19. Tätigkeitsbericht 2011/2012

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Tätigkeitsbericht 2011/2012
des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten

Der Eidg. Datenschutz- und Öffentlichkeitsbeauftragte hat der Bundesversammlung periodisch einen Bericht über seine Tätigkeit vorzulegen (Art. 30 DSG). Der vorliegende Bericht deckt den Zeitraum zwischen 1. April 2011 und 31. März 2012 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. 410.019.d/f

Inhaltsverzeichnis

Vorwort – Bilanz und Ausblick

Im Staatsschutzbereich sind letztes Jahr erhebliche Verbesserungen erzielt worden. Die von uns bei jeder sich bietenden Gelegenheit eingebrachte Botschaft, die Rechtsstellung der Betroffenen sei mit dem indirekten Auskunftsrecht zu schwach ausgestaltet und würde höchstwahrscheinlich einer Überprüfung durch den Europäischen Menschenrechtsgerichtshof nicht standhalten, führte im Rahmen einer Revision des Bundesgesetzes über die Wahrung der inneren Sicherheit (BWIS) in der Dezembersession 2011 zu einer Anpassung durch das Parlament. Neu gilt grundsätzlich das direkte Auskunftsrecht gemäss Artikel 8 und 9 des Datenschutzgesetzes (DSG); es kann aber aufgeschoben werden, wenn dies Staatsschutzinteressen gebieten. Die gesuchstellende Person kann in solchen Fällen die Prüfung durch den EDÖB veranlassen, der bei Fehlern eine Empfehlung abgeben kann.

Nachdem gegen das revidierte Gesetz kein Referendum ergriffen wurde, dürfte es der Bundesrat auf Anfang Juli 2012 in Kraft setzen. Gleichzeitig beschäftigte sich auch das Bundesgericht aufgrund der Beschwerde eines Gesuchstellers mit der heute geltenden Regelung in Art. 18 BWIS und beurteilte mit seinem Entscheid vom 2. November 2011 erstmals deren EMRK-Konformität. Dabei verbesserte es die Rechtsstellung der Betroffenen markant. Grundsätzlich hielt das oberste Gericht fest, dass ein indirektes Auskunftsrecht EMRK-konform sei, solange Staatsschutzinteressen dies rechtfertigten. Allerdings verlangten die Bundesrichter im Widerspruch zum Wortlaut der Bestimmung, dass der EDÖB bei Fehlern zuhanden der Staatsschutzorgane nicht nur Empfehlungen, sondern verbindliche Anweisungen abgeben könne. Nur so sei der durch den EDÖB und den Abteilungspräsidenten des Bundesverwaltungsgerichts wahrzunehmende Kontrollmechanismus hinreichend wirksam und erfülle die Anforderungen einer unabhängigen Überprüfung der Datenbearbeitung durch die Staatsschutzorgane. Der revidierte Art. 18 BWIS räumt nun dem Bundesverwaltungsgericht explizit die Möglichkeit ein, die Behebung von Fehlern mit einer Verfügung zu veranlassen. Wir gehen davon aus, dass bei Inkraftsetzung des revidierten BWIS das Urteil des Bundesgerichts weiterhin Gültigkeit hat und die Empfehlungen des EDÖB folglich verbindlichen Charakter haben müssen.

Auch im vergangenen Jahr legten wir einen Schwerpunkt im Bereich Ausbildung von Jugendlichen und setzen damit unsere bisherigen Anstrengungen fort, weil wir der Überzeugung sind, dass im Zeitalter der sozialen Netzwerke besondere Initiativen zur Sensibilisierung der jungen Nutzerinnen und Nutzer erforderlich sind, und weil wir uns nicht mit Appellen an die Adresse von Schulen und Eltern begnügen wollen. Dabei suchen wir – nicht zuletzt unserer beschränkten Mittel wegen – Partnerschaften. Das 2011 mit dem Rat für Persönlichkeitsschutz gestartete Projekt NetLa erreichte viele

Schülerinnen und Schüler. Allein im November, dem letzten Monat der Kampagne, besuchten über 6000 Personen mit über 225'000 Klicks das multimediale Portal. Zur Sensibilisierung junger Erwachsener für Datensicherheit bei der Nutzung neuer Medien haben wir neu ein Lehrmittel entwickelt, das in Form einzelner Lektionen seit Anfang dieses Jahres kostenlos online abrufbar ist. Zielgruppe sind Schüler der Sekundarstufe II. An den Universitäten Neuenburg und Lausanne haben wir bei Ausbildungsveranstaltungen für Studierende mitgewirkt. Zudem haben wir zusammen mit der Datenschutzbehörde des Kantons Genf, der Universität Genf, dem Observatoire technologique Genf, dem IDHEAP Lausanne und anderen Akteuren den interaktiven Dienst Thinkdata.ch entwickelt. Die französischsprachige Webseite, demnächst auch auf Deutsch verfügbar, bietet allen an Datenschutz und Transparenz interessierten oder damit konfrontierten Akteurinnen und Akteuren in unterschiedlichen Rollen rasch greifbare Antworten an. Im Augenblick suchen wir finanzielle Mittel, um das Angebot weiterzuentwickeln und auch in weiteren Sprachen zur Verfügung stellen zu können. Zum vierten Mal haben wir überdies gemeinsam mit den Universitäten von Bern, Freiburg und Neuenburg den Schweizerischen Datenschutzrechtstag durchgeführt.

Auch 2011 haben wir zahlreiche Kontrollen und Sachverhaltsabklärungen durchgeführt. So prüften wir bei fünf Betrieben des öffentlichen Verkehrs die Videoüberwachung und schlugen einige Verbesserungen vor, welche auch akzeptiert wurden. Im Rahmen der Umsetzung des Schengen-Abkommens haben wir der Schweizer Botschaft in Moskau einen Kontrollbesuch abgestattet und in der Folge verschiedene Empfehlungen abgegeben. Die Sachverhaltsabklärung bei einem Tennisclub mit biometrischem Reservationssystem haben wir im Berichtsjahr ebenso erfolgreich abgeschlossen wie diejenige zur Bonitätsdatenbearbeitung. Im Laufe der mittlerweile beendeten Abklärungen zur Datenplattform «Car Claims Information Pool» der Motorfahrzeugversicherungen haben wir verschiedentlich Verbesserungen erreicht. Weiter haben wir einem Dienstleister für Breitensportveranstaltungen verschiedene Änderungen vorgeschlagen und sind noch im Schriftenwechsel über deren Umsetzung. Im Zusammenhang mit einem neuen Computerspiel, das seinem Hersteller unerlaubt Daten über die Computer der User übermittelt, haben wir eine Sachverhaltsabklärung eröffnet.

Von den zahlreichen Ämterkonsultationen weise ich insbesondere auf die Revision von Bundesgesetz und Verordnung zur Überwachung des Post- und Fernmeldeverkehrs hin. Hier konnten wir erwirken, dass für den Einsatz von «GovWare» eine gesetzliche Grundlage geschaffen wird. Bei der Erarbeitung ebensolcher Grundlagen für die Überwachung der Nutzung der elektronischen Infrastruktur in der Bundesverwaltung haben wir ebenfalls auf die Notwendigkeit einer klaren Regelung von Aufzeichnung und Aufbewahrung, aber auch der Formen der Auswertung der so genannten Randdaten hingewiesen.

Im Rahmen der Gesetzesrevision in Sachen SwissDRG haben wir die verschiedenen Akteure kontaktiert und gefordert, dass die Versicherungen nur die Daten erhalten, die sie wirklich benötigen. Bei der Totalrevision des Versicherungsvertragsgesetzes haben wir auf die Verankerung des Instituts des Vertrauensarztes hingewirkt.

Unter den Veröffentlichungen auf unserer Webseite während des Berichtsjahrs, aufgelistet in Ziffer 3.3., sind vor allem die Erläuterungen zur revidierten e-Privacy-Direktive der EU und zum boomenden Cloud Computing als Möglichkeit der Datenverarbeitung erwähnenswert.

Im Bereich des Öffentlichkeitsprinzips hat sich auch im vergangenen Jahr einiges getan. Die Zahl der Zugangsgesuche in der Bundesverwaltung hat sich beinahe verdoppelt, während bei uns 65 Schlichtungsanträge eingingen. Wir konnten im Berichtsjahr 30 Schlichtungen durchführen und erreichten in der überwiegenden Mehrzahl der Fälle eine für den Gesuchsteller günstigere Lösung. Alle Empfehlungen sind unter Ziffer 2.3.1 zusammengefasst und auf unserer Webseite abrufbar. Das Bundesverwaltungsgericht musste sich auf Beschwerde hin mit vier Empfehlungen auseinandersetzen und hat unsere Argumentation jeweils gestützt. Im Rahmen der Revision des Kartellgesetzes haben wir zudem erfolgreich darauf hingewirkt, dass die Wettbewerbsbehörden nicht vom BGÖ ausgenommen werden.

Es ist schon heute absehbar, dass uns verschiedene Themen auch im kommenden Berichtsjahr beschäftigen werden. Dazu gehört das politisch heikle Ansinnen der USA, im Rahmen eines «Hit-no-Hit»-Verfahrens in Erfahrung bringen zu wollen, ob eine bestimmte Person mit ihrem Fingerabdruck oder ihrer DNA in einer der Schweizerischen Datenbanken Codis oder Afis verzeichnet ist. In den Verhandlungen ist darauf zu achten, dass Betroffene, die zu Unrecht in diesen beiden Datenbanken landeten, in den USA die gleichen Rechte zugesichert erhalten wie in der Schweiz. Eine solche Garantie ist indes nicht einfach zu bekommen, da die USA bekanntlich aus unserer Sicht grundsätzlich nicht über einen angemessenen Datenschutz verfügen. Deshalb darf die Beurteilung im Einzelfall nicht einem der Verwaltung unterstellen Privacy Officer obliegen, sondern muss von einer unabhängigen richterlichen Behörde vorgenommen werden. Wichtig ist zudem, dass in jenen Fällen, in denen eine Übereinstimmung der Daten festgestellt wurde, das weitere Verfahren im Rahmen der rechtlich verankerten Rechtshilfeverfahren abgewickelt wird. Das heisst, die Voraussetzungen für die Herausgabe von Personendaten sind im Einzelfall auf der Basis der geltenden Abkommen zu prüfen. Es darf keinen Automatismus geben. Klar ist auch, dass ein solcher Austausch auf die schwere Kriminalität zu beschränken ist und die Schweiz Gegenrecht erhalten muss.

Weiter auf Trab halten uns die sozialen Netzwerke, namentlich die Geschäftspolitik von Facebook. Diese ist bekanntlich darauf ausgerichtet, Zugriff auf möglichst viele Informationen über die eigenen Nutzerinnen und Nutzer zu erhalten, um daraus Profile zu Werbezwecken zu generieren. Damit macht das Unternehmen Milliardenumsätze und ändert zu diesem Behufe laufend die allgemeinen Geschäftsbedingungen – zum Nachteil der Nutzer und ohne ihre Einwilligung einzuholen. Neu geraten nicht mehr nur Mitglieder, sondern auch Nichtnutzer ins Visier von Facebook. Im Entwurf der Nutzungsbedingungen vom März 2012 heisst es, diese gälten auch für Nichtnutzer, die «mit Facebook ausserhalb der USA interagieren». Für sie gilt neu, dass sie mit der Weitergabe ihrer Daten in die USA und der dortigen Verarbeitung einverstanden sind. Das umfasst auch die Verarbeitung zu Werbezwecken. Das Skandalöse daran ist, dass die meisten «Nichtnutzer» gar nicht wissen, dass sie mit Facebook «interagieren» – und wie kommt das? Auf vielen Webseiten ist Facebook mittels dem so genannten «Like-Button» eingebunden (sichtbar bspw. durch das kleine Signet «f»). Der Besuch des Users auf der aufgerufenen Seite wird automatisch an Facebook gemeldet – wohlverstanden auch ohne dass der Nutzer den Like-Button angeklickt hat. Damit können auch von eigentlichen Facebook-Abstinenten sehr präzise Persönlichkeitsprofile erstellt werden. Wir werden nun ein geschärftes Augenmerk darauf richten, dass Betreiber solcher Webseiten ihren Besuchern die Möglichkeit geben zu entscheiden, ob sie mit einer solchen Weiterleitung einverstanden sind. Nicht verwunderlich ist, dass sich mittlerweile auch auf parlamentarischer Ebene Misstrauen breit macht. Die Walliser Nationalrätin Viola Amherd reichte im September 2011 ein Postulat ein, in welchem sie den Bundesrat auffordert, die Rechtslage in Bezug auf die Social Media zu überprüfen, bestehende Lücken zu benennen und die Frage zu beantworten, ob ein eigenes Social-Media-Gesetz geschaffen werden soll. In der Begründung heisst es unter anderem, dass die Social Media «eine neue Dimension in der Kommunikation und in der Mediennutzung (bewirken), welche die Durchsetzung nationaler Gesetze und Grundwerte auszuhebeln drohen». Kommentar überflüssig!

Im Bereich der Urheberrechte ist nach dem Logistep-Urteil des Bundesgerichts einiges in Bewegung geraten. Zur Erinnerung: Das Bundesgericht entschied, dass das heimliche Ausforschen von IP-Adressen durch diese Firma mit dem Zweck, vermutete Urheberrechtsverletzer zivilrechtlich zu belangen, nicht erlaubt ist. Bei den Rechteinhabern hat dieses Urteil einige Aufregung ausgelöst. Das Bundesgericht hat dann in seinem Geschäftsbericht 2010 auf die aktuelle unbefriedigende Gesetzessituation hingewiesen und den Gesetzgeber aufgefordert, einen den neuen Technologien angepassten Urheberrechtsschutz zu gewährleisten. Diese bemerkenswerte und unübliche Initiative des Gerichts hat bis heute beim Bundesrat keine Reaktion ausgelöst. Inzwischen sind im Parlament Vorstösse zur Verbesserung der

Situation eingereicht worden. Klar ist, dass der Schutz der Urheberrechte im Internet ein sehr sensibles Thema ist und nicht nur in der Schweiz sehr kontrovers diskutiert wird (die in Deutschland erfolgreiche Piratenpartei lässt grüssen). Unsere Haltung, die wir bereits im Verfahren eingenommen haben, hat sich nicht verändert: Eine IP-Adresse darf auf der Basis des geltenden Gesetzes nur verwendet werden, um im Rahmen eines Strafverfahrens einen Urheberrechtsverletzer zweifelsfrei zu ermitteln. Erst dann sind zivilrechtliche Forderungen angebracht.

Am 9. Dezember 2011 hat der Bundesrat den Bericht über die Evaluation des Bundesgesetzes über den Datenschutz verabschiedet und dem Parlament unterbreitet. Neben der positiven Feststellung, dass das Datenschutzgesetz im Bereiche der Herausforderungen, die bereits zum Zeitpunkt des Inkrafttretens bestanden, einen spürbaren Effekt erzielte und sich die Schaffung des EDÖB als wirksames Instrument erwiesen habe, um diese Schutzwirkung des Gesetzes zu erhöhen, wird klar Handlungsbedarf ausgemacht:

«Nach der Meinung des Bundesrates sollte Hauptziel der Revision des Datenschutzgesetzes die Anpassung desselben an die technologischen und gesellschaftlichen Entwicklungen seit seinem Inkrafttreten sein. Entsprechend beabsichtigt der Bundesrat, seine Reformüberlegungen schwergewichtig auf die mit den technologischen und gesellschaftlichen Entwicklungen verbundenen vier zentralen Problembereiche auszurichten; 1. auf die Zunahme von Datenbearbeitungen; 2. auf die Datenbearbeitungen, die weder für die Betroffenen noch für den EDÖB ohne Weiteres erkennbar sind; 3. auf die zunehmend internationale Dimension von Datenbearbeitungen; 4. auf die zunehmende Schwierigkeit, einmal bekannt gegebene Daten weiterhin kontrollieren zu können.

Vor diesem Hintergrund möchte der Bundesrat untersuchen, mit welchen Massnahmen insbesondere die folgenden Zielsetzungen erreicht werden können:

- früheres Greifen des Datenschutzes: Im Rahmen einer Gesamtkonzeption sollen allfällige Datenschutzprobleme soweit sinnvoll und möglich schon bei der Entwicklung neuer Technologien festgestellt und geprüft werden. Damit soll verhindert werden, dass bestehende Datenschutzprobleme lediglich nachträglich durch Korrekturprogramme behoben werden (Vertiefung des Konzepts «Privacy by Design»). Daneben sollen datenschutzfreundliche Technologien gefördert werden.
- verstärkte Sensibilisierung der betroffenen Personen: Die betroffenen Personen sollen stärker für die mit den technologischen Entwicklungen einhergehenden Risiken für den Persönlichkeitsschutz sensibilisiert werden.

- Erhöhung der Transparenz: Die Transparenz über Datenbearbeitungen soll erhöht werden, insbesondere in den neuen komplexen Konstellationen, in denen Datenbearbeitungen weder für die Betroffenen noch für den EDÖB ohne Weiteres erkennbar sind. Dabei wird aber im Auge zu behalten sein, dass die betroffenen Personen nicht mittels einer Informationsflut überfordert werden.
- Verbesserung der Datenkontrolle und -herrschaft: Die Kontrolle und die Herrschaft über einmal bekannt gegebene Daten sind ein wichtiger Aspekt. Es soll geprüft werden, ob die Aufsichtsmechanismen des EDÖB gestärkt und ob die Rechtsansprüche der Betroffenen sowie deren Durchsetzung an die aufgrund der technologischen Entwicklungen veränderten Verhältnisse angepasst werden sollten. In diesem Zusammenhang sind etwa eine Stärkung der kollektiven Rechtsdurchsetzung und eine Präzisierung des Rechts auf Vergessen zu erwägen.
- Schutz von Minderjährigen: Dem Umstand, dass sich Minderjährige der Risiken und Folgen der Verarbeitung personenbezogener Daten weniger bewusst sind als Erwachsene, soll Rechnung getragen werden.»

Der Bundesrat will ferner untersuchen, ob und inwieweit die Unabhängigkeit des EDÖB noch verstärkt werden sollte. Als prüfungswürdig erachtet er auch einen Ausbau des Instruments der Selbstregulierung, etwa indem Branchenorganisationen eine «gute Praxis» definieren, die anschliessend vom EDÖB genehmigt werden könnte.

Diese bundesrätliche Zielrichtung vertreten wir schon seit Jahren, und wir sind sehr froh, dass nun der Handlungsbedarf auf dieser Ebene erkannt worden ist. Etwas Sorge bereiten könnte der Zeitplan, wenn der Bundesrat die in Gang befindlichen Reformschritte in Europa abwarten will. Natürlich muss ein schweizerisches Reformvorhaben mit der europäischen Entwicklung koordiniert werden. Das sollte aber die Exekutive nicht daran hindern, parallel dazu eine Expertengruppe einzusetzen, die sich aus schweizerischer Sicht mit der Problematik befasst. Auch beim Datenschutz muss es der Ehrgeiz unseres Landes sein, eigenständige Lösungen zu entwickeln, statt sich auf den autonomen Nachvollzug von EU-Recht zu beschränken.

Hanspeter Thür

Abkürzungsverzeichnis

ADV	Verordnung über die Amtshilfe nach Doppelbesteuerungsabkommen
AFAPDP	Association francophone des Autorités de protection des données personnelles
AHVN13	13-stellige AHV-Nummer
AkkBV	Verordnung über das schweizerische Akkreditierungssystem und die Bezeichnung von Prüf-, Konformitätsbewertungs-, Anmelde- und Zulassungsstellen
ATSG	Bundesgesetz über den Allgemeinen Teil des Sozialversicherungsrechts
BABS	Bundesamt für Bevölkerungsschutz
BAFU	Bundesamt für Umwelt
BAG	Bundesamt für Gesundheit
BAK	Bundesamt für Kultur
BAV	Bundesamt für Verkehr
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
BLW	Bundesamt für Landwirtschaft
BPG	Bundespersonalgesetz
BPI	Bundesgesetz über die polizeilichen Informationssysteme des Bundes
BSV	Bundesamt für Sozialversicherungen

BÜPF	Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs
BVGer	Bundesverwaltungsgericht
BWIS	Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit
DBA	Doppelbesteuerungsabkommen
DBG	Bundesgesetz über die direkte Bundessteuer
DRG	Diagnoses related Groups
DSG	Bundesgesetz über den Datenschutz
EDA	Eidgenössisches Departement für auswärtige Angelegenheiten
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDI	Eidgenössisches Departement des Innern
EFD	Eidgenössisches Finanzdepartement
EFK	Eidgenössische Finanzkontrolle
EJPD	Eidgenössisches Justiz- und Polizeidepartement
EKIF	Eidgenössische Kommission für Impffragen
ENSI	Eidgenössisches Nuklearsicherheitsinspektorat
EPA	Eidgenössisches Personalamt
ESTV	Eidgenössische Steuerverwaltung
EVA	Elektronische Visumausstellung
EVD	Eidgenössisches Volkswirtschaftsdepartement
FATCA	Foreign Account Tax Compliance Act
fedpol	Bundesamt für Polizei
FDV	Verordnung über Fernmeldedienste
FINMA	Eidgenössische Finanzmarktaufsicht
FMG	Fernmeldegesetz
GDK	Konferenz der kantonalen Gesundheitsdirektorinnen und -direktoren
GEWA	Datenverarbeitungssystem zur Bekämpfung der Geldwäscherei

GKI	Gemeinsame Kontrollinstanz von Schengen
ISAS	Informationssystem innere Sicherheit
IschV	Verordnung über den Schutz von Informationen des Bundes
ISIS	Staatsschutz-Informationssystem
ISV-NDB	Verordnung über die Informationssysteme des Nachrichtendienstes des Bundes
JANUS	Gemeinsames Informationssystem der kriminalpolizeilichen Zentralstellen des Bundes
KKJPD	Konferenz der kantonalen Justiz- und Polizeidirektorinnen und -direktoren
KNS	Eidgenössische Kommission für nukleare Sicherheit
KVG	Bundesgesetz über die Krankenversicherung
KVV	Verordnung über die Krankenversicherung
LRV	Luftreinhalte-Verordnung
MWSTV	Mehrwertsteuerverordnung
NDB	Nachrichtendienst des Bundes
N-SIS	Nationaler Teil des Schengener Informationssystems
OECD	Organisation for Economic Co-operation and Development (Oganisation für wirtschaftliche Zusammenarbeit und Entwicklung)
PEP	Policy Enforcement Point
PKI	Public Key Infrastructure
RHG	Bundesgesetz über die Harmonisierung der Einwohnerregister und anderer amtlicher Personenregister
RVOG	Regierungs- und Verwaltungsorganisationsgesetz
SAKE	Schweizerische Arbeitskräfteerhebung
SAS	Schweizerische Akkreditierungsstelle
SchKG	Bundesgesetz über Schuldbetreibung und Konkurs
SECO	Staatssekretariat für Wirtschaft
SIS	Schengener Information System

SODK	Konferenz der kantonalen Sozialdirektorinnen und Sozialdirektoren
Swissmedic	Schweizerisches Heilmittelinstitut
UPI	Unique Person Identification
UVEK	Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation
UVG	Bundesgesetz über die Unfallversicherung
UWG	Bundesgesetz gegen den unlauteren Wettbewerb
VBGÖ	Verordnung über das Öffentlichkeitsprinzip der Verwaltung
VBS	Departement für Verteidigung, Bevölkerungsschutz und Sport
VBZ	Verkehrsbetriebe Zürich
VDSG	Verordnung zum Bundesgesetz über den Datenschutz
VIS	Visa-Informationssystem
VÜPF	Verordnung über die Überwachung des Post- und Fernmeldeverkehrs
VVG	Bundesgesetz über den Versicherungsvertrag
VZV	Verordnung über die Zulassung von Personen und Fahrzeugen zum Strassenverkehr
WEKO	Wettbewerbskommission
ZAS	Zentrale Ausgleichsstelle
ZEMIS	Zentrales Migrationsinformationssystem
ZVV	Verkehrsverbund des Kantons Zürich

1. Datenschutz

1.1 Grundrechte

1.1.1 Outsourcing im Rahmen der Volkszählung

Das Ankündigungsschreiben, mit dem das Bundesamt für Statistik Personen um die Teilnahme an Erhebungen bittet, informiert auf unsere Veranlassung hin neu transparent über die Freiwilligkeit der Mitwirkung. Fortschritte wurden auch im Bereich der Qualitätssicherung durch das mit der Erhebung beauftragte Unternehmen erzielt.

In unserem 18. Tätigkeitsbericht 2010/2011 haben wir unter Ziffer 1.1.1 über unsere Kontrolle bezüglich Datenbearbeitungen und Informationsfluss im Zusammenhang mit der Volkszählung berichtet. In der Zwischenzeit konnte der Teil der Überprüfung, der das Bundesamt für Statistik (BFS) betrifft, fast zu Ende geführt werden. Auf unsere Kritik hin verbessert das BFS den Informationsgehalt der Ankündigungsschreiben, mit denen die Bürger um die Teilnahme an einer Erhebung gebeten werden. Bisher fehlte jeweils eine klare Information über eine allfällige Teilnahmeverpflichtung, aus Besorgnis, die Rücklaufquote könnte dadurch negativ beeinflusst werden. Das BFS hat im letzten Jahr verschiedene Arten der transparenteren Information getestet und uns einen akzeptablen Vorschlag gemacht: Neu wird jedem Ankündigungsschreiben, das in allgemeiner Form über die Erhebung informiert, ein kleiner Faltprospekt (Leporello) beigelegt. In diesem soll klar über die Teilnahmeverpflichtung informiert werden. Die Umsetzung dieser Verbesserung werden wir anhand einiger konkreter Beispiele überprüfen. Wir vertreten die Meinung, dass die adäquate Information über die Freiwilligkeit oder Verpflichtung der Teilnahme für alle Erhebungen des BFS erforderlich ist.

Ein weiterer von uns kritisierter Punkt, in dem wir uns bisher nicht einigen konnten, betrifft die Kontrolle der Mitarbeitenden des privaten Instituts, welches die Erhebung durchführt. Wir erachten die Qualitätskontrolle, wie sie bis anhin praktiziert wurde, als unverhältnismässig. Unsere Argumentation überzeugte das betroffene Unternehmen jedoch vorerst nicht. Es wies darauf hin, dass die von ihm entwickelte Praxis in der Branche weit verbreitet sei und eine anders ablaufende Qualitätskontrolle die Bedürfnisse des Auftraggebers (hier des BFS) nicht erfüllen könne. Unsere Abklärungen haben ein ähnliches Bild ergeben. Jedoch rechtfertigt die Tatsache, dass eine gewisse Praxis weit verbreitet ist, in keiner Weise eine unrechtmässige Datenbearbeitung.

Wir möchten mit dem betroffenen Unternehmen eine Lösung finden, die als Musterlösung für die Branche dienen kann. Der technische Fortschritt und die ständige Verbilligung von Speichermedien, die unterdessen auch eine akustische Aufnahme des

gesamten Erhebungsmaterials ermöglichen würde, sollen dabei berücksichtigt werden. Inzwischen haben wir mit dem Unternehmen das weitere Vorgehen vereinbart. Es wird uns ein Qualitätssicherungskonzept, das den Ansprüchen des Datenschutzes Rechnung trägt, zur Prüfung unterbreiten, und wir werden seine Umsetzung begleiten. In diesem Bereich führen wir die Kontrolle fort und berichten weiter darüber.

1.1.2 Bürgeranfragen zu statistischen Erhebungen

In letzter Zeit melden sich vermehrt Bürger mit Fragen zu statistischen Erhebungen bei uns. Dabei geht es vor allem um die Verhältnismässigkeit der Evaluationen, die Verwendung der AHV-Nummer in der Statistik und die Verpflichtung zur Antworterteilung. Wir haben unsere Tätigkeiten in diesem Bereich entsprechend weitergeführt.

Allgemein stellen wir fest, dass die Zahl der Bürgeranfragen im statistischen Bereich in den letzten zwei Jahren kontinuierlich gewachsen ist. Vor allem drei Themenbereiche beschäftigen die Bürgerinnen und Bürger:

- Umfang des Fragenkatalogs: Hier wird oft bemängelt, es seien zu viele Fragen, die überdies zu tief in die Privatsphäre eindrängen. Das Bundesamt für Statistik (BFS) publiziert zu jeder Erhebung eine Fülle an Informationen, manchmal auch den Fragenkatalog. Wenn nicht, wird er uns auf Anfrage zugänglich gemacht. Unsere Rolle beschränkt sich in diesem Bereich allerdings auf das Überprüfen der Plausibilität der Fragen.
- Verwendung der AHV-Nummer: Für die Betroffenen besteht hier ein Widerspruch zwischen der genauen Identifizierung der befragten Person und dem nicht personenbezogenen Zweck einer Erhebung von Personendaten in der Statistik. Nebst der Beratung Betroffener haben wir uns im Bereich der Gesetzgebung für eine klarere Regelung eingesetzt (vgl. Ziffer 1.1.3 des vorliegenden Tätigkeitsberichts).
- Verpflichtung zur Antworterteilung: Dies ist der häufigste Grund, weshalb sich Bürgerinnen und Bürger an uns wenden. Bis heute besteht nur im Rahmen der Schweizerischen Arbeitskräfteerhebung (SAKE) und der Strukturerhebung (als Teil der Volkszählung) eine Antwortpflicht. Aufgrund einer parlamentarischen Initiative soll die Verpflichtung zur Antworterteilung im Rahmen der SAKE aufgehoben werden. Wir haben darauf hingewirkt, dass das BFS in Zukunft transparenter über die Freiwilligkeit oder die Verpflichtung zur Teilnahme an einer Erhebung informiert (vgl. Ziffer 1.1.1 des vorliegenden Tätigkeitsberichts).

1.1.3 Verwendung der AHV-Nummer in der Statistik

Die AHV-Nummer spielt in der Statistik eine bedeutende Rolle. Wir haben die rechtlichen Grundlagen für deren Verwendung genauer untersucht.

Anhand des Projekts des Bundesamts für Statistik (BFS) zur Modernisierung der Ausbildungsstatistik haben wir die Verwendung der AHV-Nummer in der Statistik generell genau untersucht. Umstritten war, ob die bestehenden gesetzlichen Grundlagen genügen, damit das BFS Schulen zur Lieferung der AHV-Nummern verpflichten kann. Die Ausgangslage haben wir in unserem 18. Tätigkeitsbericht 2010/2011 unter Ziffer 1.1.3 näher umschrieben.

In unserer Stellungnahme vertreten wir den Standpunkt, dass das BFS nur für indirekte Erhebungen gestützt auf das Registerharmonisierungsgesetz über genügende gesetzliche Grundlagen verfügt. Das BFS hat darauf ein Gutachten erstellen lassen, in welchem der Rechtsgutachter zum gegenteiligen Schluss kam.

Uns ist bewusst, dass die AHV-Nummer als notwendiges Verknüpfungselement eine zentrale Rolle für das BFS spielt. Nur mit diesem Identifikationselement können verschiedene Erhebungen miteinander verknüpft werden. Um die schon für Juristen komplizierte Rechtslage für die Teilnehmenden einer Erhebung einfacher zu gestalten, haben wir uns daher mit dem BFS geeinigt, dass es bei der nächsten Revision des Bundesstatistikgesetzes eine neue Norm schafft. Sie soll die Verwendung der AHV-Nummer für den gesamten Bereich der Statistik regeln.

1.1.4 Theoretische Aspekte der neuen AHV-Nummer

Die neue AHV-Nummer ist seit 2008 in Kraft und ersetzt seither schrittweise die alte. Wir haben uns mit dem Bundesamt für Sozialversicherungen und der Zentralen Ausgleichsstelle in Verbindung gesetzt, um herauszufinden, wie diese neue Nummer zugeteilt und verwendet wird und wer ihre Nutzer sind.

Seit 2008 ist die alte 11-stellige AHV-Nummer schrittweise durch die neue mit 13 Ziffern (AHVN13) ersetzt worden. Für diesen Übergang war die Zentrale Ausgleichsstelle (ZAS) zuständig. Wir setzten uns mit dem Bundesamt für Sozialversicherungen (BSV) und der ZAS in Verbindung, die uns den Prozess der Zuteilung dieser neuen Nummer, ihre Verwendung und die noch bestehenden Probleme erläutert haben.

Beim Übergang von der alten zur neuen AHV-Nummer sind in zwei unterschiedlichen Situationen Probleme aufgetreten. Es kann nämlich vorkommen, dass eine Person mehrere AHV-Nummern besitzt, oder dass dieselbe Nummer verschiedenen Personen zugeteilt wird. Im ersten Fall liegt die Lösung in einer Verschmelzung der Nummern:

Eine Nummer wird ausgewählt und die anderen werden deaktiviert – sie können nicht mehr zugeteilt werden. Im zweiten Fall werden alle Nummern deaktiviert, und den verschiedenen Personen werden neue Nummern zugesprochen.

Derzeit sind 20 Millionen Personen im UPI, dem von der ZAS geführten nationalen Versichertenregister für die AHVN13, eingetragen. Nach Schätzungen der ZAS haben höchstens 1% der Fälle mehr als eine zugeteilte Nummer, während 10´000 bis 20´000 Personen sich eine identische Nummer teilen. Diese letzteren Fälle werden laufend beseitigt, sobald sie entdeckt werden.

Diese problematischen Fälle beruhen zum Teil auf menschlichem Versagen bei der Bereinigung des alten Registers vor der Zuteilung der neuen Nummern, aber auch auf technischen Schwierigkeiten bei der elektronischen Kommunikation zwischen den Bundesregistern und dem UPI. Sie können teilweise auch der Qualität der Register, welche die Daten an das UPI liefern, zugeschrieben werden.

Für verschiedene Organisationen besteht die Möglichkeit, sich bei der ZAS als systematischer Nutzer der AHVN13 anzumelden. Die ZAS kann eine solche Eintragung nicht verweigern. Parallel zur Veröffentlichung der gemeldeten Organisation im online abrufbaren elektronischen Verzeichnis ermittelt jedoch die ZAS, ob der Status als systematischer Nutzer anerkannt ist. Beantragt der Nutzer nachträglich den Zugriff auf das UPI-Register, wird ihm dieser entsprechend seiner Befugnis als systematischer Nutzer gewährt.

Die ZAS stellt systematischen Nutzern Abfrage-Tools zur Verfügung, mit denen Identifikationsdaten ausgehend von einer AHVN13 aufgefunden oder die Nummer einer Person ausgehend von Identifikationsdaten beschafft werden können. Mit Hilfe dieser Tools kann auch die Gültigkeit einer AHVN13 überprüft werden. Um Fehler bei der erneuten Synchronisation zu vermindern, verlangt die ZAS von Drittregistern die Führung der AHV-Nummer in Verbindung mit mindestens fünf weiteren Datenfeldern: Name, Vorname, Geburtsdatum, Geschlecht und Staatsangehörigkeit.

Wir konnten feststellen, dass sich die ZAS der Probleme im Zusammenhang mit der Eindeutigkeit der AHV-Nummer bewusst ist und dass sie die Verwendung dieser Nummer in allen Bereichen nicht unbedingt empfiehlt (vgl. Ziffer 1.3.12 des vorliegenden Tätigkeitsberichts), insbesondere auf sehr heiklem Gebiet wie dem der elektronischen Gesundheitsdienste (eHealth).

1.1.5 Dunkelziffer bei der Jugendgewalt

Im Rahmen einer Ämterkonsultation nahmen wir Stellung zur Einführung einer regelmässigen nationalen Erhebung zur Dunkelziffer im Bereich der Jugendgewalt und -kriminalität.

Im Rahmen einer nationalen Erhebung zur Dunkelziffer bei der Jugendgewalt war vorgesehen, auch zehnjährige Kinder zu befragen. Wir bemängelten in unserer Stellungnahme zum Einen die fehlende Erwähnung der gesetzlichen Grundlagen, auf die sich eine solche Erhebung stützen sollte. Zum Anderen hat die Erhebung nach unserer Ansicht auf freiwilliger Basis zu erfolgen, d.h. die Teilnehmenden müssen nach vorgängiger Information aus freien Stücken einwilligen. Kinder können dies rechtsgenügsam tun, wenn sie bezüglich des Gegenstands der Einwilligung urteilsfähig sind. Angesichts der Menge und der Art von Personendaten, die in der Erhebung bearbeitet werden sollen, vertraten wir aber die Meinung, dass neben dem befragten Kind auch dessen Eltern resp. gesetzliche Vertreter einwilligen müssen. Ebenfalls müssten Dritte (bspw. die Eltern oder andere Verwandte), deren Personendaten bearbeitet würden, vor der Speicherung derselben informiert werden.

1.1.6 Erleichterter Datenaustausch zwischen Bundes- und Kantonsbehörden

Im Oktober 2007 wurde im Nationalrat ein Postulat eingereicht, das den Bundesrat damit beauftragte, Möglichkeiten eines erleichterten Datenaustauschs zwischen Bundes- und Kantonsbehörden zu prüfen. Eine breit angelegte Untersuchung erbrachte den Nachweis, dass an einem allfällig mangelhaften Datenaustausch nicht der Datenschutz Schuld ist.

Verschiedene Vorkommnisse, insbesondere aus dem Umkreis der Sozialfürsorge, haben in den letzten Jahren in breiten Bevölkerungskreisen den Eindruck erweckt, dass der Datenaustausch zwischen Bundes- und Kantonsbehörden zu wünschen übrig lässt. Es wurde wiederholt der Verdacht geäussert, ein rigoroser Datenschutz verhindere in dringlichen Situationen einen kurzfristig notwendigen Datenaustausch. Unter diesem Gesichtspunkt hat Nationalrat Lustenberger am 5. Oktober 2007 ein Postulat eingereicht, das den «Erleichterten Datenaustausch zwischen Bundes- und Kantonsbehörden» forderte. Es beauftragte den Bundesrat zu prüfen, wie besagter Datenaustausch vereinfacht werden könnte. Der Postulant hat die Gefahr eines Missbrauchs in den Bereichen Sozialhilfe, Einbürgerungen, Steuerwesen und Sozialversicherungen als besonders

hoch eingestuft. Er hat es deshalb auch als notwendig erachtet, zu überprüfen, ob der Datenschutz in diesen Bereichen ein Hindernis für einen effizienten Datenaustausch darstelle.

