Dienstes dahingehend informiert, dass dieser zu Beginn lediglich für einzelne grössere Städte (Zürich, Bern, Basel, Luzern) aufgeschaltet wird. Am Tag der Aufschaltung musste der EDÖB dann

feststellen, dass – entgegen der vorgängigen Information von Google – die Schweiz quasi flächendeckend inklusive kleiner Städte und Dörfer aufgeschaltet wurde. Auch die Information über die Kamerafahrten auf der Webseite von Google, Inc. liess in keiner Weise einen Rückschluss über den Umfang der bearbeiteten Bilder zu. So war dann die von Google auf Anfrage in der Sitzung vom 04. September 2009 ausgehändigte Liste über die aufgeschalteten Orte auch um ein Vielfaches grösser, als die auf der Webseite von Google publizierte Liste. Unabhängig davon musste der EDÖB darüber hinaus feststellen, dass Aufnahmen auch an Orten getätigt wurden, welche nicht vorher angekündigt worden waren.

**Beweis:** Artikel aus Liberté vom 14. August 2009
*(Anhang 15)*

66. Da der EDÖB keine die Möglichkeit hatte und es auch nicht seine Aufgabe ist (der EDÖB ist keine Genehmigungsinstanz), den Dienst Google Street View für die Schweiz vorgängig zu testen, war es ihm erst nach Aufschaltung des Dienstes möglich, zu erkennen, dass Bilder aus dem Privatbereich der betroffenen Personen (namentlich aus reinen Wohngebieten) aufgeschaltet wurden. Die Verantwortung, einzig und alleine Bilder aus dem Gemein- und Öffentlichkeitsbereich aufzuschalten und die Privatsphäre der betroffenen Personen zu achten, liegt alleine bei Google, Inc. bzw. der Google Schweiz GmbH. Vor diesem Hintergrund von einer unerwarteten Kehrtwende des EDÖB zu sprechen, entbehrt jeglicher Grundlage.





## VII. Fazit

67. Aufgrund der obigen Erwägungen kommt der EDÖB zu dem Schluss, dass der Betrieb des Dienst Street View von Google für den Gemein- und Öffentlichkeitsbereich dann keine Persönlichkeitsverletzung darstellt, wenn eine angemessene Unkenntlichmachung gewährleistet ist, so dass ein Personenbezug verneint werden kann. Falls die Unkenntlichmachung in diesem Bereich nicht funktioniert, kann eine betroffene Person nach Meinung des EDÖB aufgrund der Zoom-Funktionen individualisiert dargestellt und identifiziert werden.

    In einem solchen Fall geht der EDÖB von einer unrechtmässigen Persönlichkeitsverletzung aus. Trotz eines (im besten Fall anzunehmenden) Wirkungsgrades von über 98% gehen die nicht unkenntlich gemachten Bilder in die Tausende. Aus diesem Grund vertritt der EDÖB die Meinung, dass (nicht zuletzt aufgrund der Möglichkeiten der individualisierten Darstellung der betroffenen Personen) die von Google, Inc. getroffenen Massnahmen zur Unkenntlichmachung nicht ausreichen.

Er vertritt daher die strikte Auffassung, dass bei Aufnahmen aus der Privatsphäre der betroffenen Person immer eine Persönlichkeitsverletzung vorliegt.

68. Aus diesen Gründen ist den Begehren des EDÖB stattzugeben.

EIDGENÖSSISCHER DATENSCHUTZ- UND ÖFFENTLICHKEITSBEAUFTRAGTER

Hanspeter Thür





**Anhänge:**

1. Empfehlung des EDÖB vom 11. September 2009
2. Schreiben der Google Switzerland GmbH vom 14. Oktober 2009
3. Email vom 18. März; 2009 E2009.03.18-0041
4. Schreiben von Türk an Google B2009.06.03-0018
5. Schreiben der Google Switzerland GmbH vom 4. September 2009
6. Aufnahme eines Kamerafahrzeuges von Google und dazugehöriger Auszug aus dem E-Autoindex des Kantons Zürich
7. Auszug Safe Harbor Zertifizierung von Google, Inc.
8. Staatenliste der Staaten mit einem angemessenen Datenschutzniveau
9. Fachartikel: Large-scale Privacy Protection in Google Street View
10. Stichproben von Ansichten in Google Street View
11. Artikel Blick am Abend vom Montag 24. August 2009, NZZ, BZ
12. Beschwerden betroffener Personen
13. Auszug aus der Ankündigung von Google, Inc. auf deren Webseite
14. Überblickskarten zur Abdeckung von Google Street View in anderen Ländern
15. Artikel aus Liberté vom 14. August 2009

### 4.1.8 Weiterzug betreffend «KSS Schaffhausen»

Bern, den 10. Juni 2008

**WEITERZUG**

**gemäss Art. 29 Abs. 4 des Bundesgesetzes über den Datenschutz (DSG) vom 19. Juni 1992**

in der Sache

**Schlussbericht und Empfehlung des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) vom 11. April 2006**

betreffend

**die Erhebung biometrischer Daten beim Erwerb einer Dauerkarte in den Sport- und Freizeitanlagen KSS Schaffhausen**





#### I. Begehren

Folgenden Begehren sei stattzugeben:

Die Empfehlungsadressatin sei auszufordern auf die zentrale Speicherung von biometrischen Daten in Form von Templates der Fingerabdrücke zu verzichten und diese biometrischen Daten - auch diejenigen, welche bereits zentral erfasst wurden - auf einer Sicherheitskarte (smartcard), welche in der Einflusssphäre und unter Kontrolle der betroffenen Person verbleibt, abzulegen. Damit soll die Verifizierung der Identität ausschliesslich auf diesem Sicherheitsmedium stattfinden (*smartcard match on card*), so dass die biometrischen Daten zu keinem Zeitpunkt die gesicherte Umgebung des Mediums und die Kontrolle der betroffenen Person verlassen.

#### II. Sachverhalt

1. Im Januar 2005 hat die KSS Sport- und Freizeitanlagen Schaffhausen (nachfolgend KSS genannt) ein neues Zugangskontrollsystem (biometrisches Erkennungssys-

tem[1] für die biometrische Verifizierung[2] von Abonnenten) für den Hallenbad- und Wellnessbereich eingeführt. Dieses sieht vor, dass neben den Personalien auch biometrische Daten[3] in Form von Templates[4] des Fingerabdrucks[5] des Abonnenten erhoben und gespeichert werden. Bei jedem Eintritt in das Hallenbad- oder den Wellnessbereich muss der Kunde seine Dauerkarte sowie zusätzlich seinen Finger einsetzen, um das Drehkreuz am Eingang passieren zu können.

2. Ziel der KSS ist es, durch das neue Zugangskontrollsystem Missbräuche bei der Benutzung persönlicher, nicht übertragbarer Dauerkarten einzudämmen. Nach einer halbjährigen Pilotphase wurde das neue System im Sommer 2005 definitiv eingeführt. Langfristig ist ein Ausbau des Systems für weitere Sport- und Freizeitangebote (wie Freibad im Sommer oder Eisbahn im Winter) geplant.

   Der EDÖB erfuhr von der durch die KSS vorgenommene Erhebung biometrischer Daten durch diverse Zeitungsberichte und Fragen seitens besorgter Bürger.

3. In diesem Rahmen hat der EDÖB bei den KSS zwischen Juni 2005 und April 2006 gemäss Art. 29 DSG eine umfassende Überprüfung im Hinblick auf die Einhaltung der Datenschutzbestimmungen bei der Bearbeitung biometrischer Daten vorgenommen.





4. Mit Schreiben vom 6. Juni 2005 hat der EDÖB die KSS schriftlich über die geplante Datenschutzkontrolle und Sachverhaltsabklärung vor Ort betreffend das neue Zugangskontrollsystem informiert. Zusätzlich wurden vom EDÖB die Dokumentation des neue Systems angefordert und um die Beantwortung eines beigelegten Fragenkataloges gebeten. (siehe Anhang 2: Schreiben des EDÖB vom 6. Juni 2005 (Sachverhaltsabklärung))

5. Mit Schreiben vom 29. Juni 2005 hat die KSS den Fragekatalog des EDÖB beantwortet und um Terminvorschläge gebeten. (siehe Anhang 3: Schreiben der KSS vom 29. Juni 2005)

[1] Siehe Anhang 1: Definitionen zur Biometrie, Nr. 3
[2] Siehe Anhang 1: Definitionen zur Biometrie, Nr. 8
[3] Siehe Anhang 1: Definitionen zur Biometrie, Nr. 6
[4] Siehe Anhang 1: Definitionen zur Biometrie, Nr. 5
[5] Siehe Anhang 1: Definitionen zur Biometrie, Nr. 2

6. Mit Schreiben vom 4. August 2005 hat der EDÖB Terminvorschläge unterbreitet und um Nennung der an der Sachverhaltsabklärung anwesenden Personen gebeten. Zudem hat der EDÖB letzte Rückfragen gestellt. (siehe Anhang 4: Schreiben des EDÖB vom 4. August 2005)

7. Mit Schreiben vom 19. August 2005 hat die KSS die letzten Rückfragen schriftlich beantwortet und den Termin für die Sachverhaltsabklärung vor Ort auf den 21. September 2005 festgelegt. (siehe Anhang 5: Schreiben der KSS vom 19. August 2005)

8. Am 25. August 2005 hat der EDÖB den Termin für die Sachverhaltsabklärung per E-Mail bestätigt. (siehe Anhang 6: E-Mail des EDÖB vom 25. August 2005 (Bestätigung des Termins))

9. Mit Anruf vom 7. September 2005 hat die KSS mitgeteilt, dass die Sachverhaltsabklärung von Seiten der KSS auf unbestimmte Zeit verschoben werden musste. (siehe Anhang 7: Anruf der KSS vom 7. September 2005 (Verschiebungsanfrage))

10. Am 21. November 2005 fand die Sachverhaltsabklärung des EDÖB bei den KSS in Schaffhausen statt.

11. Mit Schreiben vom 30. November 2005 hat der EDÖB den KSS das weitere Vorgehen im Rahmen der Datenschutzkontrolle per E-Mail angekündigt. (siehe Anhang 8: E-Mail des EDÖB vom 30. November 2005 (Vorgehen Datenschutzkontrolle))

12. Am 14. Dezember 2005 hat der EDÖB den KSS ein Fact-Sheet geschickt, mit der Bitte um materielle Bereinigung des Textes sowie um Beantwortung aufgetretener Rückfragen. (siehe Anhang 9: Schreiben des EDÖB vom 14. Dezember 2005 (Fact-Sheet))

13. Mit Schreiben vom 20. Januar 2006 hat die KSS um eine Fristverlängerung gebeten. (siehe Anhang 10: Schreiben der KSS vom 20 Januar 2006 (Bitte um Fristerstreckung))

14. Am 24. Januar 2006 hat der EDÖB per E-Mail eine Fristverlängerung bis zum 3. Februar 2006 gewährt. (siehe Anhang 11: E-Mail des EDÖB vom 24. Januar 2006 (Fristerstreckung bis 3. Februar 2006))

15. Mit Schreiben vom 1. Februar 2006 hat die KSS die Richtigkeit des Fact-Sheets bestätigt und die gestellten Rückfragen beantwortet. (siehe Anhang 12: Schreiben der KSS vom 1. Februar 2006 (Bestätigung der Richtigkeit des Fact-Sheets))

16. Die Ergebnisse der Sachverhaltsabklärung wurden vom EDÖB in einem separaten und detaillierten Bericht (Schlussbericht des EDÖB vom 11. April 2006) festgehalten. Dieser Schlussbericht erging zusammen mit der Empfehlung zuhanden der KSS. (siehe Anhang 13: Schreiben des EDÖB vom 11. April 2006 (Schlussbericht) und Anhang 14: Schreiben des EDÖB vom 11. April 2006 (Empfehlung))

17. Mit Schreiben vom 18. Mai 2006 hat die KSS um eine Fristverlängerung bezüglich Stellungnahme zum Schlussbericht und zur Empfehlung gebeten. (siehe Anhang 15: Schreiben der KSS vom 18. Mai 2006 (Bitte um Fristverlängerung))

18. Mit Schreiben vom 24. Mai 2006 hat der EDÖB eine Fristerstreckung bis zum 19. Juni 2006 gewährt. (siehe Anhang 16: Schreiben des EDÖB vom 24. Mai 2006 (Fristerstreckung bis 19. Juni 2006))

19. Mit Schreiben vom 19. Juni 2006 hat die KSS um eine Fristverlängerung bezüglich Stellungnahme zum Schlussbericht und zur Empfehlung gebeten. (siehe Anhang 17: Schreiben der KSS vom 19. Juni 2006 (zweite Bitte um Fristverlängerung))

20. Mit Schreiben vom 21. Juni 2006 hat der EDÖB eine zweite Fristerstreckung bis 10. August 2006 gewährt. (siehe Anhang 18: Schreiben des EDÖB vom 21. Juni 2006 (zweite Fristerstreckung bis 10. August 2006))

21. Mit Schreiben vom 10. August 2006 hat die KSS die fünf vom EDÖB unterbreiteten Empfehlungen akzeptiert. Bezüglich der Verbesserungsvorschläge und die Angabe der vertraulichen Informationen hat sich die KSS nicht geäussert. (siehe Anhang 19: Schreiben der KSS vom 10. August 2006 (Stellungnahme zu unseren 5 Empfehlungen))

22. Mit Schreiben vom 31. August 2006 hat der EDÖB die KSS um Nachlieferung der Stellungnahmen zu den Verbesserungsvorschlägen, Angaben über vertrauliche Informationen und Erläuterung der Stellungnahme der KSS zu Empfehlung Nr. 4 (Anonymisierung der Transaktionsdaten) – mit Frist bis zum 15. September 2006

– gebeten. (siehe Anhang 20: Schreiben des EDÖB vom 31. August 2006 (Bitte um Nachlieferung der Stellungnahme zu den Verbesserungsvorschlägen und zur Erläuterung der Stellungnahme zu Empfehlung Nr. 4))

23. Mit Schreiben vom 15. September 2006 hat uns die KSS um eine weitere Fristerstreckung bis 19. Oktober 2006 gebeten. (siehe Anhang 21: Schreiben der KSS vom 15. September 2006 (Bitte um Fristverlängerung))

24. Mit Schreiben vom 20. September 2006, wurde eine Fristerstreckung bis 19. Oktober 2006 durch den EDÖB gewährt. (siehe Anhang 22: Schreiben des EDÖB vom 20. September 2006 (Fristerstreckung bis 19. Oktober 2006))

25. Mit Stellungnahme vom 18. Oktober 2006, hat die KSS, folgende Massnahmen zur Empfehlung Nr. 2 (dezentralisierte Speicherung der Templates) vorgeschlagen: «*Die Dauerkarten werden durch beschreibbare Medien ersetzt, die Software wird so angepasst, dass die Daten auf der Karte gespeichert werden können. …Programmieren, Testen und die Inbetriebnahme kann bis zum 01. Mai 2007 garantiert werden. Die Einführung kann ebenfalls auf Saisonbeginn, mithin 15. Mai 2007, stattfinden*». (siehe Anhang 23: Schreiben der KSS vom 18. Oktober 2006 (Massnahmen zur Empfehlung Nr. 2))

26. Mit Schreiben vom 10. November 2006 haben wir KSS mitgeteilt, dass wir die Kontrolle für abgeschlossen erachten würden, vorbehältlich der Einreichung eines Implementierungsberichts bezüglich die Umsetzung der erlassenen Empfehlungen und Verbesserungsvorschläge und unter Hinweis auf die im erwähnten Schreiben genannten drei Punkte. Deshalb wurde die KSS dazu aufgefordert, uns per 01. Juni 2007 einen Implementierungsbericht bezüglich der Umsetzung sämtlicher vom EDÖB erlassenen Empfehlungen und Verbesserungsvorschläge zuzustellen. (siehe Anhang 24: Schreiben des EDÖB vom 10. November 2006 (Bitte um Zustellung einem Implementierungsbericht bezüglich der Umsetzung sämtlicher vom EDÖB erlassenen Empfehlungen und Verbesserungsvorschläge))

27. Mit Schreiben vom 22. November 2006, hat der EDÖB der KSS die zuvor angekündigte Aufschaltung des Schlussberichts am 24. November 2006 auf seiner Website bestätigt. (siehe Anhang 25: Schreiben des EDÖB vom 22. November 2006 (Bericht zur Publikation))

28. Mit Schreiben vom 1. Juni 2007, teilte die KSS mit, dass «*aus Gründen der Arbeitsüberlastung […] bisher weder die Direktion der KSS noch die Herstellerfirma […] dazu [kam], den verlangten Bericht zu erstellen*». (siehe Anhang 26: Schreiben der KSS vom 1. Juni 2007 (Bemerkungen zum kürzen Implementierungsbericht))

29. Mit Schreiben vom 28. Juni 2007, hat der EDÖB wiederholt zur Kenntnis genommen, dass KSS gemäss Ihren Antworten vom 10. August 2006 und 18. Oktober 2006 die vier Empfehlungen vom 11. April 2006 akzeptiert hatte. Der EDÖB hat dabei wieder auf seinen Brief vom 10. November 2006 (abgeschlossene Kontrolle, vorbehältlich der Einreichung eines Implementierungsberichts) hingewiesen und die KSS um Erläuterungen zum Implementierungsbericht gebeten. (mit Frist bis zum 31. Juli 2007 zur Einreichung einer kurzen Übersicht und zum 30. September zur Einriechung des Implementierungsberichts ). (siehe Anhang 27: Schreiben des EDÖB vom 28. Juni 2007 (Nachforderung für die Frist um die Beschaffung des Implementierungsberichts))

30. Mit Schreiben vom 26. Juli 2007, teilte die KSS mit, dass «*unter Hinweis auf die bisher entstandenen Kosten, keine weitere Vorkehren mehr geplant*» seien. (siehe Anhang 28: Schreiben der KSS vom 26. Juli 2007)

31. Aufgrund dieser neuen Informationen seitens der KSS, hat der EDÖB mit Schreiben vom 27. August 2007 der KSS mitgeteilt, dass er sich zu einer Nachkontrolle entschieden hatte, um zu überprüfen, ob die Empfehlungen und Verbesserungsvorschläge umgesetzt wurden. (siehe Anhang 29: Schreiben des EDÖB vom 27. August 2007 (Nachkontrolle)).