Der Bundesrat hat das Eidgenössische Justiz- und Polizeidepartement (EJPD) mit der Vorbereitung des Berichts beauftragt. Die Federführung lag beim Bundesamt für Justiz (BJ), das eine Arbeitsgruppe eingesetzt hat. Neben je einem Vertreter des Bundesamts für Sozialversicherung (BSV), der Eidgenössischen Steuerverwaltung (EStV), des Bundesamts für Migration (BFM), des Bundesamts für Polizei (fedpol), der Konferenz der kantonalen Sozialdirektorinnen und -direktoren (SODK), der Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD) und je einem kantonalen Vertreter respektive einer Vertreterin aus den Bereichen Einbürgerung, Steuern und Datenschutz wurden jeweils auch unsere für den entsprechenden Fachbereich zuständigen Sachbearbeiter zu den Sitzungen eingeladen.

Im Frühjahr 2009 hat das BJ die Büro Vatter AG beauftragt, den Austausch von Personendaten zwischen Behörden des Bundes, der Kantone und der Gemeinden zu prüfen. Die Studie kam zum Schluss, dass der Datenaustausch hauptsächlich zwischen kantonalen und kommunalen Behörden erfolgt und daher die Einflussmöglichkeit des Bundes beschränkt ist. Der Bundesrat konnte zur Kenntnis nehmen, dass der Datenfluss insgesamt gut funktioniert. Die dazu notwendigen gesetzlichen Grundlagen sind vorhanden und der Datenschutz behindert ihn nicht. Die Studie hat ferner aufgezeigt, dass die ursprünglich bemängelten Schwierigkeiten bei der Informationsbeschaffung nicht auf Datenschutzbestimmungen, sondern vielmehr auf die oft mangelnden Rechtskenntnisse der betroffenen Behördenorgane zurückzuführen sind. Dies führt zu der für uns wichtigen Schlussfolgerung des Berichts, dass eine Revision des Datenschutzgesetzes deshalb nicht notwendig ist.

Die Studie hat aber auch Schwachpunkte im Datenaustausch zwischen den Behörden aufgezeigt. Der Bundesrat ist den Empfehlungen der Studie grossteils gefolgt. Mit Beschluss vom 22. Dezember 2010 hat er sodann dem EJPD, dem Eidgenössischen Departement des Innern (EDI) und dem Eidgenössischen Volkswirtschaftsdepartement (EVD) verschiedene Prüfungsaufträge erteilt. Ende November 2011 hat das BJ im Statusbericht «Erleichterter Datenaustausch zwischen Bundes- und Kantonsbehörden» diese Aufträge und die bisherigen Ergebnisse zusammenfassend dargestellt. Die Umsetzung des Postulats Lustenberger hat uns als Begleitern aufgezeigt, dass der teils grosse Aufwand für den Datenaustausch nicht dem Datenschutz angelastet werden kann.

1.1.7 Thinkdata.ch – ein Instrument zur Sensibilisierung für den Datenschutz und das Öffentlichkeitsprinzip

Wir haben uns an einer von ThinkServices in Genf angeregten Arbeitsgruppe beteiligt. Diese Gruppe hat ein für Organisationen bestimmtes Tool zur Sensibilisierung für den Datenschutz und das Öffentlichkeitsprinzip entwickelt. Dieses in französischer Sprache ausgearbeitete Tool wurde anlässlich des 6. Datenschutztages vorgestellt.

Auf Ersuchen der Genfer Datenschutz- und Öffentlichkeitsbehörde entschlossen wir uns im Januar 2011 zur Teilnahme an der Arbeitsgruppe «Documents, Société, Transparence» (Dokumente, Gesellschaft, Öffentlichkeitsprinzip). Die Gruppe, die sich unter anderem aus Forschern der Universität Genf und der Universität Lausanne, kantonalen und eidgenössischen Datenschutzbehörden und unabhängigen Persönlichkeiten zusammensetzt, trat im Jahr 2011 einmal monatlich zusammen. Das Ziel, auf das sich die Gruppe rasch geeinigt hatte, war die Entwicklung eines für Organisationen bestimmten Tools zur Sensibilisierung für den Datenschutz und das Öffentlichkeitsprinzip.

Es ging darum, sich über die Organisationen im Allgemeinen spezifisch an deren unterschiedliche Akteure, je nach ihrem Aufgabenbereich, zu richten. So wurden vier Gruppen bestimmt: Führungskräfte, Personalverantwortliche, IT-Verantwortliche und Angestellte. Das Tool stellt aus der Warte der Berufe, aber auch nach der Art der Daten unterschiedliche, auf wahren Geschichten beruhende Szenarien vor. Diese Szenarien beschreiben zum Zweck der Sensibilisierung des Nutzers ein Problem im Zusammenhang mit dem Datenschutz oder dem Öffentlichkeitsprinzip. Die Szenarien werden mit Ratschlägen verbunden, damit die Nutzer ihre Position bestimmen und die Datenbearbeitung in ihren Organisationen verbessern können.

Eine erste Version dieses Tools wurde anlässlich des 6. Datenschutztages am 27. Januar 2012 ins Netz gestellt (www.thinkdata.ch).

1.2 Datenschutzfragen allgemein

1.2.1 Datenschutz bei Trauerspenden

In Traueranzeigen wird oft dazu aufgefordert, eine Geldspende zugunsten einer bestimmten Institution zu tätigen. Leiten solche Organisationen Angaben über entsprechende Spenden den Angehörigen weiter, kann es sich um eine Weitergabe von Personendaten handeln. Vorliegend wird erläutert, unter welchen Voraussetzungen eine solche Weitergabe datenschutzrechtlich zulässig ist.

Wird in Traueranzeigen dazu aufgefordert, einer wohltätigen Organisation eine Spende zukommen zu lassen, besteht bei den Trauerfamilien oftmals das Bedürfnis, über die Spender und allenfalls die Höhe der Summe informiert zu werden, um die Spenden verdanken zu können. Wir haben im Rahmen von mehreren Anfragen festgestellt, dass betroffene Organisationen unsicher sind, welche Informationen sie in seinem solchen Fall weitergeben dürfen.

Leitet eine wohltätige Organisation die Namen von Spendern (oder allfällige andere, eine Identifizierung der Spender ermöglichende Angaben) weiter, handelt es sich um eine Weitergabe von Personendaten. Dementsprechend gelten die datenschutzrechtlichen Rahmenbedingungen. Dies bedeutet, dass solche Angaben der Trauerfamilie nur mit Einwilligung der betroffenen Spender mitgeteilt werden dürfen. Da es sich nicht um besonders schützenswerte Personendaten handelt, reicht dabei ein Opt-out. Dies kann beispielsweise umgesetzt werden, indem die Spender auf dem Mitteilungsfeld des Einzahlungsscheins einen Vermerk anbringen können, wenn sie mit einer Weiterleitung nicht einverstanden sind. Bei denjenigen Personen, die von dieser Möglichkeit Gebrauch gemacht haben, dürfen nur unpersönliche Angaben (z.B. die Spendenhöhe) weitergeleitet werden.

Um auch solche Spenden zu verdanken, kann die Trauerfamilie die Dankesschreiben der wohltätigen Organisation übergeben, welche sie an die Spender weiterleitet, ohne deren Identität gegenüber der Trauerfamilie offen zu legen.

1.2.2 Datenschutz in Bibliotheken

Benutzerdaten von Bibliotheken sind weniger harmlos, als sie auf den ersten Blick erscheinen mögen. Zusammengefügt können sie ein aussagekräftiges Persönlichkeitsprofil ergeben. Wir haben daher einen Aufsatz sowie Erläuterungen zum datenschutzkonformen Umgang mit solchen Daten veröffentlicht.

Eine Meldung aus den USA hat vor einigen Jahren die Bibliothekswelt aufgeschreckt: Das «Federal Bureau of Investigation» (FBI) hat im Rahmen des Kampfs gegen den Terrorismus die Herausgabe von Nutzerdaten amerikanischer Bibliotheken verlangt. Spätestens in diesem Moment wurde offensichtlich, dass die vermeintlich harmlosen Daten über ausgeliehene Bücher und Recherchen in Bibliothekscomputern unter Umständen zu einem aussagekräftigen Persönlichkeitsprofil verknüpft werden können. Es drängte sich daher auf, den Umgang mit Personendaten in Bibliotheken zu überprüfen und gegebenenfalls den datenschutzrechtlichen Anforderungen anzupassen.

Wir haben die Einladung zu einer Tagung der Vereinigung juristischer Bibliotheken der Schweiz zum Anlass genommen, die unterschiedlichen Datenbearbeitungen in Bibliotheken zu analysieren und eine Stellungnahme zu einem datenschutzkonformen Umgang mit den dabei anfallenden Personendaten zu erarbeiten. Sie soll insbesondere Antwort darauf geben, wie Bibliotheken die für die Abwicklung ihrer Dienstleistungen notwendigen Personendaten bearbeiten können, ohne dabei unnötigerweise Angaben anzuhäufen, welche zu den besonders heiklen Persönlichkeitsprofilen gebündelt werden können. Der Fokus liegt hierbei auf den Stamm- und Ausleihdaten der Medienausleihe sowie auf die bei der Nutzung öffentlich zugänglicher Computer mit Internetanschluss hinterlassenen Spuren.

Die Stammdaten sind dabei auf die für die Abwicklung der Ausleihe notwendigen Daten zu beschränken und nach Beendigung der «Kundenbeziehung» bzw. nach Ablauf allfälliger gesetzlicher Aufbewahrungsfristen zu löschen. Die Ausleihdaten sind nach der vollständigen Abwicklung eines Ausleihvorgangs zu löschen. Auch in Verbundsystemen dürfen die einzelnen Bibliotheken nur Zugriff auf die Daten derjenigen Nutzer haben, welche in der jeweiligen Bibliothek tatsächlich Bücher ausgeliehen haben.

Werden den Kunden Computer mit Internetanschluss zu Verfügung gestellt, muss einerseits das System so konfiguriert sein, dass die Nutzungsdaten nach Beendigung der Session automatisch gelöscht werden und keine Daten der Vornutzer eingesehen werden können. Andererseits empfehlen wir, die Computer nicht zur anonymen Nutzung zur Verfügung zu stellen. Zur eigenen Sicherheit ist es angebracht, dass sich Nutzer vorab registrieren müssen und dass diese Daten während eines halben Jahres aufbewahrt werden.

Weitere Informationen zu einem datenschutzkonformen Umgang mit Personendaten in Bibliotheken finden sich im erwähnten Aufsatz (www.derbeauftrage.ch unter Dokumentation – Datenschutz – Artikel, Referate, Gutachten unter «Weitere Beiträge») sowie auf unserer Webseite www.derbeauftragte.ch unter Themen – Datenschutz – sonstige Themen.

1.2.3 Befreiung von der Gebührenpflicht für Radio und Fernsehen

Die Billag AG hat zusammen mit den Sozialversicherungen per 1. Januar 2011 ein datenschutzkonformes Vorgehen für die Gebührenbefreiung von Ergänzungsleistungsbezügern eingeführt. Neu genügt es, wenn die betroffenen Personen eine Bestätigung ihrer Sozialversicherung einreichen.

Im 17. Tätigkeitsbericht 2009/2010 haben wir in Ziffer 1.2.9 festgehalten, dass es unverhältnismässig sei, zur Gebührenbefreiung einen rechtskräftigen Entscheid über den Anspruch auf Ergänzungsleistungen samt deren Höhe zu verlangen. Die Billag AG hat in der Folge zusammen mit den Sozialversicherungen eine standardisierte Bestätigung ausgearbeitet. Darin wird lediglich der Bezug von Ergänzungsleistungen ausgewiesen, ohne deren Höhe auszuführen. Seit dem 1. Januar 2011 stellen die Sozialversicherungen diese Bescheinigung zuhanden der Billag AG aus und geben sie an die Bezüger ab.

1.2.4 Videoüberwachung beim öffentlichen Verkehr

Gestützt auf das Personenbeförderungsgesetz haben wir bei fünf Transportunternehmen Kontrollen der Videoüberwachung vorgenommen. Unabhängig davon hielt das Bundesamt für Justiz fest, dass wir für die Beurteilung der Rechtmässigkeit zuständig seien, soweit die Videoüberwachungsmassnahmen die konzessionierte Tätigkeit betreffen.

Auf den 1. Januar 2010 traten das Personenbeförderungsgesetz sowie das revidierte Eisenbahngesetz in Kraft. Danach unterstehen Unternehmen des öffentlichen Verkehrs sowohl für ihre konzessionierten und bewilligten Tätigkeiten als auch für privatrechtliches Handeln dem Bundesgesetz über den Datenschutz. Die Aufsicht obliegt dabei uns. Die Videoüberwachung wird zudem in beiden Gesetzen sowie in der Verordnung über die Videoüberwachung im öffentlichen Verkehr ausdrücklich geregelt (vgl. unseren 18. Tätigkeitsbericht 2010/2011, Ziff. 1.2.3). Da sie im öffentlichen Verkehr vermehrt eingesetzt wird, haben wir uns entschieden, bei verschiedenen konzessionierten Transportunternehmen Kontrollen durchzuführen.

Wir überprüften die Videoüberwachung in den Fahrzeugen (Zügen, Trams, Busse), an Bahnhöfen/Haltestellen und in Infrastrukturanlagen (Gebäude, Depots). Unsere fünf Kontrollen ergaben, dass die betreffenden Unternehmen die Videoüberwachung gut umgesetzt haben und die datenschutzrechtlichen Aspekte ernst nehmen. Sie weisen überall mittels Piktogrammen auf die Videoüberwachung hin und regeln Verantwortlichkeiten, Zugriffe, Datenflüsse, Aufbewahrungsdauer und Voraussetzungen der Weitergabe der Bilder klar. Die Auswertung erfolgt nur durch bestimmte Personen, in einem separaten Raum auf gesicherten Computern und nur bei einem Vorfall bzw. Schadensfall. Tritt dieser ein, werden die entsprechenden Bilder ausgewertet, auf einem separaten Datenträger (USB-Stick oder CD-Rom) gespeichert und den Strafverfolgungsbehörden übergeben.

Dagegen hat noch keines der kontrollierten Unternehmen ein schriftliches Konzept für die Behandlung von Auskunftsgesuchen ausgearbeitet. In der Praxis hat aber auch noch niemand ein solches Auskunftsgesuch betreffend die Videoüberwachung gestellt. Daher wurden die Bilder bisher ausschliesslich aufgrund von Vorfällen bzw. Schadensfällen ausgewertet. Wir wiesen die Unternehmen darauf hin, dass ein solches Konzept nicht kompliziert sein müsse. Die Person, die ihr Auskunftsrecht geltend macht, muss sich ausweisen und Datum, Zeit und Ort angeben, an welchen sie sich im Aufnahmebereich einer vom Unternehmen betriebenen Kamera befunden hat (vgl. auch unser Musterschreiben unter www.derbeauftragte.ch, Dienstleistungen – Datenschutz – Musterbriefe – Videoüberwachung). Die Auswertung der Bilder kann sodann gleich wie im Ereignisfall erfolgen. Sollten die Bilder bereits überschrieben worden sein, ist die betroffene Person unter Angabe der Aufbewahrungsfristen entsprechend zu informieren. Die Aufnahmen, zwischen denen je nach Fall auch ein paar Minuten liegen können, werden der betroffenen Person entweder ausgedruckt, auf CD-Rom oder als Filmsequenz bekannt gegeben. Wichtig ist, dass vor der Bekanntgabe sämtliche Drittpersonen unkenntlich gemacht oder gelöscht werden. Das Unternehmen kann im Konzept diese verschiedenen Bekanntgabemöglichkeiten auflisten und darauf hinweisen, dass im konkreten Fall über die genauen Modalitäten entschieden wird.

Bei unseren fünf Kontrollen mussten wir keine Empfehlung erlassen, machten jedoch gegenüber den einzelnen Unternehmungen wo nötig Verbesserungsvorschläge, bspw. betreffend das oben erwähnte Konzept. Weitere Verbesserungsvorschläge betrafen unter anderem die Erstellung eines schriftlichen Videoüberwachungsreglements, die bessere Absicherung der Tür zu einem Serverraum und die sichere Gestaltung von Passwörtern. Die Unternehmen haben diese Verbesserungsvorschläge angenommen.

In Zusammenhang mit den neuen gesetzlichen Regelungen stellte Privatim, die Vereinigung der kantonalen Datenschutzbeauftragten, dem Bundesamt für Justiz (BJ) verschiedene Fragen zur Abgrenzung unserer Zuständigkeiten gegenüber der ihrigen

sowie zum anwendbaren Recht. Dies, nachdem das BJ in einem Gutachten im Dezember 2010 festgehalten hatte, dass die Bestimmung im Personenbeförderungsgesetz, die die Regelung und die Aufsicht des Datenschutzes beim Bund belässt, verfassungskonform sei. In seiner Antwort an Privatim wies das BJ darauf hin, dass im Einzelfall zu entscheiden sei, was zu den konzessionierten und bewilligten Tätigkeiten gehöre. Soweit die Videoüberwachung eines Tramdepots oder einer Haltestelle solche Tätigkeiten betreffe, richte sich die Beurteilung der Rechtmässigkeit der Massnahme nach dem Bundesgesetz, und der EDÖB sei für die Aufsicht zuständig. Dagegen richteten sich die datenschutzrechtlichen Aspekte des Arbeitsverhältnisses grundsätzlich nach den kantonalen Vorgaben.

1.2.5 Datenaustausch über Schwarzfahrer

Aufgrund einer beim Bundesamt für Verkehr eingereichten aufsichtsrechtlichen Beschwerde prüften wir die Frage, ob es datenschutzrechtlich zulässig ist, wenn Transportunternehmen ihre Daten über Fahrgäste austauschen, die ohne gültigen Fahrausweis unterwegs waren und erwischt wurden.

In Zusammenhang mit einer aufsichtsrechtlichen Beschwerde bat uns das Bundesamt für Verkehr (BAV), den datenschutzrechtlichen Aspekt näher zu prüfen. Dabei ging es um die Frage, ob es zulässig ist, wenn die Transportunternehmen PostAuto, SBB, Thurbo und VBZ ihre Daten über Schwarzfahrer austauschen. Unsere Abklärungen ergaben Folgendes:

Unternehmen, die eine Konzession nach dem Bundesgesetz über die Personenbeförderung haben, müssen Tarife erstellen, die gegenüber allen gleich anzuwenden sind. Reisende, die keinen gültigen Fahrausweis vorweisen, haben einen Zuschlag zu bezahlen; er kann erhöht werden, wenn die betroffene Person zum wiederholten Mal ohne gültiges Billet erwischt wird.

Gestützt auf diese gesetzlichen Grundlagen hat der Zürcher Verkehrsverbund (ZVV) einen Datenpool geschaffen. Dieser ZVV-Datenpool ist eine verbundweite, zentral geführte Datenbank, in der die von den Inkassostellen (SBB, VBZ, PostAuto, Thurbo) erfassten und pendenten Schwarzfahrerdaten abgeglichen werden und auf welche diese Stellen Zugriff haben. Zweck dieses Datenpools ist die einheitliche Durchsetzung des Tarifs und die rechtsgleiche Behandlung der Fahrgäste im Verbund. Seine Grundlage bildet die «Richtlinie über den Datenschutz für die Erhebung von Gebühren sowie die Erfassung von Personendaten und deren Aufbewahrung und Verwendung im ZVV-Datenpool bei Fahren ohne gültigen Fahrausweis». Der Datenpool bezieht sich zudem einzig auf das Gebiet des ZVV.

Im vorliegenden Fall hatten sowohl die SBB als auch die VBZ die über die beschwerdeführende Person erhobenen Daten im ZVV-Datenpool erfasst. Die SBB erhebt die Daten der ohne gültigen Fahrausweis angetroffenen Personen und erledigt das Inkasso sowohl in ihrem eigenen Interesse als auch als beauftragte Datenbearbeiterin für andere Transportunternehmen des ZVV. Die SBB geben dem Datenpool ausschliesslich Daten bekannt, die sie im Rahmen der Abwicklung des Kontrollauftrages des ZVV erhoben haben. So hat im vorliegenden Fall die SBB die Kontrolle in der Zürcher S-Bahn im Auftrag des ZVV getätigt und die Daten in den Pool eingespeist. Unabhängig davon hat auch die VBZ als Inkassostelle die Daten derselben Person in den ZVV-Datenpool eingespeist. Beide Unternehmen, SBB und VBZ, haben einen klar definierten Zugriff auf diesen Pool, und die Daten werden zwei Jahre nach dem jeweiligen Vorfall gelöscht.

Es ist klar ersichtlich, dass im vorliegenden Fall die Daten zur einheitlichen Durchsetzung des Tarifs und also gemäss den erwähnten Vorgaben im ZVV-Datenpool erfasst worden sind. Somit hat datenschutzrechtlich keine unzulässige Datenbekanntgabe stattgefunden.

1.2.6 Videoüberwachung durch Private im öffentlichen Raum

Was tun, wenn sich auf der Strasse vor dem eigenen Grundstück immer wieder verdächtige Personen aufhalten oder der Vorgarten zur Mülldeponie wird? Als vermeintlich einfache Lösung bietet es sich an, eine Videokamera zu installieren, welche die Strasse vor dem Garten überwacht. Dies ist mit wenigen Ausnahmen jedoch unzulässig. Wir haben dazu ergänzende Informationen zu unserem Merkblatt «Videoüberwachung durch private Personen» veröffentlicht.

Videoüberwachungen zu Sicherheitszwecken haben sich in der Schweiz längst etabliert. Immer häufiger werden auf Grundstücken Kameras montiert, welche vor unerwünschten Besuchern schützen und im Falle von Sachbeschädigungen, Einbrüchen und dergleichen bei der Täterfindung helfen sollen. Oft besteht dabei das Bedürfnis, den öffentlichen Raum vor dem privaten Grundstück mit zu überwachen. Damit wird aber in die Persönlichkeitsrechte einer Vielzahl von Personen eingegriffen. So haben sich in letzter Zeit Anfragen von Betroffenen gehäuft, die auf öffentlichem Grund von solchen privaten Videokameras erfasst worden sind. Diese Bürgerinnen und Bürger fühlen sich durch die Kameras gestört, in ihrer Bewegungsfreiheit eingeschränkt und stellen zu Recht die Frage, ob eine solche Überwachung zulässig ist.

Es ist grundsätzlich Sache der Polizei, für Sicherheit und Ordnung auf öffentlichem Grund zu sorgen. Besteht auf einem Grundstück ein Sicherheitsproblem, welches vom öffentlichen Grund ausgeht, muss daher als erste Massnahme die Polizei kontaktiert

werden. Für private Videoüberwachungsanlagen auf öffentlichem Grund bleibt damit in der Regel kein Platz. Genaueres hierzu und zu den möglichen Ausnahmen kann in unseren ergänzenden Informationen zum Merkblatt «Videoüberwachung durch private Personen» auf www.derbeauftrage.ch unter Themen – Datenschutz – Videoüberwachung nachgelesen werden.

1.2.7 Varianten der datenschutzkonformen Speicherung biometrischer Daten

Nach dem Urteil im Fall KSS, wonach eine rein zentrale Speicherung biometrischer Daten im Freizeitbereich unverhältnismässig sei, stellt sich die Frage, wie solche Daten gespeichert werden dürfen, um den datenschutzrechtlichen Anforderungen zu genügen. Wir haben verschiedene Varianten geprüft und die Ergebnisse auf unserer Webseite veröffentlicht. Diese Varianten sollen einerseits den unterschiedlichen Bedürfnissen von Systembetreibern gerecht werden, andererseits die Persönlichkeitsrechte der betroffenen Personen wahren.

Biometrische Daten sind besondere Personendaten. Sie erlauben die Identifikation einer Person aufgrund ihrer vom eigenen Körper produzierten Merkmale, die weder frei ausgewählt noch ausgewechselt oder leicht abgeändert werde können. Daher gefährdet jeder Missbrauch biometrischer Merkmale die Persönlichkeit der Betroffenen besonders stark. Im Umgang mit solchen Daten sind also strenge Anforderungen in Bezug auf den Datenschutz und die Datensicherheit einzuhalten. Dies hat im Entscheid KSS auch das Bundesverwaltungsgericht erkannt und eine einfache zentrale Speicherung biometrischer Daten im Freizeitbereich ohne weitere Sicherheitsmassnahmen für unverhältnismässig erklärt.

Biometrische Erkennungssysteme werden auch im Freizeitbereich immer häufiger eingesetzt. Der Entscheid des Bundesverwaltungsgerichts wirft daher die Frage auf, wie diese Daten gespeichert werden können, ohne die Persönlichkeitsrechte der betroffenen Menschen zu verletzen. Wir haben mehrere Varianten geprüft und dabei ein besonderes Augenmerk auf die verschiedenen Bedürfnisse der Systembetreiber, insbesondere auf die einfache Umsetzung in der Praxis, gelegt. Wir sind dabei zum Schluss gelangt, dass beim Einsatz biometrischer Erkennungssysteme im Freizeitbereich die folgenden Erfordernisse immer und zwingend erfüllt sein müssen, um dem besonders hohen Risiko einer Persönlichkeitsverletzung Rechnung zu tragen:

- Solche Systeme dürfen nur mit der Einwilligung der betroffenen Personen zum Einsatz gelangen. Mit anderen Worten müssen alle Betroffenen über die Anlage

angemessen informiert werden und es muss eine gleichwertige Alternative ohne die Verwendung biometrischer Merkmale zur Auswahl stehen.

- Biometrische Rohdaten enthalten mehr Informationen zur jeweiligen Person als Templates (codiert gespeicherte biometrische Rohdaten) und lassen unter Umständen Aussagen über den Gesundheitszustand oder die Rassenzugehörigkeit einer Person zu. Da für biometrische Erkennungssysteme diese Informationsmenge nicht notwendig ist, müssen Templates anstelle von Rohdaten verwendet werden.
- Um das Risiko einer unautorisierten Verwendung zu minimieren, müssen die Templates zudem verschlüsselt gespeichert werden.

Für die weitere Konzeption eines biometrischen Erkennungssystems im Freizeitbereich sehen wir drei Möglichkeiten:

- Die biometrischen Daten werden dezentral auf einem Datenträger gespeichert, der sich im Besitz des jeweiligen Kunden befindet. Damit ist gewährleistet, dass der Betroffene die Herrschaft über seine biometrischen Daten behält, also diese nicht ohne seine bewusste Mitwirkung verwendet werden können. Diese Variante setzt die Anforderungen des Datenschutzes am besten um und ist daher zu bevorzugen.
- Die biometrischen Daten werden zentral gespeichert. Der Bezug zu weiteren Personendaten ist aber nur mit Hilfe eines Zuordnungscodes möglich, der auf einer Karte gespeichert ist, die sich im Besitz des Betroffenen befindet. Damit verlassen die biometrischen Daten zwar seinen Herrschaftsbereich; da der Bezug zu weiteren Daten des Betroffenen jedoch nicht ohne sein bewusstes Mitwirken hergestellt werden kann, sind die Möglichkeiten eines Missbrauchs stark eingeschränkt.
- Die biometrischen Daten werden zentral gespeichert. Der Bezug zu weiteren Personendaten besteht nicht und kann auch nachträglich nicht hergestellt werden. Es dürfen dabei nur biometrische Charakteristika ohne Spuren verwendet werden (z.B. Finger- oder Handvenenmuster, Handkontur, nicht aber Fingerabdrücke; vgl. dazu unseren unten genannten Leitfaden). Da kein Bezug zu weiteren Personendaten existiert, sind die Möglichkeiten eines Missbrauchs stark eingeschränkt. Durch die Verwendung biometrischer Charakteristika ohne Spuren wird zudem sichergestellt, dass die biometrischen Merkmale nicht ohne Wissen der betroffenen Personen erhoben und verwendet werden können.

Genaueres hierzu kann der Ergänzung zu unserem Leitfaden zu biometrischen Erkennungssystemen unter www.derbeauftragte.ch unter Dokumentation – Datenschutz – Leitfäden entnommen werden.

1.2.8 Biometrisches Erkennungssystem für die Reservation von Sportplätzen: Abschluss des Verfahrens

Ein Tennisclub hat ein Reservationssystem mit biometrischer Personenerkennung eingeführt. Unsere Kontrolle vor Ort hat ergeben, dass das System angepasst werden muss, um den datenschutzrechtlichen Anforderungen zu genügen. Der Tennisclub hat unsere Empfehlung akzeptiert und setzt zurzeit die verlangten Änderungen um.

Wir haben bereits im letzten Jahr bei unserer Kontrolle des Reservationssystems festgestellt, dass es die datenschutzrechtlichen Anforderungen in einigen Punkten nicht erfüllt (siehe unseren 18. Tätigkeitsbericht 2010/2011, Ziffern 1.2.6 und 4.1.2). So wurden die Clubmitglieder über die Datenbearbeitung im Rahmen des biometrischen Erkennungssystems zu wenig gut informiert, das System war ohne Zugangsbeschränkung auf der Webseite des Clubs frei zugänglich, es waren keine Löschfristen für die Mitgliederangaben (inkl. der biometrischen Daten) definiert und die Mittel zur Gewährleistung der physischen oder logischen Datensicherheit waren nicht ausreichend. Insbesondere wurden aber auch die Fingerabdruckdaten ohne weitere Sicherheitsmassnahmen zentral gespeichert, was gemäss Urteil des Bundesverwaltungsgerichts in Sachen KSS unverhältnismässig ist.

Der Tennisclub stimmt mit uns überein, dass sein bisheriger Umgang mit biometrischen Daten nicht den datenschutzrechtlichen Anforderungen entspricht. Da dies jedoch ohne schlechte Absichten geschehen sei und der Club die Persönlichkeitsrechte seiner Mitglieder wahren möchte, hat er unsere Empfehlungen vollumfänglich akzeptiert. Die Information an die Mitglieder wurde stark verbessert, die Webseite datenschutzkonform ausgestaltet, Löschfristen wurden definiert und diverse Massnahmen zur Verbesserung der Datensicherheit bereits umgesetzt. Auf den Beginn des nächsten Clubjahres wird zudem das bisherige Reservationssystem so umgestaltet, dass die biometrischen Daten künftig auf einer Karte gespeichert sind, welche sich im Besitz des jeweiligen Mitglieds befindet (vgl. die Ergänzung zu unserem Leitfaden zu biometrischen Erkennungssystemen auf unserer Webseite www.derbeauftragte.ch unter Dokumentation – Datenschutz – Leitfäden). Damit werden ab Umstellung des Systems beim Tennisclub keinerlei biometrische Daten mehr zentral gespeichert, womit die Mitglieder die Kontrolle über ihre biometrischen Daten zurückerhalten.

Mit diesen Anpassungen erfüllt der Tennisclub unsere Forderung nach einem verhältnismässigen und damit datenschutzkonformen Einsatz biometrischer Erkennungssysteme vollständig, so dass das Verfahren erfolgreich abgeschlossen werden kann.

1.2.9 Zentrale Speicherung von Kundenfotos bei Skistationen

Im Rahmen der Sachverhaltsabklärung bei einer Skistation haben wir das Zutrittssystem eines bekannten Herstellers einer vertieften Kontrolle unterzogen. Dabei hat sich gezeigt, dass das System die datenschutzrechtlichen Anforderungen grösstenteils erfüllt, für die zentrale Speicherung der Kundenfotos im Bereich der Datensicherheit aber noch Verbesserungen notwendig sind.

In der Schweiz verwenden viele Skistationen für die Zutrittskontrolle Systeme desselben Herstellers. Nachdem im Rahmen einer Sachverhaltsabklärung bei einer Schweizer Skistation Fragen bezüglich der Datenschutzkonformität ihres Systems aufgetaucht sind, haben wir mit dem Hersteller Kontakt aufgenommen, um seine Produkte gemeinsam zu analysieren und allfällige Verbesserungen zentral bei ihm umzusetzen. Dabei konnten wir feststellen, dass das System die meisten datenschutzrechtlichen Prinzipien berücksichtigt, sofern die Skistationen es richtig konfiguriert haben. Die Einstellungen können nämlich so vorgenommen werden, dass nur die notwendigen Angaben der Kundinnen und Kunden erhoben, sie nur so lange wie nötig gespeichert und die Zugriffsrechte auf einzelne Datenkategorien restriktiv geregelt werden. Das System ist zudem übersichtlich, so dass falsche Daten einfach korrigiert oder gelöscht werden können. Damit kann die Anlage so betrieben werden, dass die Datenbearbeitung verhältnismässig ist und die Datenrichtigkeit gewährleistet werden kann. Es hängt also von den jeweiligen Skistationen ab, ob die Systeme datenschutzkonform betrieben werden.

Einzig betreffend die Datensicherheit haben wir festgestellt, dass insbesondere der Schutz der Fotodaten noch angepasst werden muss. Das System ist zwar so konzipiert, dass die Daten nicht ohne weiteres ausgelesen und für andere Zwecke verwendet oder gar entwendet werden können. Angesichts der Tatsache, dass die Fotodatenbank aber auch besonders schützenswerte Personendaten enthalten kann, muss dieser Schutz noch verbessert werden. Wir sind zurzeit daran, mit dem Hersteller zu prüfen, welche Massnahmen bei künftigen Systemen umgesetzt werden können, um die datenschutzrechtlichen Anforderungen vollumfänglich zu erfüllen.

1.2.10 Bearbeitung von Personendaten anlässlich von Sportveranstaltungen

Im Rahmen von Anlässen des Breitensports werden die Personendaten von Teilnehmenden verschiedenen Bearbeitungen unterzogen. Wir haben daher einen Dienstleistungsanbieter der Branche einer Sachverhaltsabklärung unterzogen. Dabei wurden sowohl seine eigenen Datenbearbeitungen als auch die für die Veranstalter der Sportevents angebotene Benutzeroberfläche betrachtet.

Grundsätzlich brauchen Veranstalter eines Sportanlasses einen Rechtfertigungsgrund für die Bearbeitung von Personendaten. Für die Teilnehmenden ist bei der Anmeldung offensichtlich, dass ihre Daten im Rahmen der Veranstaltung zur Aufbereitung der Startliste, Zustellung von Informationen und Startnummer, Erstellung der Ranglisten für den Aushang, Siegerehrung, Berichterstattung in den Medien sowie für Speaker-Durchsagen bearbeitet werden. Diese Verwendungen sind durch das private Interesse der Veranstalter und das öffentliche Interesse am Sportanlass gerechtfertigt.

Eine Datenbekanntgabe durch den Veranstalter im Internet, etwa in Form einer Publikation von Startlisten, Ranglisten oder einer Verknüpfung mit Veranstaltungsfotos, liegt jedoch in der Regel nicht auf der Hand. Daher muss über diese Art der Bekanntgabe bei der Anmeldung informiert werden. Ein entsprechender Hinweis kann in der Datenschutzerklärung erfolgen oder sich aus dem Beschrieb der im Startgeld enthaltenen Leistungen ergeben. Die betroffene Person muss jedoch die Möglichkeit haben, einer solchen Publikation ihrer Daten im Internet zu widersprechen.

Ebenso ist die Weitergabe der Personendaten durch den Veranstalter an Dritte, bspw. an Fotografen, die nach der Veranstaltung Bilder der Teilnehmenden verkaufen, oder an Firmen, die Werbezwecke verfolgen, ohne vorgängige Information nicht zulässig. Hier genügt jedoch ein Hinweis im Reglement resp. in der Datenschutzerklärung nicht, da diese Art der Datenbearbeitung im Rahmen einer Sportveranstaltung ungewöhnlich ist. Nötig ist eine gültige Einwilligung der Teilnehmenden; sie setzt voraus, dass bei der Anmeldung explizit auf die Weitergabe der Personendaten, den Zweck der Weitergabe sowie die Widerspruchsmöglichkeiten hingewiesen wird.

Wir halten deshalb fest, dass der Veranstalter auf dem Anmeldeformular bzw. in der Onlineanmeldung die vorgesehenen Bearbeitungszwecke transparent und umfassend darstellen und allfällige Dritte, denen die Daten bekannt gegeben werden sollen, benennen muss. Weiter muss er den Teilnehmenden die Möglichkeit geben, die Bekanntgabe ihrer eigenen Personendaten (im Internet, in Zeitungen, an Dritte etc.) zu

verbieten. Dies kann etwa durch Ankreuzen eines entsprechenden Kästchens auf dem Formular oder die Angabe einer Kontaktmöglichkeit (E-Mail, Telefon etc.), über welche der Teilnehmer sein Widerspruchsrecht geltend machen kann, geschehen.

Die den Veranstaltern angebotene Administrationsoberfläche fördert die verhältnismässige Datenbearbeitung. So hat der Dienstleister die im System erfassten Personendaten auf die für die Organisation der Veranstaltung notwendigen begrenzt. Dazu gehört auch die Löschung der freiwillig für veranstaltungsrelevante SMS angegebenen Telefonnummern nach Veranstaltungsende. In Bezug auf die Datenbanken wird den Veranstaltern eine Lösung angeboten, welche eine klare Trennung der einzelnen Datenbestände beinhaltet und ihnen ermöglicht, die notwendigen Informationen aufzubereiten. Weiter ist die Generierung von Listen auf die zur Durchführung der Veranstaltung notwendigen Informationen beschränkt. Für die den Veranstaltern gehörenden Personendaten ist der Auskunfts- und Löschungsprozess noch anzupassen, falls die Begehren fälschlicherweise an den Dienstleister gerichtet werden.

1.2.11 Veröffentlichung von Hooliganbildern durch einen Fussballclub

Ein Fussballclub ist nicht berechtigt, auf seiner Internetseite Fotos von angeblichen «Petardenwerfern» zu veröffentlichen, auch nicht verbunden mit der Aufforderung, allfällige Angaben zu den abgebildeten Personen zu melden. Eine solche Öffentlichkeitsfahndung ist, bei Vorliegen der entsprechenden Voraussetzungen, ausschliesslich Aufgabe der Polizei.

Ein Fussballclub veröffentlichte auf seiner Internetseite Fotos von zwei Personen mit der Aufforderung an die Betrachter, allfällige Hinweise zu den Abgebildeten (einem angeblichen Petardenwerfer und seinem Helfer) per Mail zu melden. Die Männer konnten rasch identifiziert werden, worauf die Bilder wieder entfernt wurden.

Wir wiesen den Fussballclub darauf hin, dass er nicht berechtigt sei, Fotos wie beschrieben zu veröffentlichen. Es fehlt unseres Erachtens dafür ein Rechtfertigungsgrund im Sinne des Datenschutzgesetzes, da weder die Einwilligung der betroffenen Person noch ein überwiegendes privates oder öffentliches Interesse noch ein Gesetz vorliegt. Vielmehr muss der Fussballclub die Fotos verbunden mit einer Strafanzeige der Polizei übergeben. Diese ihrerseits muss dann prüfen, ob die Voraussetzungen einer Veröffentlichung auf ihrer Internetseite gegeben sind, wie dies beispielsweise die Stadtpolizei Zürich in Zusammenhang mit einer entsprechenden Öffentlichkeitsfahndung gemacht hat.

1.2.12 Formular für die vertrauensärztliche Kontrolluntersuchung

Die vertrauensärztliche Kontrolluntersuchung zur Verkehrstauglichkeit sowie die entsprechenden Formulare sind auf Bundesebene geregelt. Dagegen ist für die Beurteilung der Datenbearbeitung durch das kantonale Strassenverkehrsamt die kantonale Datenschutzbehörde zuständig.

In Zusammenhang mit den verkehrsmedizinischen Kontrolluntersuchungen hatten wir verschiedene Anfragen. Diese Untersuchungen sind auf Bundesebene, nämlich in der Verordnung über die Zulassung von Personen und Fahrzeugen zum Strassenverkehr (VZV) geregelt. Artikel 27 der Verordnung legt fest, wer sich einer solchen vertrauensärztlichen Kontrolle unterziehen muss. Darunter fallen insbesondere alle Autofahrer ab dem 70. Altersjahr. Das Formular in Anhang 2 der VZV führt diejenigen Punkte auf, die Teil der Untersuchung sind. Dagegen ist das Ergebnis der kantonalen Behörde mit einem Formular nach Anhang 3 VZV bekannt zu geben (Art. 27 Abs. 3 VZV). Zuständig für die Beurteilung, ob das kantonale Strassenverkehrsamt mit diesen Daten korrekt umgeht, ist die entsprechende kantonale Datenschutzbehörde.

1.2.13 Kontrollen betreffend die Ausarbeitung der Bearbeitungsreglemente in der Bundesverwaltung

Im Rahmen unserer Aufsichtstätigkeit kontrollierten wir über zwanzig Bundesämter auf die Einhaltung ihrer gesetzlichen Pflicht, ein Bearbeitungsreglement für bestimmte Datensammlungen vorzulegen. Dabei traten erhebliche Lücken zutage. Dies bot uns die Gelegenheit, die Datenschutzberater der betroffenen Bundesämter auf ihre gesetzlichen Pflichten und auf unsere Erläuterungen zur Ausarbeitung eines solchen Bearbeitungsreglements hinzuweisen.

Im vergangenen Tätigkeitsjahr überprüften wir über zwanzig Bundesämter auf die Einhaltung ihrer gesetzlichen Pflicht zur Ausarbeitung eines Bearbeitungsreglements für Datensammlungen, die den Kriterien von Artikel 21 Absatz 1 der Verordnung zum Datenschutzgesetz (VDSG) entsprechen. Der Artikel schreibt vor, dass die Bundesorgane ein Bearbeitungsreglement für automatisierte Datensammlungen zu erstellen haben, namentlich wenn diese besonders schützenswerte Daten oder Persönlichkeitsprofile beinhalten oder durch mehrere Bundesorgane benutzt werden.

Bei dieser Kontrolle ging es darum, das Vorhandensein von Bearbeitungsreglementen zu überprüfen und nicht, uns zu deren Inhalt zu äussern. Wir kontrollierten rund

dreissig Datensammlungen und stellten generell fest, dass die Pflicht zur Erstellung eines Bearbeitungsreglements oft gar nicht bekannt ist. So gab es vielfach überhaupt keine Reglemente, oder sie waren vor mehreren Jahren verfasst und seither nicht mehr aktualisiert worden. Andere Datensammlungen waren weiterhin in unserem Register gemeldet, obwohl sie gar nicht mehr existierten. Wir nahmen daher diese Kontrolle zum Anlass, die Datenschutzberater der betroffenen Bundesämter auf ihre gesetzlichen Verpflichtungen hinzuweisen, und machten sie auf unsere Erläuterungen zum Thema Bearbeitungsreglement aufmerksam, die wir auf unserer Webseite www.edoeb.admin.ch, unter Dokumentation – Datenschutz – Leitfäden – Technische und organisatorische Massnahmen, veröffentlicht haben. Ausserdem erinnerten wir sie daran, dass unabhängig von der genannten gesetzlichen Verpflichtung jegliche Einrichtung eines Informationssystems in der Bundesverwaltung schon in der Phase der Voranalyse zu jedem Informatikprojekt die Ausarbeitung eines Bearbeitungsreglements erfordert, wie es das Hermes-Verfahren klar vorsieht (vgl. Handbuch Hermes, Punkt 3.3.4, Systemadaptation; bzw. Punkt 3.3.3, Systementwicklung).

Unsere Kontrolle bewirkte eine wichtige Sensibilisierung für die aufgedeckten Mängel, verfügten doch zu Beginn unserer Kontrolle nur zehn der 34 kontrollierten Datensammlungen über ein Bearbeitungsreglement, während nach Abschluss der Kontrolle sämtliche Datensammlungen, die den Kriterien von Art. 21 VDSG entsprechen, mit einem solchen Reglement versehen waren.

1.2.14 Anforderungen an ein Bearbeitungsreglement

Das Bearbeitungsreglement wird bereits in den Planungsphasen eines Projektes erstellt und in der Systembetriebsphase nachgeführt. Für die Nachführung benötigt die jeweils verantwortliche Person die entsprechenden Informationen, namentlich über Systemänderungen und die durchgeführten Kontrollen.

Das Reglement soll für Transparenz im Umfeld des Datenschutzes und der Daten- bzw. Informationssicherheit sorgen. Die erste Version des Bearbeitungsreglements ist Ende der Projektplanungsphasen verfügbar. Es wird in der Folge während des Systembetriebs nachgeführt. In der Betriebsphase sind insbesondere sowohl Systemänderungen als auch die Durchführung von Kontrollen und deren Erkenntnisse zu dokumentieren. Dabei gilt es zu beachten, dass eine solche Dokumentation nur dann nachgeführt werden kann, wenn die Person, welche das Reglement erstellt und in der Folge ergänzt, die notwendigen Informationen erhält.

Unsere Anforderungen an ein Bearbeitungsreglement finden sich auf unserer Webseite www.derbeauftragte.ch unter Dokumentation – Datenschutz – Leitfäden

– Technische und organisatorische Massnahmen in der Spalte rechts. In Hermes, dem Standard der Schweizerischen Bundesverwaltung für die Führung und Abwicklung von Projekten der Informations- und Kommunikationstechnik, wird schon im Stadium der Voranalyse mehrmals auf das Datenschutzbearbeitungsreglement hingewiesen. Das Bearbeitungsreglement ist eine verständliche Zusammenfassung wichtiger Punkte aus Sicht des Datenschutzes und der Informationssicherheit. Wurden noch detailliertere Informationen ausgearbeitet (bspw. Sicherheitskonzept, detaillierte Dokumentation der Prozesse), so ist – nach einer Zusammenfassung im Reglement – auf diese zu verweisen. Das Bearbeitungsreglement ist in möglichst kurzer und verständlicher Form zu führen, so dass das System auch von Nicht-Experten verstanden bzw. beurteilt werden kann.

1.3 Internet und Telekommunikation

1.3.1 Geolokalisierung mit mobilen Geräten

Mittels mobilen Geräten werden Geopositionsdaten für standortbezogene Dienste erhoben. Werden diese Daten über einen längeren Zeitraum gespeichert, ergeben sie ein detailliertes Bewegungsprofil der Gerätebenutzer. Wir haben daher im Rahmen einer Sachverhaltsabklärung die entsprechenden Datenbearbeitungen von Apple analysiert, derweil Apple von sich aus ein Update der Software zur Verfügung gestellt hat, mit dem die Erfassung von Geopositionsdaten unterbunden werden kann.

Im Frühjahr 2011 wurde bekannt, dass die mobilen, mit iOS betriebenen Geräte Geopositionsdaten speichern, an Apple senden und zudem auf den zur Synchronisierung eingesetzten Computern ablegen. Da die Sammlung von Positionsdaten zu einer Person resp. zu einem Gerät eine Personendatenbearbeitung darstellt, haben wir eine Sachverhaltsabklärung durchgeführt.

Gemäss der Stellungnahme von Apple wurden nicht alle auf den betroffenen Mobilgeräten gespeicherten Hotspot- und Mobilfunkantennenstandorte durch das Gerät selbst erfasst. Apple selber stellte Informationen zu möglicherweise in der Nähe des Telefons befindlichen Standorten zur Verfügung. Der Zweck dieser Sammlung ist eine schnellere Positionsbestimmung für verschiedene Anwendungen.

Weiter wurden die Antennenstandorte im Empfangsbereich des Gerätes aufgrund eines Programmierfehlers auch nach dem Deaktivieren der Ortsdienste erfasst und an Apple gesendet. Mit dem iOS-Update vom 4. Mai 2011 wurde dieser Fehler behoben. Zusätzlich wird seit dem Update die Datei mit den Geopositionsdaten nicht mehr über das Programm «iTunes» auf anderen Geräten gesichert. Die «crowd-sourced» WIFI-, Hotspot- und Mobilfunkantennen-Informationen werden nach sieben Tagen, alle temporären Ortsinformationen beim Abschalten der Ortsdienste gelöscht.

Die mit dem besagten Update am Betriebssystem vorgenommenen Anpassungen ermöglichen den Benutzerinnen und Benutzern die Löschung der Ortsinformationen sowie die Unterbindung ihrer Erfassung und Weiterleitung. Damit waren die datenschutzrechtlichen Forderungen erfüllt und wir konnten die Sachverhaltsabklärung abschliessen.

Anzumerken bleibt, dass es unabhängig vom Betriebssystem nach wie vor auch in den Händen der Benutzer liegt, welchen «Apps», Programmen oder Herstellern sie ihre (Positions-)Daten anvertrauen und gegebenenfalls Informationen für ein detailliertes

(Bewegungs-)Profil liefern. Um die damit verbundenen Risiken möglichst klein zu halten, sollten sie einerseits die AGB und die Datenschutzerklärung beachten, andererseits die Zugriffseinstellungen für die Programme anpassen.

1.3.2 Online-Marketing: Schutz der Internetbenutzer

Im November 2009 hat das EU-Parlament die Direktive zum Schutz der Privatsphäre im Internet revidiert. Eine wesentliche Änderung betrifft die Vorgaben für die Speicherung von respektive den Zugriff auf Informationen wie etwa Cookies auf einem User-Terminal. Die bisherige Opt-out-Lösung der alten Direktive wurde durch eine so genannte «Informed-Consent»-Lösung, also durch ein Opt-in des Users nach eingehender Information über Art und Zweck der Datenbearbeitung abgelöst.

Die Annahme, das Surfen im Web sei anonym, ist falsch. Das Internet ist ein interaktives Medium, und über jeden Besuch auf einer Webseite werden Informationen gesammelt. Beispielsweise findet das «Online-Tracking», also das Aufzeichnen von Benutzerverhalten über mehrere Seiten einer Webseite, auf verschiedenen Wegen mit verschiedenen Mitteln zu verschiedenen Zwecken statt. Es stellt ein Eingriff in die Privatsphäre dar, der technisch zwar bedingt umgehbar ist, der aber wegen seiner mangelnden Sichtbarkeit von den meisten Usern nicht beachtet wird.

Die neuen EU-Vorgaben warfen vor allem in der Online-Marketingbranche hohe Wellen. Sie realisiert einen grossen Teil der Werbeeinnahmen mittels «Online Behavioral Advertising» (OBA). Darunter sind im weitesten Sinne sämtliche Werbeangebote zu verstehen, die auf Grund der vorherigen Sammlung von Internet-Nutzungsdaten – meistens mittels Tracking-Cookies – dem Anwender individuell angezeigt werden. Verunsichert durch die EU-Vorgaben sahen wesentliche Akteure die Online-Werbung gefährdet und befürchteten das Ende der Gratisdienstleistungen im Internet.

Die European Advertising Standards Alliance und das Interactive Advertising Bureau Europe wollten einer strikten Gesetzgebung in den EU-Mitgliedstaaten zuvorkommen und verfassten einen Verhaltenskodex («Code of Conduct») als Selbstregulierungsmassnahme für ihre Mitglieder. Dieser Kodex sieht im Wesentlichen einen Opt-out-Mechanismus vor, mit dem der User der Erfassung seines Surfverhaltens widersprechen kann. Die Artikel-29-Datenschutzgruppe – das unabhängige Beratungsgremium der Europäischen Kommission in Fragen des Datenschutzes – hat jedoch in einem Papier vom Dezember 2011 erneut festgehalten, dass diese Selbstregulierungsmassnahmen den gesetzlichen Anforderungen nicht genügten. Grundsätzlich müssten Information und Transparenz

bei der Anwendung von OBA-Tools verbessert werden. Weiter sei der vorgeschlagene Opt-out-Mechanismus gegen den Erhalt von zielgerichteter Onlinewerbung unvereinbar mit der Opt-in-Bestimmung der Direktive über die Cookies.

Einige Mitgliedstaaten der EU haben die Vorgaben der Richtlinie bereits in ihr nationales Recht umgesetzt, derweil sich andere Länder noch schwer tun. Tatsächlich scheint es eine grosse Herausforderung zu sein, den gesetzlichen Vorgaben des «Informed Consent» zu genügen, aber gleichzeitig die Benutzerfreundlichkeit beim Surfen nicht wesentlich einzuschränken.

Während sich die europäischen Länder mit der Cookie-Problematik beschäftigen, wird in den Vereinigten Staaten um eine eigene Lösung gekämpft, die den nahezu unbegrenzten Zugriff auf private Daten im Internet durch Konzerne beschränken soll. Die Regierung Obama hat ein umfassendes Gesetzesvorhaben auf den Weg gebracht, das bei Demokraten, aber auch in Industriekreisen Unterstützung findet – laut einem Bericht des «Wall Street Journal» beispielsweise bei Microsoft. Aber auch die obersten kommerziellen Stäbe, die Handelsorganisation FTC und das «Chamber of Commerce» sind aktiv geworden: Wachsende Sorgen der Bürger auf der einen Seite, und ein nahezu uneingeschränkter Tracking-Betrieb und munterer Handel mit privaten Daten auf der anderen Seite, zwingen die Regierung augenscheinlich zum Einschreiten.

Auch den einzelnen Nutzern bieten sich Möglichkeiten, die Aufzeichnung des eigenen Surfverhaltens durch Drittanbieter zu unterbinden. Führende Webbrowser wie Internet Explorer, Mozilla Firefox, Google oder Safari haben Privacy-Funktionen. Als erstes empfiehlt es sich, jeweils die neuste Version des Browsers zu installieren. Danach lassen sich durch Suchfunktionen und spezifische Einstellungen Cookies verwalten. Eine weitere Methode, um das Tracking zu reduzieren, lässt sich mit dem Browser im Modus «Private Browsing» bewerkstelligen, bei Chrome heisst die Funktion «Incognito». Zu beachten ist aber, dass das «Private Browsing» Cookies nicht blockiert. Jedoch werden alle Cookies beim Schliessen des Browsers gelöscht und die Surf-History wird effektiv versteckt. Das Installieren von speziellen «Plug-ins» oder «Add-ons» im Browser kann weiter dazu beitragen, die eigene Privatsphäre zu verwalten.

Wir unterstützen einerseits private Initiativen, die den Schutz der Privatsphäre im Online-Marketingbereich verbessern, und sind mit den Branchenvertretern in der Schweiz im Gespräch. Andererseits verfolgen wir die Entwicklungen im Ausland intensiv. Selbstverständlich ist ein Sonderfall Schweiz nicht denkbar, allein schon deshalb, weil Webseiten von Schweizer Dienstleistern oder Werbenetzwerke an den Landesgrenzen keinen Halt machen. Es ist unbestritten, dass die Transparenz und Information beim Einsatz von Tracking-Tools gewährleistet sein muss. Je nach Sensibilität der bearbeiteten

Daten gelten erhöhte Anforderungen an die Informationspflichten; unter Umständen muss ein betroffener User der Bearbeitung sogar ausdrücklich zugestimmt haben, damit sie zulässig ist.

1.3.3 E-Mail-Spam

Zum Thema E-Mail-Spam erreichen uns immer wieder Anfragen, etwa zur Qualifikation von E-Mail-Adressen als Personendaten. Zudem wurde in den letzten Jahren der Rechtsrahmen den technischen Herausforderungen angepasst. Das gibt uns Anlass, die aktuelle Rechtslage kurz darzustellen.

Unter Spam versteht man unverlangte, meist unerwünschte und wiederholte Massensendungen von E-Mails. Das Thema hat uns bereits mehrfach beschäftigt (vgl. unseren 9. Tätigkeitsbericht 2001/2002, Ziff. 8.2, und unseren 10. Tätigkeitsbericht 2002/2003, Ziff. 8.1 und 13.7.3). Die Eidgenössische Datenschutzkommission hat mit Urteil vom 15. April 2005 unsere Auffassung bestätigt: E-Mail-Adressen sind Personendaten im Sinne des Datenschutzgesetzes – unabhängig davon, ob es sich um Phantasiebezeichnungen handelt oder nicht. Entscheidend ist demnach der Schutzzweck des Gesetzes: «Wenn Personen aktive Kommunikationswege (Telefonnummern, E-Mail-Adressen) zur Verfügung stellen und über diese erreicht werden können, liegt eine eindeutige Koppelung zwischen den Personen und diesen Daten vor. Der Schutz der informationellen Selbstbestimmung steht in dem ihr gesetzlich gewährten Rahmen der Person zu. Von daher bestimmt – vorbehältlich anderer Regelung – nur sie allein, ob ihre Daten bearbeitet werden dürfen oder nicht. Dabei kann keine Rolle spielen, ob diese Daten aus Zahlenfolgen oder Phantasiebezeichnungen bestehen, sofern sie eindeutig zu einer Person gehören. Bei Telefonnummern leuchtet dies von vornherein ein. Bei E-Mail-Adressen verhält es sich nicht anders.» (Urteil der Eidgenössischen Datenschutzkommission vom 15. April 2005, E. 2.4.)

Eine Sammlung von E-Mail-Adressen (wie sie die Versender von Spam anlegen) ist damit eine Personendatensammlung und die Person, deren E-Mail-Adresse darin verzeichnet ist, hat gestützt auf das Datenschutzgesetz einen Auskunftsanspruch gegen den Inhaber. Die Herkunft der Daten muss dabei offen gelegt werden, soweit die entsprechenden Angaben für den Inhaber verfügbar sind.

Wer von Spam belästigt wird, dem bieten weitere Bundesgesetze rechtliche Mittel, um dagegen vorzugehen: Seit dem 1. April 2007 untersagt die schweizerische Gesetzgebung ausdrücklich den Versand von Spam. Das Bundesgesetz gegen den

unlauteren Wettbewerb (UWG) sieht verschiedene Abwehrmassnahmen gegen Spam vor. Das Fernmeldegesetz (FMG) hält fest, welche Massnahmen die Fernmeldeanbieter gegen Spam ergreifen müssen.

Damit der Massenversand von Werbung über Internet oder Fernmeldedienste rechtlich zulässig ist, müssen die folgenden Voraussetzungen erfüllt sein:

- Werbemitteilungen dürfen nur dann an Kundinnen und Kunden verschickt werden, wenn diese vorher ausdrücklich dem Erhalt zugestimmt haben (Opt-in-Lösung). Der Absender muss somit grundsätzlich vor dem ersten Versand die ausdrückliche Einwilligung der Empfängerinnen und Empfänger eingeholt haben.
- Der Absender der Werbung muss eindeutig erkennbar sein. Seine Adresse muss korrekt wiedergegeben, seine Identität darf nicht versteckt oder gefälscht sein.
- In jeder Werbemitteilung muss der Absender den Empfängerinnen und Empfängern die Möglichkeit bieten, gratis und auf einfache Weise weitere Werbesendungen abzubestellen; der Absender muss die Empfängerinnen und Empfänger deutlich auf diese Gelegenheit hinweisen.

Auf unserer Webseite www.derbeauftragte.ch unter Häufige Fragen – Datenschutz Informationstechnologie – Spam sind die rechtlichen Grundlagen zum Thema detailliert dargestellt, inklusive konkrete Tipps, wie man Belästigung durch Spam vermeiden kann.

1.3.4 Strassenansichten im Internet

In unserem 18. Tätigkeitsbericht 2010/2011, Ziff. 1.3.3, haben wir über das Urteil des Bundesverwaltungsgerichts in Sachen Google Street View berichtet, welches unsere Empfehlungen in allen wesentlichen Punkten gutgeheissen und für verbindlich erklärt hat. Google hat gegen dieses Urteil Beschwerde ans Bundesgericht erhoben. Das Bundesverwaltungsgericht und auch wir haben zu den Vorbringen der Beschwerdeführerin Stellung genommen und beantragen die vollumfängliche Abweisung. Das Urteil des Bundesgerichts ist in nächster Zeit zu erwarten.

1.3.5 Einbindung von Social Plug-ins in Webseiten

Das Einbinden von Webinhalten von Drittanbietern ist kein neues Phänomen. Waren es zu Beginn etwa Börseninformationen oder Wetterberichte, gibt es im Zeitalter verstärkter Interaktivität die Möglichkeit der Kommentierung und Einbindung von Artikeln oder Blogs. Zur Vereinfachung der Interaktivität bieten die Anbieter Sozialer Netzwerke den Webseitenbetreibern Social Plug-ins an. Damit stellen sich aber auch Datenschutzprobleme.

Wir haben uns bereits im Jahr 2006 zur analogen Problematik der so genannten «Webbugs» geäussert, die Datenschutzproblematik dargestellt und Handlungsmöglichkeiten für Webseitenbetreiber und Internetnutzer aufgezeigt (siehe www.derbeauftragte.ch, unter Themen – Datenschutz – Technischer Datenschutz – Technische Themen). Die Einbindung von Social Plug-ins ist mit diesem Thema vergleichbar; die starke Verbreitung der Plug-ins verschärft jedoch die Datenschutzproblematik. Insbesondere ist hier auf die Tracking-Möglichkeiten der Anbieter hinzuweisen, denn die Information zu einem Webseitenbesuch wird schon beim Aufrufen der Seite, welche Social Plug-ins beinhaltet, übertragen.

Um den Anforderungen des Schweizer Datenschutzgesetzes Genüge zu tun, muss der Webseitenbetreiber beim Einbinden der Inhalte von Drittanbietern besonders darauf achten, dass er die Nutzer seiner Webseite umfassend über die damit verbundenen Datenbearbeitungen informiert. Detaillierte Hinweise darauf, welche Punkte in einer Datenschutzerklärung enthalten sein müssen und wie beim Verfassen dieser Erklärung vorgegangen werden sollte, sind ebenfalls auf unserer Webseite (www.derbeauftragte.ch, Häufige Fragen – Datenschutz – Handel und Wirtschaft – Datenschutzerklärungen im E-Commerce) abrufbar.

Die Webseitenbetreiber haben ausserdem geeignete technische und organisatorische Massnahmen zu treffen, um ungerechtfertigte Persönlichkeitsverletzungen zu vermeiden. Mit Bezug auf den konkreten Fall der Social Plug-ins weisen wir auf die im Netz frei abrufbaren datenschutzkonformen Implementierungsmöglichkeiten (Zwei-Klick-Empfehlungsbuttons) hin.

Die Internetnutzer müssen ihrerseits Verantwortung wahrnehmen, indem sie ihr Surfverhalten und die Konfiguration ihrer Software den heutigen Gegebenheiten des Internets anpassen und dabei die ihren jeweiligen Bedürfnissen entsprechende Mischung aus Schutz der Privatsphäre und Nutzerkomfort finden.

1.3.6 Vermieterbewertungsplattform im Internet

Auf einer Webseite können Mieter ihre Vermieter kommentieren und bewerten. Die Betreiber der Informations- und Bewertungsplattform erhoffen sich dadurch mehr Transparenz im Mietermarkt. Aus datenschutzrechtlicher Sicht können solche Plattformen jedoch rechtliche Probleme mit sich bringen.

Auf einer Internetplattform können Mieter in der ganzen Schweiz anonym ihre Erfahrungen mit ihren Vermietern mitteilen. Die Mieter geben zunächst die Daten ihres Vermieters bekannt. Danach geben sie eine Bewertung auf der Basis von standardisierten Fragen ab. Pro Frage werden null bis fünf Sterne vergeben, die mittels eines Bewertungssystems in einen so genannten Weiterempfehlungsgrad umgerechnet werden.

Grundsätzlich können Bewertungsplattformen für bestimmte Zielgruppen als Informationsquelle sinnvoll sein. Die Gefahr ist jedoch gross, dass es zu Persönlichkeitsverletzungen kommt. Aus datenschutzrechtlicher Perspektive ist zunächst festzuhalten, dass sich der Betreiber der Bewertungsplattform die Veröffentlichung von Personendaten auf seiner Webseite zurechnen lassen muss. Die Vermieter wurden bis anhin nicht über die Eintragung ihrer Daten informiert und konnten weder ihr noch der anschliessenden Bewertung zustimmen. Die Veröffentlichung von Daten über Vermieter auf einer Webseite stellt aber eine Bearbeitung von Personendaten im Sinne des Datenschutzgesetzes dar, die offensichtlich nur durch die Einwilligung der betroffenen Personen gerechtfertigt werden kann. Wir haben die Betreiber der Plattform darauf hingewiesen, dass es unverzichtbar ist, die Vermieter über die Bearbeitung ihrer Personendaten und den Zweck ausführlich zu informieren und ihre Zustimmung einzuholen.

Weiter muss beachtet werden, dass Einträge über eine Firma oder Person auf einer Webseite die Persönlichkeit verletzen können. Um dies zu verhindern, sollte der Betreiber der Seite bestimmte Vorkehrungen treffen. Insbesondere für anonyme Kritiken sollten sich die Mieter einloggen müssen, damit sie für den Plattformbetreiber identifizierbar sind – und bei groben Persönlichkeitsverletzungen auch belangt werden können. Dies war auf der genannten Webseite nicht der Fall. Es konnte sich irgendjemand mit der blossen Angabe einer E-Mail-Adresse registrieren und seine Belange, Kommentare und Bewertungen anonym auf der Plattform anbringen.

Wir haben den Betreibern die datenschutzrechtlichen Defizite ihrer Informations- und Bewertungsplattform erläutert und mögliche Verbesserungsvorschläge mit ihnen diskutiert. Die Verantwortlichen haben diese Hinweise entgegen genommen und suchen

nach Wegen, die Plattform unter diesen Voraussetzungen umzugestalten. Bis die Berichtigungen umgesetzt sind, ist die Webseite nicht mehr in Betrieb.

1.3.7 Internet-Tauschbörsen – Rechtslage nach dem Logistep-Urteil

Das Logistep-Urteil des Bundesgerichts hat uns auch in diesem Berichtsjahr noch beschäftigt. Wir haben insbesondere aufgezeigt, unter welchen Voraussetzungen aus unserer Sicht die Bearbeitung von Personendaten durch Private bei der Verfolgung von Urheberrechtsverletzungen im Internet auch nach dem Urteil datenschutzkonform erfolgen kann.

Im 18. Tätigkeitsbericht 2010/2011, Ziff. 1.3.5, haben wir über das Urteil des Bundesgerichts in Sachen Logistep (BGE 136 II 508) berichtet. Das Gericht gab in den tragenden Erwägungen vorab einem Unbehagen angesichts der offensichtlich als ungenügend empfundenen heutigen gesetzlichen Regelung Ausdruck. In seinem Geschäftsbericht 2010 (S. 17) richtete es denn auch explizit den Hinweis an den Gesetzgeber, es sei dessen Sache, «die notwendigen Massnahmen zu treffen, um einen den neuen Technologien angepassten Urheberrechtsschutz zu gewährleisten.»

In der Urteilsbegründung klang aber unseres Erachtens auch der Vorwurf an die Adresse von Logistep bzw. die ihrer Auftraggeber an, zum Teil von ihnen selbst geschaffene Unsicherheiten ausgenützt zu haben, um (überhöhte) Zivilforderungen geltend zu machen; und dies bevor die Täterschaft mutmasslicher Urheberrechtsverletzer in einem Strafverfahren verbindlich festgestellt wurde, das rechtsstaatlichen Ansprüchen genügt.

Gemäss unseren Abklärungen im Jahr 2008 unterscheidet sich das Vorgehen anderer Rechteinhaber bei der Verfolgung mutmasslicher Urheberrechtsverletzer gerade in diesem Punkt wesentlich von demjenigen, wie es Logistep praktiziert hatte: So wartet etwa IFPI Schweiz (der Dachverband der Ton- und Tonbildträgerhersteller) immer eine rechtskräftige strafrechtliche Verurteilung ab, bevor sie Urheberrechtsverletzer mit Zivilforderungen konfrontiert. Wir haben IFPI Schweiz bereits im März 2008 mitgeteilt, dass sie mit dieser Vorgehensweise aus unserer Sicht nicht gegen das Datenschutzgesetz verstösst.

Im Nachgang zum Logistep-Entscheid sind IFPI Schweiz und SAFE (Schweizerische Vereinigung zur Bekämpfung der Piraterie) mit uns in Kontakt getreten. Sie haben uns versichert, dass ihr Vorgehen demjenigen entspricht, wie es uns im Frühjahr 2008 vorgeführt worden war. Wir haben den beiden Interessenverbänden daher

mitgeteilt, dass uns weiterhin möglich erscheint, ein überwiegendes und die mit diesen Datenbearbeitungen verbundenen Persönlichkeitseingriffe damit rechtfertigendes Interesse anzunehmen,

- wenn sichergestellt ist, dass die Datenerhebung und -speicherung nicht über das hinausgeht, was absolut notwendig ist, um (bei der voraussichtlich örtlich zuständigen Behörde) Strafanzeige gegen mutmassliche Urheberrechtsverletzer zu erstatten;
- wenn sichergestellt ist, dass Verhandlungen zwischen Rechteinhaber und (mutmasslichem) Urheberrechtsverletzer über Schadenersatzforderungen nur auf dessen Initiative hin oder aber nach einer rechtskräftigen strafrechtlichen Verurteilung stattfinden;
- und wenn die Rechteinhaber ihre Anstrengungen verstärken, die Beschaffung der Personendaten und den Zweck ihrer Bearbeitung für die betroffenen Personen möglichst erkennbar zu machen. Dazu müssen sie insbesondere auf ihren Webseites an leicht zugänglicher und auffindbarer Stelle ihre Vorgehensweise (einschliesslich detaillierter Angaben zu Art und Umfang der gesammelten Daten) vollständig offen legen und deutlich machen, dass Schadenersatzansprüche nur gegenüber rechtskräftig strafrechtlich verurteilten Urheberrechtsverletzern verfolgt werden.

Zudem haben wir SAFE und IFPI darauf hingewiesen, dass Datensammlungen bei uns registriert werden müssen, wenn regelmässig besonders schützenswerte Personendaten oder Persönlichkeitsprofile bearbeitet oder regelmässig Personendaten an Dritte bekannt gegeben werden.

Unter diesen Voraussetzungen ist nach unserer Auffassung eine datenschutzkonforme Verfolgung von Urheberrechtsverletzungen im Internet nach wie vor möglich. Da wir aber von Gesetzes wegen nicht etwa dazu ermächtigt sind, Datenbearbeitungen formell zu genehmigen, kann eine rechtsverbindliche Beurteilung von Datenbearbeitungen letztlich – wie im Fall Logistep – nur durch die zuständigen Gerichte erfolgen.

In diesem Zusammenhang gilt es noch auf Folgendes hinzuweisen: Sollten die Strafgerichte eine gefestigte Rechtsprechung entwickeln, wonach privat ermittelte IP-Adressen in Strafverfahren generell nicht verwertbar sind, müsste unsere Beurteilung anders ausfallen. Aus datenschutzrechtlicher Sicht wäre dann eine rechtmässige Aufzeichnung und Weitergabe der IP-Adressen durch Private bei der Verfolgung von Urheberrechtsverletzungen nach geltendem Recht nicht länger möglich: Die Datenerhebung wäre für den angestrebten Zweck von vornherein ungeeignet und die Datenbearbeitung damit unverhältnismässig.

1.3.8 Elektronische Überwachung: Kopierschutz bei Computerspielen

Ein im Herbst veröffentlichtes Computerspiel hat in der Presse für Aufsehen gesorgt. Der zum Spiel gehörende Kopierschutz soll die Computer der Nutzer ausspionieren und dem Hersteller Informationen über die auf dem jeweiligen Computer gespeicherten Daten, über das Nutzungsverhalten und vieles mehr übermitteln. Wir sind zurzeit daran, das in die Kritik geratene Programm auf seine Datenschutzkonformität hin zu überprüfen.

Jeder Nutzer, der das fragliche Computerspiel spielen möchte, muss eine zusätzliche Applikation installieren und sich via eine dazugehörige Internetplattform beim Hersteller des Spiels registrieren. Damit soll verhindert werden, dass Raubkopien verwendet werden. Die Installation der Applikation und die Registrierung sind denn auch zwingend notwendig, und zwar unabhängig davon, ob das Spiel im Multiplayermodus online oder ausschliesslich im Einzelspielermodus offline gespielt wird. Nach Veröffentlichung des Spiels wurde in den Medien breit darüber berichtet, dass die Spieler mit Hilfe dieser Applikation ausspioniert werden. So sollen dem Hersteller detaillierte Angaben über sämtliche Aktivitäten auf dem fraglichen Computer sowie über alle auf dem Computer gespeicherte Dateien übermittelt werden, ohne dass der Nutzer etwas davon merkt. Durch spätere Medienberichte wurde diese Darstellung teilweise relativiert.

In der Zwischenzeit haben sich viele verunsicherte Spieler bei uns gemeldet. Wir haben diese Meldungen zum Anlass genommen, den Hersteller an seinem Schweizer Sitz zu kontaktieren und seine Personendatenbearbeitung rund um das neu erschienene Spiel einer datenschutzrechtlichen Kontrolle zu unterziehen. Die Abklärungen sind zurzeit im Gange. Wir werden zum geeigneten Zeitpunkt die Öffentlichkeit über das Resultat dieser Kontrolle informieren.

1.3.9 Verwendung von Adressdaten aus Kontaktformularen zur Evaluation von Webseiten

Betreiber von Webseiten sind im Besitz der Adressdaten derjenigen Besucher, welche das Kontaktformular für eine Mitteilung oder eine Anfrage nutzen. Es ist naheliegend, diese Adressen für den Versand eines Fragebogens zur Evaluation der Webseite zu verwenden. Da es sich bei den Adressdaten aber um Personendaten handelt, ist eine solche Verwendung nicht ohne weiteres zulässig.

Wie wir im Rahmen einer Anfrage feststellen konnten, besteht bei Webseitenbetreibern das Interesse, Adressdaten, die via Kontaktformular erhoben werden, für weitere

Zwecke zu verwenden. Insbesondere die Verwendung für den Versand eines Fragebogens zur Beurteilung der Webseite bietet sich hier an: Alle hinter den Adressen stehenden Personen waren bereits einmal auf der fraglichen Webseite und können damit Aussagen etwa über Benutzerfreundlichkeit oder Design machen. Zudem liegen die Adressdaten bereits in digitaler Form vor, was eine Weiterverwendung vereinfacht.

Die Besucher der Webseite dagegen gehen beim Ausfüllen des Kontaktformulars davon aus, dass die dort gemachten Angaben einzig für die Abwicklung ihrer Anfrage verwendet werden. Erhalten diese Personen nun plötzlich einen Fragebogen zur Evaluation der Webseite, so wird dies nicht nur für verständlichen Unmut sorgen. Vielmehr verstösst ein solcher Versand gegen die Bearbeitungsgrundsätze des Datenschutzgesetzes.

Um dies zu verhindern, muss bei der Verwendung solcher Adressdaten für weitere Zwecke Folgendes beachtet werden:

Der Webseitenbetreiber muss die Benutzer des Kontaktformulars darüber informieren, dass ihre Daten für weitere Zwecke verwendet werden können. Dabei muss ausdrücklich erwähnt werden, um welche Zwecke es sich handelt (Evaluationen, Versand von Produktinformationen etc.). Die Information ist in einer für die Zielgruppe gut verständlichen Sprache abzufassen und an einem gut sichtbaren Ort zu platzieren (vorzugsweise auf dem Kontaktformular selbst).

Jeder Benutzer sollte die Weiterverwendung seiner Personendaten auf einfache und kostenlose Art untersagen können (Opt-out). Auch hier bietet es sich an, im Kontaktformular selbst eine entsprechende Funktion einzubauen (z.B. mit einem Kästchen, das angeklickt werden kann). Aber auch später müssen die Nutzer jederzeit die Möglichkeit haben, einfach und kostenlos die weitere Verwendung ihrer Daten zu untersagen.

1.3.10 Einbindung ausländischer Suchmaschinen auf Webseiten des Bundes

Wer auf einer Webseite des Bundes Informationen sucht, etwa zu bestimmten Politikbereichen oder zu Gesundheitsthemen, darf darauf vertrauen, dass mit den dabei anfallenden Daten über seine Person sehr sorgsam umgegangen wird. Bundesorgane haben besonderes Augenmerk auf die datenschutzrechtlichen Vorgaben zu legen.