32. Bei der ersten Nachkontrolle am 11. September 2007, wurde festgestellt, dass die Empfehlung Nr. 1 umgesetzt war und dass die Empfehlungen 3, 4 und 5 erst nach einem Software-Release bis Ende Jahr umgesetzt werden könnten. Was die Empfehlung Nr. 2 anbelangt (dezentrale Speicherung der Templates), wurde der Anbieter der technischen Lösung angefragt, wie Smartcards eingesetzt werden können und welche Kosten damit verbunden seien. Der Geschäftsleiter hat uns mitgeteilt, dass die KSS bisher keine Smartcards nachgefragt hat, aber dass die Anpassung für die KSS allerdings kostenneutral sei (bis auf die Anschaffungskosten für die Smartcards, d.h. rund 5 Franken pro Stück). Zusätzlich hat er mitgeteilt, dass das System schon dazu geeignet ist, Smartcards auszulesen. Der Betriebsleiter der KSS schätzte die bei der KSS im Umlauf befindliche Dauerkarten auf ca. 15'000.

33. Mit Schreiben vom 4. Dezember 2007 teilte der EDÖB der KSS mit, dass er sich für eine zweite Nachkontrolle vor Ort entschieden hatte, um die Umsetzung der Empfehlungen 3 und 4 überprüfen zu können. Dazu setzte er der KSS eine Frist bis 15. Januar 2008 an, um einen Termin zu nennen, bis wann Sie die Empfehlung Nr. 2 im Jahr 2008 umsetzen wollten. (siehe Anhang 30: Schreiben des EDÖB vom 4. Dezember 2007). Eine Besprechung über die Umsetzung der Empfehlung Nr. 2 wurde nachträglich zwischen den Beteiligten vereinbart.

34. Mit Schreiben vom 14. Januar 2008 teilte uns die KSS mit, dass sie davon ausgingen, dass Ihnen die eröffnete Frist einstweilen abgenommen war. (siehe Anhang Anhang 31: Schreiben der KSS vom 14. Januar 2008).

35. Bei der zweiten Nachkontrolle am 17. Januar 2008 hat der EDÖB feststellen können, dass die Empfehlungen 3 und 4 umgesetzt worden waren. Die Besprechung über die Empfehlung Nr. 2 führte dazu, dass deren Umsetzung grundsätzlich möglich sein sollte, unter Berücksichtigung der auf die KSS zukommenden Kosten für die Neuanschaffung von Smartcards, auf welchen die biometrischen Daten in dezentraler Form gespeichert werden können.





36. Mit Schreiben vom 29. Februar 2008 hat die KSS mitgeteilt, dass sie die Umsetzung der Empfehlung Nr. 2 ablehnt, da sie diese als *unverhältnismässig* («*Zum einen müssten neue Karten eingekauft werden, was hohe Anschaffungskosten verursacht, zum andern wäre zusätzlicher logistischer Aufwand durch die Erfassung und Ausstellung der neuen Karte unvermeidbar*») erachtet. (siehe Anhang 32: Schreiben der KSS vom 29. Februar 2008 (Ablehnung der Empfehlung Nr. 2)).

## III. Formelles

37. Die KSS hat unsere Empfehlung Nr. 2 bezüglich der dezentralen Speicherung von Templates mit Schreiben vom 10. August 2006 akzeptiert, diese aber dann nicht befolgt. Schliesslich, mit Schreiben vom 29. Februar 2008 hat die KSS unsere Empfehlung Nr. 2 abgelehnt. Damit kann der EDÖB gemäss Art. 29 Abs. 4 DSG die Angelegenheit dem Bundesverwaltungsgericht zum Entscheid vorlegen.

## IV. Erwägungen

### 1. Biometrische Daten als Personendaten im Sinne von Art. 3 lit. a DSG

38. Gemäss Art. 3 lit. a DSG, sind unter «*personenbezogene Daten*», alle Angaben zu verstehen, «*die sich auf eine bestimmte oder bestimmbare Person beziehen*»

(Basler Kommentar zum DSG, Urs Maurer-Lambrou/Andreas Steiner zu Art. 3 DSG, Rz. 4). Gemäss Art. 2 Abs. 1 DSG ist das DSG für das Bearbeiten von Daten natürlicher und juristischer Personen durch private Personen sowie durch Bundesorgane anwendbar.

39. Biometrische Daten[6] werden als personenbezogenen Daten qualifiziert, da sie sich auf den eigenen Körper (biometrische Charakteristiken[7]) beziehen und Informationen über physiologischen (dazu zählen Fingerabdrücken und Finger-Bild, Iris, Gesichts, Handgeometrie, usw.) oder verhaltenstypischen (dazu zählen Unterschrift, Tastenanschlag, Gangart usw.) Merkmale von bestimmten oder bestimmbaren Personen enthaltenen können. Der Einsatz von biometrischen Erkennungssystemen beinhaltet Risiken für die Grundrechte und -freiheiten und hat sich zu einer grossen Herausforderung für den Datenschutz entwickelt. Aufgrund dieser Risiken, haben gewisse Mitgliedstaaten der EU gemäss Art. 20 Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (siehe Anhang 33: Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr) http://ec.europa.eu/justice_home/fsj/privacy/law/index_de.htm, Regelungen bezüglich Vorabkontrollen für biometrische Daten oder Erkennungssystemen (Frankreich, Italien, Luxemburg, Slowakei, Slowenien) sowie besonders schützenswerten Personendaten (Deutschland, Griechenland, Litauen, Österreich, Portugal) festgelegt.

40. Wie die Art. 29-Datenschutzgruppe der EU in ihrem Arbeitspapier über Biometrie, S. 2, 5 f. (siehe Anhang 34: Arbeitspapier über Biometrie (WP Nr. 80)) (angenommen am 1. August 2003) http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2003_en.htm festhält, sind «*biometrische Daten […] Daten besonderer Art, da sie sich auf die verhaltenstypischen und physiologischen Merkmale einer Person beziehen und unter Umständen ihre eindeutige Identifizierung ermöglichen. Allerdings hängt die eindeutige Identifizierung von verschiedenen Faktoren wie dem Umfang der Datenbank und der Art der verwendeten biometrischen Daten ab. […] Biometrische Daten dürften stets als Informationen über eine natürliche Person einzustufen sein, da sie naturgemäß Aufschluss über eine bestimmte Person geben*».

41. Gemäss Hornung (Der Personbezug biometrischer Daten, Datenschutz und Datensicherheit (DuD), 28 (2004) 7, S. 430 f.) kann «*ein Personenbezug von Templates*

[6] Siehe Anhang 1: Definitionen zur Biometrie, Nr. 6
[7] Siehe Anhang 1: Definitionen zur Biometrie, Nr. 2

*[…] nicht grundsätzlich verneint werden, weil auch diese (extrahierte) Informationen über eine Person enthalten und ihr über Zuordnungslisten zugeordnet sein können. Biometrische Daten sollten dann nicht als personenbezogene Daten eingestuft werden, wenn sie wie ein Template so gespeichert werden, dass eine Identifizierung der betroffenen Person durch den Verantwortlichen für die Verarbeitung oder Dritte mit angemessenen Mitteln ausgeschlossen ist. Bei der Präsentation biometrischer Merkmale entstehen in aller Regel personenbezogene Daten. Das ist beim Enrolment stets, beim Matching immer dann der Fall, wenn die Identität des Betroffenen durch die verantwortliche Stelle auf anderem Wege feststellbar ist. In diesem Fall sind auch die jeweiligen Referenzdaten personenbezogen. Gleiches gilt, wenn diese mit einem Zuordnungssystem gespeichert sind. Bei einer Speicherung auf Chipkarten, auf denen der Name des Inhabers aufgedruckt ist, handelt es sich nur dann nicht um personenbezogene Daten, wenn die Karte selbst über einen Sensor verfügt*».

42. Im vorliegenden Fall ist die von den KSS durchgeführten Datenbearbeitungen gerade auf die Verifizierung ausgerichtet. Die Überprüfung der Zugangsberechtigung wird durch die Vergleichung des Fingerabdrucks einer Person mit dem in der zentralen Datenbank abgespeicherten Template erfüllt. Damit handelt es sich bei den von den KSS gesammelten biometrischen Daten um Personendaten gemäss Art. 3 lit. a DSG.





## 2. Datenschutzgrundsätze

### 2.1. Zweckbindung

43. Personendaten dürfen nur zu dem Zweck bearbeitet werden, welcher bei der Beschaffung angegeben wurde oder der aus den Umständen ersichtlich oder gesetzlich vorgesehen ist (Art. 4 Abs. 3 DSG). Die von den KSS erhobenen biometrischen Daten dienen der Verifizierung der Zugangsberechtigung der betroffenen Personen. Zwar nimmt die KSS bei den Zugangskontrollen keine Zweckänderung vor, allerdings ist eine Änderung des Bearbeitungszwecks im vorliegenden Falle von den Betroffenen durch die zentrale Speicherung der biometrischen Daten nicht kontrollierbar. Daher sind technische Lösungen zur Verifizierung der Zugangsberechtigung vorzuziehen, bei welchen keine zentrale Speicherung von biometrischen Daten vorgenommen wird. Da bei einer zentralen Datenspeicherung die betroffene Person die Kontrolle über die über sie gesammelten biometrischen Daten vollständig verliert, birgt ein zentraler Datenbestand die Gefahr einer Verlet-

zung der informationellen Selbstbestimmung mit sich, welche gemäss Art. 13 Abs. 2 der Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (SR 101; BV) garantiert wird.

44. In der Praxis hängt die Reichweite der informationellen Selbstbestimmung der betroffenen Personen von den verwendeten technischen Verfahren und Lösungen ab. Einige Lösungen ermöglichen die individuelle Kontrolle über die personenbezogenen Referenzdaten, andere ermöglichen die individuelle Kontrolle sowohl über die personenbezogenen Referenzdaten als auch über die personenbezogenen Transaktionsdaten (Lesen und Vergleichen).

45. Datenschutzrechtlich, sollten die betroffenen Personen so viel Kontrolle wie möglich über die eigenen Daten haben. Im Fall der KSS, haben wir daher eine dezentrale Speicherung empfohlen. Damit die biometrischen Daten den Kontrollbereich der betroffenen Person nicht verlassen, haben wir den Einsatz von einem milderen Mittel «Smartcards match on card» empfohlen, so dass die biometrische Daten auf dem Sicherheitsmedium gespeichert werden und die Verifizierung auf dem Sicherheitsmedium stattfindet.





### 2.2. Verhältnismäßigkeit der Datenbearbeitung

46. Die Bearbeitung von Personendaten hat sich am Grundsatz der Verhältnismässigkeit zu orientieren (Art. 4 Abs. 2 DSG). Dies bedeutet, dass ein Datenbearbeiter nur diejenigen Daten bearbeiten darf, die er für einen bestimmten Zweck objektiv tatsächlich benötigt und die im Hinblick auf den Bearbeitungszweck und die Persönlichkeitsbeeinträchtigung in einem vernünftigen Verhältnis stehen (Basler Kommentar zum DSG, Urs Maurer-Lambrou/Andreas Steiner zu Art. 4 DSG, Rz. 11). Eine Datenbearbeitung ist dann verhältnismässig, wenn sie sich inhaltlich auf das absolut Notwendige beschränkt, um ein bestimmtes Ziel zu erreichen.

    Dies bedingt auch, dass keine für den verfolgten Zweck nicht benötigten Überschussinformationen anfallen. Ebenso ist es unzulässig, Personendaten auf Vorrat zu erheben, sofern der damit verfolgte Zweck dies nicht unabdingbar erfordert.

47. Wie die Art. 29-Datenschutzgruppe der EU in ihrer Stellungnahme zum Einsatz von Biometrie festhält (siehe Anhang 34: Arbeitspapier über Biometrie (WP Nr. 80), S. 6, Nr. 3.2), sind bei der Beurteilung der Verhältnismässigkeit «*die Risiken für den Schutz der Grundrechte und – freiheiten des Einzelnen zu berücksichtigen, vor allem die Frage, ob der beabsichtigte Zweck nicht auch auf eine weniger in die Rechte der Betroffenen eingreifende Weise zu erreichen ist*».

Grundsätzlich sind daher vor dem Einsatz biometrischer Erkennungssysteme immer auch andere geeignete Alternativen zu überprüfen, welche weniger stark in die Grundrechte der Betroffenen eingreifen und mit denen der angestrebte Zweck ebenfalls erreicht werden kann.

48. Der Einsatz biometrischer Erkennungssysteme stellt je nach Ausgestaltung im konkreten Einzelfall einen mehr oder weniger intensiven Eingriff in die Persönlichkeitsrechte der Betroffenen dar. Die Eingriffe in die Grundrechte der Betroffenen müssen daher schon bei der Auswahl und Ausgestaltung des biometrischen Verfahrens berücksichtigt werden. Grundsätzlich muss ein möglichst datensparsames System ausgewählt werden, welches in einem vernünftigen Verhältnis zum angestrebten Zweck steht.

49. Vor diesem Hintergrund müsste die Konzeption des Zugangskontrollsystems im Hinblick auf den zu erreichenden Zweck ausgestaltet sein und insbesondere die nachfolgenden Kriterien in die hierfür notwendigen Erwägungen mit einbeziehen:

    1.) Ermöglicht das System eine biometrische Identifizierung oder Verifizierung und ist es zur Erreichung des Zwecks notwendig die betroffene Person zu identifizieren bzw. reicht eine Verifizierung aus?

    2.) Wie werden die biometrischen Daten gespeichert (zentral oder dezentral) und ist eine zentrale Speicherung notwendig?

    3.) Welche biometrischen Charakteristiken werden verwendet und sind diese für die Zweckerreichung notwendig?

    4.) Welche technischen und organisatorischen Massnahmen werden getroffen, um die Zuverlässigkeit und Sicherheit des biometrischen Erkennungssystems zu gewährleisten?

50. Zu 1.)

    Die biometrische Identifizierung einer betroffenen Person stellt einen schwer wiegenderen Eingriff in deren Persönlichkeit dar als deren blosse Verifizierung. Aus diesem Grund sollten Systeme zur biometrischen Identifizierung nur eingesetzt werden, wenn es zur Erreichung des beabsichtigten Zwecks zwingend notwendig ist, die betroffene Person aufgrund ihrer biometrischen Daten zu identifizieren. Die biometrische Verifizierung sollte vorwiegend nur dann zum Einsatz kommen, wenn eine strenge Authentifizierung nicht in einem ausreichenden Masse durch traditionelle Authentifizierungsmöglichkeiten, wie Passwörter oder Zugangschips (Tokens)

realisiert werden kann und eine eigentliche Identifizierung der betroffenen Person nicht zwingend notwendig ist.

51. Zu 2.)

    Der Grundsatz der Verhältnismässigkeit gebietet, bei biometrischen Systemen, die auch ohne zentrale Speicherung der biometrischen Daten auskommen, dass die biometrischen Charakteristiken möglichst nicht in einer zentralen Datenbank gespeichert werden, sondern nur auf einem dezentralen Medium, das ausschliesslich dem Benutzer zugänglich ist. Der Europarat hält in seiner Stellungnahme fest, (siehe Anhang 35: Rapport d'étape sur les principes de l'application de la Convention 108 à la collecte et au traitement des données biométriques, Nr. 48). www.coe.int/t/f/affaires_juridiques/coop%E9ration_juridique/protection_des_donn%E9es/documents/rapports_et_%E9tudes_des_comit%E9s_de_protection_des_donn%E9es/O-Biometrie_2005.asp#TopOfPage, «*le choix d'une base de données pour la fonction de vérification requiert une justification particulière*» (dass die Implementierung einer zentralen Datenbank zum Zweck der biometrischen Verifizierung besondere Rechtfertigungsgründe voraussetzt).

52. Ist hingegen die Identifizierung der betroffenen Person zur Erreichung des angestrebten Zwecks notwendig, so ist eine zentrale Speicherung der biometrischen Daten in vielen Fällen geboten.

53. Der Zürcher Datenschutzbeauftragter hat in seinem 11. Tätigkeitsbericht (siehe Anhang 36: Datenschutzbeauftragter Kanton Zürich, Tätigkeitsbericht 2005, S.12 f.) bezüglich des Einsatzes eines biometrischen Systems durch eine Gemeinde für die Zugangskontrolle ins Schwimmbad festgehalten, dass «*das Template auf einer bei der betroffenen Person verbleibenden Smartcard abgelegt und beim Wiedereintritt mit dem erzeugten Prüfmuster verglichen werden. Aus datenschutzrechtlicher Sicht sind Systeme vorzuziehen, bei denen auch das Einlesen des Fingerabdrucks und der Verifizierungsvorgang in der Nützersphäre stattfinden. Biometrische Daten dürfen nicht bei der Schwimmbad-Betreiberin abgelegt werden*».

54. Der EDÖB hat schon im Jahre 2004, in seinem Bericht über das Pilotprojekt Secure Check am Flughafen Zürich-Kloten, die dezentrale Speicherung empfohlen. (siehe Anhang 37: Bericht über das Pilotprojekt Secure Check - Einsatz von Biometrie beim Check-In und Boarding am Flughafen Zürich-Kloten, Nr. 6.5.2, 6.6.1, 6.6.2 und 7.1)

55. In Frankreich hat die Commission nationale de l'informatique et des libertés (CNIL) in verschiedene Fälle die dezentrale Speicherung empfohlen[8]. Bezüglich Délibération n°2007-138 du 21 juin 2007 autorisant la mise en œuvre par la SARL Magic Form d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès à un club de sport (siehe Anhang 38: Délibération n°2007-138 du 21 juin 2007 (CNIL)) hat die CNIL folgendes empfohlen: «*Le gabarit de l'empreinte digitale des personnes concernées sera exclusivement stocké sur un support individuel exclusivement détenu par la personne concernée et dont elle décide librement de l'utilisation*».

56. *Im Fall Comité d'entreprise d'Effia Services, Syndicat Sud Rail / Effia Services* hat das Tribunal de grande instance de Paris am 19. April 2005 folgendes bezüglich die Benützung eines biometrisches Erkennungssystems (welches den Fingerabdruck als Erkennungsmerkmal nutzte) erwägt: «*Son utilisation qui met en cause le corps humain et porte ainsi atteinte aux libertés individuelles peut cependant se justifier lorsqu'elle a une finalité sécuritaire ou protectrice de l'activité exercée dans des locaux identifiés. […] Or, il n'est pas prétendu par la société Effia Services que la seule mise en place d'un système de badge ne serait pas de nature à permettre de contrôler efficacement les horaires des salariés sans avoir recours à un procédé d'identification comportant des dangers d'atteinte aux libertés individuelles dont*



[8] Délibération n°2007-138 du 21 juin 2007 autorisant la mise en œuvre par la SARL Magic Form d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès à un club de sport, S. 2 (siehe Anhang 38: Délibération n°2007-138 du 21 juin 2007 (CNIL));
Délibération n°2006-102 du 27 avril 2006 portant autorisation unique de mise en œuvre de dispositifs biométriques reposant sur la reconnaissance de l'empreinte digitale exclusivement enregistrée sur un support individuel détenu par la personne concernée et ayant pour finalité le contrôle de l'accès aux locaux sur les lieux de travail, S. 1 f. (siehe Anhang 39: Délibération n°2006-102 du 27 avril 2006 (CNIL)) http://www.cnil.fr/index.php?id=2013;
Délibération n°2005-115 du 7 juin 2005 portant autorisation de la mise en œuvre par la Chambre de Commerce et d'Industrie de Nice-Côte d'Azur d'un traitement automatisé de données à caractère personnel ayant pour finalité la gestion d'une carte de fidélité impliquant l'utilisation d'un dispositif biométrique de reconnaissance des empreintes digitales, S. 3 (siehe Anhang 40: Délibération n°2005-115 du 7 juin 2005 (CNIL));
Délibération n°04-018 relative à une demande d'avis présentée par le Centre hospitalier de Hyères concernant la mise en œuvre d'un dispositif de reconnaissance de l'empreinte digitale ayant pour finalité la gestion du temps de travail de ses personnels, S. 1 f. (siehe Anhang 41: Délibération n°04-018 (CNIL)) http://www.cnil.fr/index.php?id=1550;
Délibération n°04-017 relative à une demande d'avis de l'établissement public Aéroports de Paris concernant la mise en œuvre d'un contrôle d'accès biométrique aux zones réservées de sûreté des aéroports d'Orly et de Roissy, S. 1 (siehe Anhang 42: Délibération n°04-017 (CNIL)) http://www.cnil.fr/index.php?id=1551

*la nécessité n'est pas démontrée. Il s'ensuit que l'objectif poursuivi n'est pas de nature à justifier la constitution d'une base de données d'empreintes digitales des personnels travaillant dans les espaces publics des gares de la Sncf, le traitement pris dans son ensemble n'apparaissant ni adapté ni proportionné au but recherché. Il y a lieu de faire interdiction à la société Effia Services de mettre en place le système de «badgeage» par empreintes digitales*». (siehe Anhang 43: Tribunal de grande instance de Paris 1ère chambre, section sociale Jugement du 19 avril 2005 Comité d'entreprise d'Effia Services, Syndicat Sud Rail / Effia Services, S. 2) http://www.legalis.net/jurisprudencedecision.php3?id_article=1433

57. In Luxemburg hat die Commission nationale pour la protection des données bezüglich Délibération n°89/2005 du 21 décembre 2005 de la Commission nationale pour la protection des données relative à la demande d'autorisation préalable introduite par l'établissement public Domaine Thermal de Mondorf en matière de traitement à des fins de surveillance contenant des données biométriques (siehe Anhang 44: Délibération n°89/2005 du 21 décembre 2005 de la Commission nationale pour la protection des données, S. 18) http://www.cnpd.lu/objets/deliberation_89_2005.pdf folgendes empfohlen: «*les moyens adoptés par le requérant pour atteindre ces finalités doivent être les plus respectueux possible des droits fondamentaux et des libertés de la personne concernée: or, tout système centralisé de données – comme le traitement envisagé par le requérant - présente un risque particulier de dérive, qui n'existe pas quand les données ne sont pas centralisées. Qui plus est, les systèmes de centralisation de données biométriques qui laissent des traces, comme les empreintes digitales, présentent plus de risques pour la protection des libertés et des droits fondamentaux de la personne que les traitements qui ne prévoient pas une telle centralisation*».

58. Die dezentrale Speicherung von biometrischen Daten wurde ebenfalls in Griechenland[9], Italien[10] und Slowenien[11] empfohlen.

[9] Siehe Anhang 45: Decision Nr. 9/2003 (Hellenic Republic authority for the protection of personal data), S. 4

[10] Uso delle impronte digitali per i sistemi di rilevamento delle presenze nei luoghi di lavoro (siehe Anhang 46: Verifica preliminare (art. 17 del Codice) – 21 luglio 2005, Bollettino del n. 63/luglio 2005 (Garante per la protezione dei dati personali), S. 3) http://www.garanteprivacy.it/garante/doc.jsp?ID=1150679
Trattamento dei dati biometrici di dipendenti per garantire la salute pubblica (siehe Anhang 47: Prescrizioni del Garante [art. 154, 1 c) del Codice] - 15 febbraio 2008 Bollettino del n. 92/febbraio, S. 2) http://www.garanteprivacy.it/garante/doc.jsp?ID=1497675

[11] Empfehlung Nr. 751-01-26/2005-01 (administrative procedure on deciding over introduction of biometric measures initiated on request of the Bank of Slovenia) (siehe Anhang 48: Empfehlung Nr. 751-01-26/2005-01 (Slowenien), S. 2) http://www.ip-rs.si/index.php?id=369

59. Zu 3.)

Wie die Art. 29-Datenschutzgruppe in ihrer Stellungnahme zum Einsatz von Biometrie, S. 6 und f. festhält, «*sind biometrische Systeme, die zur Zugangskontrolle (für Identifikation oder Verifikation) eingesetzt werden, mit geringeren Gefahren für den Schutz der Grundrechte und -freiheiten des Einzelnen verbunden, wenn sie entweder auf Körpermerkmalen basieren, die keine Spuren hinterlassen (z.B. in Form der Hand, aber keine Fingerabdrücke), oder wenn sie zwar Körpermerkmale verwenden, die Spuren hinterlassen, die Daten jedoch nicht auf einem Medium speichern, das sich nicht im Besitz der betroffenen Person befindet (mit anderen Worten, wenn die Daten nicht im Gerät, das den Zugang kontrolliert, oder in einer zentralen Datenbank gespei-chert werden*)».

Zudem sind biometrische Erkennungssysteme weniger geeignet, die Grundrechte und -Freiheiten des Einzelnen zu verletzen, wenn sie sich nicht auf Körpermerkmale abstützen, welche unbemerkt von der betroffenen Person erhoben werden können (z.B. Fingerabdruck auf einem Glas, etc.).

60. Dazu hat die CNIL in Délibération n°2006-103 du 27 avril 2006 folgendes emfohlen (siehe Anhang 49: Délibération n°2006-103 du 27 avril 2006 (CNIL), S. 2; www.cnil.fr/index.php?id=2012&print=1):

«*Les personnes habilitées énumérées ci-dessus ne peuvent avoir accès au gabarit de l'empreinte digitale que de façon temporaire et pour les stricts besoins de son inscription sur le support individuel ou de sa suppression*».

61.Zu 4.)

Die Zuverlässigkeit und Sicherheit des biometrischen Erkennungssystems hat einen bedeutenden Einfluss auf eine mögliche Verletzung und die Gefahren im Hinblick auf den Schutz der Grundrechte und -freiheiten des Einzelnen. Vor diesem Hintergrund ist es notwendig die nachfolgenden Elemente im Hinblick auf die Konzeption von solchen Systemen in die Erwägungen mit einzubeziehen: Die Architektur des Systems (insbesondere dessen Ausgestaltung, Zuverlässigkeit und die Installationsorte der Lesegeräte sowie das verwendete Kommunikationsnetzwerk und die Art der Speicherung der biometrischen Daten), die Extraktionsalgorithmen (Zahl der erhobenen Charakteristiken der biometrischen Information) und Vergleichsal-

gorithmen[12] (FAR/FRR) sowie die technischen und organisatorischen Sicherheitsmassnahmen (insbesondere die Verschlüsselung der Daten).

62. Dazu hat die OCDE empfohlen, dass die Sicherheit des biometrischen Erkennungssystems sich auf die «Lignes directrices de l'OCDE sur la vie privée» und die «Lignes directrices de l'OCDE sur la sécurité» stützt (siehe Anhang 51: Technologies fondées sur la biométrie (document DSTI/ICCP/REG(2003)2/FINAL), S. 5) http://appli1.oecd.org/olis/2003doc.nsf/linkto/dsti-iccp-reg(2003)2-final

63. Im Fall der KSS geht es um eine biometrische Verifizierung mit Erfassung von Fingerabdrücken (die Spuren hinterlassen), welche zentral gespeichert werden, ausschliesslich darum, den Missbrauch von Dauerkarten (Saisonabonnemente und Jahreskarten) automatisiert zu verhindern. Im Hinblick auf die Bearbeitungszwecke, kann der EDÖB die Einführung des biometrisches Erkennungssystems unter Vorbehalt akzeptieren. Obwohl, allerdings die von KSS eingeführten Massnahmen und durchgeführten Datenbearbeitungen geeignet sind das angestrebte Ziel zu erreichen, stehen diese nicht in einem vernünftigen Verhältnis zum Eingriff in die Grundrechte der betroffenen Personen. Die Konformität der Datenbearbeitung mit dem Datenschutzgesetz, insbesondere mit den Grundsätzen des Datenschutzes, muss vorgängig überprüft werden. Diesbezüglich, stellen die von der KSS erwähnten hohen Anschaffungskosten und der zusätzliche logistische Aufwand (siehe Anhang 32: Schreiben der KSS vom 29. Februar 2008 (Ablehnung der Empfehlung Nr. 2)) kein stichhaltiges Argument dar. Dabei ist zunächst darauf hinzuweisen, dass es sich hier nicht um Anschaffungs- sondern Änderungskosten handelt. Hätte sich die KSS rechtzeitig über die datenschutzrechtlichen Anforderungen an einer solchen Anlage informiert, wären diese Änderungskosten nicht entstanden. Es liegt in der Verantwortung des Inhabers einer Datensammlung dafür zu sorgen, dass eine Anlage zum vornherein datenschutzkonform ist.

    Infolgedessen, sind die von KSS durchgeführten Datenbearbeitungen (zentrale Speicherung der biometrischen Daten) als unverhältnismässig zu qualifizieren (Basler Kommentar zum DSG, Urs Maurer-Lambrou/Andreas Steiner zu Art. 4 DSG, Rz. 9 und 11).

[12] Siehe Anhang 50: FIDIS Deliverable 3.10 Biometrics in identity management, S. 26 ff., Nr. 3.1.4 http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.10.biometrics_in_identity management.pdf)

### 3. Schlussfolgerung

64. Aus den dargelegten Gründen und nach einer Interessenabwägung, hat der EDÖB in seiner Empfehlung vom 11. April 2006 den Einsatz von einem milderen Mittel, «Smart-cards match on card», empfohlen: «*Nach Ansicht des EDSB wird beim Einsatz von Biometrie im Privatbereich der Persönlichkeitsschutz der Betroffenen am ehesten gewahrt, indem: die biometrischen Daten auf einem Sicherheitsmedium, das sich in der alleinigen Kontrolle der betroffenen Person befindet, auslesesicher gespeichert werden; die betroffene Person jeden Zugriff auf die Daten explizit und bewusst freigeben muss; und die Verifizierung der Identität ausschliesslich auf diesem Sicherheitsmedium stattfindet, so dass die biometrischen Daten zu keinem Zeitpunkt die gesicherte Umgebung des Mediums und die Kontrolle der betroffenen Person verlassen*.» (siehe Anhang 14: Schreiben des EDÖB vom 11. April 2006 (Empfehlung), Kapitel II, Nr. 2, S. 3). Der EDÖB hat demnach empfohlen, dass «*auf die zentrale Speicherung der biometrischen Daten in Form von Templates der Fingerabdrücke verzichtet wird und diese biometrischen Daten – auch diejenigen, welche bereits zentral erfasst wurden – auf einer Smart Card, welche in der Benutzersphäre und unter Kontrolle der betroffenen Person verbleibt, abgelegt werden*». (siehe Anhang 14: Schreiben des EDÖB vom 11. April 2006 (Empfehlung), Kapitel III, Nr. 2, S. 4)





65. Eine Dezentralisierung der biometrischen Daten, welche den betroffenen Personen lediglich eine beschränkte Kontrolle über ihre personenbezogenen Daten gewährleistet (bspw. «Template on card», siehe Anhang 1: Definitionen, Nr. 10, 13 und 14) ist aus Sicht des EDÖB als ungenügend anzusehen; da die biometrische Referenzdaten ohne Kenntnis der betroffenen Personen exportiert, kopiert und unbefugt weiterverarbeitet werden könnten.

## V. Fazit

66. Aus den dargelegten Gründen, sind die von der KSS vorgenommene Datenbearbeitungen datenschutzwidrig. Die KSS ist daher auszufordern die von ihr zur Verifizierung verwendeten biometrischen Daten (Templates der Fingerabdrücke) dezentral zu speichern, mittels einer Smartcard Match on card, welche sich in der Einflusssphäre und unter Kontrollbereich der betroffenen Person befindet, sowie über welche die biometrische Verifizierung stattfindet. Damit sollen die biometrischen Daten zu keinem Zeitpunkt die gesicherte Umgebung des Mediums und die Kontrolle der betroffenen Person verlassen. Daher ist das eingangsgestellte Be-

gehren gutzuheissen und die Empfehlungsadressatin insbesondere zu verpflichten, auf die zentrale Speicherung von biometrischen Daten in Form von Templates der Fingerabdrücke zu verzichten.