Wer Webdienste anbietet, bearbeitet regelmässig Personendaten. So sind bereits die reinen IP-Adressen nach der Rechtsprechung des Bundesgerichts zumindest dann als Personendaten zu qualifizieren, wenn der Aufwand für die Bestimmung der betroffenen Person nicht derart gross ist, dass nach der allgemeinen Lebenserfahrung nicht

mehr damit gerechnet werden muss, dass ein Interessent diesen auf sich nehmen wird. Auch durch Techniken wie den Einsatz von Cookies oder die Auswertung der so genannten «Referrer» (Angaben über die Internetadresse der Webseite, von der der Benutzer durch Anklicken eines Links zur aktuellen Seite gekommen ist) lässt sich häufig ein Personenbezug herstellen.

Die meisten Bundesorgane bieten Webdienste an, und wir beraten sie in diesem Zusammenhang öfters. Dabei stellte sich die Frage, ob Bundesorgane von ausländischen Privatunternehmen angebotene Suchmaschinen in ihre Webangebote integrieren dürfen. Als problematisch erwies sich im untersuchten Fall, dass es nicht möglich war, die Suchfunktion zu verwenden, ohne dass detaillierte Informationen darüber, wer was gesucht hat, an das in den Vereinigten Staaten von Amerika domizilierte Privatunternehmen fliessen. Die Suchalgorithmen basieren gerade darauf, dass diese Daten (neben der IP-Adresse auch weitere eindeutige Benutzeridentifikatoren und Angaben zum Suchverhalten, wie Suchanfragen und angeklickte Resultate) aufgezeichnet und ausgewertet werden. Überdies sollten die Daten gemäss Datenschutzerklärung der Privatfirma für weitere Zwecke verwendet werden, insbesondere für die Verfeinerung der unternehmenseigenen Software zur Einblendung personalisierter Werbung. Das betreffende Unternehmen betreibt Rechenzentren rund um den Globus. Wie viele Personen innerhalb der Firma und welche weiteren Stellen (private Drittfirmen, staatliche Behörden) Zugriff auf diese Daten nehmen dürfen oder können ist nicht genau bekannt und kaum kontrollierbar. Wegen der Fülle an dort abrufbaren Daten sind derartige Unternehmen zudem regelmässig Ziel von Hackerangriffen aus der ganzen Welt.

Solche Dienstleistungen mögen auf den ersten Blick günstig erscheinen, haben aber eine Kehrseite: Man erkauft sie sich teuer, indem die Nutzer sie mit der Preisgabe von persönlichen Daten und dem Verlust der Kontrolle darüber «bezahlen» müssen.

Seit dem 1. Dezember 2010 gilt für Bundesbehörden eine umfassende Informationspflicht beim Beschaffen von Personendaten. Weder der Bearbeitungszweck noch die Kategorien der Datenempfänger noch die Modalitäten der Geltendmachung des Auskunftsrechts wären beim Einsatz der von uns untersuchten Suchmaschine des amerikanischen Privatunternehmens auch nur annähernd hinreichend bekannt, um dieser gesetzlichen Informationspflicht zu genügen.

Aus diesen Gründen erscheint uns die Einbindung von Suchfunktionen, wie sie ausländische Unternehmen vermeintlich «gratis» anbieten, auf Webseites der Bundesverwaltung als problematisch und kaum in gesetzeskonformer Weise möglich.

1.3.11 Die Überwachung der Informations- und Kommunikationsmittel beim Bund

Die Bundesverwaltung hat ein Interesse daran, die Nutzung der Informations- und Kommunikationsmittel zu überwachen. Damit sollen der Betrieb der Systeme sichergestellt und Missbräuche verhindert werden. Um diese Überwachung rechtskonform durchführen zu können, wurden die notwendigen gesetzlichen Grundlagen erarbeitet.

Genau wie in der Privatwirtschaft besteht auch innerhalb der Bundesverwaltung ein Interesse daran, die Nutzung der Informations- und Kommunikationsmittel zur Sicherstellung des Betriebs und zur Verhinderung von Missbräuchen zu überwachen. In erster Linie geschieht dies durch die Auswertung der bei der Nutzung anfallenden Daten, den so genannten Randdaten. Sie zeigen zum Beispiel beim Surfen, welche IP-Adresse wann wie lange mit welcher URL (Adresse einer Internetseite) kommuniziert hat. Konkret kann also anhand dieser Daten das Surfverhalten eines Mitarbeiters nachträglich ausgewertet werden. Zudem kann so auch eruiert werden, wie zum Beispiel ein Schadprogramm («Malware») in ein System eindringen konnte.

Als Protokolldaten fallen die Randdaten automatisch an (Logfiles). Sie stellen Personendaten gemäss Datenschutzgesetz dar, weil sie sich auf eine bestimmte oder bestimmbare Person beziehen. Deshalb benötigen Bundesorgane für ihre Bearbeitung eine gesetzliche Grundlage (Legalitätsprinzip). Im Berichtsjahr beteiligten wir uns an einer Arbeitsgruppe unter der Leitung des Bundesamtes für Justiz, die zum Zweck hatte, eine solche Grundlage auszuarbeiten. Die grundsätzlichen Bestimmungen wurden im Regierungs- und Verwaltungsorganisationsgesetz (RVOG) eingefügt, und für die Details wurde eine neue Verordnung (Verordnung vom 22. Februar 2012 über die Bearbeitung von Personendaten, die bei der Nutzung der elektronischen Infrastruktur des Bundes anfallen) ausgearbeitet. Ziel der Bestimmungen im RVOG und in dieser Verordnung ist es, einerseits die Aufzeichnung und Aufbewahrung der Randdaten (inklusive Aufbewahrungsfristen), andererseits die Formen der Auswertung, die Voraussetzungen dafür und die Verfahrensgrundsätze klar zu regeln. Insbesondere sind hier die berechtigten Interessen des Arbeitgebers, der Systembetreiber und der Arbeitnehmer berücksichtigt worden.

1.3.12 E-Government-Standards und die neue AHV-Nummer

In bestimmten Bereichen des E-Government-Umfeldes soll die seit 1. Juli 2008 existierende 13-stellige Versichertennummer der AHV als Personenidentifikator verwendet werden. Es wurde ein so genannter «eCH-Standard» formuliert, welcher den Anwendungsbereich beschreiben soll. Dazu haben wir uns im Sinne einer Klarstellung und Ergänzung geäussert.

Der Verein eCH fördert, entwickelt und verabschiedet E-Government-Standards. Getragen wird er von Bund, Kantonen, Städten und Gemeinden sowie Wirtschaft und Wissenschaft. Die Standards haben den Status von Empfehlungen, wobei ihr Einsatz auf Stufe Bund, Kantone oder Städte und Gemeinden für verbindlich erklärt werden kann.

Als registerübergreifende Personenidentifikation soll die neue 13-stellige Versichertennummer der AHV in die amtlichen Personenregister von Gemeinden, Kantonen und Bund eingeführt werden. Dafür wurde ein eCH-Standard erarbeitet, welcher den Anwendungsbereich der neuen AHV-Versichertennummer als Personenidentifikator umschreibt. Zu diesem Standard haben wir die gesetzlichen Grundlagen und die wesentlichen Aspekte der Verwendung der neuen AHV-Versichertennummer für Verwaltungssysteme einzeln aufgeführt und im Rahmen der geplanten Verwendung beurteilt.

Die rechtliche Grundlage für die systematische Verwendung der neuen AHV-Nummer als Personenidentifikator findet sich im AHV-Gesetz. Das Registerharmonisierungsgesetz (RHG) erlaubt als bundesrechtliche Spezialgesetzgebung ihre systematische Verwendung in bestimmten Registern auch ausserhalb des Sozialversicherungsbereichs. Wir haben betont, dass dies nur im Rahmen des Zwecks und des Geltungsbereichs des RHG zulässig ist. Das Hauptziel des Gesetzes liegt in der Schaffung einer modernen Rechtsgrundlage zur Nutzung der kantonalen und kommunalen Einwohnerregister für statistische Zwecke.

Als Schlussfolgerung haben wir festgehalten, dass die AHV-Nummer nur im Geltungsbereich des RHG, d.h. fokussiert auf die statistische Auswertung der im Gesetz erwähnten Register, verwendet werden kann. Für den allgemeinen Einsatz in einem E-Government-System ausserhalb des Geltungsbereichs des RHG fehlt eine gesetzliche Grundlage.

Weitere Artikel zum Thema neue AHV-Nummer befinden sich in Ziff. 1.1.3 und 1.1.4 des vorliegenden Tätigkeitsberichts.

1.3.13 Vorentwurf zur GEVER-Verordnung

Wir haben bei der Erarbeitung eines Vorentwurfes zu einer GEVER-Verordnung mitgewirkt und später im Rahmen der Ämterkonsultation Stellung genommen. Die GEVER-Verordnung findet ihre gesetzliche Grundlage in Artikel 57h des Regierungs- und Verwaltungsorganisationsgesetzes, wonach jedes Bundesorgan zur Registrierung, Verwaltung, Indexierung und Kontrolle von Schriftenverkehr und Geschäften ein Dokumentationssystem führen kann.

Wir haben insbesondere auf die durchgängige Unterscheidung zwischen dem GEVER-System für über- und interdepartementale Prozesse und den GEVER-Systemen der einzelnen Verwaltungseinheiten der Bundesverwaltung aufmerksam gemacht. Weiter haben wir mehrfach betont, dass sich die Bekanntgabe von Personendaten in einem GEVER-System nach Artikel 19 des Datenschutzgesetzes (DSG) zu richten hat. In diesem Zusammenhang haben wir Absatz 3 dieses Artikels hervorgehoben, wonach Bundesorgane Personendaten nur durch ein Abrufverfahren zugänglich machen dürfen, wenn dies ausdrücklich vorgesehen ist, bspw. in einer Verordnung. Handelt es sich jedoch um besonders schützenswerte Personendaten sowie Persönlichkeitsprofile, muss das Abrufverfahren in einem Gesetz im formellen Sinn ausdrücklich vorgesehen sein. Das aktuelle RVOG beinhaltet keine solche Formulierung. Das bedeutet, dass für die Bekanntgabe von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen durch ein Abrufverfahren in einem GEVER-System zurzeit keine gesetzliche Grundlage vorhanden ist.

1.3.14 Programm GEVER-Bund: Bearbeitung vertraulicher und besonders schützenswerter Daten

Im Rahmen der Arbeitsgruppe betreffend Fragen des Datenschutzes und der Informationssicherheit beantragten wir für vertrauliche Dokumente und für besonders schützenswerte Daten gleichwertige Sicherheitsmassnahmen. Die vorgeschlagene neue GEVER-Architektur ist zwar ein pragmatischer Ansatz, bietet jedoch nicht unbedingt sämtliche erforderlichen Vertraulichkeitsgarantien.

Wir waren seit der Schaffung der neuen GEVER-Architektur an der Arbeitsgruppe beteiligt, die sich mit den Themen Datenschutz und Datensicherheit sowie mit dem Schutz und der Sicherheit von Informationen befasste. Die Arbeitsgruppe gelangte zum Schluss, dass die erforderlichen Sicherheitsmassnahmen für die nach der

Informationsschutzverordnung (ISchV) als vertraulich klassifizierten Dokumente und für die gemäss DSG als besonders schützenswert geltenden Daten gleichwertig sein sollten.

In einem ersten Schritt wurde ein umfangreicher Katalog der technischen Anforderungen zuhanden der anerkannten Anbieter von GEVER-Lösungen ausgearbeitet; dieser wurde jedoch von der Projektleitung nicht genehmigt. Die vorgeschlagene neue architektonische Lösung (GEVER-LA) zielt gewissermassen darauf ab, die fehlende hohe Vertraulichkeitsstufe in den GEVER-Systemen durch ein komplementäres Dualsystem auszugleichen, das den Verschlüsselungsbedarf innerhalb von GEVER und zwischen verschiedenen GEVER-Systemen abdeckt. Es ist zu bemerken, dass die geplante Chiffrierung nur die wenigen vertraulichen und/oder besonders schützenswerten Dokumente beträfe. Die Verschlüsselung innerhalb der GEVER wäre somit durch einen «Policy Enforcement Point» (PEP) gewährleistet, der alle zweckdienlichen Schlüssel enthielte und einem vom betroffenen Amt verwalteten «Policy Server» unterstellt würde. Erstaunlicherweise setzt die vorgeschlagene Lösung für die Verschlüsselung im Verkehr zwischen verschiedenen Systemen eben diesen PEP (ausgestattet mit einer neuen departementsübergreifenden «Public Key Infrastructure» [PKI]) als Ergänzung zur SEDEX Plattform ein und nutzt nicht die nunmehr in praktisch jedem Bundesamt verfügbare standardisierte Lösung «Secure Messaging» (mit ihrer untrennbar verbundenen PKI). Auf den ersten Blick bietet der pragmatische Ansatz GEVER-LA allerdings kaum eine vollumfängliche Vertraulichkeitsgarantie gegenüber den internen Administratoren des Leistungsbezügers (die den PEP und den «Policy Server» verwalten) sowie gegenüber den externen Lösungsanbietern (alle nicht vertraulichen und nicht besonders schützenswerten Dokumente – also eine deutlich überwiegende Mehrheit – sind nicht verschlüsselt und damit technisch für das Personal des Leistungsanbieters lesbar).

1.4 Justiz/Polizei/Sicherheit

1.4.1 Umsetzung Schengen: Kontrolle bei der Schweizer Botschaft in Moskau

Im Rahmen der Schengen-Zusammenarbeit befassten wir uns bei unserer Kontrolle der Schweizer Botschaft in Moskau mit den verschiedenen Aspekten des Datenschutzes bezüglich der Verfahren zur Visumserteilung. Dies umfasste die Verwaltung der Visumsdossiers, die Methoden der Anwerbung von Mitarbeitenden und ganz allgemein die getroffenen Sicherheitsmassnahmen. Am Ende richteten wir verschiedene Empfehlungen und Verbesserungsvorschläge an die Botschaft, aber auch an zwei Direktionen des Aussendepartements.

Die Kontrolle bei der Schweizer Botschaft in Moskau war die vierte dieser Art, die wir im Rahmen der Schengen-Zusammenarbeit durchführten. Nach Kairo, Kiew und Istanbul wurde die schweizerische Vertretung in Moskau aufgrund der besonders grossen Anzahl ausgestellter Visa ausgewählt. Während nämlich das Schweizer Konsulat in St. Petersburg die Visa für die nordwestliche Zone des Landes ausstellt, ist die Vertretung in Moskau für das übrige Land zuständig. So wurden im Jahr 2010 rund 63´000 Visa ausgestellt. Die Visumsabteilung der Botschaft arbeitet bei der Terminorganisation mit einem externen russischen Unternehmen zusammen. Dieses Call Center ist für die Zuteilung der Termine an die einzelnen Antragsteller verantwortlich.

Weitere Visumsanträge werden gebündelt von Reiseveranstaltern eingereicht, die in Absprache mit den übrigen Schengen-Mitgliedstaaten akkreditiert worden sind. Dank dieser Vorgehensweise kann der Visumsprozess erleichtert werden, da die Veranstalter die Aufgabe übernehmen, sämtliche erforderlichen Dokumente für alle Antragsteller zu sammeln und eine erste Überprüfung auf Vollständigkeit der Dokumente vorzunehmen.

Nach einer Prüfung der von der Schweizer Vertretung in Moskau übermittelten Dokumentation kontrollierten wir bei unserem zweitägigen Besuch vor Ort die internen Visumsvergabeverfahren und die getroffenen Sicherheitsmassnahmen. Anlässlich eines Besuchs bei dem externen Unternehmen konnten wir uns vergewissern, dass dort die erforderlichen Sicherheitsmassnahmen gemäss den im Rahmen des Schengen-Abkommens aufgestellten Anforderungen angemessen umgesetzt werden.

Bei der Ortsbesichtigung erkundigten wir uns bei den schweizerischen und lokalen Mitarbeitern der Visumsabteilung nach den verschiedenen Bearbeitungsschritten eines Visumsverfahrens. Die für die endgültige Entscheidung über die Ausstellung oder

Verweigerung eines Visums zuständigen schweizerischen Mitarbeiter wurden zudem eingehender zu den Suchmethoden befragt, die sie bei der Abfrage der Datenbanken N-SIS und ZEMIS über die EVA-Maske anwenden.

Im Anschluss an die Ortsbesichtigung nahmen wir Einsicht in die Logfiles des Systems N-SIS bei fedpol und des Systems ZEMIS beim BFM, um zu überprüfen, ob die Zugriffe während des zweiten Kontrolltages ordnungsgemäss protokolliert worden waren. Darüber hinaus unterzogen wir diese Logfiles einer eingehenden Analyse, um die Plausibilität der von den Mitarbeitenden an diesem Tag durchgeführten Abfragen zu ermitteln. So konnten wir uns vergewissern, dass der Aspekt der Suchmethoden keine Probleme bereitet.

Gemäss unseren Feststellungen gibt es anderswo allerdings mehrere problematische Punkte, die einer Verbesserung bedürfen. So richteten wir verschiedene Empfehlungen und Verbesserungsvorschläge an die Schweizer Botschaft in Moskau, aber auch an zwei Direktionen des Eidgenössischen Departements für auswärtige Angelegenheiten (EDA) mit der Aufforderung, in allen seinen ausländischen Vertretungen die Konformität dieser Punkte zu überprüfen. Einige dieser Empfehlungen richten sich an die Botschaft und betreffen unzulängliche Sicherheitsmassnahmen, insbesondere in Bezug auf den Hauptserver und die gemeinsame Nutzung der Räumlichkeiten mit den Mitarbeitern des Swiss Business Hub. Wir stellten auch fest, dass die betroffenen Personen nicht ausreichend über die Datenbearbeitung informiert werden, und gaben dazu eine Empfehlung ab. Wir rieten der konsularischen Direktion des EDA, bei den Vertretungen zu überprüfen, ob die Outsourcing-Verträge, die einige von ihnen mit lokalen Unternehmen abgeschlossen haben, eine Datenschutzklausel enthalten. An die Direktion für Ressourcen des EDA richteten wir schliesslich, wie schon bei einer früheren Kontrolle, einen Verbesserungsvorschlag bezüglich der Schulung auf dem Gebiet des Datenschutzes für die schweizerischen und lokalen Mitarbeiter in den ausländischen Vertretungen.

1.4.2 Umsetzung Schengen: Logfiles des SIS

Logfiles sind Teil der meisten Informatiksysteme. Sie ermöglichen im Rückblick den Nachvollzug der verschiedenen von den Nutzern im System getätigten Vorgänge. Aufgrund der Analyse dieser Logfiles lässt sich bei Kontrollen ermitteln, ob das System korrekt genutzt wird.

Ein Logfile erscheint häufig in Form einer Excel-Tabelle, in welche die für den Nachvollzug der von den Nutzern getätigten Vorgänge erforderlichen Informationen übertragen werden. Wir konzentrieren uns hier besonders auf die Logfiles des Schengener Informationssystems (SIS), doch gelten diese Überlegungen grösstenteils auch für andere Systeme.

Die Logfiles des SIS bezwecken die Nachverfolgung der Suchabläufe, die von den Nutzern getätigt worden sind. Dabei sind die wichtigsten in den SIS-Logfiles gespeicherten Informationen die Identität des Nutzers, das Datum und die genaue Zeit der Suche sowie die in die Suchmaske eingegebenen Daten. Diese Daten können Name, Vorname oder Geburtsdatum der gesuchten Person sein. Andere für die Analyse weniger wichtige Informationen sind ebenfalls in diesen Logfiles enthalten, etwa Daten über die vom System für die Ausführung der Abfrage verwendeten Prozesse. Die verschiedenen Informationen eines Logfiles – oder Eingaben – sind gewöhnlich in chronologischer Folge aufgeführt, können aber auch anders sortiert sein.

Wenn wir als Aufsichtsbehörde eine Kontrolle im Rahmen der Schengen-Abkommen vornehmen, beantragen wir bei fedpol den Zugriff auf die Logfiles des SIS. Zu diesem Zweck geben wir die Liste der betroffenen Nutzer sowie einen genau bestimmten Zeitraum an. Liste und Zeitraum werden so festgelegt, dass die spätere Analyse der uns zugestellten Logfiles möglichst stichhaltig ausfällt.

Mit der Auswertung können wir feststellen, ob die erfolgten Abfragen tatsächlich protokolliert worden sind. Dank einer eingehenderen Analyse können wir die Plausibilität und die Rechtmässigkeit der von den Nutzern getätigten Suchvorgänge überprüfen. Im Zweifelsfall nehmen wir eine gründlichere Kontrolle vor, indem wir den betreffenden Nutzer direkt zu den Gründen befragen, die ihn zu der verdächtigen Suche veranlasst haben. Der Nutzer wird so mit den von ihm in der Suchmaske eingegebenen Informationen konfrontiert und muss sich rechtfertigen.

Die Logfiles des SIS-Systems werden ein Jahr lang aufbewahrt. Danach werden sie vernichtet, und die durch die Nutzung des Systems hinterlassenen Spuren gehen verloren.

1.4.3 Koordinationsgruppe Schengen der Schweizerischen Datenschutzbehörden

Über die «Koordinationsgruppe der Schweizerischen Datenschutzbehörden im Rahmen der Umsetzung des Schengen-Assoziierungsabkommens» koordinieren wir unsere Aufsichtstätigkeiten betreffend die in der Schweiz im Bereich Migration, Polizei und Justiz vorgenommene Datenbearbeitung mit den kantonalen Datenschutzbehörden.

Die Koordinationsgruppe der Schweizerischen Datenschutzbehörden trat am 16. Februar 2011 und am 8. November 2011 zusammen. Bei diesen beiden Tagungen informierten wir die kantonalen Datenschutzbehörden über die wichtigsten von der Gemeinsamen Kontrollinstanz (GKI) Schengen bearbeiteten Punkte und ihre Tätigkeiten. Wir setzten unsere kantonalen Kollegen auch über die Ergebnisse unserer Kontrolle

bei der Schweizer Vertretung in Moskau in Kenntnis. Die Kantone ihrerseits stellten die Resultate ihrer Kontrolltätigkeiten bei den kantonalen Nutzern des SIS vor. Um in Fällen missbräuchlicher Nutzung des SIS zu privaten oder Ausbildungszwecken Abhilfe zu schaffen, hat die Koordinationsgruppe ein Schreiben in französischer, deutscher und italienischer Sprache verfasst, das die Dienststellen, die den Nationalen Teil des Schengener Informationssystems (N-SIS) nutzen, für das Problem sensibilisieren soll; dieses Schreiben wurde an die betroffenen eidgenössischen und kantonalen Behörden übermittelt.

1.4.4 Direktes Auskunftsrecht im Bereich innere Sicherheit (BWIS)

Im Rahmen der Änderung des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit hat das Parlament beschlossen, das indirekte Auskunftsrecht durch ein direktes zu ersetzen, vergleichbar mit dem für die Informationssysteme JANUS und GEWA geltenden. In den anderen von uns bemängelten Punkten ist das Parlament dem Vorschlag des Bundesrates gefolgt.

Im Dezember 2011 verabschiedete das Parlament eine Änderung des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit (BWIS). Im Gegensatz zum Entwurf des Bundesrates, der das direkte Auskunftsrecht in Anwendung von Artikel 8 und 9 des Datenschutzgesetzes (DSG) vorsah, beschloss das Parlament in der Differenzbereinigung zwischen den beiden Räten die Einrichtung eines direkten Auskunftsrechts, das sich zu einem grossen Teil auf die Bestimmungen betreffend dasjenige bei den Informationssystemen JANUS und GEWA stützt, wie sie im Bundesgesetz über die polizeilichen Informationssysteme des Bundes (BPI) enthalten sind.

Neu müssen die Auskunftsgesuche beim Nachrichtendienst des Bundes (NDB) eingereicht werden. Er kann seine Antwort in drei Fällen aufschieben:

- Wenn im Zusammenhang mit den über den Gesuchsteller bearbeiteten Daten ein überwiegendes Interessen an einer Geheimhaltung besteht, namentlich im Rahmen der frühzeitigen Erkennung und Bekämpfung von Gefährdungen durch Terrorismus, von verbotenem Nachrichtendienst, gewalttätigem Extremismus, Vorbereitungen zu verbotenem Handel mit Waffen und radioaktiven Materialien sowie zu verbotenem Technologietransfer und im Rahmen einer Strafverfolgung oder eines anderen Untersuchungsverfahrens.
- Wenn die überwiegenden Interessen einer Drittperson es erfordern.
- Wenn über die gesuchstellende Person keine Daten bearbeitet werden.

In diesen drei Fällen teilt der NDB der gesuchstellenden Person den Aufschub der Auskunft mit und weist sie darauf hin, dass sie das Recht hat, von uns zu verlangen, dass wir prüfen, ob die Datenbearbeitung rechtens und der Aufschub gerechtfertigt ist. Wir führen die verlangten Prüfungen durch und teilen der gesuchstellenden Person mit, dass entweder in Bezug auf sie keine Daten unrechtmässig bearbeitet werden oder dass wir im Falle von Fehlern bei der Datenbearbeitung oder betreffend den Aufschub der Auskunft eine Empfehlung an den NDB gerichtet haben. Wir weisen die gesuchstellende Person auch darauf hin, dass sie vom Bundesverwaltungsgericht (BVGer) verlangen kann, diese Mitteilung oder gegebenenfalls den Vollzug der Empfehlung zu überprüfen. Das BVGer führt auf Verlangen des Gesuchstellers die Prüfung durch und teilt ihm dies anschliessend mit. Im Falle von Fehlern richtet das BVGer eine Verfügung zu deren Behebung an den NDB. Sobald das Geheimhaltungsinteresse dahingefallen ist, spätestens aber nach Ablauf der Aufbewahrungsdauer, erteilt der NDB dem Gesuchsteller Auskunft. Personen, die nicht registriert sind, informiert der NDB spätestens drei Jahre nach Eingang ihres Gesuches über diese Tatsache. Ausnahmsweise können wir empfehlen, dass der NDB sofort Auskunft erteilen solle, wenn und soweit damit keine Gefährdung der inneren oder äusseren Sicherheit verbunden ist. Diese neue Regelung erfordert noch einige Präzisierungen in Bezug auf ihre praktische Anwendung.

Was die Verankerung der in der Verordnung über die Ausdehnung der Auskunftspflichten und des Melderechts von Behörden, Amtsstellen und Organisationen zur Gewährleistung der inneren und äusseren Sicherheit enthaltenen Normen im BWIS anbelangt, hat das Parlament unseren Bemerkungen nicht Rechnung getragen (vgl. unseren 18. Tätigkeitsbericht 2010/2011, Ziff. 1.4.6).

1.4.5 Auskunftsgesuche zum Informationssystem ISIS

2011 erreichte die Zahl der Auskunftsgesuche betreffend das Informationssystem ISIS den dritthöchsten Stand seit 1998. Im Dezember beschloss das Parlament die Einführung eines direkten Auskunftsrechts, das mit der für die Informationssysteme JANUS und GEWA geltenden Berechtigung vergleichbar ist.

Im Jahr 2011 wurden in unserem Sekretariat 66 indirekte Auskunftsgesuche zum Informationssystem ISIS eingereicht. Das ist die dritthöchste Zahl seit 1998. 2010 waren 410 Gesuche geprüft worden (vgl. unseren 18. Tätigkeitsbericht 2010/2011, Ziff. 1.4.7), zwei Jahre zuvor 148 (vgl. unseren 16. Tätigkeitsbericht 2008/2009, Ziff. 1.4.4).

Das Parlament beschloss am 23. Dezember die Änderung des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit (BWIS). In diesem Rahmen wurde Artikel 18 über das Auskunftsrecht abgeändert; die neue Regelung führt ein direktes

Auskunftsrecht ein, das mit der für die Informationssysteme JANUS und GEWA geltenden Berechtigung vergleichbar ist.

Für weitere Einzelheiten zu dieser Neuregelung siehe Ziff. 1.4.4. des vorliegenden Tätigkeitsberichts.

1.4.6 Pilotbetrieb des Informationssystems ISAS

Die für den Pilotbetrieb ISAS geltende Rechtsgrundlage wurde so angepasst, dass sie die tatsächlichen Verhältnisse und nicht die geplante endgültige Betriebssituation widerspiegelt. Eine abschliessende Liste der Datenfelder muss auch für einen Pilotbetrieb definiert werden. Entsprechend haben der Bundesrat und das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport zwei Verordnungen betreffend den Pilotbetrieb ISAS abgeändert.

Wir hatten den Nachrichtendienst des Bundes (NDB) ersucht, uns einen Zwischenbericht zum Pilotbetrieb ISAS zu übermitteln (vgl. unseren 18. Tätigkeitsbericht 2010/2011, Ziff. 1.4.8). Zu diesem Bericht haben wir namentlich in zwei wichtigen Punkten Bemerkungen abgegeben.

Erstens stellten wir fest, dass die Realität des Pilotbetriebs nicht der Rechtsgrundlage entsprach, welche festhielt, das Informationssystem ISAS bestehe aus mehreren Datenbanken. In Wirklichkeit ist das ISAS aber eine einzige Datenbank. Wir ersuchten daher den NDB, das Informatikkonzept entsprechend der geltenden Rechtsgrundlage anzupassen, oder diese so abzuändern, dass sie die tatsächliche Situation des Pilotbetriebs ISAS widerspiegelt. Der NDB entschied sich für eine Anpassung der Rechtsgrundlage.

Zweitens waren die verschiedenen Datenfelder nicht in der Rechtsgrundlage aufgeführt. Stattdessen umfasste sie eine Beschreibung des Modells der verwendeten Datenbank. Diese war zudem so ausgestaltet, dass Datenfelder von den Nutzern definiert werden konnten. Eine solche Definition der Datenfelder während des Pilotbetriebs ist jedoch nicht im Einklang mit den Datenschutzanforderungen. Während eines Pilotbetriebs kann die Bearbeitung von besonders schützenswerten Daten oder Persönlichkeitsprofilen zwar in einer vorläufigen, untergeordneten Rechtsgrundlage geregelt werden. Die Datenfelder müssen allerdings ebenso wie für den endgültigen Betrieb eines Informationssystems abschliessend bestimmt werden. Erweisen sich im Laufe des Pilotbetriebs neue Datenfelder als notwendig, muss die entsprechende Bestimmung abgeändert werden. Analog haben wir den NDB aufgefordert, eine

abschliessende Liste der Datenfelder des Informationssystems ISAS zu erstellen und sie in die für den Pilotbetrieb geltende Rechtsgrundlage aufzunehmen. Dem kam der NDB nach.

Die Änderung der Verordnung über die Informationssysteme des Nachrichtendienstes des Bundes (ISV-NDB) ist am 1. Januar 2012 in Kraft getreten; die Verordnung beschreibt den Ist-Zustand des Pilotbetriebs ISAS, nicht etwa den möglichen definitiven Betrieb des Informationssystems. Zum gleichen Zeitpunkt ist eine Änderung der Verordnung des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport (VBS) über die Datenfelder und die Abfrageberechtigungen in den Informationssystemen ISAS und ISIS in Kraft getreten. Diese Änderung betrifft namentlich die abschliessende Liste der Datenfelder des Informationssystems ISAS.

1.4.7 Überprüfungsgesuche betreffend N-SIS und die Informationssysteme JANUS und GEWA

Pro Jahr erhalten wir durchschnittlich sieben Überprüfungsgesuche betreffend die Informationssysteme JANUS und GEWA. Zum nationalen Teil des Schengener Informationssystems haben die europäischen Datenschutzbehörden seit dem Beitritt der Schweiz zum Schengen-Raum 15 Überprüfungsgesuche an uns gerichtet, und drei Personen haben ähnliche Gesuche eingereicht.

Im Rahmen der Auskunftsgesuche zu den Informationssystemen JANUS und GEWA sieht das Bundesgesetz über die polizeilichen Informationssysteme des Bundes (BPI) vor, dass das Bundesamt für Polizei (fedpol) seine Auskunft aufschiebt, wenn betreffend die Daten der gesuchstellenden Person überwiegende Interessen der Strafverfolgung an einer Geheimhaltung bestehen oder wenn die gesuchstellende Person nicht registriert ist. In beiden Fällen teilt fedpol der gesuchstellenden Person diesen Aufschub mit und weist sie darauf hin, dass sie vom EDÖB verlangen kann zu prüfen, ob allfällige Daten rechtmässig bearbeitet werden und ob überwiegende Geheimhaltungsinteressen den Aufschub rechtfertigen. Seit der Inkraftsetzung des BPI am 5. Dezember 2008 haben wir 22 solche Überprüfungsgesuche erhalten (fünf im Jahr 2009, zwölf im Jahr 2010 und fünf im Jahr 2011) .

Gemäss der für den nationalen Teil des Schengener Informationssystems (N-SIS) geltenden Gesetzgebung hat jedermann das Recht, von den Kontrollbehörden die Überprüfung der ihn betreffenden Daten sowie deren Verwendung zu verlangen. Seit dem Beitritt der Schweiz zum Schengen-Raum am 12. Dezember 2008 haben uns drei Personen um Überprüfungen im N-SIS ersucht. Im selben Zeitraum haben wir von unseren europäischen Kollegen 15 Überprüfungsgesuche erhalten. Auch von im Ausland

wohnhaften Personen sind mehrere solche Gesuche bei uns eingegangen; sie entsprachen eher Auskunftsgesuchen zum N-SIS als Überprüfungsgesuchen. Wir leiteten diese Gesuche an das fedpol weiter und wiesen die betroffenen Personen darauf hin, dass für das N-SIS in der Schweiz ein direktes Auskunftsrecht gilt und Gesuche daher direkt an dessen Verwaltungsstelle, also an das fedpol, zu richten sind.

1.4.8 Klarere Vorgaben für die Überwachung des Post- und Fernmeldeverkehrs (BÜPF)

Im Rahmen der Ämterkonsultationen zur Teilrevision der Verordnung zur Überwachung des Post- und Fernmeldeverkehrs sowie zu den Vernehmlassungsergebnissen der Totalrevision des Bundesgesetzes haben wir Stellungnahmen abgegeben. Dabei haben wir uns auch zum Einsatz von sogenannten Staatstrojanern geäussert.

Die Überwachung des Post- und Fernmeldeverkehrs durch Strafverfolgungsbehörden wurde im vergangenen Jahr in den Medien eingehend diskutiert, insbesondere auch die Überwachung mittels «GovWare» (auch «Staatstrojaner» genannt). Wir haben im Rahmen der Ämterkonsultation zur Teilrevision der Verordnung zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF) Stellung genommen und unter anderem darauf hingewirkt, dass die Terminologie für den Geltungsbereich an diejenige im Bundesgesetz zur Überwachung des Post- und Fernmeldeverkehrs (BÜPF) angeglichen wird. So werden die der VÜPF unterstellten Fernmeldedienst- und Internetzugangsanbieter klarer umschrieben. Unser zum Antennensuchlauf gemachter Einwand, dass der Kreis der beschuldigten Personen durch die Angabe von Suchkriterien bereits in der Überwachungsanordnung klarer definiert werden muss, wurde im Antrag an den Bundesrat ausgewiesen und sollte im Rahmen der anstehenden Totalrevision des BÜPF erneut geprüft werden.

In der Diskussion über den Einsatz von «GovWare» zur Strafverfolgung wurden wir in die Kommission für Rechtsfragen des Nationalrates eingeladen. Wir haben darauf hingewiesen, dass Eingriffe in die Grundrechte einer formellen und materiellen gesetzlichen Grundlage bedürfen, die zudem genügend bestimmt sein muss. Dies gilt wegen ihren vielfältigen Konfigurationsmöglichkeiten für den Funktionsumfang der Software ebenso wie für die Anforderungen an den Überwachungsantrag und den Deliktkatalog. Die Schaffung einer klaren Rechtsgrundlage für den Einsatz der Software zur Verfolgung von schweren Straftatbeständen, einschliesslich des dazugehörigen öffentlichen Diskurses, erscheint uns auch im Hinblick auf die Arbeit der Strafverfolgungsbehörden wichtig zu sein. Die gesetzliche Grundlage soll mit der laufenden Totalrevision des BÜPF geschaffen werden.

1.4.9 Schulung des Nachrichtendienstes

Zusammen mit der Datenschutzberaterin durften wir beim Nachrichtendienst des Bundes eine Weiterbildung durchführen. Zuerst vermittelten wir den Mitarbeitenden einen allgemeinen Einblick in den Datenschutz. Danach folgte ein Teil zum Auskunftsrecht in Theorie und Praxis.

Zusammen mit der Datenschutzberaterin des Nachrichtendienstes des Bundes (NDB) haben wir für die Weiterbildung der Mitarbeitenden das Datenschutzmodul gestaltet. Dieses Modul mit dem Titel «Direktes und indirektes Auskunftsrecht in Theorie und Praxis» trugen wir insgesamt sechsmal vor, viermal auf Deutsch und zweimal auf Französisch. In einem ersten Teil brachten wir den Teilnehmerinnen und Teilnehmern die allgemeinen Grundsätze des Datenschutzgesetzes näher und wiesen darauf hin, dass jede Person in ihrem täglichen Leben immer wieder mit dem Datenschutz konfrontiert werde. Beispiele dazu waren das Bearbeiten von Personendaten durch Kreditauskunfteien, im Gesundheitsbereich, bei der Videoüberwachung, durch Unternehmen beim Umgang mit Kundendaten und durch Bundesbehörden, etwa für das Führen des Fahrberechtigungsregisters.

Der Hauptteil des Moduls bildete das Auskunftsrecht. Nach einigen Ausführungen zum direkten Auskunftsrecht nach Datenschutzgesetz erläuterten wir das zurzeit noch für das Informationssystem ISIS des NDB geltende so genannte indirekte Auskunftsrecht. Dabei erklärten wir, wie wir beim Prüfen dieser indirekten Auskunftsgesuche in der Praxis vorgehen. Danach führte die Datenschutzberaterin des NDB aus, wie der NDB registrierten Personen, die ein Auskunftsgesuch gestellt haben, Auskunft erteilt, wenn allfällige Geheimhaltungsinteressen zur Wahrung der inneren Sicherheit weggefallen sind.