EIDGENÖSSISCHER DATENSCHUTZ- UND
ÖFFENTLICHKEITSBEAUFTRAGTER

Hanspeter Thür





**Beilagen:**

Anhang 1: Definitionen zur Biometrie

Anhang 2: Schreiben des EDÖB vom 6. Juni 2005 (Sachverhaltsabklärung)

Anhang 3: Schreiben der KSS vom 29. Juni 2005

Anhang 4: Schreiben des EDÖB vom 4. August 2005

Anhang 5: Schreiben der KSS vom 19. August 2005

Anhang 6: E-Mail des EDÖB vom 25. August 2005 (Bestätigung des Termins)

Anhang 7: Anruf der KSS vom 7. September 2005 (Verschiebungsanfrage)

Anhang 8: E-Mail des EDÖB vom 30. November 2005 (Vorgehen Datenschutzkonrolle)

Anhang 9: Schreiben des EDÖB vom 14. Dezember 2005 (Fact-Sheet)

Anhang 10: Schreiben der KSS vom 20 Januar 2006 (Bitte um Fristerstreckung)

Anhang 11: E-Mail des EDÖB vom 24. Januar 2006 (Fristerstreckung bis 3. Februar 2006)

Anhang 12: Schreiben der KSS vom 1. Februar 2006 (Bestätigung der Richtigkeit des Fact-Sheets)

Anhang 13: Schreiben des EDÖB vom 11. April 2006 (Schlussbericht)

Anhang 14: Schreiben des EDÖB vom 11. April 2006 (Empfehlung)

Anhang 15: Schreiben der KSS vom 18. Mai 2006 (Bitte um Fristverlängerung)

Anhang 16: Schreiben des EDÖB vom 24. Mai 2006 (Fristerstreckung bis 19. Juni 2006)

Anhang 17: Schreiben der KSS vom 19. Juni 2006 (zweite Bitte um Fristverlängerung)

Anhang 18: Schreiben des EDÖB vom 21. Juni 2006 (zweite Fristerstreckung bis 10. August 2006)

Anhang 19: Schreiben der KSS vom 10. August 2006 (Stellungnahme zu unseren 5 Empfehlungen)

Anhang 20: Schreiben des EDÖB vom 31. August 2006 (Bitte um Nachlieferung der Stellungnahme zu den Verbesserungsvorschlägen und zur Erläuterung der Stellungnahme zu Empfehlung Nr. 4)

Anhang 21: Schreiben der KSS vom 15. September 2006 (Bitte um Fristverlängerung)

Anhang 22: Schreiben des EDÖB vom 20. September 2006 (Fristerstreckung bis 19. Oktober 2006)

Anhang 23: Schreiben der KSS vom 18. Oktober 2006 (Massnahmen zur Empfehlung Nr. 2)

Anhang 24: Schreiben des EDÖB vom 10. November 2006 (Bitte um Zustellung einem Implementierungsbericht bezüglich der Umsetzung sämtlicher vom EDÖB erlassenen Empfehlungen und Verbesserungsvorschläge)

Anhang 25: Schreiben des EDÖB vom 22. November 2006 (Bericht zur Publikation)

Anhang 26: Schreiben der KSS vom 1. Juni 2007 (Bemerkungen zum kürzen Implementierungsbericht)

Anhang 27: Schreiben des EDÖB vom 28. Juni 2007 (Nachforderung für die Frist um die Beschaffung des Implementierungsberichts)

Anhang 28: Schreiben der KSS vom 26. Juli 2007

Anhang 29: Schreiben des EDÖB vom 27. August 2007 (Nachkontrolle)

Anhang 30: Schreiben des EDÖB vom 4. Dezember 2007 (zweite Nachkontrolle und Frist bis 15.01.2008)

Anhang 31: Schreiben der KSS vom 14. Januar 2008 (Abgenommene Frist)

Anhang 32: Schreiben der KSS vom 29. Februar 2008 (Ablehnung der Empfeh lung Nr. 2)

Anhang 33: Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Daten-verkehr

Anhang 34: Arbeitspapier über Biometrie (WP Nr. 80)

Anhang 35: Rapport d'étape sur les principes de l'application de la Convention 108 à la collecte et au traitement des données biométriques

Anhang 36: Datenschutzbeauftragter Kanton Zürich, Tätigkeitsbericht 2005

Anhang 37: Bericht über das Pilotprojekt Secure Check - Einsatz von Biometrie beim Check-In und Boarding am Flughafen Zürich-Kloten

Anhang 38: Délibération n°2007-138 du 21 juin 2007 (CNIL)

Anhang 39: Délibération n°2006-102 du 27 avril 2006 (CNIL)

Anhang 40: Délibération n°2005-115 du 7 juin 2005 (CNIL)

Anhang 41: Délibération n°04-018 (CNIL)

Anhang 42: Délibération n°04-017 (CNIL)

Anhang 43: Tribunal de grande instance de Paris 1ère chambre, section sociale Jugement du 19 avril 2005 Comité d'entreprise d'Effia Services, Syndicat Sud Rail / Effia Services

Anhang 44: Délibération n°89/2005 du 21 décembre 2005 de la Commission nationale pour la protection des données

Anhang 45: Decision Nr. 9/2003 (Hellenic Republic authority for the protection of personal data)

Anhang 46: Verifica preliminare (art. 17 del Codice) – 21 luglio 2005, Bollettino del n. 63/luglio 2005 (Garante per la protezione dei dati personali)

Anhang 47: Prescrizioni del Garante [art. 154, 1 c) del Codice] - 15 febbraio 2008 Bollettino del n. 92/febbraio

Anhang 48: Empfehlung Nr. 751-01-26/2005-01 (Slowenien)

Anhang 49: Délibération n°2006-103 du 27 avril 2006 (CNIL)

Anhang 50: FIDIS Deliverable 3.10 Biometrics in identity management

Anhang 51: Technologies fondées sur la biométrie (document DSTI/ICCP/REG (2003)2/FINAL)

### 4.1.9 Resolution zur Verstärkung der internationalen Zusammenarbeit im Bereich Datenschutz und Schutz der Privatsphäre

**31st International Conference of Data Protection and Privacy Commissioners**

**Madrid, 4th – 6th November 2009**

## Resolution concerning the strengthening of the international cooperation in the field of data and privacy protection

The Swiss Federal Data Protection and Information Commissioner, Switzerland

The Data Protection Commission, France

The Data Protection Commission, Burkina Faso

The Information Commission, Québec (Canada)

The Federal Data Protection and Information Commissioner, Germany

The Office for Personal Data Protection, Czech Republic

The Privacy Commissioner, New Zealand

[The Privacy Commissioner, Canada]

The Spanish Data Protection Agency

**Resolution**

The 31st International Conference of Data Protection and Privacy Commissioners

**Recalling:**

(a) the resolution of the 31st Conference on International Standards of Privacy

(b) the resolution of the 30th Conference on the urgent need for protecting privacy in a borderless world, and for reaching a Joint Proposal for Setting International Standards on Privacy and Personal Data Protection

(c) the resolution of the 30th Conference concerning the Establishment of a Steering Group on Representation at Meetings of International Organisations

(d) the resolution of the 29th Conference on Development of International Standards

(e) the London Initiative presented during the 28th Conference

(f) the Montreux Declaration adopted at the 27th Conference that in particular appeal to prepare a legal binding instrument which clearly sets out in detail the rights to data protection and privacy and in which the commissioners agreed to intensify the exchange of information, the coordination of their supervisory activities and the development of common standards

(g) the Venice Declaration adopted at the 22nd Conference

(h) the resolution of the 21st conference on accreditation features of data protection authorities to the international conference which fix the conditions that a data protection authority must fulfil to be accredited.





**Noting that**

(a) the International Conference of Data and Privacy Commissioners is held annually since 31 years and is becoming an ever more important forum for the international data protection community;

(b) the number of accredited authorities is steadily increasing and these new authorities are expanding the global reach of the Conference;

(c) the work accomplished by the Website Working Group to create a website of the International Conference to facilitate in particular the cooperation and information sharing among the accredited authorities constitutes an important step for the international cooperation.

**Considering that**

(a) the globalisation of personal data processing and exchanges independently of the business unit, and the introduction of new information and communication technologies require an effective and universal protection of the rights

and fundamental freedoms, in particular the right to data and privacy protection with regard to processing of personal data;

(b) the growing need to coordinate the investigations and the interventions of the data protection authorities require the strengthening of the international cooperation in the field of data and privacy protection, in particular the implementation of an independent worldwide organisation in charge of data and privacy protection;

(c) the International Conference could so have an important role in promoting and implementing the right to data and privacy protection;

(d) it is necessary to evaluate the institutional needs of the Conference and to consider whether the Conference needs a more formal structure and if so, to define the mandate, the tasks and the financing.

**Therefore resolves:**

To establish a working group coordinated by the organizing authorities of the 31st and 32nd International Conference[1] and to entrust this group with the following tasks:

a. to evaluate the institutional needs of the International Conference;

b. to develop options with the aim of creating a permanent Secretariat as a more formal structure of the International Conference; and

c. to submit a report on the matter with concrete proposals during the 32nd conference.

[1] This mandate could be entrusted to the «contact group» on the Resolution on International Standards of Privacy to be adopted by the 31st Conference

## 4.2 Öffentlichkeitsprinzip

### 4.2.1 Empfehlung an das Justiz- und Polizeidepartement: «Auflösungsvereinbarungen von Arbeitsverträgen»

Siehe Abschnitt 4.2.1 im französischen Teil des Berichtes.

### 4.2.2 Empfehlung an das Bundesamt für Migration: «Rohdaten ZEMIS»





Bern, den 5. März 2009

**Empfehlung**

**gemäss**

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

**zum Schlichtungsantrag von**

**X**
**(Antragsteller)**

**gegen**

**Bundesamt für Migration (BFM), Bern**

## I. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte stellt fest:

1. Der Antragsteller (Journalist) reichte gestützt auf das Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsgesetz BGÖ, SR 152.3) am 08. Februar 2008 beim Bundesamt für Migration (BFM) ein Zugangsgesuch zu einer Auflistung mit der «Anzahl der Einreisesperren für das Jahr 2007 von Jahrgang 14- bis 17-Jährige und 18- bis 24-Jährige aufgeschlüsselt nach: - Gründe für die Einreisesperre, - Nationalitäten».

2. Am 15. Februar 2008 teilte das BFM dem Antragsteller mit, dass nach Einführung des Zentralen Migrationsinformationssystems (ZEMIS) im März 2008 die gewünschte Auswertung «mit einfachen Mitteln möglich» sei. Sollte der Gesuchsteller jedoch eine Auswertung aus dem «alten ZAR-System» (Zentrales Ausländerregister) wünschen, so müsste eine kostendeckende Gebühr erhoben werden. In der Folge zog der Antragsteller sein Zugangsgesuch umgehend mit E-Mail vom 15. Februar 2008 zurück.

3. Am 20. März 2008 liess das BFM dem Antragsteller einen 600-seitigen Auszug mit einer Auflistung aller Einreisesperren des Jahres 2007, geordnet nach Alter, Kontinente und Ländern zukommen.

4. Am 28. März 2008 reichte der Antragsteller beim BFM folgendes Zugangsgesuch ein:

   «1. Im Zemis erfasste anonymisierte Rohdaten betreffend Einreisesperren für das Jahr 2007. Diese Berichte möchte ich mit allen erfassten Parametern haben (wie zum Beispiel Alter, Nationalität, Grund der Einreisesperre, verfügter Kanton etc.)

   2. Format Excel, jede Einreisesperre auf einer Zeile erfasst

   3. Falls der Aufwand nicht massiv grösser ist, wünsche ich die unter 1 beschriebenen Daten auch für die Jahre 2000 bis 2006»).

5. Mit E-Mail vom 28. März 2008 und Brief vom 31. März 2008 teilte das BFM dem Antragsteller mit, dass sein Gesuch nochmals geprüft worden sei und das BFM zum Schluss gekommen sei, «dass wir ihnen keine anonymisierte Persondaten aus dem Zentralen Migrationsregister (ZEMIS) bekannt geben können.» Das Amt hielt fest, dass «Die Bestimmungen des Öffentlichkeitsgesetzes (…) nicht anwendbar (sind), wenn spezielle Bestimmungen anderer

Bundesgesetze abweichende Voraussetzungen für den Zugang zu bestimmten Informationen vorsehen (Art. 4 BGÖ). Dies trifft für das ZEMIS zu: (…)». Das BFM verwies auf Art. 14 der Verordnung über das Zentrale Migrationsinformationssystem (Zemis-Verordnung, SR 142.513), der abschliessend regle, «an welche Adressaten und für welche Zwecke anonymisierte Personendaten bekannt gegeben werden dürfen. Eine Bekanntgabe an Medienunternehmen für kommerzielle Zwecke ist demnach ausgeschlossen.» Die ZEMIS-Verordnung, so das BFM, beziehe sich auf das Bundesgesetz über das Informationssystem für den Ausländer- und Asylbereich (BGIAA, SR 142.51), dessen Art. 13 die Bekanntgabe von elektronischen Datensätzen oder Listen noch wesentlich einschränkender regle. Weiter führte das BFM aus, dass an dieser Ausgangslage auch das Öffentlichkeitsgesetz nichts ändere, denn es sehe ausdrücklich einen Vorbehalt von abweichenden Regelungen in den Spezialgesetzen und Verordnungen vor (Art. 4 BGÖ).

Im Übrigen bezweifelte das BFM, «dass die in einem elektronischen Registratursystem (wie ZEMIS) enthaltenen Personendaten amtliche Dokumente im Sinne von Art. 5 des Öffentlichkeitsgesetzes darstellen.

Das BFM schloss seinen Brief vom 31. März mit der Bemerkung, dass «Wir (…) jedoch gerne bereit (sind), für Sie besondere statistische Auswertungen über die im ZEMIS enthaltenen Einreiseverbote durchzuführen (Art. 20 Abs. 4 ZEMIS-Verordnung). Diese statistischen Auswertungen dienen der Information der Öffentlichkeit über die Praxis der Behörden im Ausländer- und Asylbereich und somit auch den Anliegen des Öffentlichkeitsgesetzes.»

6. Der Antragsteller reichte am 22. April 2008 beim Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (Beauftragter) einen Schlichtungsantrag ein. Nebst einer Auflistung der Kontakte mit dem BFM erwähnt er darin den 600-seitigen Auszug aus ZAR.

7. Auf die Aufforderung des Beauftragten, die Verweigerung detailliert zu begründen, verwies das BFM mit Schreiben vom 30. April 2008 auf seine Stellungnahme vom 31. März 2008 an den Antragsteller, in dem es die Ablehnungsgründe ausführlich dargelegt habe.

8. Auf Nachfrage stellte das BFM dem Beauftragten am 25. Februar 2009 den gesamten E-Mail- und Briefverkehr mit dem Antragsteller zu. Weiter teilte das BFM ihm am 26. Februar 2009 mit, dass die «beantragte Spezialauswertung ohne zusätzlichen Programmieraufwand seitens des ISC-EJPD [Informatik Ser-

vice Center des Eidg. Justiz- und Polizeidepartements, der Beauftragte] weder aus ZAR, noch aus ZEMIS möglich» sei.

Auf telefonische Nachfrage wurde präzisiert, dass das BFM nur «fixe Statistikauswertungen» aus ZEMIS erstellen könne.

Das ISC bestätigte dem Beauftragten am 2. März 2009 telefonisch, dass mit Daten aus ZAR und ZEMIS nur jene statistischen Auswertungen vorgenommen werden können, für die entsprechende Software geschrieben worden sei. Davon abweichende statistische Auswertungen aus ZEMIS könnten erst nach Schaffung eines entsprechenden Data-Warehouse-Systems erstellt werden.

Im Rahmen des Schlichtungsverfahrens bestätigte das BFM dem Beauftragten auf dessen Anfrage, dass es sich bei dem 600-seitigen Ausdruck, der dem Antragsteller am 20. März 2008 zugestellt worden ist, nicht um einen Auszug aus ZEMIS, sondern aus ZAR handelt.[1]



## 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. Der Antragsteller hat ein Zugangsgesuch nach Art. 6 BGÖ beim BFM eingereicht und ablehnende Antworten erhalten. Als Teilnehmer an einem vorange-

[1] ZEMIS wurde erst am 1. März 2008 in Betrieb genommen. Das Begehren um Zugang bezog sich auf Daten aus dem Jahr 2007.
[2] BBl 2003 *2023*

gangenen 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.[3]

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





## B. Sachlicher Geltungsbereich

1. Das BFM ist der Ansicht, dass das Öffentlichkeitsgesetz nicht zur Anwendung gelangt, weil die in Art. 13 BGIAA und Art. 14 ZEMIS-Verordnung Spezialbestimmungen im Sinne von Art. 4 BGÖ seien.

   Der Beauftragte kann dieser Argumentation nicht folgen. Zwar sieht das Öffentlichkeitsgesetz tatsächlich einen Vorbehalt von Spezialbestimmungen in anderen Bundesgesetzen vor, wenn diese «von diesem Gesetz abweichende Voraussetzungen für den Zugang zu bestimmten Informationen vorsehen» (Art. 4 Bst. b BGÖ). Allerdings gilt es dabei zu beachten, dass dieser Vorbehalt grundsätzlich für die nach Inkrafttreten des Öffentlichkeitsgesetzes erlassenen Spezialbestimmungen zum Tragen kommt (Vorrang des neueren Rechts, «lex posterior»). Das BGIAA, vom Gesetzgeber am 20. Juni 2003 angenommen, ist am 29. Mai 2006, also vor dem Öffentlichkeitsgesetz in Kraft getreten und muss nunmehr im Lichte des Öffentlichkeitsgesetzes ausgelegt werden.

   Entscheidend ist vorliegend für den Beauftragten jedoch der Umstand, dass der vom BFM angeführte Art. 13 BGIAA die Bekanntgabe von Personendaten regelt. Vorliegend hat der Antragsteller jedoch explizit Zugang zu anonymisierten Rohdaten verlangt.

   *Nach Ansicht des Beauftragten gelangt das BGÖ vorliegend uneingeschränkt zur Anwendung.*

[3] BBl 2003 *2024*

2. Der Antragsteller umschreibt in seinem Zugangsgesuch genau, welche Parameter die Rohdaten aufweisen sollen und in welchem Format und welcher Darstellung («Excel, jede Einreisesperre auf einer Zeile erfasst») er die gewünschten Dokumente zugestellt erhalten will.

   Dem hält das BFM jedoch entgegen, es bezweifle, «dass die in einem elektronischen Registratursystem (wie ZEMIS) enthaltenen Personendaten amtliche Dokumente im Sinne von Art. 5 des Öffentlichkeitsgesetzes darstellen. In diesem Fall wäre das Öffentlichkeitsgesetz unter keinen Umständen anwendbar.»

   Das Zugangsrecht besteht grundsätzlich auch zu «virtuellen Dokumenten». Gemeint sind damit Dokumente, die durch einen «einfachen elektronischen Vorgang» aus Informationen, die (noch) nicht physisch auf Papier festgehalten sind, sondern erst in einem Ordnungssystem (Aktenführungs- oder Informationssystem) enthalten sind, generiert werden können (Art. 5 Abs. 2 BGÖ). In der Botschaft zum Öffentlichkeitsgesetz heisst es dazu, dass das Recht auf Zugang auch amtliche Dokumente umfasst, die «erst *latent* vorhanden sind und die leicht durch eine elementare Computermanipulation hergestellt werden können».[4]

   Grundsätzlich unterliegen nicht nur Einzeldaten aus einer Datensammlung, sondern die Gesamtheit aller darin vorhandenen Informationen dem Zugangsrecht.[5] Bei Datensammlungen mit Personendaten erfolgt ein Zugang entsprechend den Vorgaben von Art. 9 BGÖ in Verbindung mit Art. 19 Abs. 1bis des Bundesgesetzes über den Datenschutz (DSG, SR 235.1).

   *In Bezug auf den vorliegenden Fall bedeutet dies, dass die in ZEMIS enthaltenen Informationen (auch wenn es Personendaten sind) amtliche Dokumente im Sinne von Art. 5 Abs. 1 und 2 BGÖ sind.*

3. Gemäss übereinstimmenden Aussagen des BFM und des ISC-EJPD bedarf die Erstellung der amtlichen Dokumente entsprechend den Vorgaben des Antragstellers (anonymisierte Rohdaten betreffend Einreisesperren, Format Excel jede Einreisesperre auf einer Zeile erfasst) eine Anpassung der Auswertungssoftware. Dieser Massnahme würde zwar zum gewünschten Erfolg führen, kann aber definitiv nicht mehr als einfacher elektronischer Vorgang gemäss Art. 5 Abs. 2 BGÖ qualifiziert werden. Demgegenüber hat das BFM - soweit es die ihm zur Verfügung stehenden technischen Möglichkeiten erlaubten - in

[4] BBl 2003 *1196*

[5] Bundesamt für Justiz; Umsetzung des Öffentlichkeitsprinzips in der Bundesverwaltung: Häufig gestellte Fragen, Ziffer 4.4 Datenbanken, 29.06.2006

einem «einfachen elektronischen Vorgang» einen 600-seitigen Ausdruck mit einer Auflistung aller Einreisesperren für das Jahr 2007 aus dem ZAR erstellt und dem Antragsteller zukommen lassen.

*Nach Ansicht des Beauftragten hat das BFM mit der Zustellung des Ausdrucks aller Einreisesperren für das Jahr 2007 dem Antragsteller den Zugang entsprechend den Vorgaben des Öffentlichkeitsgesetzes rechtmässig und angemessen gewährt. Das BFM kann darüber hinaus nicht verpflichtet werden, die Daten und Informationen Rohdaten in dem vom Antragsteller gewünschten Format zur Verfügung zu stellen, weil dies nicht mittels eines «einfachen elektronischen Vorgangs» gemäss Art. 5 Abs. 2 BGÖ zu bewerkstelligen ist.*

4. Können die gewünschten virtuellen Dokumente nicht mittels eines «einfachen elektronischen» Vorgangs» gemäss Art. 5 Abs. 2 BGÖ generiert werden, muss die Behörde dem Antragsteller mitteilen, dass er – sollte er am Zugang zu den gewünschten Dokumenten festhalten – für die anfallenden Kosten aufkommen müsse.[6] Entsprechend den Bestimmungen über die Gebührenerhebung muss dem Antragsteller ein konkreter Gebührenbetrag mitgeteilt werden (Art. 14ff. der Verordnung über das Öffentlichkeitsprinzip der Verwaltung, Öffentlichkeitsverordnung, VBGÖ, SR 152.31), damit der Antragsteller darüber befinden kann, ob er an seinem Gesuch festhalten möchte (Art. 16 Abs. 2 VBGÖ).

   *Der Beauftragte empfiehlt dem BFM, dass dem Antragsteller mitzuteilen, mit welchen Kosten die Erstellung der Rohdaten in der von ihm gewünschten Art und Weise verbunden ist.*

5. Bundesbehörden müssen den Zugang nur zu jenen amtlichen Dokumenten gewähren, die *nach* Inkrafttreten des Öffentlichkeitsgesetzes (1. Juli 2006) von ihnen erstellt oder ihnen mitgeteilt worden sind (Art. 23 BGÖ).

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

1. Das Bundesamt für Migration teilt dem Antragsteller mit, mit welchem Gebührenbetrag für die Erstellung der von ihm gewünschten anonymisierten Rohdaten zu rechnen ist.

[6] BBl 2003 *1196*

2. Das Bundesamt für Migration erlässt eine Verfügung nach Art. 5 des Verwaltungsverfahrensgesetzes, wenn es der Empfehlung in Ziffer 1 nicht Folge leisten will.

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

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

   Gegen diese Verfügung kann der Antragsteller beim Bundesverwaltungsgericht Beschwerde führen (Art. 16 BGÖ).

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

5. Die Empfehlung wird eröffnet:

   - X

   - Bundesamt für Migration
     3003 Bern-Wabern

Jean-Philippe Walter

### 4.2.3 Empfehlung an die Eidgenössische Steuerverwaltung: «Cockpits/Amtsreportings»

Bern, den 3. April 2009

**Empfehlung**

**gemäss**

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

**zum Schlichtungsantrag von**

**X**
**(Antragsteller)**

**gegen**

**Eidgenössische Steuerverwaltung (ESTV), Bern**

**I. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte stellt fest:**

1. Der Antragsteller wandte sich mit E-Mail vom 25. März 2008 an die Eidgenössische Steuerverwaltung (ESTV) und wollte wissen, «welche Berichte in der Eidg. Steuerverwaltung periodisch erstellt werden (Jahres- oder Quartalsberichte, periodische Sachberichte etc. verfasst von einzelnen Abteilungen und des Amtes).»

2. Mit E-Mail vom 27. März 2008 nahm die ESTV auf eineinhalb Seiten Stellung zu ihrem Berichtswesen und ihrer Geschäftsverwaltung. Sie hielt dazu u.a. fest, dass die Berichterstattung seit dem Jahr 2001 über ein internes Berichts- und Steuerungssystem (genannt «Cockpits») erfolge. Dabei berichte jeder Fachbereich dreimal jährlich über den Stand der Zielerreichung in seinem Wirkungsgebiet. Die Reportings der Fachabteilungen würden zu einem Amtsreporting aggregiert, das auch der Departementsleitung vorgelegt würde. Dieses interne Controlling unterscheide sich von den herkömmlichen Monats- und Jahresberichten (bis 2001), indem der Blick nicht nur zurück, sondern auch nach vorne gerichtet werde. Das Cockpits sei eine wichtige Basis für die Führungsabläufe. Formal sei das Cockpits auf die internen Bedürfnisse der Führungspersonen ausgerichtet. Es sei für Dritte ohne zusätzliche ausführliche Erklärungen nicht geeignet. Das Cockpits werde auch als Basis genutzt für die Berichterstattung nach aussen, sei jedoch als solches nicht zur Weitergabe bestimmt. Die ESTV fügte der Stellungnahme je eine schematische Darstellung der Prozessabläufe zu den Cockpits und der Geschäftsverwaltung bei.

3. Gestützt auf das Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsgesetz BGÖ, SR 152.3) reichte der Antragsteller am 24. April 2008 bei der ESTV ein Gesuch um Zugang zu den «Cockpits»-Berichten der dem Direktor der ESTV unterstellten Abteilungen sowie der beiden Hauptabteilungen für die Jahre 2006, 2007, 2008» sowie «für dieselbe Zeitspanne die Amtsreportings». Der Antragsteller ersuchte um Zustellung der Dokumente in elektronischer Form.

4. Am 6. Mai 2008 teilte die ESTV dem Antragsteller mit, dass sie ihm zu diesen Dokumenten keinen Zugang gewähre, und begründete die Verweigerung mit Verweis auf Art. 7 Abs. 1 Bst. b BGÖ (Beeinträchtigung der zielkonformen Durchführung konkreter behördlicher Massnahmen). Die ESTV argumentierte, dass es sich «beim ‚Cockpits' (…) um das zentrale Führungsinstrument des Direktors der ESTV (handelt), das mit Informationen aus den unterstellten Organisationseinheiten der ESTV gespiesen wird. Auf Basis dieser Grundlagen werden die Führungsentscheide der Amtsleitung getroffen.» Das Cockpits, so die ESTV weiter, enthalte «nebst der Berichterstattung der ESTV-Einheiten über den Erreichungsgrad der allgemeinen Amtsziele insbesondere eine in die Zukunft gerichtete strategische Standortbestimmung sowie eine Fülle von Kennzahlen und Ziffern aus der aktuellen Praxis. Ein Einblick würde zum Teil detaillierte Rückschlüsse auf die generelle und insbesondere künftige Arbeits-

weise der ESTV erlauben. In diesem Sinne erfüllt das Cockpits ausser einer Controlling- insbesondere auch eine Steuerungsfunktion. Die Umsetzung der teilweise mehrjährigen Planung diverser Massnahmen würde erheblich in Frage gestellt, wenn ihre Grundlage Dritten oder gar der Öffentlichkeit bekannt gegeben werden müssten.»

5. Am 14. Mai 2008 reichte der Antragsteller beim Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (Beauftragter) einen Schlichtungsantrag ein. Darin bemängelte der Antragsteller, dass die ESTV in ihrer Verweigerungsbegründung nur auf die Cockpits-Berichte, nicht aber auf die Amtsreportings eingehe. Weiter hielt er u.a. fest, dass die ESTV über ihre Tätigkeit im Vergleich zu anderen Bundesämtern äusserst zurückhaltend berichtete. So habe sie seit 2001 keinen Jahres- oder Tätigkeitsbericht mehr erstellt. Die Angaben zu Handen der Öffentlichkeit seien meistens statistischer Natur oder allgemein gehaltene Informationen zu Steuerfragen. Nach Meinung des Antragstellers würden konkrete Angaben zur Geschäftsführung eines Amtes, zu Strategien oder eine Betrachtung der vorangegangenen Tätigkeit nicht generell von Art. 7 BGÖ erfasst, denn «[a]uch die ESTV steht in der Pflicht, gegenüber der Öffentlichkeit Angaben zu seiner [sic!] Tätigkeit zu machen.»





6. Am 16. Mai 2008 forderte der Beauftragte die ESTV auf, ihm alle entsprechenden Dokumente sowie eine detaillierte Begründung für die Zugangsverweigerung einzureichen. In ihrem Antwortschreiben vom 24. Juni 2008 hielt die ESTV an ihrer Argumentation fest, dass das Cockpits das zentrale Führungssystem des Direktors (respektive der Geschäftsleitung) sei und die Beiträge der unterstellten Organisationseinheiten explizit zuhanden des Direktors respektive der Geschäftsleitung erfolgten. Zudem erfülle «das Cockpits ausser einer Controlling- insbesondere auch eine Steuerungs- und Leitungsfunktion. Die ESTV ist daher der Ansicht, es handle sich vorliegend um Informationen, welche sich der Direktor (zuhanden seiner Geschäftsleitung) zur Führung des Amtes, mithin zum persönlichen Gebrauch zusammentragen lässt. Die aggregierte Form dieser Informationen – das so genannte Amtsreporting – überlässt der Direktor ESTV anschliessend dem Departementschef EFD zur persönlichen Information. Zusätzlich wird einzig die Eidg. Finanzkontrolle (EFK) zu Kontrollzwecken mit diesem Dokument bedient. Diese Reportings sind deshalb aus der Sicht der ESTV keine amtlichen Dokumente und unterstehen deshalb nicht dem Öffentlichkeitsgesetz.»

Für den Fall, dass der Beauftragte die zu beurteilenden Informationen als amtliche Dokumente qualifiziere, vertrat die ESTV die Ansicht, dass der Zugang gestützt auf die Ausnahmegründe der wesentlichen Beeinträchtigung der freien Willens- und Meinungsbildung (Art. 7 Abs. 1 Bst. a BGÖ), Beeinträchtigung der zielkonformen Durchführung konkreter behördlicher Massnahmen (Art. 7 Abs. 1 Bst. b BGÖ) und der Offenbarung von Berufs-, Geschäfts- oder Fabrikationsgeheimnissen (Art. 7 Abs. 1 Bst. g BGÖ) verweigert werden müsse. Die ESTV reichte in Absprache mit dem Beauftragte lediglich die für das Jahr 2007 relevanten Unterlagen ein (2 Amtsreportings und 2 Beiträge der beiden Hauptabteilungen für das Frühlingsreporting in Papierform, die restlichen Beiträge und das gesamte Dezemberreporting elektronisch auf einer CD-ROM).

7. Auf Anfrage teilte die ESTV dem Beauftragten am 25. März 2009 mit, dass Cockpits mit sämtlichen Abteilungsberichten rund 800 Seiten pro Jahr umfassen. Ingesamt ergebe dies «für 3 Jahre zwischen 2000 und 3000 Seiten». Ausserdem präzisierte es, dass die Mitglieder der Geschäftsleitung und deren Stellvertreter sowie «einige wenige ausgewählte andere Personen (insb. des Direktionsstabs)» Zugriff auf die elektronischen Ordner mit sämtlichen Berichten der Abteilungen und der Amtsreportings hätten.

   Gemäss Staatskalender zählt die Geschäftsleitung der ESTV 8 Mitglieder. Mit anderen Worten haben damit mindestens 10 Personen Zugang zu den Cockpits.





## 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

[1] BBl 2003 *2023*

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 ESTV eingereicht und ablehnende Antworten 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.





## B. Sachlicher Geltungsbereich

1. Der Antragsteller bemängelt in seinem Schlichtungsantrag, dass die ESTV im Vergleich zu anderen Bundesämtern nur sehr zurückhaltend informiere und seit 2001 keine Jahres- oder Tätigkeitsberichte mehr erstelle. Der Antragsteller wirft damit die Frage auf, ob und in welchem Umfang eine Behörde verpflichtet ist, über ihre Aktivitäten und Entscheide zu informieren, respektive, ob der Antragsteller einen Anspruch auf bestimmte Informationen hat.

   Die Informationspflicht der Behörden kann unterschieden werden in eine «*allgemeine*» und eine *spezialgesetzliche* Pflicht zur Information.

2. Die «*allgemeine*» *Informationspflicht* ist in Art. 180 der Bundesverfassung (BV, SR 101) festgehalten, gemäss welcher der Bundesrat die Öffentlichkeit rechtzeitig und umfassend über seine Tätigkeit informiert, soweit nicht überwiegende öffentliche oder private Interessen entgegenstehen.

[2] BBl 2003 *2024*

Konkretisiert wird diese Informationspflicht in Art. 10 des Regierungs- und Verwaltungsorganisationsgesetzes (RVOG; SR 172.010). Demnach versorgt der Bundesrat (und die einzelnen Bundesbehörden)[3] die Bundesversammlung, die Kantone und die Öffentlichkeit mit einheitlichen, frühzeitigen und kontinuierlichen Informationen über seine Lagebeurteilungen, Planungen, Entscheide und Vorkehren. Die Pflicht der Regierung zur Information der Öffentlichkeit ist allerdings nicht unbegrenzt, denn diese hat nur Anspruch auf Informationen, wenn durch deren Bekanntgabe keine überwiegenden öffentlichen oder privaten Interessen beeinträchtigt werden.

Beide Bestimmungen enthalten inhaltliche, zeitliche und organisatorische Elemente zur Informationstätigkeit. Hinsichtlich der Modalitäten der Informationstätigkeit (genauer Inhalt, Zeitpunkt, Informationsmittel, Adressatenkreis) bleiben sie jedoch relativ unbestimmt. Der Regierung kommt daher ein gewisses Ermessen in der Ausübung und Ausgestaltung ihrer Informationstätigkeit zu.[4]

*Diese einerseits grundlegenden, anderseits aber inhaltlich allgemein gehaltenen Bestimmungen zur staatlichen Informationspflicht verleihen dem Einzelnen kein individuelles Recht auf bestimmte Informationsleistungen staatlicher Organe.*

3. Bei den *spezialgesetzlichen Informationspflichten* verpflichtet der Gesetzgeber einzelne staatliche Organe zur Bekanntgabe von Informationen und legt dabei sowohl den Inhalt als auch den Umfang in einem Erlass fest. Zu unterscheiden ist dabei zwischen der Pflicht zur aktiven und jener zur passiven Information.

4. Bei der *aktiven Information* hat der Gesetzgeber spezialgesetzliche Bestimmungen erlassen, welche die Behörden verpflichten, *aus eigener Initiative* bestimmte Informationen bekannt zu geben. Diese Kategorie zeichnet sich dadurch aus, dass sich die Pflicht zur aktiven Information auf bestimmte Dokumente respektive auf bestimmte Bereiche beschränkt. Als Beispiele können insbesondere die Pflicht des Beauftragten zur Publikation seines jährlichen Tätigkeitsberichtes (Art. 30 des Bundesgesetzes über den Datenschutz, DSG, SR 235.1) und die Pflicht zur Veröffentlichung der vorliegenden Empfehlung (Art. 13 Abs. 3 Verordnung über das Öffentlichkeitsprinzip der Verwaltung, Öf-

[3] Brunner / Mader (Hrsg.), Stämpflis Handkommentar zum BGÖ, Einleitung, Rz. 78; Botschaft zum Regierungs- und Verwaltungsorganisationsgesetz (RVOG) vom 20. Oktober 1993, BBl 1993 III 1068

[4] Mader, St. Galler Kommentar zu Art. 180 Abs. 2, Rz. 35

fentlichkeitsverordnung, VBGÖ, SR 152.31) genannt werden.[5] Fehlt hingegen eine entsprechende spezialgesetzliche Konkretisierung, ist die Behörde nicht verpflichtet, von sich aus einen Jahres- und Tätigkeitsbericht zu erstellen.