Als Ausblick erklärten wir, wie das Auskunftsrecht bei der Bundeskriminalpolizei für das System Bundesdelikte geregelt ist. Es folgten eine kurze Zusammenfassung der mündlichen Beratungen des Bundesgerichts zum Urteil vom 2. November 2011 betreffend ein indirektes Auskunftsgesuch, sowie ein Hinweis auf die damals aktuellen Beratungen im Parlament betreffend die Revision des Auskunftsrechts beim NDB. Inzwischen hat das Parlament für das Informationssystem ISIS eine analoge Regelung wie für das System Bundesdelikte verabschiedet (vgl. Ziff. 1.4.4 des vorliegenden Tätigkeitsberichts).

1.5 Gesundheit und Forschung

1.5.1 SwissDRG: Revision von Krankenversicherungsgesetz und -verordnung

Die Regelung der datenschutzkonformen Übermittlung von Gesundheitsdaten im Rahmen der Rechnungsstellung im stationären, akut-somatischen Bereich im System SwissDRG stellt für alle Beteiligten eine grosse Herausforderung dar. Nach dem Scheitern der Tarifpartner muss nun eine gesetzliche Lösung gefunden werden.

Seit dem 1. Januar 2012 ist die neue Spitalfinanzierung in Kraft. Kernstück sind die Fallkostenpauschalen («Diagnoses Related Groups» oder kurz: DRG) im Bereich der stationären akut-somatischen Behandlung. Für die Schweiz wurde im Prinzip das deutsche System (G-DRG) adaptiert und so SwissDRG kreiert.

Entsprechend dem schweizerischen Gesundheitssystem hätten die Tarifpartner (der Versicherungsverband santésuisse, der Spitalverband H+ und die Konferenz der kantonalen Gesundheitsdirektorinnen und -direktoren GDK) sich in einem für die ganze Schweiz gültigen und durch den Bundesrat genehmigten Tarifstrukturvertrag auch über die systematische Übermittlung der Diagnose- und Prozedurendaten mit der Rechnung zum Zweck der Rechnungsprüfung einigen sollen. Diese Vereinbarung hätte gewährleisten sollen, dass die Krankenversicherer in Einklang mit dem datenschutzrechtlichen Grundsatz der Verhältnismässigkeit und mit der Rechtsprechung des Bundesverwaltungsgerichts nur diejenigen Daten erhalten, welche sie für die Rechnungsprüfung wirklich benötigen. Die Tarifparteien verabschiedeten bereits im Juli 2009 einen Tarifstrukturvertrag, welcher auch vom Bundesrat genehmigt wurde. Allerdings hielt dieser fest, dass gerade die Übermittlung von Diagnose- und Prozedurendaten noch nicht ausreichend geregelt sei, und forderte die Parteien zur Nachbesserung auf.

Die Verhandlungen der Tarifpartner, an welchen wir selbstverständlich nicht teilgenommen haben und über deren Verlauf wir nur indirekt informiert wurden, verliefen offenbar sehr harzig. Wir erhielten den Eindruck, dass Fragen des Datenschutzes mit Finanzfragen vermischt wurden. Schliesslich trafen die Tarifpartner eine entsprechende Zusatzvereinbarung, doch die Mitglieder des Spitalverbandes H+ lehnten den Vertrag in einer internen Abstimmung im August 2011 ab. Da eine einvernehmliche Regelung durch die Tarifpartner innert nützlicher Frist nicht mehr zu erwarten war und eine Vielzahl von möglicherweise unterschiedlichen kantonalen Regelungen verhindert werden musste, schritt das zuständige Eidgenössische Departement des Innern (EDI) ein und erklärte, dass es die Datenübermittlung gesetzlich regeln werde. Mit einer Revision des

Bundesgesetzes über die Krankenversicherung (KVG) sollen nun die Leistungserbringer verpflichtet werden, auf der Rechnung die Diagnosen und Prozeduren codiert aufzuführen. Die Details bezüglich der Übermittlung der Daten soll der Bundesrat unter Wahrung des Verhältnismässigkeitsprinzips in der Verordnung über die Krankenversicherung (KVV) regeln. Diesbezüglich haben wir intensiv mit dem Generalsekretariat des EDI zusammengearbeitet und entsprechende Lösungsvorschläge präsentiert. Unsere Forderung lautet, einfach formuliert: Die Versicherer sollen diejenigen Daten bekommen, welche sie wirklich benötigen. Zudem muss sichergestellt werden, dass innerhalb der Versicherung nur diejenigen Personen Zugang zu diesen hochsensiblen Daten haben, die ihn wirklich brauchen. Das haben die Versicherer durch geeignete technische und organisatorische Massnahmen wie etwa Verschlüsselungstechnologien zu garantieren und muss regelmässig überprüft werden.

Die Entwicklung bezüglich SwissDRG muss genau beobachtet werden. Das Schaffen einer unabhängigen Clearingstelle für die Rechnungsprüfung bleibt eine ernsthaft zu prüfende Alternative zum jetzt bestehenden System.

1.5.2 Bundesgesetz über das elektronische Patientendossier

Im Rahmen einer Ämterkonsultation nahmen wir Stellung zum Vorentwurf des neuen Bundesgesetzes über das elektronische Patientendossier. Es regelt wichtige Aspekte wie etwa den Zugang zum Dossier. Einige zentrale Datenschutzanforderungen wurden auf unser Verlangen im Gesetzesentwurf berücksichtigt, welcher Ende 2011 in die Vernehmlassung geschickt wurde.

Das elektronische Patientendossier ist das zentrale Element in eHealth. Es ist ein virtuelles Dossier, über das dezentral behandlungsrelevante Daten einer Patientin oder eines Patienten in einem Abrufverfahren zugänglich gemacht werden. Dabei handelt es sich um besonders schützenswerte Personendaten. Ihre Bearbeitung muss konkret und verbindlich geregelt werden. Aus diesem Grund haben wir verlangt, dass die Anforderungen des Datenschutzes und der Datensicherheit als Voraussetzung für eine Zertifizierung im Gesetz explizit erwähnt werden.

Bei der Regelung der Einwilligung haben wir gefordert, dass diese nur gültig ist, wenn sie nach angemessener Information über die Art und Weise der Datenbearbeitung und deren Auswirkungen freiwillig erfolgt ist. Der Gesetzesentwurf wurde dementsprechend angepasst.

Identifikatoren sind Merkmale, die einen Menschen bestimmbar machen. Mit der Authentifizierung wird überprüft, ob eine Person wirklich die ist, für die sie sich ausgibt. Nach erfolgreicher Authentifizierung kann die Person für den Zugriff auf ihre

Daten autorisiert werden. Die Qualität des Verfahrens steht und fällt mit der Qualität des Identifikators. Wenn dieser ungeeignete Merkmale enthält, dann besteht das Risiko, dass die Zuordnung zu einer Person nicht eindeutig ist. Die Zentrale Ausgleichsstelle (ZAS), die Herausgeberin der neuen AHV-Nummer (AHVN13), geht selber davon aus, dass circa 200´000 Personen mehr als eine AHVN13 zugeteilt erhalten haben. Die ZAS empfiehlt deshalb, die AHV-Nummer mit mindestens fünf weiteren Merkmalen zu verknüpfen. Dem schliessen wir uns an.

Des Weiteren fordern wir, dass mit der AHVN13 weder eine direkte noch indirekte Verknüpfung mit Gesundheitsdaten möglich sein darf. Dies weil sie mit zunehmender Verwendung im Bereich der Verwaltung (Bund und Kantone) mit zahlreichen anderen Datensätzen verknüpft wird. Gemäss Gesetzesentwurf kann der Bundesrat vorsehen, dass zertifizierte Gemeinschaften die Versichertennummer als Merkmal zur Identifikation von Patienten verwenden können. Für diesen Fall empfehlen wir, die AHVN13 systematisch so umzuwandeln, dass sie als sektorielle Nummer verwendet werden kann.

1.5.3 Systematische Aktenerfassung durch die SUVA

Eine Sachverhaltsabklärung hat gezeigt, dass bei der SUVA die notwendigen Massnahmen für eine systematische Aktenerfassung getroffen sind und somit prinzipiell auch das Auskunftsrecht gemäss Datenschutzgesetz gewährleistet werden kann.

Ein Anwalt hat uns schriftlich auf Ungereimtheiten in Bezug auf ein von der SUVA geführtes Dossier hingewiesen. Er hatte im Auftrag seines Klienten im Verlauf einer gerichtlichen Auseinandersetzung mehrere Akteneinsichtsgesuche gemäss Artikel 46 des Bundesgesetzes über den Allgemeinen Teil des Sozialversicherungsrechts (ATSG) getätigt. Hierbei stellte er fest, dass der Umfang des Dossiers variierte und die erhaltenen Akten zum Teil unterschiedlich nummeriert waren. Da die systematische Aktenerfassung eine grundlegende Voraussetzung für die Gewährleistung des Auskunftsrechts gemäss Datenschutzgesetz ist, haben wir eine Sachverhaltsabklärung durchgeführt. Ziel war nicht die Klärung des vom Anwalt angezeigten Falles, sondern die grundsätzliche Überprüfung, ob es bei der SUVA Anzeichen gibt dafür, dass die systematische Aktenerfassung nicht gewährleistet ist.

Unsere Sachverhaltsfeststellung hat sodann ergeben, dass verschiedene Elemente die systematische Aktenerfassung und insbesondere die konsistente Nummerierung der Akten negativ beeinflussen könnten: Einerseits muss die zuständige Agentur im Fall einer gerichtlichen Auseinandersetzung zwischen einer versicherten Person und der SUVA das Originaldossier an die Rechtsabteilung des SUVA-Hauptsitzes in Luzern

übermitteln, damit diese es dem Gericht zustellen kann. So verbleiben der zuständigen Agentur und auch der Rechtsabteilung am Hauptsitz lediglich Kopien. Andererseits befindet sich die SUVA derzeit in einer Übergangsphase vom Papierdossier zur elektronischen Posteingangsverarbeitung. So muss im Einzelfall jeweils in der zuständigen Agentur entschieden werden, welches das massgebliche Dossier ist (Papier- oder elektronisches Dossier). Diese Umstände, gerade wenn sie, wie im vom Anwalt angezeigten Fall, in Kombination auftreten, stellen potentielle Fehlerquellen dar. Unsere Sachverhaltsabklärung hat aber gezeigt, dass die SUVA die notwendigen grundsätzlichen Massnahmen für die Gewährleistung einer systematischen Aktenerfassung auch in dieser Übergangsphase getroffen hat. Somit bestand kein Grund für den Erlass einer Empfehlung.

1.5.4 Sachverhaltsabklärung bei der SUVA

Wir haben bei der SUVA eine Sachverhaltsabklärung im Bereich Case Management durchgeführt. Dabei hat sich herausgestellt, dass das Case Management an und für sich keine Datenschutzprobleme verursacht. Allerdings zeigten sich Mängel in der Verwaltung der Zugriffsberechtigungen auf die Versichertendaten. Die SUVA hat das Problem erkannt und mit Sofortmassnahmen die Zahl der Berechtigten reduziert.

Im Rahmen einer Sachverhaltsabklärung bei der SUVA wurde unter anderem das Rollen- und Berechtigungskonzept überprüft. Es kennt vier Stufen der Zugriffsberechtigung: Der Zugriff für Mitarbeiter auf Dossiers in ihrer Agentur, auf Dossiers in fremden Agenturen, für Mitarbeiter in Abteilungen (z.B. Rechtsdienst) und der Zugriff auf Dossiers über Berufsunfälle. Unsere Abklärungen haben ergeben, dass eine unverhältnismässig grosse Anzahl von Mitarbeitern über eine Berechtigung für Zugriffe auf Dossiers in fremden Agenturen verfügt. Zwar wurde einem Mitarbeiter diese Berechtigung erst gewährt, wenn es für die Bearbeitung eines Dossiers erforderlich war. Danach wurde sie allerdings nicht wieder rückgängig gemacht. Ein weiterer Mangel des Konzepts der SUVA ist, dass die Zugriffsberechtigungen für alle Dossiers einer Agentur gelten.

Die Direktion der SUVA hat als erste Sofortmassnahme eine Reduktion der Zugriffsberechtigungen auf agenturfremde Dossiers in die Wege geleitet. Mitarbeiter verlieren den Zugriff auf fremde Agenturen, wenn sie ihn nicht mehr benötigen. Die Massnahme steht auch im Zusammenhang mit einer grösseren Anpassung des Rollen- und Berechtigungskonzepts. Wir werden im Sommer 2012 die Ergebnisse zusammen mit der SUVA analysieren und kritisch beurteilen.

Dieser Fall ist ein klassisches Beispiel für eine Datenschutzverletzung, die aus einem systematischen Mangel in einem Berechtigungskonzept resultiert. Es werden zwar Regeln für die Vergabe von Rollen und Zugriffsberechtigungen aufgestellt. Die Änderung der Rolle oder Berechtigung ist aber nicht geregelt. Das Ergebnis ist eine historisch gewachsene Sammlung von Berechtigungen, die jede Verhältnismässigkeit vermissen lässt. Zu einem Verfahren für die Vergabe von Zugriffsrechten gehört deshalb immer auch eines für deren Entzug.

1.5.5 Kreisschreiben 7.1 des Bundesamtes für Gesundheit

Das Bundesamt für Gesundheit hat im August 2011 ein Kreisschreiben an sämtliche Krankenversicherer versandt. Es weist unserer Ansicht nach problematische Aspekte auf, namentlich hinsichtlich der Vorlage der Bearbeitungsreglemente, der Nachvollziehbarkeit von diagnosebezogenen Daten sowie des Case Management.

Das Bundesamt für Gesundheit (BAG) hat im August 2011 unter dem Titel «Datenschutzkonforme Organisation und Prozesse der Krankenversicherer» das Kreisschreiben 7.1 an sämtliche Krankenversicherer des obligatorischen Bereichs verschickt. Es soll sie an die geltenden Datenschutzgrundsätze und -vorgaben erinnern. Auch wird auf das Inkrafttreten neuer Artikel des Krankenversicherungsgesetzes (KVG) und deren Umsetzung hingewiesen.

Einige Punkte möchten wir hervorheben, da sie bei uns Erstaunen ausgelöst haben: Das Kreisschreiben enthält zunächst Aussagen, wonach die Krankenversicherer ohne substantiierte Rechnungsstellung keine Zahlung an die Leistungserbringer ausrichten müssen. Insbesondere fanden wir erstaunlich, dass das BAG diese Regeln letzten Sommer versandte, stand doch die Einführung von SwissDRG bevor, in deren Rahmen die Datenübermittlung zwischen Leistungserbringern und Krankenversicherern erst noch in einer neuen Verordnung geregelt werden muss. Das Kreisschreiben befasst sich weiter mit Case Management. Dabei bleibt für uns die Frage offen, wem die Case Manager organisatorisch unterstellt sind und auf welche Daten sie Zugriff haben. Es gilt aus unserer Sicht sicherzustellen, dass die von den Case Managern bearbeiteten Daten nach Abschluss eines Falles nicht in das auch anderen Mitarbeitern zugängliche Dossier gelangen. Eine Einwilligung in das Case Management kann unseres Erachtens keine Erweiterung der gesetzlichen Ermächtigung zur Datenbearbeitung mit sich bringen.

Ein spezifischer Punkt dieses Kreisschreibens hat auch Konsequenzen für uns: Das Inkrafttreten des Artikels 84b KVG betrifft uns insofern, als dass uns die Krankenversicherer ab dem 1. Januar 2012 ihr Bearbeitungsreglement unaufgefordert zur

Beurteilung vorlegen müssen. Wie wir jedoch bereits gegenüber der zuständigen Kommission erklärt haben und Ständerätin Erika Forster-Vannini anlässlich der Sitzung der Kammer vom 6. Dezember 2007 ausdrücklich wiederholt hat, verfügen wir derzeit nicht über die personellen Ressourcen, um systematisch alle Bearbeitungsreglemente der nach KVG zugelassenen Krankenversicherer zu beurteilen. Vielmehr werden wir entsprechend den uns zur Verfügung stehenden Ressourcen und den von uns gesetzten Prioritäten Stichprobenkontrollen durchführen. Da Krankenversicherer nach KVG Organe des Bundes sind, haben sie bereits heute aufgrund der Verordnung zum Datenschutzgesetz (VDSG) die Pflicht, die erforderlichen technischen und organisatorischen Massnahmen zum Schutz der Persönlichkeit und der Grundrechte der Person, über die Daten bearbeitet werden, zu treffen. Zudem müssen sie ein Datenbearbeitungsreglement für jede von ihnen betriebene automatisierte Datensammlung führen, aktuell halten und uns zur Verfügung stellen. In diesem Sinne wiederholt und verdeutlicht Artikel 84b bereits bestehende gesetzliche Verpflichtungen. Neu ist hingegen, dass die Krankenversicherer ab dem 1. Januar 2012 gemäss Art. 84b KVG ihre Bearbeitungsreglemente veröffentlichen müssen. Diese Pflicht besteht dabei unabhängig von einer durch uns allenfalls vorgenommenen Beurteilung.

Wenn wir das Bearbeitungsreglement eines Krankenversicherers beurteilen, so wird dies in Form einer Sachverhaltsabklärung gemäss Art. 27 Abs. 2 DSG erfolgen. Der betreffende Krankenversicherer wird selbstverständlich schriftlich informiert. Sollte eine Empfehlung notwendig sein, so sind wir ohnehin dazu verpflichtet, das Eidgenössische Departement des Innern (EDI) als zuständiges Departement zu informieren. Wir können uns durchaus vorstellen, gleichzeitig auch das BAG zu benachrichtigen – und es wäre wünschenswert, dass letzteres uns über anlässlich eines Audits festgestellte datenschutzrechtliche Probleme bei einem Krankenversicherer informieren würde.

Zur Gültigkeit eines Bearbeitungsreglements halten wir folgendes fest: Auch mit dem neuen Art. 84b KVG haben wir keine Kompetenz zur Vorabklärung solcher Sachverhalte erhalten. Die Krankenversicherer nach KVG haben als Bundesorgane ein Bearbeitungsreglement zu erstellen, das den gesetzlichen Anforderungen zu entsprechen hat. Die Gültigkeit eines Datenbearbeitungsreglements ergibt sich daraus, dass die betreffende Versicherung es für sich als gültig und damit als verbindlich erklärt – auch ohne unsere Beurteilung.

1.5.6 Datenübermittlung durch die Spitex an ein Forschungszentrum

Mit Hilfe einer Einweg-Funktion (Hash-Funktion) kann man aus identifizierenden Daten einen Nummerncode erstellen, welcher es ermöglicht, Daten pseudonymisiert für Qualitätssicherungs- oder Forschungszwecke zur Verfügung zu stellen.

Heute benutzen die meisten Spitex-Organisationen moderne Informationssysteme, um die Daten der betreuten Personen effizient bearbeiten zu können. Diese Daten können auch für Qualitätssicherungs- oder Forschungszwecke verwendet werden. Dafür benötigt man eine zentrale Datenbank, in welche die dezentralen Spitex-Stellen ihre Angaben exportieren können. Aus Datenschutzgründen ist darauf zu achten, dass nur anonyme Daten weitergegeben werden. Für den Ablauf ist es notwendig, dass die im Verlauf der Zeit neu erfassten Informationen der zu betreuenden Personen an zentraler Stelle richtig zugeordnet werden können. Dies hat man mit einer so genannten Einweg- oder Hash-Funktion gelöst. So wird aufgrund der Ausgangsdaten (eindeutige Nummer ergänzt mit einem Zusatzcode [Salt] zur Erhöhung der Sicherheit) ein Pseudonym erzeugt, welches man aufgrund der eindeutigen Ausgangsdaten (pro Person) immer wieder erzeugen kann. Eine Umkehrung, also vom Pseudonym auf die Ausgangsdaten zu schliessen, ist aber nicht möglich. Mit einem solchen Vorgehen ist die Anonymität der zu betreuenden Personen gewährleistet, weil keine weiteren identifizierenden Daten wie bspw. Name oder Adresse weitergegeben werden.

Im Weiteren ist es wichtig, dass man auch die Datenfelder auf identifizierende Daten analysiert, die für die Qualitätssicherung oder Forschung zusammen mit dem Pseudonym an die zentrale Stelle übermittelt werden. Bei dieser Analyse ist uns aufgefallen, dass die Bekanntgabe der Berufsbezeichnung zusammen mit dem Geburtsjahr heikel sein kann, weil bei seltenen Berufen oder Funktionen die jeweilige Person bestimmt werden kann. In solchen Fällen ist es notwendig, die Berufsbezeichnung nicht festzuhalten oder einen übergeordneten Begriff zu verwenden.

1.5.7 Datenübermittlung in klinischen Studien

Klinische Studien, die sowohl die Behandlung von Patienten als auch die Forschung mit deren Personendaten bezwecken, stellen die Beteiligten vor datenschutzrechtlich heikle Probleme. Wir haben uns für sachgerechte Lösungen eingesetzt.

Swissmedic entschied 2010, bei internationalen Studien keine «Case Report Forms» (Falldokumentationen) zu akzeptieren, auf welchen Personendaten der Teilnehmer des klinischen Versuch enthalten sind. Dieser Entscheid stützte sich auf eine Stellungnahme

unsererseits; auf Anfrage von Swissmedic hatten wir uns zu der Frage geäussert, welche Anforderungen eine aus datenschutzrechtlicher Sicht genügende Pseudonymisierung erfüllen soll.

Gestützt auf den erwähnten Entscheid von Swissmedic sistierte eine kantonale Ethikkommission die Stellungnahme zum klinischen Versuch einer Forschungsgruppe. Diese Gruppe wandte sich in der Folge an uns, um eine datenschutzkonforme Lösung für die therapeutischen Studien im pädiatrisch-onkologischen Bereich zu finden. Solche Studien werden unter speziellen Umständen durchgeführt: Sie umfassen im Durchschnitt drei oder vier Patienten in der Schweiz, maximal aber 40. Aufgrund der kleinen Zahl von Kindern, die an seltenen Tumorkrankheiten leiden, ist eine Optimierung der Diagnostik und der Behandlung nur möglich, wenn eng mit ausländischen Institutionen zusammengearbeitet wird. Die Forschenden argumentierten, es sei dabei aus Gründen der Patientensicherheit notwendig, bei entsprechenden Anfragen und Gesprächen den vollen Namen und das Geburtsdatum zu übermitteln.

Wir organisierten eine Sitzung mit Vertretern der Forschungsgruppe und Swissmedic, um eine sachgerechte, datenschutzfreundliche Lösung für die Probleme zu finden. In einer im Anschluss an die Sitzung verfassten Stellungnahme äusserten wir uns zu den Bedingungen, die aus datenschutzrechtlicher Sicht erfüllt sein müssen. Ausgangspunkt bot dabei die Bestimmung des Zwecks, der mit den geplanten Datenbearbeitungen verfolgt werden sollte. Vorliegend waren es deren zwei: einerseits eine verbesserte Diagnostik und Behandlung der an der Studie teilnehmenden Personen, andererseits die Forschung mit den gewonnenen Erkenntnissen. Folgende Bedingungen sollten unserer Meinung nach erfüllt werden:

- In der ersten Phase eines klinischen Versuchs können die verschiedenen mitbehandelnden Stellen unter den geschilderten speziellen Bedingungen als erweitertes Behandlungsteam angesehen werden, in welchem auch Personendaten (unter Einhaltung der entsprechenden gesetzlichen Bestimmungen) übermittelt werden. Insbesondere müssen die Beteiligten darauf achten, dass die Daten nur in sicherer Art und Weise übermittelt werden und nur berechtigten Ansprechpartnern zugänglich sind.
- Im Studiendesign müssen die verschiedenen Phasen der Studie klar erkennbar sein. Die Einwilligung der Versuchspersonen muss alle Phasen umfassen.
- Der Übergang von Behandlung zu Forschung muss im Studiendesign ebenfalls ersichtlich sein. Einhergehend mit diesem Übergang müssen die Personendaten anonymisiert werden.
- Was den europäischen Kontext der Studie anbelangt, müssen die Eltern respektive die Kinder in die Bekanntgabe der Daten ins Ausland einwilligen. Werden

die aus der Schweiz übermittelten Daten von ausländischen Institutionen zu eigenen Zwecken weiterverwendet (bspw. Aufbau einer eigenen Forschungsdatenbank), müssen die betroffenen Personen ebenfalls einwilligen.

1.5.8 Schneeballsystem in der Forschung

Wir führten eine Sachverhaltsabklärung zu einem Forschungsprojekt an der ETH Zürich durch. Die Beschaffung der Kontaktdaten für die Anfrage neuer Forschungsteilnehmer folgte dabei dem Schneeballprinzip.

Wir führten im vergangenen Berichtsjahr eine Sachverhaltsabklärung an der ETH Zürich durch. Anlass dazu gab ein Forschungsprojekt, welches soziale Beziehungsnetze mit Fokus auf das Verkehrsverhalten untersucht. Dabei folgte die Rekrutierung neuer Teilnehmer nach dem Schneeballprinzip dem sozialen Netzwerk der befragten Personen; die Teilnehmer gaben den Forschenden die Kontaktdaten ihres Bekanntenkreises und gewisse Zusatzinformationen preis. Diese neuen Kontaktpersonen wurden von den Forschenden anschliessend über das Projekt informiert und ihrerseits um Teilnahme gebeten.

Nachdem wir zunächst eine solcherart kontaktierte Person über ihre Rechte informiert hatten, wurden wir letztes Jahr von der ETH Zürich nach Ausstrahlung eines Fernsehbeitrages um Unterstützung gebeten. Daraufhin entschlossen wir uns, eine Sachverhaltsabklärung durchzuführen. Wir stellten fest, dass die beteiligten Mitarbeitenden der ETH Zürich für datenschutzrechtliche Aspekte sensibilisiert sind und sich dafür einsetzen, die entsprechenden gesetzlichen Vorschriften einzuhalten. So wurden einige unserer Vorschläge umgehend umgesetzt, bspw. im Rahmen der Zugriffskontrolle auf die Forschungsdaten.

Im Bereich der rechtlichen Grundlagen ergaben unsere Abklärungen ein überraschendes Resultat. Normalerweise braucht ein Bundesorgan, um besonders schützenswerte Personendaten oder Persönlichkeitsprofile bearbeiten zu können, entsprechende Regelungen auf gesetzlicher Stufe. Die Forschung wird jedoch durch das Datenschutzgesetz mit erleichterten Bearbeitungsvorschriften teilweise privilegiert. Dies bedeutet konkret für den von uns beurteilten Sachverhalt, dass die ETH entsprechende Regelungen auf Verordnungsstufe bräuchte. Die für die Mitarbeitenden erlassene interne Richtlinie für die Integrität in der Forschung genügt dieser geforderten Normenstufe jedoch nicht. Die von uns vorgeschlagenen Gesetzesarbeiten betreffen die gesamte ETH. Deshalb hat die ETH Zürich mit dem ETH-Rat Kontakt aufgenommen, und die gesetzgeberischen Arbeiten sind zusammen mit dem Bundesamt für Justiz initiiert worden.

1.6 Versicherungen

1.6.1 Totalrevision des Versicherungsvertragsgesetzes

Das Versicherungsvertragsgesetz wird generalüberholt. Im nun dem Parlament unterbreiteten Entwurf ist vorgesehen, dass das Institut «Vertrauensarzt» endlich auch im Privatversicherungsbereich verankert werden soll.

Das über hundertjährige Versicherungsvertragsgesetz (VVG) genügt den heutigen Anforderungen nicht mehr. Mit einer Totalrevision soll es nun umfassend an die veränderten Gegebenheiten und Bedürfnisse angepasst werden. Wir haben uns im Rahmen der Ämterkonsultation zu datenschutzrelevanten Punkten der Vorlage geäussert.

Viele Arbeitgeber sichern ihre Lohnfortzahlungspflicht durch Kollektivkrankentaggeldversicherungen ab. Namentlich bei hohen zu versichernden Einkommen veranlassen die Versicherungsunternehmen vor Vertragsabschluss eine Gesundheitsprüfung. Dies kann die Ablehnung einzelner Arbeitnehmer oder die Aufnahme von Vorbehalten in Bezug auf einen bestimmten Arbeitnehmer zur Folge haben, was wiederum zu einem Dilemma führt: Der Arbeitgeber muss wissen, wann eine zur Finanzierung der Lohnfortzahlung abgeschlossene Versicherung nicht zahlen wird, da er in diesem Fall persönlich leistungspflichtig wird. Dies kann vor allem für Kleinbetriebe gravierende Folgen haben. Auf der anderen Seite kann der Arbeitnehmer ein schützenswertes Interesse an der Geheimhaltung gesundheitlicher Beeinträchtigungen haben.

Der ursprüngliche Vernehmlassungsentwurf wollte in diesem Interessenkonflikt den Arbeitnehmer entscheiden lassen, ob eine Ablehnung oder ein Vorbehalt dem Arbeitgeber mitzuteilen ist. Hätte er befürchten müssen, bei einer Offenlegung des Gesundheitszustands die Stelle zu verlieren, so hätte er die Möglichkeit haben sollen, die Vertraulichkeit durchzusetzen. Im Gegenzug wäre in diesem Fall die Lohnfortzahlungspflicht des Arbeitgebers auf das im Obligationenrecht vorgesehene Mindestmass begrenzt worden. Die Lösung stiess in der Vernehmlassung indes nur auf wenig Zustimmung. Deshalb wurde im Entwurf, der jetzt dem Parlament vorliegt, auf diese Bestimmung verzichtet. Das ist aus unserer Sicht bedauerlich. Die geschilderte Problematik wird immerhin teilweise dadurch gemildert, dass es nach neuem Recht der Kollektivkrankentaggeldversicherung untersagt sein wird, dem Arbeitgeber Daten über die Gesundheit oder die Intimsphäre des Arbeitnehmers bekannt zu geben. Wir haben in unserer Stellungnahme verdeutlicht, dass sich die Mitteilung des Versicherungsunternehmens an den Arbeitgeber nach einer Gesundheitsprüfung also strikt auf die Information zu beschränken haben wird, ob eine Aufnahme (allenfalls

unter Vorbehalt) oder eine Ablehnung erfolgte. Diese Präzisierung findet sich nun auch in der Botschaft.

Sehr erfreulich und wichtig ist für uns, dass unser seit langem immer wieder geäussertes Anliegen der Verankerung des Instituts des Vertrauensarztes im Privatversicherungsrecht in die Revisionsvorlage aufgenommen wurde. Der obligatorische Anwendungsbereich wird vorläufig allerdings noch auf die Krankenzusatz- und die Taggeldversicherung begrenzt sein. Längerfristig ist aus unserer Sicht eine kohärente Regelung des Vertrauensarztinstituts für das ganze Privat- und Sozialversicherungsrecht anzustreben.

1.6.2 Missbrauchsbekämpfung bei Motorfahrzeugversicherungen

Unsere Abklärungen in Sachen «Car Claims Information Pool», einer elektronischen Datenplattform von Motorfahrzeugversicherungen, sind abgeschlossen. Vorschläge zur Verbesserung von Datenschutz und Datensicherheit wurden akzeptiert.

Durch elektronischen Datenaustausch über den «Car Claims Information Pool» (CC-Info) bekämpfen schweizerische Motorfahrzeugversicherer Missbräuche. So soll etwa aufgedeckt werden, wenn ein Schaden an einem Fahrzeug bei einem zweiten Versicherer erneut geltend gemacht wird.

Wir haben im Berichtsjahr unsere Abklärungen zu CC-Info (vgl. unseren 18. Tätigkeitsbericht 2010/2011, Ziff. 1.6.1) abgeschlossen und einige Vorschläge zur Erhöhung von Datenschutz und Datensicherheit unterbreitet: So war es beim Zugriff auf CC-Info, der durch die beteiligten Versicherer über das Internet stattfindet, bis anhin möglich, dass mehrere Personen mit demselben Benutzeraccount gleichzeitig im System eingeloggt sind, was das Risiko unautorisierter Zugriffe erhöhte. Der Login-Prozess wurde so angepasst, dass ein (erneutes) Einloggen nicht mehr möglich ist, wenn ein Benutzer mit denselben Authentifizierungsmerkmalen bereits im System aktiv ist. Verbesserungen konnten wir auch hinsichtlich der zukünftigen Behandlung von Auskunftsbegehren erreichen. Es bestehen nun klare Richtlinien dazu, wie solche Begehren zu behandeln sind.

Die im Rahmen der Sachverhaltsabklärung involvierten Beteiligten zeigten durchwegs eine der Sache angemessene Sensibilität für datenschutzrechtliche Fragen. Wir sind überzeugt, dass unsere Verbesserungsvorschläge in sinnvoller Weise zur weiteren Erhöhung des Datenschutzniveaus von CC-Info beitragen konnten, ohne die Funktionalität und Praktikabilität des Systems unangemessen zu beeinträchtigen.

1.6.3 Amtshilfe an kantonale Steuerbehörden durch die Unfallversicherung

In einer rechtlichen Einschätzung kamen wir zum Schluss, dass Artikel 97 des Unfallversicherungsgesetzes abschliessend regelt, in welchen Fällen ein obligatorischer Unfallversicherer – in Abweichung von der gesetzlichen Schweigepflicht – den kantonalen Steuerbehörden Daten bekannt geben muss.

Wir wurden von einem obligatorischen Unfallversicherer um eine rechtliche Einschätzung gebeten zur Frage, ob die Versicherer gegenüber den kantonalen Steuerbehörden gestützt auf Artikel 112 Absatz 2 des Bundesgesetzes über die direkte Bundessteuer (DBG) in jedem Fall zur Amtshilfe verpflichtet seien, oder ob sich die Auskunftspflicht auf die in Artikel 97 des Unfallversicherungsgesetzes (UVG) erwähnten Fälle beschränke. Wir sind zu folgendem Schluss gekommen:

Obligatorische Unfallversicherer gelten als Bundesorgane und unterstehen demzufolge in diesem Bereich dem Datenschutzgesetz (DSG). Das heisst, sie dürfen Personendaten bearbeiten und bekannt geben, wenn dafür eine gesetzliche Grundlage besteht. Besonders schützenswerte Personendaten sowie Persönlichkeitsprofile dürfen sie nur bearbeiten und bekannt geben, wenn ein Gesetz im formellen Sinn es ausdrücklich vorsieht.

Zur Erfüllung ihrer Aufgaben im Bereich der obligatorischen Unfallversicherung bearbeiten die Versicherer regelmässig besonders schützenswerte Personendaten. Deshalb ist für die Bearbeitung solcher Daten eine formell-gesetzliche Grundlage notwendig, worin ausdrücklich geregelt ist, wie die Daten bearbeitet und wem welche Daten bekannt gegeben werden dürfen. Soweit die obligatorischen Unfallversicherer besonders schützenswerte Personendaten an die Steuerbehörden bekannt geben sollen, bedarf es einer Regelung in einem Bundesgesetz. Unterliegt ein Bundesorgan einer gesetzlichen Geheimhaltungspflicht, so hat es gemäss Art. 19 Abs. 4 lit. b DSG die Datenbekanntgabe abzulehnen, einzuschränken oder mit Auflagen zu verbinden.

Grundsätzlich ist ein obligatorischer Unfallversicherer aufgrund von Art. 112 Abs. 2 und Art. 112a DBG gegenüber den Steuerbehörden auskunftspflichtig. Dieser allgemeinen Auskunftspflicht steht jedoch die gesetzliche Schweigepflicht von Artikel 33 des Bundesgesetzes über den Allgemeinen Teil des Sozialversicherungsrechts (ATSG) gegenüber, welche auch für obligatorische Unfallversicherer gilt. Von ihr kann nur dann abgewichen werden, wenn eine gesetzliche Grundlage im ATSG selber oder in einer Einzelgesetzgebung vorhanden ist.

Die Ausnahmen von der Schweigepflicht im Anwendungsbereich der obligatorischen Unfallversicherung finden sich in Art. 97 UVG. Darin wird detailliert geregelt, in welchen Fällen die Unfallversicherer – in Abweichung von Art. 33 ATSG – Dritten Daten bekannt geben dürfen. Art. 97 UVG enthält in Abs. 1 lit. c und Abs. 2 je eine explizite Regelung für die Bekanntgabe an Steuerbehörden im Zusammenhang mit der Quellen- und der Verrechnungssteuer. In allen übrigen Fällen richtet sich die Datenbekanntgabe nach Art. 97 Abs. 6 UVG.

Im Gegensatz zu anderen Sozialversicherungsgesetzen (bspw. Art. 50a Abs. 1 lit. e des AHV-Gesetzes oder Art. 86a Abs. 1 lit. e des Bundesgesetzes über die berufliche Alters-, Hinterlassenen- und Invalidenvorsorge, kurz: BVG) enthält das UVG für eine Datenbekanntgabe an Steuerbehörden keine Regelung im Einzelfall und auf schriftlich begründetes Gesuch hin. Ob es sich hier um ein gesetzgeberisches Versehen oder um eine bewusste Unterlassung handelt, müsste durch die zuständigen Gerichte geklärt werden.

Wir sind daher auf der Basis der derzeitigen Gesetzeslage zum Schluss gekommen, dass Art. 97 UVG abschliessend regelt, in welchen Fällen von der gesetzlichen Schweigepflicht nach Art. 33 ATSG abgewichen werden darf und ein obligatorischer Unfallversicherer den Steuerbehörden Daten bekannt geben muss. Art. 112 und Art. 112a DBG gelangen damit nicht zur Anwendung, da sonst auf diesem Weg die spezialgesetzlichen Regelungen von Art. 97 UVG ausgehebelt würden.

Fehlt es an einer gesetzlichen Grundlage, können Bundesorgane Personendaten ausnahmsweise gestützt auf Art. 19 Abs. 1 lit. a-d DSG bekannt geben. Diese Ausnahmen gelten jedoch nur in Einzelfällen, welche in Art. 19 DSG abschliessend aufgezählt und eng auszulegen sind. Gestützt auf diese Bestimmungen könnte ein obligatorischer Unfallversicherer ausnahmsweise den kantonalen Steuerbehörden die erforderlichen Daten bekannt geben.