Von der aktiven ist *die passive Information* zu unterschieden. Dabei sind staatliche Organe verpflichtet, *auf Ersuchen einer interessierten Person* bestimmte Informationsdienstleistungen zu erbringen. Die Bekanntgabe von Informationen in Zusammenhang mit dem Öffentlichkeitsgesetz, also der Zugang zu amtlichen Dokumenten, ist ein Anwendungsfall der passiven Information.[6] Mit anderen Worten befasst sich auch das Öffentlichkeitsgesetz mit der staatlichen Informationstätigkeit, allerdings nur mit jener, die durch eine konkrete Einzelanfrage eines Bürgers ausgelöst wird. Es zielt hingegen nicht darauf ab, die aktive, von Behörden initiierte Informationsvermittlung zu normieren. Dies hat zur Konsequenz, dass gestützt auf das Öffentlichkeitsgesetz nicht verlangt werden kann, dass eine Behörde einen jährlichen Tätigkeitsbericht erstellen muss.

5. *Zusammenfassend* kann in Bezug auf die spezialgesetzlichen Regelungen festgehalten werden, dass staatliche Organe nur dann eine Pflicht zur Information trifft, wenn der Gesetzgeber dies explizit in einem Erlass so vorsieht und die Modalitäten der Informationstätigkeit explizit normiert. Fehlen entsprechende spezialgesetzliche Vorschriften, so ist eine Behörde nicht zur aktiven Information verpflichtet, muss aber entsprechend den Vorgaben des Öffentlichkeitsgesetzes (da ein Anwendungsfall der passiven Information) bei Vorliegen der Voraussetzungen den Zugang zu amtlichen Dokumenten gewähren.





[5] Weitere Anwendungsfälle spezialgesetzlicher Pflichten zur aktiven Information sind:
- Veröffentlichung von Erlassen und Verträgen (Art. 1 des Publikationsgesetzes; SR 170.512);
- Information der Öffentlichkeit über besondere Ereignisse, die für den Gesundheitsschutz von Bedeutung sind (Art. 12 Lebensmittelgesetz; SR 817.0);
- Veröffentlichung der wichtigsten statistischen Ergebnisse und Grundlagen (Art. 18 Bundesstatistikgesetz; SR 431.01);
- Bekanntgabe der Einträge im Handelsregister durch das Schweizerische Handelsamtsblatt (Art. 931 Obligationenrecht; SR 220);
- Information über besondere Ereignisse im Zusammenhang mit Heilmitteln, welche die Gesundheit gefährden (Art. 67 Bundesgesetz über Arzneimittel und Medizinprodukte, SR 812.21);
- Veröffentlichung der Vernehmlassungsunterlagen, eingereichte Stellungnahmen und Vernehmlassungsergebnisse (Art. 9 Bundesgesetz über das Vernehmlassungsverfahren; SR 172.061).

[6] Weitere Anwendungsfälle spezialgesetzlicher Pflichten zur passiven Information sind:
- Auskunftsgesuch betreffend die Bearbeitung eigener Personendaten durch Bundesorgane (Art. 8 Datenschutzgesetz; SR 235.1);
- Akteneinsichtsrechte (z.B. Art. 26 f. Bundesgesetz über das Verwaltungsverfahren, SR. 172.021);
- Grundsatz der freien Einsichtnahme in das Archivgut des Bundes (Art. 9 Bundesgesetz über die Archivierung, SR 152.1)

6. Die ESTV machte geltend, dass die Cockpits zum persönlichen Gebrauch des Direktors respektive der Geschäftsleitung zusammengetragen und die daraus erstellten Amtsreportings dem Departementschef des Eidgenössischen Finanzdepartements EFD zur persönlichen Information überlassen werden. Daher seien die entsprechenden Berichte keine amtlichen Dokumente und das Öffentlichkeitsgesetz gelange nicht zur Anwendung.

   Nachfolgend gilt es zu prüfen, ob die besagten Cockpits tatsächlich zum persönlichen Gebrauch bestimmte Dokumente im Sinne von Art. 5 Abs. 3 Bst. c BGÖ darstellen.

7. Gemäss Art. 1 Abs. 3 VBGÖ gilt als zum persönlichen Gebrauch bestimmtes Dokument jede Information, die dienstlichen Zwecken dient, deren Benutzung aber ausschliesslich der Autorin, dem Autoren oder einem eng begrenzten Personenkreis als Arbeitshilfsmittel vorbehalten ist, wie Notizen oder Arbeitskopien von Dokumenten.

   Einfach mag die Qualifizierung als zum persönlichen Gebrauch bestimmtes Dokument dann erscheinen, wenn dieses *ausschliesslich vom Verfasser benutzt* wird und auch bei ihm verbleibt. Dies ist vorliegend nicht gegeben, da die Einträge im Cockpits zuhanden des Direktors und der gesamten Geschäftsleitung erfolgen. Der Vollständigkeit halber sei hier klar festgehalten, dass unter Umständen auch ein bis anhin alleine dem Verfasser vorbehaltenes Dokument nach Öffentlichkeitsgesetz zugänglich sein kann.

   Die Tatsache, dass - wie im vorliegenden Fall - ein *eng begrenzter Personenkreis* Dokumente benutzt, ist für sich alleine weder ein aussagekräftiges noch ein ausreichendes Kriterium, um abschliessend zu bestimmen, ob ein Dokument lediglich dem persönlichen Gebrauch zuzuordnen ist. Wäre dem so, würde eine beträchtliche Anzahl von amtlichen Dokumenten überhaupt nicht in den Anwendungsbereich des Öffentlichkeitsgesetzes fallen, so zum Beispiel speziell auf Anordnung des Amtsdirektors oder Departementschefs erstellte Strategiepapiere, Abklärungen oder Factsheets.

   Zentral für die Beurteilung der Frage, ob es sich um ein für den persönlichen Gebrauch bestimmtes Dokument handelt, ist das Kriterium des *Arbeitshilfsmittels*. In den Erläuterungen zur Öffentlichkeitsverordnung werden als Arbeitsgrundlage oder Arbeitsmittel «handschriftliche Notizen, Arbeitskopien von Dokumenten, aber auch Korrekturvorschläge, Gedankenstützen oder Begleitnotizen»[7] erwähnt. Weiter können darunter «Dispositionen für die Aus-

[7] Erläuterungen zur Verordnung über das Öffentlichkeitsprinzip der Verwaltung, S. 3

arbeitung von Texten, Kurzzusammenfassungen, (…) und Sitzungsnotizen»[8] fallen. Diese Aufzählung zeigt deutlich, dass der Akzent auf *Hilfsmittel* gelegt wird, also Dokumente gemeint sind, die im Rahmen eines Arbeits- und Entwicklungsprozesses unterstützend verwendet werden. Dokumente und Datensammlungen mit Controlling- sowie Steuerungsfunktion enthalten keine blossen Abrisse, Skizzen oder Entwürfe, sondern Informationen, die definitive Positionen, Entscheide und Einschätzungen der einzelnen Fachbereiche wiedergeben. Es handelt sich dabei um amtliche Dokumente, die als zentrale und relevante Entscheidungsbasis für die Belange eines Amtes dienen und daher nicht als Arbeitshilfsmittel im Sinne von Art. 1 Abs. 3 VBGÖ qualifiziert werden können.

Während persönliche Sitzungsnotizen Arbeitshilfsmittel im Sinne von Art. 1 Abs. 3 VBGÖ sein können, trifft dies nicht auf (offizielle) Sitzungsprotokolle zu. Sitzungsprotokolle (auch von Direktionssitzungen) sind amtliche Dokumente und demnach im Grundsatz öffentlich zugänglich.[9] Der Gesetzgeber hat im Öffentlichkeitsgesetz keine Ausnahmeklausel für bestimmte Dokumentenkategorien (wie Sitzungsprotokolle, Cockpits oder ganz allgemein alle Dokumente der Geschäftsleitung) geschaffen. Selbst als intern oder vertraulich bezeichnete Dokumente unterstehen grundsätzlich dem Öffentlichkeitsprinzip, da der Klassifizierungsvermerk für sich allein genommen noch keine Verweigerung des Zugangs rechtfertigt.[10]

Nach Konzeption des Öffentlichkeitsgesetzes sind auch Dokumente und Informationen wie Sitzungsprotokolle und Amtsreportings grundsätzlich zugänglich und eine Beschränkung oder Verweigerung des Zugangs ist nur als Anwendungsfall von Art. 7, 8 oder 9 BGÖ möglich.

*Der Beauftragte kommt zum Schluss, dass die Berichte mit der Bezeichnung «Cockpits» und «Amtsreporting» nicht als zum persönlichen Gebrauch des Direktors der ESTV bestimmte Dokumente zu qualifizieren sind. Es handelt sich dabei amtliche Dokumente, welche in den Anwendungsbereich des Öffentlichkeitsgesetzes fallen.*

8. Folglich kann der Zugang zu den Cockpits und den daraus generierten Amtsreportings nur eingeschränkt oder verweigert werden, wenn eine Ausnahme nach Art. 7 BGÖ oder ein besonderer Fall nach Art. 8 BGÖ vorliegt oder wenn

[8] Handkommentar zum BGÖ, Art. 5, Rz. 40
[9] Bundesamt für Justiz, «Umsetzung des Öffentlichkeitsprinzips in der Bundesverwaltung: Häufig gestellte Fragen», 29.06.06, Ziffer 4.6
[10] BBl 2003 *2006*

einzelne Textpassagen zum Schutz der Privatsphäre (Art. 9 BGÖ) anonymisiert werden müssen.

Der Antragsteller verlangt Zugang zu allen Cockpits und Amtsreportings der Jahre 2006 bis 2008. Gemäss Aussagen der ESTV handelt es sich dabei um 2000 bis 3000 Seiten. Angesichts dieser grossen Dokumentenmenge gilt es, zum einen die Anforderungen an *die inhaltliche Bestimmtheit eines Dokuments* und zum anderen die *Gebührenkomponente* zu beachten.

9. Die Behörde kann vom Antragsteller einerseits verlangen, dass er sein Zugangsgesuch präzisiert (Art 7 Abs. 3 BGÖ). Anderseits ist sie jedoch auch verpflichtet, ihm Auskunft über die verfügbaren amtlichen Dokumente zu geben und ihn bei seinem Vorgehen zu unterstützen (Art. 3 Abs. 1 VBGÖ). Dies geht - insbesondere bei derart umfangreichen Dossiers - so weit, dass sie ihm beispielsweise einen Auszug aus ihrem Dokumentenmanagementsystem oder - sofern kein solches vorhanden - eine Liste mit den vorhandenen Dokumenten zukommen lassen muss.[11] Dies gibt dem Gesuchsteller die Möglichkeit, sein Gesuch zu präzisieren und dessen Ausmass besser einschätzen zu können. Macht der Gesuchsteller nicht innert 10 Tagen die für die Identifizierung der verlangten Dokumente zusätzlich erforderlichen Angaben, so gilt das Gesuch als zurückgezogen (Art. 7 Abs. 4 VBGÖ).

   *Der Beauftragte gelangt zum Schluss, dass die ESTV dem Antragsteller eine Auflistung mit allen Cockpits und Amtsreportings der Jahre 2006 – 2008 (sofern nach Inkrafttreten des Öffentlichkeitsgesetzes erstellt, Art. 23 BGÖ) zukommen lassen soll und ihn gleichzeitig auffordert, sein Zugangsgesuch zu präzisieren (Art. 3 Abs. 1 VBGÖ in Verbindung mit Art. 7 Abs. 3 und 4 VBGÖ)*.

10. Weiter trifft die Behörde auch die Pflicht, die Gesuchstellerin oder den Gesuchsteller über die zu erwartende Höhe der Gebühr zu informieren, sofern die voraussichtlichen Kosten 100 Franken übersteigen (Art. 16 Abs. 2 VBGÖ). In der Folge muss die Gesuchstellerin oder der Gesuchsteller das Interesse am Gesuch innert 10 Tagen bestätigen, ansonsten gilt es als zurückgezogen.

    Angesichts der grossen Dokumentenmenge muss davon ausgegangen werden, dass der voraussichtliche Gebührenbetrag 100 Franken sehr wahrscheinlich übersteigen wird. Sofern es bereits möglich ist, teilt die ESTV dem Antragsteller mit, welche Kosten bei der Beurteilung eines Cockpitsberichts sowie eines Amtsreportings (d.h. allfälliges Abdecken von Textpassagen nach Art. 7 - 9 BGÖ) anfallen werden.

[11] Handkommentar zum BGÖ, Art. 10, Rz. 34.

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

1. Die ESTV stellt dem Antragsteller eine Auflistung der Berichte mit den Bezeichnungen «Cockpits» und «Amtsreporting» aus den Jahren 2006 - 2008 zu (sofern nach Inkrafttreten des

   Öffentlichkeitsgesetzes erstellt, Art. 23 BGÖ) und fordert ihn auf, sein Zugangsgesuch innert 10 Tagen zu präzisieren.

2. Die ESTV erlässt eine Verfügung nach Art. 5 des Bundesgesetzes über das Verwaltungsverfahren (VwVG, SR 172.021), wenn sie in Abweichung von Ziffer 1 die Auflistung der vorhandenen Berichte nicht zustellt.

   Die ESTV 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 bei der ESTV den Erlass einer Verfügung nach Art. 5 VwVG verlangen, wenn er mit der Empfehlung nicht einverstanden ist (Art. 15 Abs. 1 BGÖ).

   Gegen die Verfügung kann der Antragsteller beim Bundesverwaltungsgericht Beschwerde führen (Art. 16 BGÖ).

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

5. In Analogie zu Art. 22a VwVG des stehen gesetzliche Fristen, die nach Tagen bestimmt sind, vom siebten Tag vor Ostern bis und mit dem siebten Tag nach Ostern still. Der Fristlauf beginnt somit am 20. April 2009.

6. Die Empfehlung wird eröffnet:

- X

- Eidg. Steuerverwaltung
  3003 Bern

Jean-Philippe Walter

### 4.2.4 Empfehlung an das Eidgenössische Departement für Umwelt, Verkehr, Energie und Kommunikation: «Zusatzdokumentation Staatsrechnung» (I)

Bern, den 19. Juni 2009

**Empfehlung**

**gemäss**

**Art. 14 des**

**Bundesgesetzes über das**

**Öffentlichkeitsprinzip der Verwaltung**

**vom 17. Dezember 2004**

**zum Schlichtungsantrag von**

**X**

**(Antragsteller)**

**gegen**

**Eidg. Departement für Umwelt, Verkehr, Energie und Kommunikation**

**I. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte stellt fest:**

1. Der Antragsteller (Journalist) verlangte gestützt auf das Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsgesetz BGÖ, SR 152.3) am 20. März 2008 beim Generalsekretariat des Eidgenössischen Departement für Umwelt, Verkehr, Energie und Kommunikation (GS UVEK) Zugang zur Zusatzdokumentation «Voranschlag 2008» und zur Zusatzdokumentation «Rechnung 2008».

2. Mit Schreiben vom 30. Mai 2008 verweigerte das GS UVEK den Zugang mit der Begründung, dass die «beantragten Dokumente […] von der Verwaltung im Auftrage einer parlamentarischen Kommission erstellt [werden]. Damit fallen diese Dokumente nicht unter das Öffentlichkeitsgesetz. Gemäss Art. 47 des Parlamentsgesetzes in Verbindung mit Art. 4 BGÖ gilt das Öffentlichkeitsgesetz nicht für die Beratungen und Sitzungsunterlagen der parlamentarischen Kommissionen und Delegationen. Für diese gilt weiterhin der Vertraulichkeitsgrundsatz.»

3. Am 4. Juni 2008 reichte der Antragsteller einen Schlichtungsantrag beim Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (Beauftragter) ein. Dabei führt er u.a. an, dass das GS UVEK nicht belege, dass die verlangten Dokumente ausschliesslich für die Parlamentskommission angefertigt worden seien. Zudem handle es sich «bei den Dokumenten klar nicht um Informationen aus einer Parlamentskommission.» Ausserdem wies er darauf hin, dass «die anderen Departemente die gewünschten Zusatzdokumentationen diskussionslos zur Verfügung gestellt haben.» Als Beispiel legte er dem Schlichtungsantrag die Zusatzdokumentation des Eidgenössischen Departements des Innern für das Jahr 2007 bei.





4. Auf die Aufforderung des Beauftragten, die Verweigerung detailliert zu begründen, verwies das GS UVEK mit Schreiben vom 1. Juli 2008 auf seine Erläuterungen vom 30. Mai 2008 an den Antragsteller.

5. Der Beauftragte informierte das GS UVEK telefonisch am 12. Mai 2009 darüber, dass seiner Einschätzung nach der Zugang gewährt werden müsste. Nach internen Abklärungen teilte das GS UVEK dem Beauftragten am 29. Mai 2009 mit, dass das GS UVEK an seiner Zugangsverweigerung festhalte und eine Empfehlung des Beauftragten wünsche.

## 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. 10 BGÖ beim GS UVEK eingereicht und ablehnende Antworten 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.