1.7 Arbeitsbereich

1.7.1 Bürgeranfragen zur Überwachung am Arbeitsplatz

Die vielen Anrufe an unseren telefonischen Beratungsdienst zum Thema Überwachung am Arbeitsplatz zeigen: Weder den Arbeitgebern noch den Arbeitnehmern ist klar, was wirklich zulässig ist.

Zahlreiche Arbeitgeber und Arbeitnehmer haben im Berichtsjahr unseren telefonischen Beratungsdienst kontaktiert und sich über die Zulässigkeit der Überwachung am Arbeitsplatz erkundigt. Dabei zeigte sich, dass hauptsächlich Videoüberwachung, Bewegungsüberwachung mittels firmeneigenen Smartphones oder anderen Geräten und die Überwachung von E-Mailverkehr und Surfverhalten die Topthemen sind.

Bei den Arbeitgebern konnten wir feststellen, dass sie sich primär nach dem datenschutzkonformen Vorgehen erkundigen. Seitens der Arbeitnehmer bemerkten wir, dass die Überwachung am Arbeitsplatz nicht prinzipiell in Frage gestellt wird; den meisten ist klar, dass überwacht wird, und das wird auch akzeptiert. Vielmehr richteten sich die Fragen darauf, was der Arbeitgeber wirklich tun darf. Oftmals handelte es sich bei den Ratsuchenden auch um Personen, die vom Arbeitgeber wegen ihres Verhaltens gerügt worden waren, Teil einer laufenden Untersuchung waren oder sogar entlassen wurden.

Das Grundproblem, aber auch die Lösung besteht in der Wahrung der Transparenz, in einer klaren Kommunikation. Der Arbeitgeber muss die Arbeitnehmer präzise darüber informieren, wie überwacht und ausgewertet wird und für welchen Zweck dies geschieht. Mit einem Nutzungs- und Überwachungsreglement muss er den Angestellten also seine Datenbearbeitungen ausdrücklich bekannt geben. Ebenso muss er klar erkennbar machen, welche Nutzung von E-Mail und Internet erlaubt und was verboten ist.

Selbstverständlich stellt sich auch in diesem Bereich immer wieder die Frage nach der Verhältnismässigkeit der vorgesehenen Überwachungsmassnahmen in Bezug auf den verfolgten Zweck. Hier müssen wir sagen, dass die technischen Möglichkeiten die Arbeitgeber teilweise zu unverhältnismässigen Überwachungsaktionen verleiten. Deshalb halten wir hier klar fest: Eine namentliche Auswertung der bei der Benutzung von Informations- und Kommunikationsmitteln (Telefon, E-Mail, Internet, Fax) anfallenden Daten ist nur dann zulässig, wenn der konkrete Verdacht eines erheblichen Missbrauchs besteht. Zudem muss feststehen, dass der Missbrauchsverdacht nicht durch ein anderes Vorgehen, das weniger stark in die Persönlichkeitsrechte der Arbeitnehmer eingreift, geklärt werden kann. Zudem: Überwachungs- und Kontrollsysteme, die der Verhaltensüberwachung dienen, sind illegal (Artikel 26 Verordnung 3 zum Arbeitsgesetz).

1.7.2 Zustellung von Pensionskassenausweisen – Urteil des Bundesverwaltungsgerichts

Fast zwei Jahre nachdem wir das Eidgenössische Departement des Innern (EDI) ersucht hatten, die unseres Erachtens gesetzeswidrige Praxis der offenen Zustellung von Pensionskassenausweisen über den Arbeitgeber zu unterbinden (vgl. unseren 17. Tätigkeitsbericht 2009/2010, Ziff. 1.7.8, und unseren 18. Tätigkeitsbericht 2010/2011, Ziff. 1.7.3) hat das Departement eine Verfügung in dieser Sache erlassen. Wir waren mit deren Inhalt nicht einverstanden und haben daher beim Bundesverwaltungsgericht (BVGer) beantragt, die Verfügung aufzuheben und die Pensionskasse anzuweisen, die persönlichen Pensionskassenausweise künftig so zuzustellen, dass ausschliesslich die versicherten Personen, insbesondere aber nicht deren Arbeitgeber, Kenntnis vom Inhalt dieser Ausweise erlangen können.

Das BVGer ist mit Urteil vom 10. April 2012 (A-4467/2011) unserer Rechtsauffassung vollumfänglich gefolgt. Es hat festgehalten, dass für die offene, ungeschützte Zustellung der persönlichen Ausweise über die Arbeitgeber keine gesetzliche Grundlage besteht. Die Pensionskasse verstosse damit gegen ihre Schweigepflicht und gegen den Grundsatz der Datensicherheit. Dies führe zu einer rechtswidrigen Persönlichkeitsverletzung der betroffenen versicherten Personen.

Das Urteil des BVGer war bei Redaktionsschluss dieses Tätigkeitsberichts noch nicht rechtskräftig.

1.7.3 Elektronisches Personaldossier in der Bundesverwaltung

Mit der Revision des Bundespersonalgesetzes wurde die Rechtsgrundlage für das elektronische Personalinformationssystem und für elektronische Personal- und Bewerbungsdossiers geschaffen.

Elektronische Personal- und Bewerbungsdossiers sind in der Privatwirtschaft eine Selbstverständlichkeit. Für Bundesorgane gilt aber das Legalitätsprinzip, das besagt, dass für jede Datenbearbeitung eine gesetzliche Grundlage bestehen muss. Für das Bearbeiten von besonders schützenswerten Personendaten und Persönlichkeitsprofilen muss sich diese Grundlage zudem in einem Bundesgesetz im formellen Sinn befinden. Personal- oder Bewerbungsdossiers enthalten höchstwahrscheinlich besonders schützenswerte Personendaten und stellen in der Regel ein Persönlichkeitsprofil dar. Weil eine Ermächtigung in einem Bundesgesetz im formellen Sinn bislang fehlte, hätten innerhalb der Bundesverwaltung eigentlich weder elektronische Personal- noch Bewerbungsdossiers geführt werden dürfen. Auch das Personalinformationssystem des Eidgenössischen Personalamtes (EPA) war bislang lediglich auf Verordnungsstufe geregelt.

Mit der Revision des Bundespersonalgesetzes (BPG, Art. 27 a-c) wurde nun die geeignete gesetzliche Grundlage für das Personalinformationssystem (BV PLUS), das elektronische Bewerbungsmanagement (eRecruiting) und das elektronische Personaldossier (ePersonaldossier) geschaffen. Die Anpassung des BPG machte zudem eine Revision der Verordnung über den Schutz von Personaldaten in der Bundesverwaltung notwendig. Die entsprechenden Bestimmungen sind am 1. Januar 2012 in Kraft getreten. Wir haben im Berichtsjahr massgeblich an der Ausarbeitung dieser Bestimmungen mitgearbeitet und das EPA unterstützt.

1.7.4 Kontrolle des Informationssystems für die Arbeitsvermittlung und die Arbeitsmarktstatistik

Die Dokumentation des Informationssystems für die Arbeitsvermittlung und die Arbeitsmarktstatistik AVAM wurde verbessert. Es bestehen aber noch Abweichungen zwischen dem Soll und dem Ist, die behoben werden müssen, wie bspw. die Prozessdokumentation im Bearbeitungsreglement, die Zugriffsregelung sowie die Chiffrierung.

Bei unserer Kontrolle haben wir festgestellt, dass einige Bereiche verbessert worden sind. Es gibt aber noch einige wichtige Punkte, die besser dokumentiert werden müssen. Wir haben u. a. darauf hingewiesen, dass die Prozesse von der Erhebung bis zur Anonymisierung oder Löschung der Daten zu dokumentieren sind. Insbesondere die Abläufe, in denen besonders schützenswerte Daten oder Persönlichkeitsprofile bearbeitet werden, müssen im Bearbeitungsreglement dokumentiert sein. So kann man nachvollziehen, wo welche Daten mit Hilfe welcher Sachmittel von welchen Stellen oder Organisationseinheiten zu welchem Zweck bearbeitet werden. Die heutige Prozessdokumentation ist auf einer A4-Seite im Reglement aufgeführt und zu wenig aussagekräftig. Sie sollte eine aussagekräftige Zusammenfassung sein, anstatt von Anfang an auf detailliertere Informationen in anderen Dokumenten zu verweisen.

Wir haben auch festgestellt, dass der Zugriff auf die Daten zu wenig restriktiv geregelt ist. Nach unseren heutigen Kenntnissen können alle Systembenutzer mit Hilfe von Namen, Vornamen, Personen- oder AHV-Nummer die Stellensuchenden kantonsweit suchen. Unseres Erachtens ist die Suche mit einer der beiden Nummern datenschutzkonform, weil sie direkt die entsprechende Person anzeigen. Die Suche mit Hilfe von Namen oder Vornamen ergibt zu viele Treffer und sollte nur möglich sein, wenn man Name und Vorname sowie eine zusätzliche Angabe eingeben kann. Eine solche wäre natürlich das Geburtsdatum, was aber nicht optimal ist, weil dieses Datum in vielen

Fällen bekannt ist, was wiederum zweckentfremdete Abfragen erlaubt. Wichtig wäre neben Namen und Vornamen eine Angabe, die der Betroffene auswendig kennt, die für andere aber nicht einfach in Erfahrung zu bringen ist. Für Ausnahmefälle könnte ermöglicht werden, nur nach dem Namen zu suchen. Diese Abfragen müssten aber revisionssicher protokolliert werden. Im Weiteren haben wir darauf aufmerksam gemacht, dass sensitive Personendaten auch auf den Datenträgern chiffriert werden müssen. Dies wird meist mit dem Hinweis abgelehnt, dass die Systemperformance stark beeinträchtigt werde. Wir haben deshalb den Verantwortlichen für das AVAM gebeten, uns detaillierte Unterlagen darüber zu unterbreiten.

1.8 Handel und Wirtschaft

1.8.1 Datenschutz beim Cloud Computing

Immer mehr Unternehmen, Behörden und Institutionen lagern ihre bisher typischerweise intern erledigten Datenverarbeitungen an externe Unternehmen aus und setzen dafür auf «Cloud Computing». Das bietet zweifelsohne viele Vorteile. Gleichzeitig dürfen die datenschutzrechtlichen und technischen Risiken nicht ausser Acht gelassen werden. Wir haben deshalb Erläuterungen zu Cloud Computing veröffentlicht, welche diese Risiken aufzeigen und die Anforderungen darlegen.

Datenschutz wird in den Diskussionen rund um Outsourcing und Cloud Computing («Rechnen in der Wolke») zwar regelmässig erwähnt, aber vielfach fälschlicherweise mit Datensicherheit gleichgesetzt. Letztere ist zweifellos ein sehr wesentliches Element, aber Datenschutz beim Cloud Computing beinhaltet sehr viel mehr. Gerade die Auslagerung von Datenbearbeitungen in eine ausländische «Public Cloud» kann den datenschutzrechtlichen Anforderungen häufig nicht in allen Teilen gerecht werden. Zum einen wird von den Cloud-Anbietern vielfach nicht transparent gemacht, wo die Daten bearbeitet werden. Zum anderen findet die Datenbearbeitung oftmals in einem Land statt, das nicht über eine ausreichende Datenschutzgesetzgebung verfügt.

Die sorgfältige Risikobeurteilung und Auswahl, Instruktion und Überwachung des Anbieters sind deshalb zentrale Aspekte, die man bei einer Datenbearbeitung in der Cloud beachten muss. Wichtige Auswahlkriterien sind Transparenz auf Seiten des Cloud-Anbieters in Bezug auf die Datenbearbeitung und die Gewährleistung der Datensicherheit. Als Faustregel gilt: Je vertraulicher, geheimer, wichtiger (weil geschäftskritisch) oder sensitiver (weil besonders schützenswert) die Daten sind, desto eher ist von ihrer Auslagerung in die Cloud, insbesondere eine ausländische Cloud, abzusehen, und desto strikter und umfassender müssen die (Datenschutz-) Sicherheitsvorkehrungen und deren Kontrolle sein. Denn letztlich bleibt der Cloud-Nutzer als Auftraggeber gegenüber betroffenen Personen verantwortlich für die Einhaltung der datenschutzrechtlichen Vorschriften und haftet bei allfälligen Persönlichkeitsverletzungen.

Die Erläuterungen dazu können auf unserer Webseite www.derbeauftrage.ch unter Themen – Datenschutz – Unternehmen abgerufen werden.

1.8.2 Datenbearbeitung durch Kredit- und Wirtschaftsauskunfteien

Wir beobachten seit längerem die Tendenz, dass Kredit- und Wirtschaftsauskunfteien immer mehr Daten über Personen bearbeiten. Wir haben dieses Jahr bei einer grossen Auskunftei eine umfassende Sachverhaltsabklärung durchgeführt und ihre Datenbearbeitungen hinsichtlich der Konformität mit dem Datenschutzgesetz geprüft. Im Zentrum unserer Abklärung stand die Bearbeitung von Daten natürlicher und juristischer Personen zur Prüfung ihrer Kreditwürdigkeit.

Wie bereits in früheren Tätigkeitsberichten erwähnt, sind wir jedes Jahr mit vielen Bürgeranfragen zum Thema Datenbearbeitung durch Kredit- und Wirtschaftsauskunfteien konfrontiert. Ausserdem beobachten wir seit Längerem, dass Auskunfteien immer umfangreichere Datenbestände über Personen bearbeiten und auch soziodemografische Angaben verwenden mit der Begründung, dass diese Daten zur Prüfung der Kreditwürdigkeit benötigt werden. Dazu gehören mitunter Informationen darüber, wo eine Person wohnt oder für wie viel Geld sie angeblich ein Haus oder eine Wohnung gekauft bzw. (um)gebaut hat. Diese Angaben werden sodann mit Google Street View verknüpft. Wir erachten diese Verknüpfung als nicht datenschutzkonform.

Wir haben im Berichtsjahr nun bei einer grossen Kredit- und Wirtschaftsauskunftei eine umfangreiche Sachverhaltsabklärung durchgeführt im Hinblick auf die Bearbeitung von Daten natürlicher und juristischer Personen zwecks Prüfung ihrer Kreditwürdigkeit. Im Zentrum unserer Abklärung standen insbesondere folgende Aspekte: Welche Daten sind zur eindeutigen Identifikation einer Person erforderlich, welche Angaben bilden die Basis für die Prüfung der Kreditwürdigkeit, woher stammen diese Informationen, wie lange werden sie gespeichert und aus welchen Angaben wird ein allfälliges Kredit-Rating (sog. Scorewert) berechnet. Wir haben weiter untersucht, wie es sich mit der Transparenz und Erkennbarkeit hinsichtlich der Datenquellen, des Dateninhalts und der Berechnung des Scorewertes verhält und wie mit Auskunfts-, Korrektur- und Löschungsbegehren umgegangen wird. Zudem haben wir abgeklärt, welche Daten die Auskunftei im Rahmen einer Kreditwürdigkeitsprüfung an Dritte weitergibt und ob sichergestellt ist, dass dies nur für den Abschluss oder die Abwicklung eines Vertrages mit der betroffenen Person geschieht. Schliesslich haben wir geprüft, ob die Gesamtheit aller bearbeiteten Daten ein Persönlichkeitsprofil darstellt.

Wir konnten mit Befriedigung feststellen, dass die Datenbearbeitung in vielen Teilen datenschutzkonform ausgestaltet war. Bei den von uns beanstandeten Punkten

konnten wir mit der Auskunftei datenschutzkonforme Lösungen finden. Sie hat sich während der ganzen Untersuchung sehr konstruktiv und kooperativ gezeigt. Die Sachverhaltsabklärung konnte erfolgreich abgeschlossen werden.

1.8.3 Bearbeitung von Personendaten durch einen Fernmeldedienstanbieter

Eine immer wiederkehrende Frage ist, inwieweit Fernmeldedienstmitarbeiter Zugriff auf Kundendaten haben. Einige Mitarbeiter benötigen den Zugang zu solchen Daten im Rahmen ihrer Funktionen. Der Zugriff zu privaten Zwecken ist jedoch ein Missbrauch, der durch geeignete organisatorische und technische Massnahmen verhindert werden muss.

Wir wurden von einem Bürger darauf hingewiesen, dass Mitarbeiter eines Fernmeldedienstanbieters uneingeschränkten Zugriff auf Kundendaten samt Randdaten und insbesondere SMS-Inhalte hätten und diese Informationen zu privaten Zwecken nutzten. Im Rahmen einer Sachverhaltsabklärung konnten wir feststellen, dass die durch den Fernmeldedienstanbieter getroffenen Massnahmen zur Verhinderung von missbräuchlichen Zugriffen verhältnismässig sind.

Zu den organisatorischen Massnahmen gehören zunächst die Notwendigkeit einer formellen Beantragung von Zugriffberechtigungen, deren Erteilung nach dem «Least-Privilege-Prinzip» (so wenig Rechte wie möglich, aber so viele wie nötig) erfolgen soll, und die Anwendung von Sicherheitskonzepten. Weiter gehört dazu eine vertragliche Vertraulichkeitspflicht sowie Sensibilisierung und Training der Mitarbeiter. Auf der technischen Ebene werden unter anderem die Zugriffe protokolliert und bei Verdachtsmomenten analysiert. Im Zusammenspiel der technischen und organisatorischen Massnahmen werden die Missbrauchsrisiken so auf ein vertretbares Mass reduziert.

Was den Zugriff auf die SMS anbelangt, haben wir festgestellt, dass sie einzig dann im System des Anbieters gespeichert werden, wenn der Empfänger nicht erreichbar ist. Sobald das zwischengespeicherte SMS zugestellt werden kann, wird es in der Kurzmitteilungszentrale gelöscht. Kann der Empfänger nicht innert einer Woche erreicht werden, so wird die Mitteilung automatisch gelöscht. Mit dieser Verarbeitung der Mitteilungen, der erwähnten Bewilligung nach dem «Least-Privilege-Prinzip» sowie weiteren technischen Massnahmen kann ein unberechtigter Zugriff auf SMS-Inhalte durch Mitarbeitende fast gänzlich ausgeschlossen werden.

1.8.4 Neuerlass der Datenverordnung-FINMA

Die obersten Organe eines von der FINMA beaufsichtigten Instituts müssen «Gewähr für eine einwandfreie Geschäftstätigkeit» bieten. Diese «Gewährsprüfung» obliegt der FINMA. Sie führt zu diesem Zweck eine Datensammlung, deren Einzelheiten durch die neue Datenverordnung-FINMA geregelt werden.

Die Finanzmarktgesetze verlangen, dass die obersten Organe eines von der FINMA beaufsichtigten Instituts «Gewähr für eine einwandfreie Geschäftstätigkeit» bieten. Das «Gewährserfordernis» ist für solche Institute eine dauernd einzuhaltende Bewilligungsvoraussetzung. Die «Gewährsprüfung» obliegt der FINMA. Sie nimmt dazu Daten von Personen, deren Gewähr für eine einwandfreie Geschäftstätigkeit nach den Finanzmarktgesetzen zweifelhaft oder nicht gegeben ist, in eine Datensammlung auf. Die gesetzliche Grundlage für die Bearbeitung solcher Daten findet sich im Finanzmarktaufsichtsgesetz (FINMAG). Die FINMA wird darin ermächtigt, die Einzelheiten zu regeln. Bislang fehlte eine solche Regelung. Mit Inkrafttreten der neuen Datenverordnung-FINMA per 1. Oktober 2011 wurde diese Lücke geschlossen. Da die FINMA im Rahmen der «Gewährsprüfung» auch besonders schützenswerte Personendaten und Persönlichkeitsprofile bearbeitet, haben wir die neue Verordnung besonders im Hinblick auf die Bearbeitung solcher Daten geprüft und der FINMA entsprechende Vorschläge unterbreitet, welche grösstenteils umgesetzt wurden.

1.8.5 Bearbeitung von Personendaten im Adresshandel

Wir haben bei einem Adresshändler eine Sachverhaltsabklärung durchgeführt und festgestellt, dass die Datenbearbeitung in einigen Bereichen nicht den Anforderungen des Datenschutzgesetzes genügt. Insbesondere müssen die vollständige Gewährung des Auskunftsrechts und die Transparenz verbessert werden.

Wir haben bei einem Adresshändler eine Sachverhaltsabklärung durchgeführt und untersucht, ob die Datenbearbeitung den Vorschriften des Datenschutzgesetzes (DSG) entspricht (siehe unseren 18. Tätigkeitsbericht 2010/2011, Ziffer 1.8.4). Insgesamt haben die Abklärungen ergeben, dass der betreffende Adresshändler bemüht ist, die Bearbeitung datenschutzkonform auszugestalten. Nichtsdestotrotz mussten wir feststellen, dass sie in einigen Bereichen nicht den Anforderungen des DSG entspricht und Verbesserungen angestrebt werden müssen.

Zusammenfassend kann erwähnt werden, dass die Transparenz der Datenbeschaffung und -bearbeitung für die betroffenen Personen ungenügend ist. Entsprechend sind hier Verbesserungen vorzunehmen. Für Betroffene stellt die Auskunftserteilung dafür

ein zentrales Instrument dar. Der Adresshändler muss dem Antragssteller auf Gesuch alle vorhandenen Daten mitteilen, die seine Person betreffen, inkl. aller vorhandenen Angaben über deren Herkunft. Nur so kann eine betroffene Person erkennen, welche Daten über sie bearbeitet werden, und beurteilen, ob sie weitere Datenschutzrechte geltend machen soll (insbesondere das Widerspruchsrecht).

Weiter betonen wir, dass die Verwendung von Daten zu Marketingzwecken eine Persönlichkeitsverletzung darstellt, wenn die betroffene Person die eigenen Angaben im Telefonverzeichnis mit einem Sterneintrag versehen hat. Nur ihre Einwilligung könnte dies rechtfertigen (vgl. dazu Ziff. 1.8.6 des vorliegenden Tätigkeitsberichts).

Schliesslich ist zu beachten, dass man Daten, welche zu Werbezwecken beschafft wurden, grundsätzlich nicht für anderweitige Zwecke bearbeiten darf. Werden sie an Dritte weitergegeben, muss der Adresshändler Vorkehrungen treffen, damit diese Zweckbindung eingehalten wird.

Zum Zeitpunkt der Erstellung dieses Tätigkeitsberichtes waren die Abklärungen noch im Gange.

1.8.6 Verwendung der im Telefonverzeichnis publizierten Adresse zu Marketingzwecken

Unseres Erachtens gibt der Abonnent mit dem Sterneintrag im Telefonverzeichnis zu verstehen, dass er sich jeglicher Verwendung seiner Daten zu Werbezwecken widersetzt, also nicht nur dem Telemarketing, sondern auch den adressierten Werbesendungen. Dieser Standpunkt entspricht indes nicht der gegenwärtigen Praxis vieler Werbefachleute, welche die mit einem Stern versehenen Adressen im Telefonverzeichnis sammeln und zum Zwecke der Kundenwerbung verwenden.

Indem er im Telefonverzeichnis neben seinen Verzeichnisdaten einen Stern anbringen lässt, spricht sich der Abonnent generell gegen deren Verwendung zu Werbezwecken aus, was unseres Erachtens nicht nur für das Telemarketing gilt, sondern auch für die adressierten postalischen Werbesendungen. Umgekehrt bedeutet das Fehlen des Vermerks, dass sich der Abonnent der Verwendung dieser Daten zum Zwecke des Direktmarketing nicht widersetzt und dass sie demnach grundsätzlich in diesem Kontext verwendet werden dürfen. Die betroffene Person hat indessen jederzeit die Möglichkeit, sich auch im Einzelfall der Bearbeitung ihrer Personendaten zu widersetzen (s. Merkblatt auf unserer Webseite unter www.derbeauftragte.ch, Dokumentation – Datenschutz – Merkblätter – Sperrung der Verwendung der Adresse zu Werbezwecken).

Im Verlauf der Sachverhaltsabklärung bei einem Adresshändler (vgl. Ziffer 1.8.5 des vorliegenden Tätigkeitsberichts) stellten wir fest, dass er sämtliche Daten aus dem Telefonverzeichnis sammelte – einschliesslich der mit einem Stern versehenen Einträge – und sie zu Marketingzwecken an Dritte weitergab. Nach Ansicht des betreffenden Adresshändlers bezieht sich der Sterneintrag nur auf die Telefonnummer und die übrigen für die Telekommunikation verwendeten Daten, nicht aber auf die Postadresse. Seiner Auffassung nach können die Angaben im Telefonverzeichnis ohne weiteres für den Versand adressierter Werbezuschriften verwendet werden, auch wenn die Einträge mit einem Stern versehen sind.

Wir kommen zu einer anderen rechtlichen Beurteilung. Artikel 88 der Verordnung über Fernmeldedienste (FDV) ist sehr allgemein formuliert: «Die in einem Verzeichnis aufgeführten Kundinnen und Kunden sind berechtigt, eindeutig kennzeichnen zu lassen, dass sie keine Werbemitteilungen von Dritten erhalten möchten und dass ihre Daten zu Zwecken der Direktwerbung nicht weitergegeben werden dürfen». Seit dem 1. April 2012 gilt zudem die Nichtbeachtung des Sterneintrags im Verzeichnis ebenfalls als unlautere Handlung im Sinne von Artikel 3 littera u des Bundesgesetzes gegen den unlauteren Wettbewerb (UWG) und kann strafrechtlich geahndet werden. Selbst wenn man der Auffassung sein sollte, dass diese Gesetzesbestimmungen nur im Telekommunikationsbereich (also für das Telemarketing) gelten, bedeutet das noch nicht, dass die Verwendung der Postadresse im Telefonverzeichnis zu Marketingzwecken rechtmässig ist. Unter dem Blickwinkel der Datenschutzgesetzgebung muss nämlich jegliche Datenbeschaffung und insbesondere ihre Zweckbestimmung für die betroffene Person erkennbar sein, und jede Bekanntgabe von Daten muss die Grundsätze der Zweckbindung und der Transparenz einhalten. Eine Verwendung der im Verzeichnis publizierten Daten zu Werbezwecken ist indes für die betroffene Person, die neben ihrem Eintrag einen Vermerk hat anbringen lassen, nicht erkennbar; eine solche Verwendung der Daten bedeutet auch eine Verletzung des Grundsatzes der Zweckbindung, da das Telefonverzeichnis vor allem die Herstellung von Telefonverbindungen (und nicht den Versand von Werbematerial) und die obligatorische Veröffentlichung der Postadresse zur eindeutigen Identifikation des Abonnenten für die Telekommunikation ermöglichen soll.

Deshalb bedeutet unseres Erachtens die Verwendung der im Telefonverzeichnis veröffentlichten Adressen zu Marketingzwecken eine widerrechtliche Persönlichkeitsverletzung, soweit sie nicht in einem konkreten Fall durch Zustimmung der betroffenen Person gerechtfertigt ist (z.B. Wettbewerb oder Geschäftsbeziehung).

1.9 Finanzen

1.9.1 Datenbekanntgabe an ausländische Steuerbehörden

Die Datenbekanntgabe an ausländische Steuerbehörden steht nach wie vor ganz oben auf der politischen Agenda, und das Thema wird in der breiten Öffentlichkeit kontrovers diskutiert. Aus datenschutzrechtlicher Sicht haben wir unser Augenmerk in dieser Frage auf die Doppelbesteuerungsabkommen, das neue Steueramtshilfegesetz sowie auf FATCA, den «Foreign Account Tax Compliance Act» gelegt.

Doppelbesteuerungsabkommen

Nach wie vor schliesst der Bundesrat mit anderen Staaten neue Doppelbesteuerungsabkommen (DBA) ab oder revidiert bestehende im Hinblick auf den Ausbau der internationalen Amtshilfe in Steuersachen und zwecks Übernahme des OECD-Standards (insbesondere betreffend Informationsaustausch). Wir haben uns bereits früher zu diesem Thema geäussert (siehe unseren 18. Tätigkeitsbericht 2010/2011, Ziff. 1.9.3). Am 13. Februar 2011 hat der Bundesrat entschieden, die Anforderungen zur Identifikation der Steuerpflichtigen und Informationsinhaber an den international geltenden OECD-Standard anzupassen. Fortan soll einem Amtshilfegesuch, das sich auf ein DBA mit einer Bestimmung zum Informationsaustausch nach Artikel 26 des OECD-Musterabkommens stützt, dann entsprochen werden, wenn darin dargetan wird, dass es sich nicht um eine «fishing expedition» handelt, und wenn der ersuchende Staat (a) den Steuerpflichtigen identifiziert, wobei diese Identifikation auch auf andere Weise als durch Angabe des Namens und der Adresse erfolgen kann, in Ausnahmefällen auch durch die Angabe einer Kontonummer; oder der ersuchende Staat (b) den Namen und die Adresse des mutmasslichen Informationsinhabers angibt, soweit sie ihm bekannt sind. Fehlen diese Angaben für die Ermittlung des Informationsinhabers durch die Schweiz, sind die Grundsätze der Proportionalität und Praktikabilität zu beachten. Gesuche mit einer Liste von Kontonummern ohne weitere Angaben würden als «fishing expeditions» angesehen, denen nicht stattgegeben würde. Aufgrund dieser Sachlage kommen wir zum Schluss, dass diese Praxis datenschutzkonform ist.

Steueramtshilfegesetz

Die Amtshilfeklauseln in den Doppelbesteuerungs- und weiteren internationalen Abkommen in Steuersachen regeln nicht, wie innerstaatlich damit umgegangen werden soll. Derzeit wird dies durch die Verordnung über die Amtshilfe nach Doppelbesteuerungsabkommen (ADV) geregelt, welche jedoch den Anforderungen an das Legalitätsprinzip nicht genügt. Deshalb hat der Bundesrat einen Entwurf für

ein Bundesgesetz über die internationale Amtshilfe in Steuersachen (Steueramtshilfegesetz, StAG) ausgearbeitet. Dieses Gesetz regelt den Vollzug der Amtshilfe im Rahmen der erwähnten Abkommen, die einen auf Steuersachen bezogenen Informationsaustausch vorsehen.

Grundsätzlich gelangt das Datenschutzgesetz auch bei der internationalen Amtshilfe zur Anwendung, sofern keine spezialgesetzliche Regelung vorliegt. Bei der internationalen Amtshilfe in Steuersachen wird das StAG jedoch fortan dem Datenschutzgesetz als lex specialis vorgehen. Wir haben im Rahmen der Ämterkonsultation den Gesetzesentwurf auf die Vereinbarkeit mit dem Datenschutzgesetz (DSG) geprüft und sind dabei zum Schluss gekommen, dass die datenschutzrechtlichen Anforderungen hinsichtlich des Legalitätsprinzips (Art. 17 DSG) und der Datenbekanntgabe an Dritte (Art. 19 DSG) erfüllt sind. Der Bearbeitungszweck, die Angaben betreffend Datenbearbeiter und -empfänger sowie zum Umfang der Datenbeschaffung, -bearbeitung und -bekanntgabe sind ausführlich geregelt und die Betroffenenrechte werden gewahrt.

«Foreign Account Tax Compliance Act»

«Foreign Account Tax Compliance Act» (FATCA) bezeichnet ein US-Gesetz, das am 1. Januar 2013 in Kraft tritt und auf die Verhinderung von Steuerhinterziehung durch US-Personen abzielt. Das Gesetzt betrifft alle ausländischen Finanzinstitute («Foreign Financial Institutes FFI»), d.h. Banken, Versicherungen etc., welche für ihre Kunden oder auf eigene Rechnung in US-Wertschriften investieren. Sie werden verpflichtet, der US-Steuerbehörde IRS («Internal Revenue Service») jährlich automatisch umfassende Informationen über US-Steuerpflichtige zu melden. Andernfalls werden sie mit einer 30% Quellensteuer («Withholding tax») auf sämtlichen Erträgen, die in den USA anfallen, bestraft. Als US-steuerpflichtige Personen gelten US-Bürger, US-Doppelbürger, Green-Card-Halter, aber auch Personen, die steuertechnisch einen «resident»-Status aufweisen. Im Minimum müssen der US-Steuerbehörde von jedem Kontoinhaber Name, Adresse, TIN («Tax Identifikation Number»), Kontonummer, Kontostand, Brutto-Einnahmen und Brutto-Abhebungen oder Transaktionen bekannt gegeben werden. Wurde ein meldepflichtiges Konto identifiziert, so ist vom Inhaber oder wirtschaftlich Berechtigten die Einwilligung zur Datenbekanntgabe in die USA und damit in die Aufhebung des Bankgeheimnisses einzuholen. Falls die betreffende Person die Zustimmung verweigert, ist die Kundenbeziehung aufzulösen und eine Meldung an die US-Steuerbehörde zu machen.

Wir stehen diesem unilateral verhängten US-Gesetz sehr kritisch gegenüber. Zum einen, weil die direkte Datenbekanntgabe von privaten Finanzinstituten an die US-Steuerbehörde de facto einem automatischen Informationsaustausch gleichkommt, dies unter Umgehung des üblichen Amtshilfeweges. Zum anderen sind wir der Meinung,

dass FATCA in verschiedener Hinsicht nicht in Einklang mit unserem Datenschutzgesetz steht. Wir hatten im Rahmen einer Anhörung vor der Aussenpolitischen Kommission des Ständerats Gelegenheit, unsere diesbezüglichen Bedenken vorzubringen. Unsere Vorbehalte beziehen sich namentlich auf die Gültigkeit der Einwilligung in die Aufhebung des Bankgeheimnisses, auf die Verhältnismässigkeit hinsichtlich der Personen, welche als US-Steuerpflichtige betrachtet werden, und hinsichtlich des Umfangs und Inhalts der Daten, die gemeldet werden müssen. Schliesslich erachten wir es als problematisch, dass die US-Steuerbehörde nicht zur Geheimhaltung der erhaltenen Informationen verpflichtet ist.

1.9.2 Studie zur Modernisierung des Betreibungswesens in der Schweiz

Die 2011 publizierte Studie des Bundesamts für Justiz zum eSchKG befasste sich mit der Modernisierung des Betreibungswesens in der Schweiz und zeigte die Chancen und Risiken eines virtuellen Betreibungsamts Schweiz mit einem zentralen Betreibungsregister auf. Dreh- und Angelpunkt eines solchen Registers ist die Einführung bzw. Verwendung eines Personenidentifikators.

Wir wurden zu einer Stellungnahme zur eSchKG-Studie im Hinblick auf eine Modernisierung des Betreibungswesens in der Schweiz eingeladen. Die Studie wollte die Potentiale eines eSchKG-Verbundes sichtbar machen und die Möglichkeiten und Risiken eines virtuellen Betreibungsamts Schweiz mit einem zentralen Betreibungsregister aufzeigen. Wir haben unseren Fokus auf die Themenbereiche Personenidentifikator und zentrale Schuldner-Datenbank gelegt.

Dreh- und Angelpunkt eines virtuellen Betreibungsamtes mit einem zentralen Betreibungsregister ist die sichere und eindeutige Identifikation von Personen. Zu diesem Zweck soll ein Personenidentifikator verwendet werden. Bei juristischen Personen ist dies einfacher zu bewerkstelligen als bei natürlichen, indem z.B. die Unternehmens-Identifikationsnummer verwendet wird. Diese Nummer kann bereits heute in einem öffentlich zugänglichen Register online abgefragt werden. Sehr viel schwieriger gestaltet sich dagegen die Verwendung einer eindeutigen Personenidentifikation bei natürlichen Personen. Im Vordergrund steht der Einsatz der Sozialversicherungsnummer (AHVN13). Dies birgt jedoch hohe Risiken für die Privatsphäre der Bürgerinnen und Bürger, weil dadurch unerwünschte Verknüpfungen ermöglicht werden. Abgesehen davon, dass laut AHV-Gesetz zuerst eine entsprechende Rechtsgrundlage geschaffen werden müsste, kommt die systematische Verwendung der AHVN13 in einem zentralen Betreibungsregister unserer Meinung nach aus folgenden Überlegungen nicht in Frage:

Die AHVN13 ermöglicht nicht in jedem Fall die zweifelsfreie Identifikation einer Person. Nicht alle natürlichen Personen, die betrieben werden können, verfügen zudem über eine AHV-Nummer. Damit die Verwendung der AHVN13 als Personenidentifikator überhaupt sinnvoll ist, müsste auch ein potentieller Gläubiger, der eine Betreibung einleiten will, oder ein Dritter, der einen Betreibungsregisterauszug über den Schuldner verlangt, diesen zweifelsfrei identifizieren können. Folglich müsste ihnen die AHV-Nummer bekannt sein. Das würde im Ergebnis zu einer ausufernden Verbreitung dieser Nummer führen und die bisher restriktive Handhabung der systematischen Verwendung geradezu aushebeln.

Eine zentrale Schuldner-Datenbank, welche das heutige System mit den dezentralen Betreibungsregistern ablösen würde, bietet durchaus viele Vorteile. Beispielsweise könnte dadurch die von uns bereits mehrmals kritisierte unterschiedliche Handhabung von Betreibungsregisterauskünften (in zeitlicher und sachlicher Hinsicht) durch die Betreibungsämter verbessert werden. Andererseits birgt eine elektronische zentrale Schuldner-Datenbank auch erhebliche Risiken. Die Daten müssten auf jeden Fall gegen zufälligen Verlust, technische Fehler, aber auch Fälschung, Diebstahl und andere widerrechtliche Verwendungen geschützt werden. Die Daten dürften nicht unbefugt geändert, kopiert oder sogar vernichtet werden können. Zudem müsste die Vertraulichkeit, Verfügbarkeit und Integrität der Daten unterschiedlichster Herkunft auch in einem zentralen System jederzeit gewährleistet sein.

Da sich die vorliegende Studie vorerst nur in allgemeiner Weise zu den Chancen und Risiken eines virtuellen Betreibungsamts Schweiz geäussert hat, gilt es abzuwarten, welche der zahlreichen aufgeworfenen Themen effektiv umgesetzt werden. Wir werden das Projekt weiter begleiten und, wo notwendig und sinnvoll, unsere Standpunkte konstruktiv in die Diskussion einbringen.

1.9.3 Revision der Mehrwertsteuerverordnung

Die Mehrwertsteuerverordnung bildet keine genügende gesetzliche Grundlage für die Verwendung der AHV-Nummer im Bereich der Mehrwertsteuer, auch nicht im Sinne einer Übergangsregelung.

Im Rahmen einer Ämterkonsultation wurden wir zu einer Stellungnahme zur Revision der Mehrwertsteuerverordnung (MWSTV) eingeladen. Im Sinne einer Übergangsregelung sollte Art. 131 Bst. a MWSTV angepasst werden, damit die AHV-Nummer auch im Bereich der Mehrwertsteuer verwendet werden könnte. Dies, obschon das AHV-Gesetz klar vorschreibt, dass die Versichertennummer ausserhalb der Sozialversicherung des Bundes nur dann systematisch verwendet werden darf, wenn ein Bundesgesetz dies vorsieht und der Verwendungszweck sowie die Nutzungsberechtigten bestimmt sind. Gemäss

Rechtsprechung kann vom Erfordernis eines Gesetzes im formellen Sinn dann abgewichen und eine Regelung auf Verordnungsstufe (als Übergangsregelung) ins Auge gefasst werden, wenn die Ausarbeitung der formal-gesetzlichen Grundlage in materieller und zeitlicher Hinsicht konkrete Formen angenommen hat. Damit soll verhindert werden, dass der Gesetzgeber durch die Schaffung von präjudizierenden Fakten (also durch die Regelung einer Sache auf Verordnungs- statt auf Gesetzesstufe) der Möglichkeit beraubt wird, von den ihm zustehenden Kompetenzen Gebrauch zu machen und seinem Willen entsprechende Gesetze zu erlassen. Eine Übergangsregelung auf Verordnungsstufe dürfte beispielsweise dann genügen, wenn der Gesetzesentwurf mitsamt der Botschaft vorliegt und wenigstens in einer Kammer der Bundesversammlung bereits beraten wurde. Im vorliegenden Fall waren diese Voraussetzungen jedoch noch nicht erfüllt, weshalb wir uns gegen die Änderung von Art. 131 Bst. a MWSTV ausgesprochen haben. Das federführende Amt hat schliesslich auf diese Anpassung verzichtet.

1.9.4 Auskunftspflicht von kantonalen Strafvollzugseinrichtungen gegenüber Betreibungsämtern

Betreibungsämter müssen vor der Zustellung des Zahlungsbefehls alle erforderlichen und zumutbaren Nachforschungen ergreifen, um einen Schuldner ausfindig zu machen. Dazu gehören auch Abklärungen bei kantonalen Strafvollzugsbehörden über den Aufenthalt von inhaftierten Personen. Solche Abklärungen sind für die Behörden zumutbar.

Eine Strafvollzugsbehörde und ein Betreibungsamt aus demselben Kanton waren sich uneinig darüber, ob und inwieweit die Strafvollzugsbehörde dem Betreibungsamt zwecks Zustellung eines Zahlungsbefehls Auskunft über den Aufenthalt von Personen in einer ihrer Institutionen geben muss. Grundsätzlich sind wir für die Beantwortung solcher Fragen nicht zuständig. Da es im vorliegenden Fall aber um die Auslegung von Bundesrecht ging, wurden wir um eine rechtliche Einschätzung gebeten.

Das betreffende kantonale Datenschutzrecht sah vor, dass eine Behörde besonders schützenswerte Personendaten bekannt geben darf, wenn sich dies aus einer gesetzlichen Grundlage klar ergibt oder die betroffene Person ausdrücklich zugestimmt hat oder die Erfüllung einer gesetzlichen Aufgabe es zwingend erfordert. Im vorliegenden Fall gibt es jedoch weder im kantonalen Recht noch im Bundesgesetz über Schuldbetreibung und Konkurs (SchKG) eine Regelung, und eine Einwilligung war auch nicht vorhanden. Es stellte sich also die Frage, ob die Strafvollzugsbehörde den Aufenthaltsort einer inhaftierten Person bekannt geben muss, weil dieser zur Erfüllung einer gesetzlichen Aufgabe des Betreibungsamtes notwendig ist.

Hat ein Schuldner in der Schweiz Wohnsitz, so gelten für die Zustellung des Zahlungsbefehls Art. 71 und 72 SchKG sowie die allgemeinen Vorschriften ab Art. 64 SchKG über die Zustellung von Betreibungsurkunden. Soll ein Verhafteter betrieben werden, der keinen Vertreter hat, setzt ihm das Betreibungsamt nach Art. 60 SchKG eine Frist zur Bestellung eines solchen, sofern nicht von Gesetzes wegen der Vormundschaftsbehörde die Ernennung obliegt. Während dieser Frist, welche bereits vor Zustellung des Zahlungsbefehls einzuräumen ist (BGE 77 III 145 E. 1), besteht für den Verhafteten Rechtstillstand. Gemäss bundesgerichtlicher Rechtsprechung liegt der Sinn und Zweck von Art. 60 SchKG darin, dass anstelle des Verhafteten sein (gesetzlicher) Vertreter die im Betreibungsverfahren notwendigen Handlungen vornehmen kann (vgl. BGE 38 I 237 sowie 108 III 3 E. 1). Der Schuldner soll in die Lage versetzt werden, sich gegenüber ungesetzlichen oder unangemessenen Betreibungshandlungen wirksam wehren zu können. Die Missachtung von Art. 60 SchKG im Falle der Zustellung eines Zahlungsbefehls habe die Ungültigkeit der betreibungsamtlichen Vorkehr zur Folge, und eine fehlerhafte Zustellung des Zahlungsbefehls, von welcher der Schuldner keine Kenntnis erlange, sei nichtig (BGE 120 III 117 E. 2.c).

Wenn das Betreibungsamt dem Inhaftierten bzw. dessen Vertreter bereits vor Zustellung des Zahlungsbefehls eine Frist nach Art. 60 SchKG ansetzen muss, so setzt dies voraus, dass das Amt Kenntnis davon hat, ob sich eine Person in Haft oder im Strafvollzug befindet. Damit stellt sich unweigerlich die Frage, wie das Betreibungsamt in den Besitz dieser Informationen gelangt bzw. wann und wie weit es Nachforschungen über den Wohn- oder Aufenthaltsort eines Schuldners anstellen muss, bevor es den Zahlungsbefehl zustellt.

Bevor das Amt Nachforschungen über den Wohn- oder Aufenthaltsort ergreift, besteht zunächst einmal die Möglichkeit, den Zahlungsbefehl nach Art. 64 und Art. 66 Abs. 1 und 2 SchKG zuzustellen, d.h. Zustellung am Wohnort, am Ort der Berufsausübung, in einem vom Schuldner bezeichneten Lokal oder durch die Post. Bei all diesen Zustellformen muss sichergestellt sein, dass der Schuldner Kenntnis vom Zahlungsbefehl erhält, ansonsten die Betreibung nichtig ist. Kann der Zahlungsbefehl nicht auf solchem Weg zugestellt werden, kann die Kenntnisnahme mittels öffentlicher Bekanntmachung (Ediktalzustellung, Art. 66 Abs. 4 SchKG) fingiert werden. Diese Zustellungsform ist gemäss Bundesgericht letztes Mittel; zu ihr darf nicht Zuflucht genommen werden, bevor vom Gläubiger und vom Betreibungsamt alle der Sachlage entsprechenden Nachforschungen unternommen wurden, um eine mögliche Zustelladresse des Schuldners herauszufinden (BGE 112 III 6 E. 4). Die Ediktalzustellung darf nicht schon dann erfolgen, wenn die Adressangabe des Gläubigers nicht genügt, sondern erst, wenn der Schuldner unerreichbar bleibt oder die Nachforschungen als aussichtslos erscheinen. Daraus lässt sich schliessen, dass ein Betreibungsamt in Einzelfällen, wo

keine Zustellung nach Art. 64 und Art. 66 Abs. 1 und 2 SchKG möglich ist und keine Anhaltspunkte über den Verbleib des Schuldners vorliegen, die Strafvollzugsbehörden und Strafanstalten anfragen muss, ob sich ein Schuldner allenfalls in Haft oder im Strafvollzug befindet. Allerdings bedeutet dies nicht, dass ein Betreibungsamt bei den Strafvollzugsbehörden aller 26 Kantone nachfragen muss. Dies wäre weder praktikabel noch zumutbar. Als zumutbar erscheint hingegen, die Strafvollzugsbehörden im eigenen Kanton um Auskunft anzugehen.

Wir sind damit zu folgendem Schluss gelangt: Die Betreibungsämter müssen Art. 60 SchKG zwingend beachten und bereits vor der Zustellung eines Zahlungsbefehls alle erforderlichen und zumutbaren Nachforschungen ergreifen, um einen Schuldner ausfindig zu machen. Die von den Strafvollzugsbehörden verlangte Auskunft ist für Betreibungsämter zur Erfüllung ihrer gesetzlichen Aufgabe (Art. 60 SchKG) zwingend erforderlich. Damit kann als Rechtsgrundlage für solche Anfragen der Betreibungsämter das kantonale Datenschutzgesetz dienen, welches vorsieht, dass Daten bekannt gegeben werden dürfen, wenn dies zur Erfüllung einer gesetzlichen Aufgabe zwingend erforderlich ist.

1.10 International

1.10.1 Internationale Zusammenarbeit

Die Internationalisierung der Bearbeitung von Personendaten und die damit einhergehenden Herausforderungen für die Achtung des Datenschutzrechts machen die Einführung eines universell verbindlichen rechtlichen Rahmens und die Verstärkung der Zusammenarbeit zwischen den Datenschutzbehörden dringend erforderlich. Die Europäische Union, der Europarat und die OECD haben ihre Arbeiten zur Revision ihrer Rechtsinstrumente aufgenommen, um den Datenschutz wirksamer zu gestalten. Wir haben uns aktiv an den Arbeiten des Europarates, der OECD, der europäischen und internationalen Konferenz der Datenschutzbeauftragten, der gemeinsamen Kontrollinstanzen Schengen und Eurodac und der französischsprachigen Vereinigung der Datenschutzbehörden beteiligt.

Europarat

2011 ist das Übereinkommen des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen 108) 30 Jahre alt geworden. Der Europarat nahm dieses Jubiläum zum Anlass, Bilanz zu ziehen und den Blick in die Zukunft zu richten. Zwar ist der Zweck des Übereinkommens weiterhin relevant. Es soll nämlich für jede natürliche Person, ungeachtet ihrer Staatsangehörigkeit oder ihres Wohnorts, sicherstellen, dass ihre Rechte und Grundfreiheiten, und insbesondere ihr Recht auf einen Persönlichkeitsbereich, bei der Verarbeitung personenbezogener Daten geschützt werden. Es erweist sich jedoch als notwendig, das Instrument an das heutige Informations- und Technologieumfeld anzupassen, um die Wirksamkeit des Datenschutzes zu verstärken. In diesem Sinne hat der beratende Ausschuss des Übereinkommens 108 (T-PD) unter dem Vorsitz des stellvertretenden Eidgenössischen Beauftragten seine Arbeit zur Modernisierung des Übereinkommens fortgeführt (siehe unseren 18. Tätigkeitsbericht 2010/2011, Ziff. 1.10.1). Im Anschluss an eine öffentliche Konsultation prüfte der Ausschuss eine erste Arbeitsunterlage mit Änderungsvorschlägen zum Übereinkommen (www.coe.int/t/dghl/standardsetting/dataprotection/modernisation_FR.asp?).

Grundlage für die laufende Arbeit ist die Notwendigkeit, die allgemeine und einfache Ausgestaltung des Übereinkommens beizubehalten, seinen technologisch neutralen Ansatz zu wahren und die Kohärenz mit dem europäischen Rechtsrahmen sicherzustellen. Es geht auch darum, den internationalen, offenen und verbindlichen Charakter des Übereinkommens zu erhalten, das derzeit dem Erfordernis eines universellen

Rechtsinstruments am besten entspricht. Die Arbeiten zielen auf eine Verstärkung des Rechts auf Datenschutz ab, um den Personen die Kontrolle über ihre Daten (zurück) zu geben. Das Übereinkommen sollte weiterhin für jegliche Datenverarbeitung im öffentlichen und privaten Sektor gelten. Sein Anwendungsbereich sollte nicht mehr auf die automatische Verarbeitung begrenzt sein, sondern auf sämtliche Arten der Verarbeitung, ungeachtet der verwendeten Mittel und Verfahren, ausgedehnt werden. Die Bearbeitung zu ausschliesslich persönlichen oder privaten Zwecken soll jedoch vom Geltungsbereich ausgenommen werden. Die Begriffsbestimmungen werden überarbeitet und ergänzt.

Im Bereich der Grundprinzipien des Datenschutzes könnte der Grundsatz der Verhältnismässigkeit klarer umrissen werden, namentlich unter dem Blickwinkel der Datenminimierung und der Wahl der Bearbeitungsmittel. Eine Bestimmung, in der die zulässigen Gründe zur Rechtfertigung einer Datenbearbeitung genannt sind, soll eingeführt werden, und es ist nicht auszuschliessen, dass die Regelung betreffend die sensitiven Daten überarbeitet wird, insbesondere mit einer Erweiterung des Datenkatalogs und einer besseren Berücksichtigung des Kontextes, in dem die Bearbeitung erfolgt. Der Ausschuss prüft auch die Einführung der Prinzipien der Haftung und des integrierten Datenschutzes («privacy by design»). Er erwägt eine Stärkung der Rechte der betroffenen Personen (insbesondere die Transparenz der Bearbeitung und das Widerspruchsrecht). Ebenfalls geprüft wird die Einführung einer Pflicht, Sicherheitsverletzungen mindestens den Kontrollbehörden zu melden. Die Rolle, die Aufgaben und die Befugnisse der Kontrollbehörden müssten genauer umschrieben werden, namentlich im Hinblick auf das Ziel, die internationale Zusammenarbeit nicht nur unter dem Gesichtspunkt des Informationsaustausches und der Unterstützung, sondern auch zur Erleichterung eines gemeinsamen Vorgehens zu verstärken. Die Kriterien zur Beurteilung der Unabhängigkeit dieser Behörden werden präziser formuliert. Die Befugnisse des Beratenden Ausschusses werden ebenfalls überarbeitet, um insbesondere eine dem Beitritt zur Urkunde vorangehende Kontrolle zu ermöglichen und eine bessere Überwachung der Anwendung des Übereinkommens durch die Parteien einzuführen.

Schliesslich sollen zwar der Grundsatz des freien Informationsaustausches zwischen den Parteien und das Erfordernis des angemessenen Schutzniveaus weiter gelten, gleichzeitig wird aber die Regelung des grenzüberschreitenden Datenverkehrs an die Realität der heutigen Welt angepasst (Internet, Cloud Computing usw.). Der Ausschuss könnte bis Ende 2012 einen Entwurf im Hinblick auf seine Verabschiedung durch das Ministerkomitee des Europarates zum Abschluss bringen. Im Rahmen seiner Tätigkeiten als Ausschussvorsitzender hatte der stellvertretende Eidgenössische Beauftragte auch die Gelegenheit, in verschiedenen internationalen Foren aufzutreten

und den Fortschritt der Arbeiten zur Modernisierung des Übereinkommens zu erläutern und deren Vorteile mit Blick auf die Einführung eines universellen verbindlichen Rechtsrahmens deutlich zu machen.

Der Beratende Ausschuss setzt seine Arbeiten zur Revision der Empfehlung Nr. R (89) 2 über den Schutz personenbezogener Daten im Arbeitsbereich fort und überprüft die Durchführung der Empfehlung Nr. R (87) 15 über die Nutzung personenbezogener Daten im Polizeibereich. Aufgrund der Ergebnisse dieser Evaluation wird er über die Zweckmässigkeit einer Überarbeitung dieser Empfehlung entscheiden. Zudem gab er eine positive Stellungnahme zum Gesuch Uruguays um einen Beitritt zum Übereinkommen 108 ab. Der Beitritt sollte im Jahr 2012 erfolgen, und Uruguay wird damit der erste nichteuropäische Mitgliedstaat des Übereinkommens werden.

Europäische Konferenz der Datenschutzbeauftragten

Am 5. April 2011 fand in Brüssel auf Einladung des Europäischen Datenschutzbeauftragten und des Vorsitzenden der Arbeitsgruppe Artikel 29 die jährliche Frühjahrskonferenz der europäischen Datenschutzbeauftragten statt. Bei dieser Konferenz kamen die Datenschutzbehörden der Mitgliedstaaten der Europäischen Union und der dem Übereinkommen 108 beigetretenen Drittländer zusammen. Die Konferenz war hauptsächlich der Überarbeitung des rechtlichen Datenschutzrahmens in Europa gewidmet. Sie verabschiedete eine Resolution, in der die Notwendigkeit hervorgehoben wird, einen globalen Rechtsrahmen für den Datenschutz zu schaffen, der den privaten und öffentlichen Sektor, einschliesslich der Bereiche Polizei und Justiz, abdeckt (siehe unsere Webseite www.derbeauftragte.ch, Themen – Datenschutz – Internationale Zusammenarbeit). Die Resolution unterstreicht auch das Erfordernis eines kohärenten Ansatzes bei den Bemühungen um eine Modernisierung der verschiedenen innerhalb der Europäischen Union, des Europarates und der OECD bestehenden Rahmengesetze. Nach Ansicht der Beauftragten sollten diese Entwicklungen eine Verbesserung des geltenden Regelungsrahmens und damit die Gewährleistung eines wirksameren rechtlichen Schutzes der Personen im Zusammenhang mit der Bearbeitung der sie betreffenden Personendaten ermöglichen. Die Beauftragten beschlossen ausserdem, die Tätigkeiten der Gruppe Artikel 29 und der Arbeitsgruppe der europäischen Konferenz für Polizei und Justiz im Bereich Sicherheit und Justiz besser zu koordinieren.

Aufsichts-Koordinationsgruppe Eurodac

Die Aufsichts-Koordinationsgruppe Eurodac (siehe unseren 18. Tätigkeitsbericht 2010/2011, Ziffer 1.10.1) hielt am 21. Oktober 2011 eine Sitzung ab, an der wir teilnahmen. Zunächst wurde das Fingerabdruck-Informationssystem Eurodac besprochen.

Dabei wurde unter anderem der Bericht über die vorzeitige Datenvernichtung in diesem System diskutiert, der inzwischen von der Koordinationsgruppe angenommen und auf der Homepage des Europäischen Datenschutzbeauftragten (www.edps.europa.eu) veröffentlicht worden ist. Nächster Schwerpunkt soll die Frage der unlesbaren Fingerabdrücke sein.

Ein weiteres Thema der Sitzung war das neue europäische Visa-Informationssystem (VIS). Die Kontrolle obliegt auch hier einerseits den nationalen Kontrollstellen, andererseits dem Europäischen Datenschutzbeauftragten. Die Aufsichtsbehörden arbeiten aktiv zusammen und sorgen für eine koordinierte Überwachung des VIS und der nationalen Systeme. Das VIS konnte auf den 11. Oktober 2011 für die erste Region in Betrieb genommen werden. Sie umfasst sechs nordafrikanische Staaten (Algerien, Ägypten, Libyen, Mauretanien, Marokko und Tunesien). Danach soll es für den Nahen Osten und später für die Golfregion gelten. Das VIS enthält Fingerabdrücke und Gesichtsbild der Visa-Gesuchsteller, also biometrische Daten; es soll ein rascheres und einfacheres Visaerteilungsverfahren ermöglichen, aber auch helfen, Betrugsfälle und das so genannte «VISA-Shopping» zu verhindern. Wie an der Sitzung mitgeteilt wurde, konnte das System seine Funktion ohne grössere Zwischenfälle aufnehmen und scheint stabil zu sein. Auch die Schweiz hat das VIS eingeführt. Das Schweizer Recht wurde bereits entsprechend revidiert.

Arbeitsgruppe Polizei und Justiz

Die Arbeitsgruppe Polizei und Justiz der Europäischen Datenschutzbeauftragten hat die Aufgabe, die gesetzgeberischen Entwicklungen im Sektor Polizeiwesen, namentlich soweit sie unter den Schengen-Besitzstand fallen, zu verfolgen und die Aufsichtstätigkeiten unter den nationalen Datenschutzbehörden zu koordinieren. In diesem Kontext gibt sie Gutachten und Stellungnahmen ab. Wir haben an den verschiedenen Tagungen im Februar, März, Juni und September 2011 teilgenommen. Die Arbeitsgruppe legte insbesondere eine gemeinsame Methodik für eine Risikoevaluation im Vorfeld der Dateninspektionen fest, um die Aufsicht effektiver zu gestalten; mit Hilfe dieser Methodik konnten fünf Risikobereiche aufgedeckt werden. Diese müssen jedoch noch präziser formuliert werden, um einen besseren internationalen Vergleich zu ermöglichen. Die Arbeitsgruppe wird eine Aufsichtspolitik entwickeln, mit der die Vorgehensweise auf der Grundlage der benannten Risiken bestimmt wird. Im Hinblick auf die Frühjahrskonferenz 2012 hat die Gruppe ein Arbeitsdokument vorbereitet, in dem die für ihre Zukunft möglichen Weichenstellungen aufgezeigt werden.

Gemeinsame Kontrollinstanz Schengen

Die gemeinsame Kontrollinstanz Schengen (GKI) trat 2011 vier Mal zusammen. Sie setzte insbesondere ihre Kontrolltätigkeiten fort und plante neue Inspektionen. Der Bericht über die Inspektion der Warnsysteme betreffend gesuchte Personen, die im Hinblick auf ihre Auslieferung festzunehmen sind, wird demnächst verfügbar sein. Dasselbe gilt für den Bericht über die Überprüfung der Folgemassnahmen im Anschluss an die Empfehlungen, die anlässlich der Kontrolle der im SIS enthaltenen Personen- oder Fahrzeugdaten zum Zweck der diskreten Überwachung oder einer spezifischen Kontrolle abgegeben wurden. Für 2012 plant die GKI eine Inspektion bezüglich der Zugriffsrechte auf das SIS I, um einen wirksamen Datenschutz zu gewährleisten. Zu diesem Zweck hat das Sekretariat einen Fragebogen ausgearbeitet, der im Anschluss an die Diskussionen bei den Sitzungen umgestaltet wurde. Im Rahmen dieser Inspektion sollen auch die Sensibilisierung und die Information der Personen geprüft werden. Des Weiteren wird die GKI eine technische Überprüfung des Inhalts des SIS I und von 4all durchführen, mit der eine Gruppe Sachverständiger aus sechs Ländern betraut wird. Ausserdem wurde die Webseite der GKI aktualisiert. Sie ist unter folgender Adresse abrufbar: http://schengen.consilium.europa.eu.

Europäische Arbeitsgruppe für die Behandlung von datenschutzrelevanten Fällen

Bei ihren früheren Tagungen konzentrierte sich die von der Europäischen Konferenz der Datenschutzbeauftragten eingerichtete europäische Arbeitsgruppe für die Behandlung datenschutzrelevanter Fälle («Case Handling Workshop»), zusammengesetzt aus Vertretern von 29 nationalen Datenschutzbehörden, auf vier Themen. Im Oktober 2011 behandelte sie zunächst Fragen betreffend grenzüberschreitende Fälle und die Art und Weise, in der die verschiedenen Datenschutzbehörden mit solchen Fällen umgehen. In einer zweiten Phase wurden soziale Netzwerksites und das Internet besprochen. Die Diskussion drehte sich hauptsächlich um Cloud Computing, wobei unsere nordischen Kollegen die Gelegenheit nutzten, um über die Ergebnisse ihrer ersten Kontrolle in diesem Bereich zu berichten. Sie hat gezeigt, dass Unternehmen und Behörden unbedingt für die Gefahren dieses Systems sensibilisiert und auf ihre Verantwortung behaftet werden müssen. Die dritte von der Arbeitsgruppe aufgegriffene Thematik betrifft die von den Datenschutzbehörden entsprechend ihren jeweiligen gesetzlichen Befugnissen angewendeten Kontrollmethoden. Anlässlich der Diskussion stellten wir fest, dass zahlreiche Datenschutzbehörden in ihrer innerstaatlichen Gesetzgebung über Sanktionsmöglichkeiten in Form von Geldstrafen gegen das kontrollierte Organ verfügen, was im schweizerischen Recht derzeit nicht bekannt ist. Schliesslich wurde die Überwachung am Arbeitsplatz thematisiert. Einige konkrete Fälle aus der Praxis

der verschiedenen Datenschutzbehörden verdeutlichen, dass immer häufiger neue Technologien, namentlich der Videoüberwachung und der Biometrie, eingesetzt werden. Dies erfordert eine aktive Informations- und Sensibilisierungsarbeit.

Internationale Konferenz der Datenschutzbeauftragten

Die 33. Internationale Konferenz der Datenschutzbeauftragten fand vom 1. bis 3. November 2011 auf Einladung des Bundesinstituts für Informationszugang und Datenschutz (IFAI) in Mexico City statt (www.privacyconference2011.org). Unter dem Thema «Privacy: The Global Age» kamen rund 700 Teilnehmer aus aller Welt in Vertretung von 80 Datenschutzbehörden, Nichtregierungsorganisationen, der Industrie und der Wissenschaft sowie der öffentlichen Verwaltungen zu der Konferenz zusammen. Wie gewohnt verlief die Konferenz in zwei Teilen: der eine war ausschliesslich den akkreditierten Datenschutzbehörden vorbehalten, der andere stand sämtlichen betroffenen Akteuren offen; diesen bot sich dabei die Gelegenheit zu einem Informations- und Meinungsaustausch über die grossen Fragen des Datenschutzes in der heutigen Zeit, darunter insbesondere die Herausforderungen aufgrund der wachsenden Internationalisierung der Bearbeitung von Personendaten, die Problematik der grossen Datenmengen («big data»), Cloud Computing, die soziale Verantwortlichkeit («accountability»), das Recht auf Vergessen, die gesetzgeberischen Entwicklungen, die Zertifizierung, die Sicherheitslücken und der integrierte Datenschutz («privacy by design»). Anlässlich von zwei Plenarsitzungen konnten wir uns in die Diskussionen einbringen die Bedeutung des Übereinkommens 108 im internationalen Kontext und die weltweite Entwicklung der verschiedenen Datenschutzgesetzgebungen hervorheben.

Neben der erfreulichen Feststellung, dass eine stetig wachsende Zahl von Staaten über eine Datenschutzgesetzgebung verfügt, wiesen wir auch darauf hin, dass eine Vernetzung und Harmonisierung der Gesetzgebungen eine wichtige Voraussetzung für ihre Interoperabilität seien. Dies erfordert die Einführung eines auf einem gemeinsamen Standard beruhenden verbindlichen internationalen Regelungsrahmens. Solange jedoch keine universell verbindlichen Normen bestehen, kommt dem Übereinkommen 108 weiterhin eine wesentliche Rolle als Grundlage für eine universell gültige Übereinkunft zu. Mit dem Hinweis darauf, dass ein zwingender rechtlicher Rahmen unerlässlich ist, sprachen wir uns auch für eine Verstärkung der internationalen Zusammenarbeit aus, insbesondere zwischen den Datenschutzbehörden, sowie für die Entwicklung des Dialogs mit sämtlichen Akteuren der Zivilgesellschaft.

Die geschlossene Konferenz der Datenschutzbeauftragten legte den Akzent auf die notwendige Verstärkung der Zusammenarbeit zwischen den Datenschutzbehörden, um namentlich im Rahmen der Durchführung von Kontrollen eine bessere Wirksamkeit zu erzielen. Sie verabschiedete insbesondere eine Resolution über die Koordination

bei der Anwendung der Bestimmungen über den Schutz der Privatsphäre auf internationaler Ebene. Die Konferenz möchte auch ihre eigene Rolle stärken und nahm zu diesem Zweck neue Verfahrensregeln an, verbunden namentlich mit der Schaffung eines Exekutivausschusses unter dem Vorsitz des Präsidenten der Datenschutzbehörde der Niederlande. Ausserdem verabschiedete die geschlossene Konferenz eine Resolution über den Datenschutz und Naturkatastrophen und eine Resolution über die Verwendung einer eindeutigen Kennung beim Einsatz des Internetprotokolls Version 6 (IpV6). Diese Resolution befürwortet insbesondere die standardmässige Beibehaltung von dynamischen IP-Adressen. Die Resolutionen sind zu finden auf unserer Webseite www.edoeb.admin.ch unter Themen – Datenschutz – Internationale Zusammenarbeit.

Arbeitsgruppe über die Informationssicherheit und den Schutz der Privatsphäre (OECD)

Die Arbeitsgruppe beschäftigte sich mit der Überprüfung der Richtlinien zu Sicherheit und Datenschutz, mit der Frage der Wirtschaftlichkeit von personenbezogenen Informationen in Relation mit Datenschutz und Sicherheit, mit den Anwendungsbereichen von medizinischen Daten in der Forschung und mit der Stärkung des Datenschutzes und der Sicherheit im Internet. Weitere Themen waren die nationalen Strategien zur Informationssicherheit und zur Bekämpfung der Internetkriminalität und schliesslich die Revision der Richtlinien zur Sicherheit der Informationsnetze.

Die rasante Entwicklung im Bereich der Privatsphäre, insbesondere die grenzüberschreitende Speicherung und Auswertung einer nie zuvor dagewesenen Menge von Personendaten, prägte die Diskussionen zur Revision der Richtlinie zu Sicherheit und Datenschutz. Weil nationale Regelungen bereits seit einiger Zeit an ihre Wirkungsgrenze stossen, wird der Einsatz von datenschutzfreundlichen Technologien als wesentlich erachtet, um den Schutz der Privatsphäre im Internet zu verbessern. Daher wurde eine Expertengruppe eingesetzt, die prüft, in welcher Art und Weise die Grundprinzipien der Richtlinie geändert werden könnten. Die Experten werden der Arbeitsgruppe Änderungsvorschläge unterbreiten.

Die Rolle von Personendaten im Internet ist auch unter dem Blickwinkel der Wirtschaftlichkeit von Informationen in Bezug auf Datenschutz und Sicherheit relevant. Ausgehend von der Frage, wie viel Personendaten wert sind, sollen in vier ausgewählten Bereichen (soziale Netzwerke, Wirtschaftsauskunfteien, Suchmaschinen und Kundenbindungsprogramme) entsprechende Berechnungen vorgenommen werden. Dabei soll auch die Frage geklärt werden, inwiefern Personendaten technische Innovation behindern könnten. Allerdings geht es darum, nicht ausschliesslich aus

wirtschaftlichen Kriterien auf einen höheren oder tieferen Datenschutz zu schliessen. Vielmehr wird es darum gehen, Risiken für die Privatsphäre zu definieren und gegebenenfalls Massnahmen vorzuschlagen, welche von Unternehmen oder Behörden umgesetzt werden könnten. Es darf nicht sein, dass die Bewertung der Personendaten durch die Bürger selber, welche oft aus Mangel an Information und Sensibilisierung ihre Personendaten völlig unterbewerten, die einzige Messlatte ist. Dazu muss die Tatsache, dass beispielsweise Suchmaschinen oder soziale Netzwerke so viele Personendaten wie möglich sammeln auch bei deren Bewertung mitberücksichtigt werden. Schliesslich ist der Wert einzelner Datensätze (wie etwa Adresse oder Telefonnummer) nicht gleich hoch wie derjenige von Kombinationen der Einzeldaten und der daraus resultierenden Profile. Eine externe Studie, die in Auftrag gegeben wurde, wird auch die Frage nach dem Preis von Personendaten beantworten müssen. Dabei sind die verschiedenen möglichen Berechnungsvektoren zu berücksichtigen.

Zur Verwendung von Personendaten in der medizinischen Forschung hat das Gesundheitskomitee erste Arbeitsschritte vorgestellt. Es geht primär darum, medizinische Daten effektiver für Forschungszwecke einsetzen zu können. Dabei sind die Implikationen für die Privatsphäre der betroffenen Patienten zu berücksichtigen. Hinzu kommt, dass in den meisten europäischen Ländern bereits ein detaillierter Rechtsrahmen für die Bearbeitung von Personendaten im medizinischen Bereich besteht. Nichtsdestotrotz sollen in diesem Bereich alle Möglichkeiten zur erleichterten Datenverwendung untersucht werden. Dafür wird eine Expertengruppe eingesetzt, die insbesondere den Implikationen für die Privatsphäre vertieft Rechnung trägt.

Angesichts der in letzter Zeit verübten diversen Hackerangriffe und der steigenden Internetkriminalität steht das Thema der Informationssicherheit stets im Vordergrund. Verschiedene OECD-Mitgliedsländer haben bereits nationale Strategien gegen Internetkriminalität und für die Stärkung der Informationssicherheit entwickelt. Die Arbeitsgruppe wird nun die verschiedenen nationalen Strategien in einer Vergleichsstudie zusammenführen. Diese Studie soll anschliessend den Ausgangspunkt für Überlegungen bilden, wie die Sicherheit der Informationsnetze auf internationaler Ebene am effektivsten bewerkstelligt werden kann.

Schliesslich wird im gleichen Zuge von der Arbeitsgruppe geprüft, ob die aus dem Jahr 2002 stammenden Richtlinien über die Sicherheit der Informationsnetze revidiert werden sollen.

Französischsprachige Vereinigung der Datenschutzbehörden

Die französischsprachige Vereinigung der Datenschutzbehörden (AFAPDP) hielt ihre 5. Konferenz am 31. Oktober 2011 in Mexico-City ab. Im Anschluss daran fand die Generalversammlung der Vereinigung statt. Ausserdem veranstaltete die Vereinigung

am 20. und 21. September 2011 in Dakar ein zweitägiges Bildungsseminar für ihre Mitglieder. Diesem Seminar ging die von der AFAPDP ausgerichtete 1. Afrikanische Regionaltagung über den Datenschutz voraus.

Diese verschiedenen Veranstaltungen boten den Anlass für einen umfassenden Erfahrungsaustausch zwischen den «bisherigen» Datenschutzbehörden und den neu eingerichteten oder im Aufbau befindlichen Behörden. Diese Kontakte bezogen sich im Wesentlichen auf die Informations- und Kommunikationstechnologien, die Biometrie, die Verantwortlichkeit der Unternehmen, den grenzüberschreitenden Datenverkehr, die Zusammenarbeit zwischen den Behörden, die Bildungs- und Sensibilisierungspolitik, sowie die Entwicklungen im Bereich des Datenschutzes in Afrika. Bei der 5. Konferenz hatten wir die Gelegenheit, die Vorteile eines Beitritts zum Übereinkommen 108, namentlich im Zusammenhang mit dem Informationsaustausch zwischen der Europäischen Union und Drittländern, sowie die Voraussetzungen für einen solchen Beitritt zu erläutern.

An ihrer Generalversammlung verabschiedete die AFAPDP vier Resolutionen. Die erste betrifft die Entwicklung eines Referenzsystems gemeinsamer Grundsätze der französischsprachigen Behörden als Rahmen für die Übermittlung von Personendaten zwischen Unternehmen. Dank dieses Bezugssystems sollen die Behörden über einen Rahmen verfügen, mit dessen Hilfe sie die Angemessenheit des Schutzes bei der Datenübertragung beurteilen können. Die zweite Resolution hat die effektive Sensibilisierung der Gesellschaft für den Datenschutz zum Inhalt. Eine dritte Resolution bezieht sich auf die Unabhängigkeit der für den Schutz von Personendaten zuständigen Behörden. Sie erinnert insbesondere daran, dass «nur eine völlig unabhängige Behörde über die für die Wahrung der Grundrechte und individuellen Freiheiten bezüglich der Personendaten notwendige Objektivität und Unparteilichkeit verfügt». Sie führt auch gewisse Kriterien für die Gewährleistung dieser Unabhängigkeit an (Rechtsgrundlage, Weisungsunabhängigkeit, Ernennungsmodalitäten, Budgetautonomie, Bereitstellung ausreichender Mittel, Freiheit bei der Personaleinstellung). Die vierte verabschiedete Resolution schliesslich betrifft die Verwendung der französischen Sprache bei der internationalen Konferenz der Datenschutzbehörden. In der an die 33. Konferenz gerichteten Resolution äussert die AFAPDP ihre Besorgnis angesichts des bei der internationalen Konferenz immer häufigeren Verzichts auf die französische Sprache, die doch über 70 Staaten gemeinsam ist. Mit Unterstützung des ibero-amerikanischen Datenschutznetzes, das vom Ausschluss der spanischen Sprache ebenso betroffen ist, setzte die AFAPDP durch, dass bei den nächsten Konferenzen eine Verdolmetschung aus dem Französischen und Spanischen, nötigenfalls mit Hilfe der verschiedenen Sprachgemeinschaften, gewährleistet wird. Die Resolutionen sind zu finden auf unserer Webseite www.edoeb.admin.ch unter Themen – Datenschutz – Internationale Zusammenarbeit.

Internationale Arbeitsgruppe Datenschutz im Telekommunikationsbereich

Im April und im September 2011 tagte die Internationale Arbeitsgruppe Datenschutz im Telekommunikationsbereich (oder «Berliner Gruppe»). Ein seit Jahren ständiges Thema ist dabei der Datenschutz bei Sozialen Netzwerken. Die neusten technischen Entwicklungen und die damit zusammenhängenden datenschutzrechtlichen Risiken wurden erörtert, insbesondere der Einsatz von Gesichtserkennungstechnologien im Internet.

Weiter wurden Arbeitspapiere zum Datenschutz beim Smart Metering, beim elektronischen Micropayment im Internet sowie bei der Datenaufzeichnung in Fahrzeugen verabschiedet. Zu den datenschutzrechtlichen Aspekten des Cloud Computings wurde zunächst ein Arbeitspapier mit Empfehlungen erarbeitet, welches im Rahmen des nächsten Treffens im April 2012 verabschiedet werden soll.

Die von der Arbeitsgruppe veröffentlichten Dokumente können auf den Webseiten www.iwgdpt.org oder www.datenschutz-berlin.de unter Europa/International – International Working Group on Data Protection in Telecommunications abgerufen werden, und zwar in Englisch und Deutsch.