## B. Sachlicher Geltungsbereich

1. Das GS UVEK verweigert den Zugang zu den Zusatzdokumentationen «Voranschlag 2008» und «Rechnung 2008» mit Verweis auf Art. 47 des Bundesgesetzes über die Bundesversammlung (Parlamentsgesetz ParlG, SR 171.10). Dieser stellt nach Ansicht des GS UVEK – und des von ihm angefragten Rechtsdienstes der Parlamentsdienste – eine Spezialbestimmung im Sinne von Art. 4 BGÖ dar.

2. Vorweg gilt es festzuhalten, dass das Öffentlichkeitsgesetz nebst der Bundesverwaltung u.a. auch für die Parlamentsdienste gilt (Art. 2 Abs. 1 Bst. c BGÖ). Sie unterstehen dem Öffentlichkeitsgesetz allerdings nur insoweit, als dass

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

sie nicht unmittelbar für die Bundesversammlung oder einzelne Organe derselben tätig sind.[3] Mit anderen Worten gilt es nur für Dokumente, welche die eigentliche Verwaltungstätigkeit der Parlamentsdienste betreffen.

3. Art. 4 BGÖ hält einen Vorbehalt von Spezialbestimmungen anderer Bundesgesetze fest, die vom Öffentlichkeitsgesetz abweichende Voraussetzungen für den Zugang zu bestimmten Informationen vorsehen oder die diese Informationen als geheim erklären.

   Art. 47 Abs. 1 ParlG besagt, dass die Beratungen der Kommissionen vertraulich sind und insbesondere nicht bekannt gegeben werden soll, wie die einzelnen Teilnehmerinnen und Teilnehmer Stellung genommen oder abgestimmt haben.

   Gemäss einer vom Parlament publizierten Information[4] gilt diese Vertraulichkeit nicht nur für die Beratungen der parlamentarischen Kommissionen und Delegationen, sondern auch für *ihre Sitzungsunterlagen*. Sie sollen demnach nicht in den Geltungsbereich des Öffentlichkeitsgesetzes fallen und sind für die Bürgerinnen und Bürger nicht zugänglich. Mit anderen Worten hat sich der Gesetzgeber in Bezug auf bestimmte eigene Tätigkeitsbereiche für ein Weiterbestehen des Geheimhaltungsprinzips ausgesprochen.

   Der Beauftragte teilt die Ansicht, wonach Art. 47 ParlG eine Spezialbestimmung im Sinne von Art. 4 BGÖ darstellt und das Öffentlichkeitsprinzip in diesem Umgang nicht zur Anwendung gelangt. Er schliesst sich der Auffassung an, dass (Sitzungs-)*Unterlagen, die unmittelbar von den Parlamentsdiensten für die Kommissionen oder Delegationen oder von diesen selbst erstellt worden sind*, nicht unter das Öffentlichkeitsgesetz fallen.

4. Offen bleibt somit, ob und in welchem Umfang Sitzungsunterlagen respektive *Dokumente, die von der Bundesverwaltung erstellt worden sind*, auch von diesem Vorbehalt erfasst werden. Das Öffentlichkeitsgesetz beantwortet diese Frage ebenso wenig wie die Botschaft des Bundesrates.

   In der parlamentarischen Debatte vertrat die zuständige Kommissionssprecherin im Ständerat die Ansicht, dass «alle Dokumente, die von der Bundesverwaltung für die Kommissionen erstellt werden, […] unter die Vertraulichkeit fallen.»[5]

[3] BBl 2003 1985, Brunner / Mader (Hrsg.), Stämpflis Handkommentar zum BGÖ, Art. 2, RZ 41ff.
[4] «Umsetzung des Öffentlichkeitsgesetzes in den Parlamentsdiensten» (www.parlament.ch, Rubriken: Wissen>Parlamentswissen>Öffentlichkeitsgesetz)
[5] Amtliches Bulletin AB 2003 S 1138 / BO 2003 E 1138

Der Beauftragte kann sich dieser Haltung aufgrund der nachfolgenden Ausführungen nur bedingt anschliessen.

5. Ausgehend von den Gründen für die Einführung (Stärkung demokratischer Rechte, Instrument zur Kontrolle der Verwaltung, Einsichtnahme in behördliche Praxis und Entscheidfindung, Verbesserung des Vertrauens in die Behörden etc.[6]) und von der Zwecksetzung des Öffentlichkeitsgesetzes (Förderung der Transparenz der Entscheidungsprozesse der Verwaltung[7]) muss gefolgert werden, dass grundsätzlich alle innerhalb der Bundesverwaltung erstellten Dokumente unters Öffentlichkeitsgesetz fallen.

   Weiter gilt es festzuhalten, dass das Öffentlichkeitsgesetz keine Dokumente aufgrund ihres Adressatenkreises vom Geltungsbereich ausnimmt.

6. Die Einführung des Öffentlichkeitsprinzips in der Verwaltung geht nicht zuletzt auf wiederholte Interventionen des Gesetzgebers zurück.[8] Folgerichtig kann es nicht dem Willen des Gesetzgebers entsprochen haben, ausnahmslos *alle* von der Bundesverwaltung erstellten Dokumente zuhanden der Bundesversammlung (oder einzelner Organe, Art. 31 ParlG) mittels einer Hintertüre wieder dem Öffentlichkeitsgesetz zu entziehen. In letzter Konsequenz würde damit – zumindest theoretisch – einer Bundesbehörde die Möglichkeit eröffnet, Informationen, die sie unter keinen Umständen der Bevölkerung zugänglich machen will, still und leise vom Geltungsbereich des Öffentlichkeitsgesetzes auszunehmen, indem sie die entsprechenden Dokumente ungefragt einer parlamentarischen Kommission zustellt.

   Die Meinung, dass alle von der Bundesverwaltung für Kommissionen erstellten Dokumente unbesehen und in jeden Fall als vertraulich gelten sollen, überzeugt aus Sicht des Beauftragten nicht.

7. Vielmehr kann nach Ansicht des Beauftragten der Zugang zu amtlichen Dokumenten, welche von einer Bundesbehörde erstellt worden sind, nur dann gestützt auf Art. 47 ParlG als Spezialbestimmung im Sinne von Art. 4 BGÖ verweigert werden, wenn die Behörde diese Dokumente aufgrund eines unmittelbaren und besonderen Auftrags einer parlamentarischen Kommission oder Delegation erstellen muss (z.B. explizit für die Kommission erstellte Berichte,

[6] BBl 2003 *1973*
[7] BBl 2003 *1976*, Art. 1 BGÖ
[8] BBl 2003 *1980*

Gutachten oder Varianten/Entwürfe zu gesetzlichen Regelungen).[9] Selbst in diesen Fällen gilt es sodann zu prüfen, ob nach Kenntnisnahme der Unterlagen respektive spätestens nachdem der politische Entscheid, für den die Dokumente eine Grundlage darstellen, gefällt ist, nicht wiederum das Öffentlichkeitsprinzip zum Tragen kommen muss. Der Beauftragte fordert daher, dass eine Bundesbehörde bei Eingang eines Gesuchs um Zugang zu Dokumenten, welche im unmittelbaren und besonderen Auftrag einer Kommission erstellt und ihr übermittelt worden sind, sich mit der zuständigen parlamentarischen Kommission oder Delegation in Verbindung setzt und abklärt, ob die Dokumente nun zugänglich gemacht werden können.

Umgekehrt kann in all jenen Fällen, in denen die Verwaltung amtliche Dokumente im Zuge ihrer öffentlichen Aufgabenerledigung bereits für sich selber oder für Dritte (Private oder andere Amtsstellen) erstellt hat, dieser Vorbehalt der Vertraulichkeit von Art. 47 ParlG nie angebracht werden. Dies gilt insbesondere auch, wenn die Dokumente nachträglich von einer parlamentarischen Kommission oder Delegation einverlangt respektive ihnen von einer Behörde aus freien Stücken zugestellt worden sind.

*Zusammenfassend gilt daher, dass der Vertraulichkeitsbegriff von Art. 47 ParlG in Bezug auf die von der Bundesverwaltung für parlamentarische Kommissionen und Delegationen erstellten Dokumente restriktiv anzuwenden ist.*





8. In Bezug auf die hier zu beurteilenden Dokumentationen zur Staatsrechnung gilt festzuhalten, dass es sich um eine Zusammenstellung von Informationen handelt, über die jedes Departement ohnehin verfügt und die routinemässig – also nicht im unmittelbaren und besonderen Auftrag – den Finanzkommissionen für deren Beratungen zur Verfügung gestellt werden. Diese Dokumente sind auch anderen, dem Öffentlichkeitsgesetz unterstehenden Stellen zugänglich.

   Aufgrund der vorangegangenen Ausführungen gelangt der Beauftragte zum Schluss, dass die Zusatzdokumentationen «Voranschlag 2008» und «Rechnung 2008» dem Öffentlichkeitsgesetz unterstehen. Da weder ein Anwendungsfall von Art. 7 BGÖ noch von Art. 8 BGÖ vorliegt, sind nach Ansicht des Beauftragten keine stichhaltigen Argumente ersichtlich, welche eine Beschränkung oder Verweigerung des Zugangs nach Öffentlichkeitsgesetz rechtfertigen.

   *Die Zusatzdokumentationen «Voranschlag 2008» und «Rechnung 2008» müssen zugänglich gemacht werden.*

[9] Ebenso: Handkommentar BGÖ, Art. 2 RZ. 42; Bundesamt für Justiz, «Umsetzung des Öffentlichkeitsprinzips in der Bundesverwaltung: Häufig gestellte Fragen», 29.06.06, Ziffer 2.5

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

1. Das Generalsekretariat UVEK gewährt den Zugang zur Zusatzdokumentation «Voranschlag 2008» und zur Zusatzdokumentation «Rechnung 2008»

2. Das Generalsekretariat UVEK erlässt eine Verfügung nach Art. 5 des Bundesgesetzes über das Verwaltungsverfahren (VwVG, SR 172.021), wenn es in Abweichung von Ziffer 1 den Zugang nicht gewähren will.

   Das Generalsekretariat UVEK 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 Generalsekretariat UVEK den Erlass einer Verfügung nach Artikel 5 VwVG verlangen, wenn er mit der Empfehlung nicht einverstanden ist (Art. 15 Abs. 1 BGÖ).

4. Gegen die Verfügung kann der Antragsteller beim Bundesverwaltungsgericht Beschwerde führen (Art. 16 BGÖ).

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

6. Die Empfehlung wird eröffnet:

- X

- Eidg. Departement für Umwelt, Verkehr, Energie und Kommunikation
  Generalsekretariat
  3003 Bern

Jean-Philippe Walter

Kopie:

Parlamentsdienste
Parlamentsgebäude
3003 Bern

### 4.2.5 Empfehlung an die Generalsekretariate der Departemente (EDI, EJPD, VBS, EFD, EVD und an das UVEK): «Zusatzdokumentation Staatsrechnung» (II)

Bern, den 2. November 2009

**Empfehlung**

**gemäss**

**Art. 14 des**

**Bundesgesetzes über das**

**Öffentlichkeitsprinzip der Verwaltung**

**zum Schlichtungsantrag von**

**X**

**(Antragsteller)**

**gegen**

**Eidg. Departement des Innern,**

**Eidg. Justiz- und Polizeidepartement,**

**Eidg. Departements für Verteidigung, Bevölkerungsschutz und Sport**

**Eidg. Finanzdepartement,**

**Eidg. Volkswirtschaftsdepartement**

**Eidg. Departement für Umwelt, Verkehr, Energie und Kommunikation**

**I. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte stellt fest:**

1. Der Antragsteller (Journalist) verlangt gestützt auf das Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsgesetz BGÖ, SR 152.3) am 18. August 2009 bei den Generalsekretariaten des Eidgenössischen Departement des Innern (EDI), des Eidgenössischen Justiz- und Polizeidepartements

(EJPD), des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport (VBS), des Eidgenössischen Finanzdepartements (EFD), des Eidgenössischen Volkswirtschaftsdepartments (EVD) und des Eidgenössischen Departements für Umwelt, Verkehr, Energie und Kommunikation (UVEK) Zugang zur *Zusatzdokumentation* zum Voranschlag der Staatsrechnung für das Jahr 2010 (Voranschlag 2010). Der Voranschlag 2010 ist öffentlich zugänglich.[1]

2. In ihren Stellungnahmen schoben die Departemente den Zugang mit dem Verweis auf den durch die Bundesversammlung noch nicht gefällten politischen Entscheid auf. Das VBS und das EFD setzten allerdings noch das Einverständnis der zuständigen parlamentarischen Kommission voraus.

3. Der Antragsteller reichte im Zeitraum vom 9. bis 25. September 2009 die Schlichtungsanträge beim Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (Beauftragter) ein.

4. Auf Anfrage des Beauftragten nahmen die Departemente betreffend die Zugänglichkeit ihrer Zusatzdokumentationen zum Voranschlag 2010 wie folgt Stellung:

   4.1. Das EFD begründete seine Verweigerung nicht weitergehend, sondern teilte dem Beauftragten am 23. September 2009 mit, dass es an der Stellungnahme und der Begründung, die es dem Antragsteller gegeben habe, festhalte. Demnach werden die alljährlichen Zusatzdokumentationen des EFD «lediglich auf Wunsch der Finanzkommissionen erstellt (wir würden sie sonst nicht verfassen, da sie uns keinen Mehrwert schaffen). Wir sind trotzdem bereit, vorausgesetzt die entsprechenden Kommissionen sind einverstanden, den Zugang zu den erwähnten Dokumenten zu gewähren. Dies im Sinne von Art. 8 Abs. 2 BGÖ aber erst, wenn das Parlament den Voranschlag 2010 genehmigt hat, für welchen die Dokumente (unter anderen) die Grundlage bilden. Die Genehmigung dürfte in der Wintersession 2009 erfolgen.»

   In den Vorbemerkungen der Zusatzdokumentation des EFD ist festgehalten, dass diese «im Auftrag und zuhanden der Finanzkommissionen der eidgenössischen Räte erstellt [wird]. Als Kommissionsunterlage dient sie für

[1] Budget 2010 http://www.efv.admin.ch/d/themen/bundesfinanzen/voranschlag/index.php

die Beratung des Voranschlags 2010 und obliegt den Bestimmungen des Bundesgesetzes über die Bundesversammlung (Parlamentsgesetz ParlG, SR 171.10). Das Öffentlichkeitsgesetz gelangt nicht zur Anwendung.»

Auf Nachfrage übermittelte das EFD dem Beauftragten ein Schreiben des Sekretariats der parlamentarischen Aufsicht über die Finanzen und AlpTransit (SFPA). Darin heisst es, dass die Mitglieder der Finanzkommissionen «grossen Wert auf die ergänzenden Erläuterungen in den sog. Zusatzdokumentationen» legen. Für die Ausarbeitung wird auf die nach gegenseitiger Absprache verabschiedeten Richtlinien aus dem Jahre 2003 verwiesen und die Verantwortlichen in den Departementen werden gebeten, die Zusatzdokumentationen bis zum 24. August 2009 einzureichen.

4.2. Das EVD beantragte in seiner Stellungnahme vom 2. Oktober 2009 erstens, den Zugang bis zur Verabschiedung des Voranschlags durch die Bundesversammlung aufzuschieben, und zweitens, ihn nur mit der Zustimmung der Finanzkommissionen zu gewähren.

Für die vorläufige Verweigerung sei, so das EVD, Art. 8 Abs. 2 BGÖ massgebend, wonach das amtliche Dokument erst zugänglich gemacht werden dürfe, wenn der politische Entscheid, für den es die Grundlage darstellt, getroffen sei. Vorliegend sei die Zusatzdokumentation für die Finanzkommissionen der Eidgenössischen Räte erstellt worden. Sie diene diesen als Basis für ihre Anträge im National- und Ständerat, die den Voranschlag 2010 beschliessen würden. Die Zusatzdokumentation weise einen unmittelbaren und direkten Zusammenhang mit einem konkreten politischen Entscheid auf und sei für diesen von beträchtlichem materiellem Gewicht, womit die zeitweilige Verweigerung des Zugangs hinreichend begründet sei. Der massgebliche politische Entscheid, für den die Zusatzdokumentation die Grundlage bilde, liege nicht in den Beschlüssen der Finanzkommissionen, sondern vielmehr im Beschluss der Bundesversammlung, bei der die Finanzgewalt liege. Der Voranschlag 2010 werde in der Wintersession 2009 verabschiedet.

Das EVD hielt fest, dass seine «Position nicht in Widerspruch zur Empfehlung des EDÖB vom 19. Juni 2009» stehe. Weiter führte das EVD aus, dass anlässlich der Generalsekretärenkonferenz vom 24. August 2009 «in Anwesenheit des EDÖB klar gestellt [wurde], dass die Departemente ihre Zusatzdokumentationen zu den Voranschlägen den Finanzkommissionen nicht routinemässig bzw. nicht ohne jeglichen Auftrag zur Verfü-

gung stellen, wie dies in der erwähnten Empfehlung des EDÖB vom 19. Juni 2009 dargestellt wurde. Vielmehr ist in diesem Zusammenhang von einer zumindest *impliziten Erwartung* der Finanzkommissionen auszugehen. Aufgrund dieser Sachlage ist es gerechtfertigt, die Zusatzdokumentation zu den Voranschlägen gleich zu behandeln wie Dokumente, die von der Bundesverwaltung aufgrund eines *unmittelbaren und besonderen Auftrags* einer parlamentarischen Kommission erstellt wurden und daran die in der Empfehlung des EDÖB vom 19. Juni 2009 gezogenen Folgerungen zu knüpfen.» Für den vorliegenden Fall gelange damit Art. 4 BGÖ zur Anwendung, der einen Vorbehalt von Spezialbestimmungen anderer Bundesgesetze enthalte, die vom BGÖ abweichende Voraussetzungen für den Zugang zu bestimmten Informationen vorsehen oder die diese Informationen als geheim erklärten. Art. 47 Abs. 1 des Bundesgesetzes über die Bundesversammlung (Parlamentsgesetz ParlG, SR 171.10) besage, dass die Beratungen der Kommissionen vertraulich seien. Somit blieben vorliegend die Dokumente bis zum Zeitpunkt des politischen Entscheides, für den die Zusatzdokumentation die Grundlage bildet, vertraulich. Nach dem Beschluss der Bundesversammlung über den Voranschlag werde sich das EVD mit den Finanzkommissionen in Verbindung setzen und abklären, ob diese mit der Herausgabe der Zusatzdokumentation einverstanden sei.

Im Übrigen stellt das EVD in Frage, ob auch Zusatzunterlagen, welche die Verwaltung aus eigenem Antrieb für parlamentarische Kommissionen erstelle, Art. 47 ParlG unterstellt seien. Diese Frage bilde gegenwärtig Gegenstand juristischer Abklärungen durch die Bundeskanzlei.

4.3. Das VBS präzisierte in seiner Stellungnahme vom 6. Oktober 2009, dass die fraglichen Zusatzdokumente auf Wunsch und zu Handen der parlamentarischen Finanzkommissionen erstellt würden. Es verwies darauf, dass die Parlamentsdienste nur so weit dem Öffentlichkeitsgesetz unterstellt seien, als sie nicht unmittelbar für die Bundesversammlung oder einzelne ihrer Organe tätig seien. «Dies muss aus Gründen der Konsequenz sinngemäss auch für die übrige Bundesverwaltung gelten: Soweit Dokumente für Organe der Bundesversammlung erstellt werden, sind diese den Bestimmungen des BGÖ nicht unterworfen.» Es sei Sache der betroffenen Organe, über die Einsicht in ihre Dokumente zu entscheiden. Das Parlamentsgesetz erkläre Dokumente für Parlamentskommissionen für vertraulich, und daher fielen auch alle Dokumente, die von der Bundesverwaltung für die Kommissionen erstellt würden, unter die Vertraulichkeit. Das VBS vertrat

daher die Ansicht, dass die in der Empfehlung des EDÖB vom 19. Juni 2009 vertretene Meinung dem ausdrücklich geäusserten Willen des Gesetzgebers nicht Rechnung trage und daher nicht zu überzeugen vermöge. Es stehe dem Gesuchsteller indes frei, bei den zuständigen Kommissionen um Einsichtnahme zu ersuchen. Letztlich könne und dürfe es nicht Sache einer Behörde der Bundesverwaltung sein, über die Offenlegung von Dokumenten zu entscheiden, die von einem Parlamentsorgan für ihre Arbeit gebraucht werde. Das VBS sei daher der Überzeugung, dass es sich bei den Zusatzdokumentationen zum Voranschlag generell um Dokumente handle, die nicht dem Öffentlichkeitsgesetz unterliegen. Weiter komme vorliegend hinzu, dass Einsicht in eine Dokumentation verlangt werde, die vom Parlament und seinen Kommissionen noch gar nicht behandelt worden seien. Selbst wenn das Dokument unter das Öffentlichkeitsgesetz fallen würde, wäre der Zugang aufgrund von Art. 8 Abs. 2 BGÖ zu verweigern.

Weiter empfahl das VBS dem Beauftragten, aus Gründen der Zuständigkeit auch die betroffenen parlamentarischen Organe (Finanzkommission, Parlamentsdienste) um eine Stellungnahme zu ersuchen.

4.4. Das UVEK anerkannt in seiner Stellungnahme vom 15. Oktober 2009 ausdrücklich das Interesse der Öffentlichkeit, über die Tätigkeiten der Verwaltung transparent informiert zu werden. Um die Finanzkommissionen der eidgenössischen Räte nicht in ihrer Meinungs- und Willensbildung zu beeinflussen, habe jedoch das UVEK den Zugang bis nach Kenntnisnahme der Dokumentation durch die Finanzkommissionen aufgeschoben. Da die Parlamentsmeinung grundsätzlich in den Kommissionen gebildet werde, könne der Zugang zur Zusatzdokumentation nach Kenntnisnahme durch die Finanzkommissionen, in Anwendung des Verhältnismässigkeitsprinzips, gewährt werden.

4.5. Das EJPD beantragte in seiner Stellungnahme vom 21. Oktober 2009 zum einen, den Zugang zur Zusatzdokumentation des EJPD zum Voranschlag 2010 bis zur Verabschiedung durch die Bundesversammlung zu verweigern. Zum anderen solle das vorliegende Schlichtungsverfahren mit vergleichbaren Verfahren, namentlich mit dem Schlichtungsantrag von X vom 09.09.2009 betreffend die Stellungnahme des Generalsekretariats EVD vom 20.08.2009 koordiniert werden. Weiter beantragte es, «die Ergebnisse der nach unseren Informationen zu den von diesem Schlichtungsverfahren betroffenen Fragen von der Konferenz der Generalsekretärinnen und Ge-

neralsekretäre (GSK) bei der Bundeskanzlei in Auftrag gegebenen Abklärungen seien abzuwarten und die zu erwartenden Festlegungen der GSK zum Vorgehen in solchen Fällen seien zu berücksichtigen.»

In seiner Begründung führte das EJPD aus, dass im Schlichtungsantrag «keine Argumente enthalten sind, welche in den Erwägungen vom 02.10.2009 des Generalsekretariats EVD zu einem offensichtlich gleich gelagerten Schlichtungsantrag von X nicht thematisiert werden […]». Daher verwies es auf die Stellungnahme des EVD und schloss sich den dort angeführten Überlegungen vorbehaltlos an. Das EJPD bat um Beachtung der Tatsache, dass «die Parlamentsdienste (Sekretariat der parlamentarischen Aufsicht über Finanzen und AlpTransit SPFA) mit Brief vom 13.08.2009 ausführlich Zusatzdokumentationen zum Voranschlag 2010 einverlangten.»

4.6. Das EDI beantragte am 23. Oktober 2009 ebenfalls, den Zugang zur Zusatzdokumentation des EDI zum Voranschlag 2010 bis zur Verabschiedung des Voranschlags 2010 durch die Bundesversammlung nicht zu gewähren. Weiter solle das vorliegende Schlichtungsverfahren mit den weiteren, bezüglich Zusatzdokumentationen zum Voranschlag 2010 hängigen Schlichtungsanträgen von XI, namentlich betreffend das EVD und das EJPD, koordiniert werden. Im Übrigen hielt das EDI ausdrücklich fest, dass dem Antragsteller der Zugang zu den Voranschlägen 2007 und 2008 nach Verabschiedung durch die Bundesversammlung jeweils zugänglich gemacht wurden. Vorliegend verlange er Einsicht in Unterlagen der laufenden Budgetperiode, bevor das zuständige politische Organ auf deren Grundlage die erforderlichen Beschlüsse fassen konnte. Das EDI hielt an Aufschub des Zugangs gestützt auf Art. 8 Abs. 2 BGÖ fest.

5. Mit Ausnahme des VBS stellten alle Departemente dem Beauftragten ihre Zusatzdokumente zum Voranschlag zusammen und ihren Stellungnahmen zur Verfügung.

   Kein Departement machte geltend, dass bestimmte Passagen der Zusatzdokumentationen bei einer späteren Zugangsgewährung aufgrund einer Ausnahmebestimmung des Öffentlichkeitsgesetzes abgedeckt werden müssten.

6. Der Beauftragte hat sich bereits in seiner Empfehlung vom 19. Juni 2009[2] mit der Frage der Zugänglichkeit von Zusatzdokumenten zur Staatsrechnung («Vor-

[2] Empfehlung vom 19. Juni 2009: UVEK / Zusatzdokumente Staatsrechnung

anschlag 2008» und «Rechnung 2008») befasst. Er ist zum Schluss gekommen, dass es sich dabei um «die Zusammenstellung von Informationen handelt, über die jedes Departement ohnehin verfügt und die routinemässig – *also nicht im unmittelbaren und besonderen Auftrag* – den Finanzkommissionen für deren Beratungen zur Verfügung gestellt werden. Diese Dokumente sind auch anderen, dem Öffentlichkeitsgesetz unterstehenden Stellen zugänglich.» In Bezug auf die zu beurteilenden Zusatzdokumente zur Staatsrechnung 2008 hielt er fest, dass weder ein Anwendungsfall von Art. 7 BGÖ noch von Art. 8 BGÖ vorliege, welcher «eine Beschränkung oder Verweigerung des Zugangs nach Öffentlichkeitsgesetz rechtfertigen» würde.

Das von der Empfehlung betroffene Departement akzeptierte die Empfehlung und stellte in der Folge dem Antragsteller die gewünschten Dokumente zu.

## 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.[3] Berechtigt, einen Schlichtungsantrag einzureichen, ist jede Person, die an einem Gesuchsverfahren um Zugang zu amtlichen Dokumenten teilgenommen hat. Für den Schlichtungsantrag genügt einfache Schriftlichkeit. Aus dem Begehren muss hervorgehen, dass sich der Beauftragte mit der Sache befassen soll. Der Schlichtungsantrag muss innert 20 Tagen nach Empfang der Stellungnahme der Behörde schriftlich eingereicht werden.

2. Der Antragsteller hat jeweils ein Zugangsgesuch nach Art. 10 BGÖ bei den Generalsekretariaten der erwähnten Departemente eingereicht und jeweils ablehnende Antworten erhalten. Als Teilnehmer an den vorangegangenen Gesuchsverfahren ist er zur Einreichung der Schlichtungsanträge berechtigt. Die

[3] BBl 2003 *2023*

Schlichtungsanträge wurden formgerecht (einfache Schriftlichkeit) und fristgerecht (innert 20 Tagen nach Empfang der Stellungnahme der Behörde) beim Beauftragten eingereicht.

3. Das Schlichtungsverfahren kann auf schriftlichem Weg oder konferenziell (mit einzelnen oder allen Beteiligten) unter Leitung des Beauftragten stattfinden. Die Festlegung des Verfahrens im Detail obliegt alleine dem Beauftragten.[4]

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





## B. Sachlicher Geltungsbereich

1. Gemäss dem Bundesgesetz über den eidgenössischen Finanzhaushalt (Finanzhaushaltgesetz, FHG) muss der Bundesrat (und mit ihm seine Verwaltung) der Bundesversammlung die Staatsrechnung zur Abnahme unterbreiten (Art. 4 FHG). Die Staatsrechung umfasst u.a. die Jahresrechnung des Bundes, die wiederum u.a. einen Anhang umfasst (Art. 10 FHG, Art. 3 FHV). Gemäss Botschaft zum FHG kennt das öffentliche im Vergleich mit dem privaten Rechnungswesen eine viel detailliertere externe Information über die geplanten Aktivitäten, deren finanziellen Auswirkungen wie auch über die finanzpolitische Prioritätenbildung, die Finanzierung der Aufgabenerfüllung und den Haushaltvollzug. Dabei wird explizit festgehalten, dass diese detaillierte Informationsoffenlegung «im Einklang mit dem Öffentlichkeitsprinzip» steht.[5] Weiter stellt der Bundesrat in seiner Botschaft klar, dass die Zusatzdokumentationen der Departemente Bestandteil dieser Berichterstattung sind.[6] Nach Ansicht des Beauftragten werden die Zusatzdokumentationen somit nicht lediglich aufgrund eines jährlich wiederkehrenden expliziten oder auch nur impliziten Auftrags der Finanzkommissionen erstellt, sondern sie müssen von den Departementen aufgrund einer gesetzlichen Verpflichtung verfasst werden. Das Schreiben der Finanzkommissionen an die Verwaltung mit dem Inhalt, die Zusatzdokumentationen einzureichen, ist nach Einschätzung des Beauftragten somit nicht als Auftrag, sondern lediglich als Aufforderung zur fristgerechten Einreichung der Dokumente zu qualifizieren.

[4] BBl 2003 *2024*
[5] BBl *2005* 13
[6] «Obwohl nicht explizit erwähnt, bilden auch die Zusatzdokumentationen der Departemente zu Handen der Finanzkommissionen beider Räte Teil der Berichterstattung.» BBl 2005 30

Der Beauftragte hält an seiner Empfehlung vom 19. Juni 2009 fest, wonach die Zusatzdokumentationen der Departemente grundsätzlich zugänglich sind.

2. Die Departemente verlangen einen Aufschub des Zugangs zu den Zusatzdokumentationen bis zur Verabschiedung des Voranschlags zur Staatsrechnung 2010 durch die Bundesversammlung. Sie stellen mehrheitlich dabei auf Art. 8 Abs. 2 BGÖ ab, der besagt, dass amtliche Dokumente erst zugänglich gemacht werden dürfen, wenn der politische oder administrative Entscheid, für den sie die Grundlage darstellen, getroffen ist.

   Nach Ansicht des Beauftragten gelangt hier nicht Art. 8 Abs. 2 BGÖ, sondern vielmehr Art. 7 Abs. 1 Bst. a BGÖ zur Anwendung. Diese Ausnahmebestimmung schützt ebenfalls den freien Meinungs- und Willensbildungsprozess im Stadium der Entscheidvorbereitung und -findung, gilt aber explizit auch für *legislative Organe*. Darunter fallen auch parlamentarische Kommissionen.

3. Vorliegend kann davon ausgegangen werden, dass die vorzeitige Bekanntgabe der Zusatzdokumentation der einzelnen Departemente tatsächlich zu einer wesentlichen Beeinträchtigung der Meinungs- und Willensbildung der Kommissionen führen könnte. Die zuständige Kommission sollte sich in einer ersten Phase jedoch ohne äusseren Druck eine Meinung bilden können. Der Beauftragte erachtet es als sinnvoll und notwendig, dass die zuständigen Finanzkommissionen unvoreingenommen und frei Kenntnis von den Zusatzdokumentationen der Departemente nehmen können. In diesem Sinne kann der Zugang gestützt auf Art. 7 Abs. 1 Bst. a BGÖ aufgeschoben werden.

4. In Bezug auf den Zeitpunkt der Zugangsgewährung gilt es nach Ansicht des Beauftragten zu beachten, dass sich die Zusatzdokumentationen an die Finanzkommissionen und nicht an die Bundesversammlung richten.[7] Der Beauftragte folgt der Einschätzung des UVEK, dass die politische Meinungs- und Willensbildung in den Finanzkommissionen erfolgt. Demnach müssen die Zusatzdokumentationen nach der Behandlung des Voranschlags 2010 durch die Finanzkommissionen von den Generalsekretariaten der Departemente zugänglich gemacht werden.

   *Der Zugang zu den Zusatzdokumentationen der einzelnen Dokumente kann gestützt auf Art. 7 Abs. 1 Bst. a BGÖ bis nach den Sitzungen der Finanzkommissionen des Nationalrates und des Ständerates aufgeschoben werden.*

[7] BBL 2005 *30*, a.a.O.

5. Zum gegebenen Zeitpunkt müssen die Generalsekretariate der Departemente von sich aus tätig werden und dem Gesuchsteller die gewünschten Dokumente zustellen.[8]

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

1. Die Generalsekretariate des EDI, EJPD, VBS, EFD, EVD und UVEK schieben den Zugang zu den Zusatzdokumentationen zum Voranschlag 2010 bis nach den Sitzungen der Finanzkommissionen des Nationalrates und des Ständerates auf.

2. Das Generalsekretariat eines Departements erlässt eine Verfügung nach Art.5 des Bundesgesetzes über das Verwaltungsverfahren (VwVG, SR 172.021), wenn es in Abweichung von Ziffer 1 den Zugang zum gegebenen Zeitpunkt nicht gewähren will.

   Das Generalsekretariat 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 bei den Generalsekretariaten den Erlass einer Verfügung nach Artikel 5 VwVG verlangen, wenn er mit der Empfehlung nicht einverstanden ist (Art. 15 Abs. 1 BGÖ).

4. Gegen die Verfügung kann der Antragsteller beim Bundesverwaltungsgericht Beschwerde führen (Art. 16 BGÖ).

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

[8] Stämpflis Handkommentar zum BGÖ, Art. 7, Rz. 10

6. Die Empfehlung wird eröffnet:

- X

- Eidg. Departement des Innern
  Generalsekretariat
  3003 Bern

- Eidg. Justiz- und Polizeidepartement
  Generalsekretariat
  3003 Bern

- Eidg. Departement für Verteidigung, Bevölkerungsschutz und Sport
  Generalsekretariat
  3003 Bern

- Eidg. Finanzdepartement
  Generalsekretariat
  3003 Bern

- Eidg. Volkswirtschaftsdepartement
  Generalsekretariat
  3003 Bern

- Eidg. Departement für Umwelt, Verkehr, Energie und Kommunikation
  Generalsekretariat
  3003 Bern

Hanspeter Thür

Kopie:

Parlamentsdienste
Parlamentsgebäude
3003 Bern