2. Öffentlichkeitsprinzip

2.1 Zugangsgesuche

2.1.1 Departemente und Bundesämter

Die Anzahl der eingereichten Zugangsgesuche hat sich 2011 gegenüber dem Vorjahr beinahe verdoppelt. Gleich bleiben die Quoten bei der Gewährung respektive Verweigerung des Zugangs. Ebenfalls eine Verdopplung zeigt sich bei der Zahl der Schlichtungsanträge. Eine signifikante Zunahme ist überdies bei den von den Behörden verlangten Gebühren festzustellen.

Gemäss den uns mitgeteilten Zahlen sind im Jahr 2011 bei den Bundesbehörden insgesamt 466 Zugangsgesuche eingereicht worden. In 203 Fällen gewährten die Behörden einen vollständigen, in 128 einen teilweisen Zugang. Bei 126 Gesuchen wurde die Einsichtnahme vollständig verweigert. Im Vergleich zum Vorjahr fällt auf, dass sich die Zahlen beinahe verdoppelt haben (vgl. Statistik Ziff. 3.5). Zum einen hängt diese Zunahme wohl mit der Tatsache zusammen, dass das Öffentlichkeitsgesetz in der Bevölkerung, insbesondere bei den Medienschaffenden, immer bekannter wird und damit auch öfters Zugangsgesuche eingereicht werden. Zum anderen kann man davon ausgehen, dass in den 5 Jahren seit Inkrafttreten des Öffentlichkeitsgesetzes bei den Behörden eine Sensibilisierung stattgefunden hat und sie begonnen haben, Zugangsgesuche systematischer statistisch zu erfassen. Keine Veränderung gegenüber dem Vorjahr lässt sich hingegen bei den Prozentsätzen der vollständigen Verweigerungen (27%), der teilweise (27%) und der vollständig gewährten Zugänge (44%) feststellen.

Am meisten Zugangsgesuche für das Jahr 2011 meldete uns das BAG (33 Gesuche). Danach folgen das ENSI und das BAFU mit jeweils 22, wobei zumindest bei ersterem ein direkter Bezug zu Fukushima zu vermuten ist. Bei den Departementen liegen das UVEK (110 Zugangsgesuche), das EDI (87) und das EDA (80) an der Spitze. 13 von 71 Behörden meldeten uns für das Berichtsjahr 2011, dass bei ihnen kein einziges Zugangsgesuch gestellt worden sei.

Die im Vorjahr festgestellte Tendenz, dass Behörden vermehrt von der im Öffentlichkeitsgesetz vorgesehenen Möglichkeit der Gebührenerhebung Gebrauch machen, hat sich im Jahr 2011 weiter fortgesetzt. Gemäss den uns eingereichten Zahlen stellten elf Ämter Gebühren im Umfang von insgesamt SFr. 13'140.- in Rechnung. Im Vergleich zu den Vorjahren stellt dies eine signifikante Zunahme von fast 10'000 Franken dar (SFr. 3460.- im 2010 und SFr. 3850.- im 2009).

In Bezug auf den Zeitaufwand für die Bearbeitung der Zugangsgesuche in der Bundesverwaltung weisen wir auch dieses Jahr darauf hin, dass die Behörden erstens nicht verpflichtet sind, den zeitlichen Aufwand zu erfassen, und dass es zweitens keine für die gesamte Bundesverwaltung geltenden Vorgaben für eine einheitliche Erfassung des Zeitaufwands gibt. Die uns auf freiwilliger Basis übermittelten Angaben sind daher nur bedingt aussagekräftig. Gemäss diesen hat der gemeldete Zeitaufwand erneut zugenommen (2009: 748 Stunden; 2010: 815 Stunden; 2011: 1519 Stunden). Der Zeitaufwand für die Mitwirkung in Schlichtungsverfahren erhöhte sich von 158 Stunden im 2010 auf 453 Stunden im 2011.

2.1.2 Parlamentsdienste

Die Parlamentsdienste meldeten uns für das Jahr 2011 ein eingegangenes Zugangsgesuch, dem vollständig entsprochen wurde.

2.1.3 Bundesanwaltschaft

Die Bundesanwaltschaft teilte uns mit, dass sie den Zugang in zwei Fällen vollständig gewährt und in einem Fall verweigert habe.

2.2 Schlichtungsanträge

Im 2011 wurden insgesamt 65 Schlichtungsanträge eingereicht (vgl. Statistik Ziff. 3.8), was einer Verdoppelung gegenüber dem Vorjahr (32 Anträge) entspricht. Am meisten Schlichtungsanträge reichten Medienschaffende ein (24), gefolgt von Unternehmen (16).

Insgesamt konnten im Berichtsjahr 30 Schlichtungsanträge abgeschlossen werden. In acht Fällen konnte zwischen den Beteiligten eine Schlichtung erzielt werden. In neun Fällen erliessen wir – da keine einvernehmliche Lösung möglich oder von vornherein ersichtlich war – Empfehlungen. Zum Teil wurden mehrere Anträge mit einer Empfehlung oder einer Schlichtung erledigt. In fünf Fällen gewährten die Ämter während des laufenden Schlichtungsverfahrens von sich aus den Zugang. Es wurden zwei Anträge zurückgezogen und in vier Fällen waren die Voraussetzungen für die Anwendung des Öffentlichkeitsgesetzes nicht gegeben. In zwei Fällen wurde der Schlichtungsantrag nicht fristgerecht eingereicht.

Diese Zahlen lassen folgende Schlüsse und Bemerkungen zu: In 254 Fällen verweigerte die Bundesverwaltung den Zugang vollständig (126) respektive teilweise (128). Dem stehen 65 bei uns eingereichte Schlichtungsanträge gegenüber. Wie im Vorjahr wurde somit im Berichtsjahr in knapp 26% aller Fälle von ganz oder teilweise abgelehnten Zugangsgesuchen ein Schlichtungsantrag eingereicht. In 15 von 17 Fällen führten die mit einer Schlichtung oder einer Empfehlung abgeschlossenen Verfahren zu einer für den Gesuchsteller günstigeren Lösung (d.h. Schlichtung, respektive ein weitergehender Zugang als ursprünglich vom Bundesamt zugestanden).

Die auf Juli 2011 in Kraft getretene Teilrevision der VBGÖ erlaubt nun, die Frist für die Durchführung von Schlichtungsverfahren, die eine besonders aufwändige Bearbeitung erfordern, angemessen zu verlängern. Antragstellende müssen aber unabhängig davon länger auf die Durchführung eines solchen Verfahrens warten, weil die Anzahl eingereichter Anträge im Berichtsjahr deutlich zugenommen hat und wir noch immer über ungenügende Ressourcen für deren Bearbeitung verfügen.

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 auf unserer Webseite www.derbeauftragte.ch unter Dokumentation – Öffentlichkeitsprinzip – Empfehlungen zu finden.

Empfehlung BAFU / Analyse der Benzine und Dieselöle (16. Mai 2011)

Die Antragstellerin verlangte beim Bundesamt für Umwelt (BAFU) Zugang zu Prüfberichten über Analysen von Benzinen und Dieselölen bei Tankstellen. Das BAFU war mit dem anonymisierten Zugang zu jenen Angaben einverstanden, welche nach der Luftreinhalteverordnung relevant sind, verweigerte jedoch den Zugang zu den übrigen Daten. Es machte geltend, den betroffenen Unternehmen sei zum einen Vertraulichkeit zugesichert worden und zum andern enthielten die Prüfberichte Geschäftsgeheimnisse dieser Unternehmen. Ausserdem sei eine Anonymisierung der Daten nicht möglich. Der Beauftragte kam zum Schluss, dass eine ausdrückliche Zusicherung der Geheimhaltung fehlt und die Prüfberichte auch keine Geschäftsgeheimnisse enthalten. Nach Einschätzung des Beauftragten können die Personendaten in den verlangten Dokumenten ohne weiteres anonymisiert werden. Demzufolge empfahl er den Zugang zu den Prüfberichten in anonymisierter Form.

Empfehlung SBB / Betriebskonzept (1. Juli 2011)

Im Zusammenhang mit der Planung der 4. Teilergänzung der S-Bahn Zürich verlangte die Antragstellerin von den Schweizerischen Bundesbahnen (SBB) das «Betriebskonzept des Bahnhofs Herrliberg-Feldmeilen». Weil die SBB das gewünschte Dokument nicht zustellte, reichte die Antragstellerin einen Schlichtungsantrag ein. In seiner Empfehlung stellte der Beauftragte fest, dass die SBB im Bereich des Baus von Eisenbahnanlagen weder rechtsetzende noch verfügende Kompetenzen hat und daher das Öffentlichkeitsgesetz keine Anwendung findet.

Empfehlung BAK / Bericht Analyse und Auswertung Pilotprojekt (4. Juli 2011)

Der Antragsteller verlangte vom Bundesamt für Kultur (BAK) den Zugang zum Analyse- und Auswertungsbericht eines Pilotprojekts. Das BAK verweigerte zunächst die Einsicht, da das verlangte Dokument als Grundlage für weitere Verhandlungen benötigt werde. Später teilte das Bundesamt mit, dass diese Verhandlungen nun abgeschlossen seien; es lehnte die Zugänglichmachung des Dokuments jedoch trotzdem ab mit der

Begründung, dass konkrete behördliche Massnahmen – nunmehr des fedpol – beeinträchtigt würden. Daraufhin ersuchte der Beauftragte das fedpol mehrmals erfolglos um Auskünfte zur Klärung der Anwendbarkeit des Öffentlichkeitsgesetzes. Schliesslich empfahl der Beauftragte den Zugang zum verlangten Bericht in teilweise anonymisierter Form.

Empfehlung SECO / Vollzugskostenbeiträge PLK (6. Juli 2011)

Im Zusammenhang mit der aufsichtsrechtlichen Tätigkeit des SECO im Rahmen des Gesamtarbeitsvertrages in der Schweizerischen Gebäudetechnikbranche verlangte die Gesuchstellerin Zugang zu Jahresrechnungen, Budgets und Revisionsberichten der Paritätischen Landeskommission (PLK) der Gebäudetechnikbranche. Das SECO lehnte die Einsicht mit der Begründung ab, die verlangten Dokumente enthielten Geschäftsgeheimnisse und die Privatsphäre Dritter wäre beeinträchtigt. Nach Einschätzung des Beauftragten enthalten die verlangten Dokumente keine Geschäftsgeheimnisse. Hinsichtlich der Personendaten empfahl er die Anonymisierung eines Teils, die Offenlegung von Personendaten aufgrund des überwiegenden öffentlichen Interesses eines anderen Teils.

Empfehlung BLW / Controlling-Formulare Milchmehrmengen (5. August 2011)

Die Antragstellerin verlangte Zugang zu den Controlling-Formularen der vom Bundesamt für Landwirtschaft (BLW) bewilligten Milchmehrmengen. Das BLW stellte der Antragstellerin 67 Formulare zu, wobei es einzelne Angaben wie z.B. Namen der Milchverwerter, Produkte und Identifikationsnummern für Produktgruppen abdeckte. Es verweigerte zudem den Zugang zu den Formularen der fünf grössten Milchverwerter und machte den Schutz von Geschäftsgeheimnissen und Personendaten geltend. Daraufhin reichte die Antragstellerin einen Schlichtungsantrag ein. Im Schlichtungsverfahren gelangte der Beauftragte zum Schluss, dass die Angaben auf diesen fünf Formularen letztlich Rückschlüsse auf die Exportstrategien der Milchverwerter ermöglichten. Da die Milchverwerter zueinander im Wettbewerb stehen, konnte nicht ausgeschlossen werden, dass die Offenlegung dieser Angaben tatsächlich negative Auswirkungen auf die Marktstrategien des einzelnen haben würde und so zu Wettbewerbsverzerrungen führen könnte. Nach Einschätzung des Beauftragten hatten diese fünf Milchverwerter daher ein sowohl berechtigtes als auch schutzwürdiges Interesse daran, dass diese Informationen nicht zugänglich gemacht wurden. Der Beauftragte qualifizierte die Angaben auf den Controlling-Formularen unter den gegebenen Umständen als Geschäftsgeheimnisse und unterstützte das BLW darin, den Zugang nicht zu gewähren.

Empfehlung ESTV / Cockpits und Amtsreportings (19. September 2011)

Nach dem Urteil des Bundesverwaltungsgerichts vom 15. September 2009 betreffend Cockpits und Amtsreportings-Dokumente hat die Eidgenössische Steuerverwaltung ESTV dem Antragsteller den verlangten Dokumentensatz mit teilweise eingeschwärzten Textpassagen zugestellt. Die ESTV begründete die Einschwärzungen weder auf den Dokumenten noch im Begleitbrief, womit sie für den Antragssteller nicht nachvollziehbar waren. Er reichte einen Schlichtungsantrag ein. Im Schlichtungsverfahren legitimierte die ESTV dem Beauftragten die Einschwärzungen und erklärte zusätzliche Textpassagen für zugänglich. Den Zugang zu weiteren Textpassagen lehnte die ESTV mit der Begründung ab, dass die freie Meinungs- und Willensbildung, die zielkonforme Durchführung behördlicher Massnahmen sowie die Privatsphäre von Dritten und Verwaltungsangestellten beeinträchtigt seien. Hinsichtlich der abgedeckten Textpassagen bestanden zwischen der ESTV und dem Beauftragten zum Teil Differenzen. Einerseits empfahl der Beauftragte entgegen der Ansicht der ESTV den Zugang zu bestimmten Passagen. Andererseits unterstützte er die ESTV darin, dass in gewissen Fällen der Zugang nicht gewährt werden muss bzw. aufgeschoben werden kann, so beispielsweise bei Daten von Drittpersonen und von Verwaltungsangestellten.

Empfehlung BFE / KNS-Protokolle (16. Dezember 2011)

Der Antragssteller verlangte beim Bundesamt für Energie (BFE) den Zugang zu allen Sitzungsprotokollen der Eidgenössischen Kommission für Nuklearsicherheit (KNS) aus dem Jahr 2009. Das BFE und der Antragssteller einigten sich auf die Zustellung eines einzigen Protokolls – dies geschah, doch das Protokoll war über weite Teile eingeschwärzt. Das Bundesamt begründete die Einschwärzungen damit, eine Offenlegung würde ausstehende politische und administrative Entscheide gefährden. Im Schlichtungsverfahren trafen sich der Beauftragte, das BFE und die KNS zu einer Besprechung. Damit offen über den Inhalt der abgedeckten Textpassagen diskutiert werden konnte, fand diese Sitzung ohne den Antragsteller statt. Der Beauftragte gab für jede Textpassage seine Einschätzung betreffend die Zugangsgewährung respektive -verweigerung ab. Aufgrund dessen und der inzwischen getroffenen politischen bzw. administrativen Entscheide erklärten sich das BFE und die KNS bereit, die meisten Textpassagen offen zu legen und nur noch zwei kurze Textstellen abzudecken. In Bezug auf diese stimmte der Beauftragte mit dem BFE und der KNS überein, dass der Zugang bis zum politischen bzw. administrativen Entscheid aufzuschieben sei.

Empfehlung BAG / Prämientarife KVG (19. Dezember 2011)

Der Antragsteller verlangte beim Bundesamt für Gesundheit (BAG) Zugang zu den eingereichten und genehmigten Prämientarifen der Krankenversicherungen sowie den Nichtgenehmigungen. Das Bundesamt stellte dem Antragsteller insgesamt vier Dokumente von zwei Krankenversicherungen vollständig zu, verweigerte jedoch einen weitergehenden Zugang mit der Begründung, die verbleibenden Dokumente enthielten entweder Informationen, die in den bereits zugestellten Dokumenten schon enthalten seien, oder Geschäftsgeheimnisse. Zudem verweigerte es den Zugang zu den Dokumenten der zwei anderen Krankenversicherungen und machte geltend, die Dokumente seien vom Zugangsgesuch zeitlich nicht erfasst. Dies stützte der Beauftragte im Schlichtungsverfahren. Budgetberechnungen und Angaben zur finanziellen Situation hingegen qualifizierte er als Geschäftsgeheimnisse und unterstützte das BAG darin, den Zugang hierzu zu verweigern. Im Übrigen empfahl er einen teilweisen Zugang.

Empfehlung BSV / Sitzungsprotokolle AHV/IV-Kommission (22. Dezember 2011)

Der Antragssteller verlangte vom Bundesamt für Sozialversicherungen (BSV) Einsicht in mehrere Sitzungsprotokolle der AHV/IV-Kommission aus dem Jahr 2009. Das BSV verweigerte den Zugang zu den Dokumenten mit der Begründung, dass die AHV/IV-Kommission als Verwaltungskommission nicht in den persönlichen Geltungsbereich des Öffentlichkeitsgesetzes falle, die Sitzungen vertraulich seien und die Dokumente Personendaten enthielten.

Im Schlichtungsverfahren machte der Beauftragte das BSV auf das rechtskräftige Urteil des Bundesverwaltungsgerichts vom 17. Juni 2011 aufmerksam, in welchem entschieden worden war, dass Verwaltungskommissionen seit dem 1. Januar 2009 ebenfalls der dezentralen Bundesverwaltung angehören und damit auch in den Geltungsbereich des Öffentlichkeitsgesetzes fallen. Das BSV blieb bei seiner Rechtsposition. Da das Bundesamt keine Ausnahmegründe darlegen konnte, empfahl der Beauftragte den Zugang zu den Sitzungsprotokollen.

2.3.2. Schlichtungen

In folgenden Fällen konnte eine Schlichtung erzielt werden:

Schlichtung BFE / Dokumente betreffend Schwallbetrieb bei der Schleuse Châtelot

Der Antragsteller verlangte beim Bundesamt für Energie (BFE) Einsicht in gesetzliche und vertragliche Dokumente betreffend den Schwallbetrieb bei der Schleuse Châtelot. Das BFE verwies den Antragsteller einerseits auf eine Medienmitteilung und andererseits auf die Zuständigkeit der französischen Behörden. In der Stellungnahme zuhanden des Beauftragten lehnte das Bundesamt den Zugang zu vier Dokumenten ab, da diese vor dem Inkrafttreten des BGÖ erstellt wurden. Hinsichtlich der übrigen Dokumente berief sich das BFE auf laufende bzw. künftige Verhandlungen, in welchen neben dem Bund mehrere kantonale Behörden und auch Frankreich betroffen seien. Im Schlichtungsverfahren bestimmten die Parteien den Umfang der relevanten Dokumente, welche den Antragsteller interessierten, und einigten sich über das weitere Vorgehen.

Schlichtung BABS / Bericht Polycom

Der Antragsteller verlangte beim Bundesamt für Bevölkerungsschutz (BABS) Einsicht in den Bericht «Polycom: Vision im Bereich IKT, Analyse und Konzept». Das BABS teilte dem Antragsteller u.a. mit, dass es sich um einen nicht fertig gestellten Bericht handle. Auf Intervention des Beauftragten hin und nachdem das BABS mit mehreren involvierten Bundesorganen Rücksprache genommen hatte, gewährte das BABS dem Antragsteller teilweise Zugang zum fraglichen Analyse-Dokument.

Schlichtung BSV / Subventionszahlungen

Der Antragssteller verlangte vom Bundesamt für Sozialversicherungen (BSV) Einsicht in Unterlagen über Subventionszahlungen, die das Bundesamt im Jahr 2007 an Institutionen mit Werkstätten und Wohnheimen für Behinderte ausgerichtet hatte. Angesichts der grossen Anzahl dieser Institutionen (und der mit dem Zugangsgesuch verbundenen Gebühren) beschränkte sich der Antragsteller auf 35 Institutionen. Das BSV anerkannte grundsätzlich das überwiegende Interesse am Zugang zur Auflistung der Subventionszahlungen, wies aber auf die Pflicht zur Anhörung der betroffenen Institutionen hin. Der Antragsteller, selber ein Institut mit Werkstatt und Wohnheim, wollte seine Identität indes nicht offen legen. Er einigte sich daher mit dem BSV darauf, dass sein Zugangsgesuch nur noch für jene Institutionen gelte, die mit der Herausgabe des Subventionsentscheides unter dieser Voraussetzung einverstanden sind. Für den

Fall, dass eine Institution die Einwilligung nicht erteile, ziehe er sein Zugangsgesuch zurück – damit verzichtete der Antragsteller auf den Erlass einer Verfügung, die ihm und der betroffenen Institution eröffnet würde.

Schlichtung EFK / Dienststellenbericht

Der Antragssteller verlangte von der Eidgenössischen Finanzkontrolle (EFK) Zugang zu zwei Dienststellenberichten über das Kooperationsbüro in Tschad. Die EFK anerkannte den grundsätzlichen Anspruch auf Zugang. Aufgrund der Komplexität des Falles (u.a. Anhörung von Personen im Ausland) und dem daraus anfallenden Aufwand orientierte sie den Antragsteller darüber, dass er mit Gebühren von mehreren Tausend Franken rechnen müsse. In der Schlichtungsverhandlung einigten sich der Antragsteller und die EFK u.a. darüber, dass die EFK nach eigenem Ermessen alle Personendaten anonymisiere respektive ganze Abschnitte mit Personendaten schwärze, und auf einen Gebührenbetrag von SFr. 500.- (für den bis zu diesem Zeitpunkt ausgeführten Arbeitsaufwand).

Schlichtung VBS / Immobilienliste Verteidigungsattachés

Die Antragsstellerin wollte Einsicht in eine Auflistung mit den Wohnungen der Verteidigungsattachés unter Angabe der Miet- bzw. Kaufkosten. Sie trat mit Verwaltungsstellen des EFD und des VBS in Kontakt, erhielt aber keinen Zugang zum Dokument, u.a. aus Sicherheitsgründen. Nachdem im Schlichtungsverfahren zuerst die Frage der Zuständigkeit geklärt werden konnte, erklärte sich das VBS bereit, der Antragstellerin die gewünschte Auflistung der Mietkosten herauszugeben, wobei die Wohnadressen abgedeckt wurden. Die Antragstellerin verzichtete auf Dokumente mit den Kaufkosten die Wohnungen in Stockholm und Washington betreffend.

Schlichtung BFM / Vertrag mit Kindertagesstätte

Das Bundesamt für Migration (BFM) schloss mit einer privaten Anbieterin eine Absichtserklärung und einen Vertrag über die Einrichtung einer Kindertagesstätte ab, in der den Angestellten des BFM garantierte Betreuungsplätze zur Verfügung stehen sollten. Eine andere Kindertagesstätte verlangte Einsicht in diese Unterlagen, was das BFM jedoch ablehnte. Im Schlichtungsverfahren gelangte der Beauftragte zur Einschätzung, dass der Zugang zu den beiden Dokumenten gewährt werde sollte und regte die Anhörung der betroffenen privaten Anbieterin an. Diese war mit der Herausgabe der Dokumente einverstanden.

Schlichtung ENSI/ Kernmantelrisse KKM

Die Antragstellerin verlangte Einsicht in die Untersuchungsergebnisse zum Zustand des Kernmantels im Kernkraftwerk Mühleberg (KKM) sowie in den Anforderungskatalog für Untersuchungen und Unterhalt der Kernmantelrisse im KKM. Das Eidgenössische Nuklearsicherheitsinspektorat (ENSI) schob den Zugang zu den verlangten Dokumenten auf und begründete dies damit, dass seine freie Meinungs- und Willensbildung beeinträchtigt würde und überdies der Entscheid betreffend den Bericht zum Langzeitbetrieb des KKM noch nicht gefallen sei. Im Schlichtungsverfahren konnten die Beteiligten mit Unterstützung des Beauftragten zum einen den Umfang der Dokumente betreffend die Kernmantelrisse eingrenzen. Zum anderen einigten sie sich darüber, dass das ENSI Passagen von Dokumenten zugänglich macht, welche die zentralen Fragen der Antragstellerin beantworten.

Schlichtung BK / Vote électronique

Der Antragsteller verlangte bei der Bundeskanzlei (BK) Einsicht in sämtliche Dokumente von Bundesrat und Bundeskanzlei betreffend die Genehmigung des Bundesrates für die Durchführung von Vote électronique bei den Nationalratswahlen 2011, die Vorbereitungen für Vote électronique bei den Wahlen 2007 sowie Zugang zu einer Auflistung sämtlicher Dokumente zu Vote électronique in der elektronischen Geschäftsverwaltung (GEVER) seit 2007. Die BK verweigerte den Zugang zu den Dokumenten zum einen mit dem Argument, dass das Öffentlichkeitsgesetz für Dokumente des Bundesrates nicht gelte, und zum andern aufgrund der Beeinträchtigung der inneren Sicherheit und der Beziehung zu den Kantonen bei der Gewährung des Zugangs. Weiter verlangte sie vom Antragsteller eine Präzisierung des umfangreichen Zugangsgesuchs. Im Schlichtungsverfahren hielt die BK grundsätzlich an ihren Positionen fest, zeigte sich aber bereit, die Antragstellerin zu zwei Gesprächen zu empfangen, um sie u.a. «aus Sicht des Bundes» über Sicherheitsfragen zwischen der Stimmabgabe und der Publikation der Ergebnisse zu informieren.

2.4 Gerichtsentscheide zum Öffentlichkeitsgesetz

2.4.1 Bundesverwaltungsgericht

Das Bundesverwaltungsgericht (BVGer) hat im Berichtsjahr vier Urteile gefällt, denen Schlichtungsverfahren beim Beauftragten vorangegangen waren.

So hat es entschieden, dass die Auflösungsvereinbarungen der Arbeitsverträge des ehemaligen Generalsekretärs des Eidgenössischen Justiz- und Polizeidepartements (EJPD) und seines Stellvertreters öffentlich zugänglich gemacht werden müssen. Das Gericht gewichtete das Interesse des Gesuchstellers – und damit jenes der Öffentlichkeit – am Einblick in die Vereinbarungen stärker als jenes der beiden Betroffenen am Schutz ihrer Privatsphäre (siehe Urteil vom 17. Februar 2011, Ref. A-3609/2010). Das Bundesgericht hatte diesen Fall zur Neubeurteilung ans BVGer zurück gewiesen (siehe unseren 18. Tätigkeitsbericht 2010/2011, Ziffer 2.4.1).

Gemäss BVGer muss die Liste mit den Interessenerklärungen der Mitglieder der Eidgenössischen Impfkommission (EKIF) öffentlich zugänglich sein. Dies geht aus dem Entscheid des Bundesverwaltungsgerichts vom 17. Juni 2011 hervor. Laut Urteil überwiegt hier das Interesse der Gesuchstellerin am Einblick in diese Liste jenes der betroffenen Kommissionsmitglieder am Schutz ihrer Privatsphäre (Urteil vom 17. Juni 2011, Ref. A-3192/2010).

Im Hinblick auf ein allfälliges Freihandelsabkommen mit der EU im Agrar- und Lebensmittelbereich hatte das EVD 2008 eine ad-hoc-Arbeitsgruppe eingesetzt und diese beauftragt, konkrete Begleitmassnahmen zu erarbeiten. Diese Arbeitsgruppe ist gemäss einem Urteil des BVGer der Bundesverwaltung zuzurechnen und unterliegt daher dem Öffentlichkeitsgesetz. Das BLW wurde somit angehalten, der Journalistin den gewünschten Zugang zum Dokument der Arbeitsgruppe, welches 250 Vorschläge für Begleitmassnahmen enthält, zu gewähren. Gemäss Urteil können die Mitglieder der Gruppe den Schutz ihrer Privatsphäre nicht umfassend gelten machen (Urteil vom 7. Dezember 2011, Ref. A-1135/2011).

Im vierten Fall ging es um ein autorisiertes Interview, das die damalige Bundesrätin Micheline Calmy-Rey einer Zeitung gewährt hatte. Dabei hatte diese mit dem Eidgenössischen Departement für auswärtige Angelegenheiten (EDA) vereinbart, das Interview vor dessen Veröffentlichung zur allfälligen Korrektur vorzulegen. Ein Gesuchsteller verlangte Zugang zur Interviewabschrift mit den Korrekturen, was das EDA jedoch ablehnte und vom Beauftragten in seiner Empfehlung vom 9. Dezember 2010 gestützt wurde, worauf der Gesuchsteller Beschwerde gegen die Verfügung einreichte. Das BVGer gab dem EDA recht und hielt in seinem Entscheid fest, dass erst ein autorisiertes Interview ohne sichtbare Korrekturen ein fertig gestelltes und somit amtliches Dokument darstellt (Urteil vom 22. Dezember 2011, Ref. A-1156/2011).

2.5 Ämterkonsultationen

2.5.1 Revision des Kartellgesetzes

Der Beauftragte hat zur Revision des Kartellgesetzes Stellung genommen. Diese hat unter anderem zum Ziel, die Wettbewerbsbehörden inklusive des Wettbewerbsgerichts neu zu organisieren (sog. Institutionenreform). Dabei ist auch vorgesehen, die neuen Wettbewerbsbehörden teilweise vom sachlichen Geltungsbereich des Öffentlichkeitsgesetzes auszunehmen. Konkret sollen fortan Verfahren zur Beurteilung von Wettbewerbsbeschränkungen, d.h. Vorabklärungen und Untersuchungen, nicht mehr unter das BGÖ fallen. Als Begründung wird angeführt, dass es inkonsequent wäre, die Verfahrensakten der Wettbewerbsbehörde dem BGÖ zu unterstellen, wenn dieselben Akten später vor Wettbewerbsgericht nicht mehr in den Anwendungsbereich des Öffentlichkeitsgesetzes fallen. Zudem bestehe bei den entsprechenden Akten für betroffene Unternehmen ein erhebliches Schutzbedürfnis. Deshalb müssten diese Verfahren vom sachlichen Geltungsbereich des BGÖ ausgenommen werden.

Der Beauftragte teilt diese Auffassung nicht und hat zuhanden des SECO eine entsprechende Stellungnahme abgegeben. Zum einen bietet das Öffentlichkeitsgesetz im Einzelfall ausreichende gesetzliche Möglichkeiten, um den Zugang zu Akten zu verweigern, einzuschränken oder aufzuschieben, insbesondere was den Schutz von Berufs-, Geschäfts- und Fabrikationsgeheimnissen und von Personendaten anbelangt. Zum anderen ist sich der Beauftragte des erhöhten Schutzbedürfnisses für gewisse amtliche Dokumente (bspw. mit Inhalten zu einem der erwähnten Geheimnisse) sehr wohl bewusst und hat dies in der Vergangenheit immer entsprechend berücksichtigt. Schliesslich darf nicht ausser Acht gelassen werden, dass die heutige WEKO und deren Sekretariat seit Inkrafttreten des Öffentlichkeitsgesetzes vollumfänglich dem BGÖ unterstehen. Während dieser ganzen Zeit musste sich die WEKO nur mit sehr wenigen Zugangsgesuchen befassen. Dies zeigt, dass das Öffentlichkeitsgesetz in der Vergangenheit die Arbeit der Wettbewerbsbehörden weder erschwert noch einen zusätzlichen administrativen Aufwand verursacht hat.

Aus Sicht des Beauftragten bestand kein Anlass, die neuen Wettbewerbsbehörden teilweise vom sachlichen Geltungsbereich des BGÖ auszunehmen. Da das SECO in dieser Frage jedoch kein Entgegenkommen zeigte, hat der Beauftragte einen Bericht an den Bundesrat verfasst, worin er seine Position nochmals ausführlich begründete. Der Bundesrat ist schliesslich der Auffassung des Beauftragten gefolgt und hat entschieden, dass die neuen Wettbewerbsbehörden – wie in der Vergangenheit – vollumfänglich dem Öffentlichkeitsgesetz unterstehen sollen.

2.5.2 Revision der Akkreditierungs- und Bezeichnungsverordnung

Im Revisionsentwurf der Akkreditierungs- und Bezeichnungsverordnung (AkkBV) war eine Norm vorgesehen, wonach Erkenntnisse aus Begutachtungen und Kontrollen der Schweizerischen Akkreditierungsstelle (SAS) vertraulich sein sollen. Der Beauftragte hat im Rahmen der Ämterkonsultation Stellung genommen und darauf hingewiesen, dass der Vorbehalt, der bestimmte Informationen als geheim (inkl. vertraulich) bezeichnet, in einem Bundesgesetz, d.h. einem formellen Gesetz, geregelt sein muss. Nur dann liegt eine Spezialbestimmung gemäss Art. 4 BGÖ vor. Die vorgesehene Vertraulichkeitsnorm wäre lediglich in einer Verordnung, d.h. in einem Gesetz im materiellen Sinne, und nicht in einem Bundesgesetz geregelt. Deshalb ist keine Spezialbestimmung vorhanden und das Öffentlichkeitsgesetz bleibt weiterhin für Berichte der SAS anwendbar.

3. Der EDÖB

3.1 Migration auf Windows 7 und Geschäftsverwaltungssystem GEVER

Dieses Jahr haben wir neue Hard- und Software erhalten und zu Windows 7 migriert. Aus diesem Anlass nahmen wir eine Neubeurteilung des tatsächlichen Bedarfs an Informatiklösungen vor, angefangen mit der Frage nach dem geeigneten Geschäftsverwaltungssystem. Die Standardsysteme erfüllen unsere Anforderungen in Sachen Vertraulichkeit der Daten noch nicht, was uns zwang, unser System EDÖB-Office in die neue Umgebung von Windows 7 zu überführen, wo es in Betrieb bleibt, bis eine gleichwertige Lösung verfügbar wird.

Wie die meisten Bundesämter erhielten auch wir dieses Jahr neue Rechner und migrierten zu Windows 7. Diese Hard- und Software-Migration erforderte eine Projektplanung und bot die Gelegenheit zu einer Neubeurteilung des tatsächlichen Bedarfs an Informatiklösungen, angefangen bei unserem eigenen Geschäftsverwaltungssystem. So konnte auf zahlreiche heute nicht mehr wirklich nützliche oder genutzte Dienstprogramme verzichtet werden. Einige andere Anwendungen wurden dagegen in ihrer portablen Version neu installiert, um die erheblichen Verzögerungen bei der Aktualisierung zu vermeiden, die mit der Zeit der Gesamtsicherheit schaden könnten (nicht behobene Sicherheitslücken, nicht verfügbare neue Funktionen), sowie um die nicht unbedeutenden Kosten zu umgehen, die durch die vom Leistungserbringer vorgenommene Paketierung einer solchen Software verursacht worden wären.

Zur Vorbereitung unserer Migration in ein GEVER-Standardprodukt haben wir unser neues Ordnungssystem vom Schweizerischen Bundesarchiv genehmigen lassen, während unsere Organisationsvorschriften schon seit ihrer Einführung im Jahr 2000 regelmässig aktualisiert werden. Die homologierten Systeme erfüllen jedoch unsere Anforderungen betreffend die Vertraulichkeit der Daten noch nicht, sodass wir gezwungen waren, unser eigenes System EDÖB-Office in die neue Umgebung Windows 7 zu überführen (wichtigste Anpassungen im Zusammenhang mit MS-Office 2007 Professional und PGP Version 10), wo es in Betrieb bleibt, bis eine gleichwertige Lösung verfügbar wird. Es sei hier daran erinnert, dass das EDÖB-Office dank der durch PGP gewährleisteten Verschlüsselung der Inhalte die hohe Vertraulichkeitsstufe der Dokumente gegenüber den internen Administratoren (Anwendung und Datenbank), den verschiedenen internen Aufgaben (Amtsdirektion, Datenschutz, indirektes Auskunftsrecht, Öffentlichkeitsprinzip) und vor allem gegenüber dem externen Lösungsanbieter – derzeit das BIT – (Arbeitsplätze, Netzwerk, Drucker, Dateien, Mitteilungen, Datenbank, Speicherung, usw.) sicherstellt.

3.2 Sechster Datenschutztag

Der Datenschutztag stand dieses Jahr im Zeichen der Themen «Datenbearbeitungen durch Unternehmen» und «Nutzung der Neuen Medien durch Jugendliche». In beiden Bereichen wurden von uns mitentwickelte Sensibilisierungsprojekte der Öffentlichkeit präsentiert.

Datenbankverantwortliche in Unternehmen und Organisationen sehen sich in Zeiten der Digitalisierung mit beträchtlichen Mengen an Personendaten konfrontiert, insbesondere mit solchen von Mitarbeitenden und Kunden. Bei der Bearbeitung dieser Daten müssen sie den technologischen und gesetzlichen Anforderungen Rechnung tragen, was gerade für kleinere und mittlere Unternehmen mit Schwierigkeiten verbunden sein kann. Der neue, anlässlich des sechsten Datenschutztags vom 27. Januar 2012 lancierte interaktive Onlinedienst «Think Data» will den Unternehmen, Organisationen, Behörden und Privatpersonen entsprechende Hilfestellung bieten und sie für die datenschutzkonforme Bearbeitung von Personendaten und die Schaffung von Transparenz sensibilisieren. So finden Firmen bei www.thinkdata.ch auf ihre jeweiligen Bedürfnisse zugeschnittene Ratschläge und Informationen, die zahlreiche Rechts- und Technologiebereiche abdecken.

Think Data ist ein nicht-kommerzielles Gemeinschaftsprojekt der Datenschutz- und Öffentlichkeitsbeauftragten des Kantons Genf, der Universität Genf, des Hochschulinstituts für Öffentliche Verwaltung IDHEAP in Lausanne, des Genfer Observatoriums für Technologien, des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten und weiterer Akteure. Der Dienst ist auf Französisch und demnächst auch auf Deutsch verfügbar.

Ebenfalls am Datenschutztag haben wir ein Lehrmittel zum Thema «Elementare Datensicherheit» publiziert, welches jungen Erwachsenen Wissenswertes und Tipps zum sicheren Umgang mit ihren Daten in den Neuen Medien vermittelt. Es behandelt insbesondere die Themen Soziale Netzwerkseiten, mobile Kommunikation und Onlineportale. Lehrerinnen und Lehrer können das umfangreiche Arbeitsdossier und die neun – voneinander unabhängigen – Lektionen im Unterricht einsetzen. Es steht allen Interessierten auf unserer Webseite zur Verfügung: www.derbeauftragte.ch, Themen – Datenschutz – Internet – Kinder&Jugendliche – Lehrmittel für 16-19 Jährige (auf Deutsch; die französische und die italienische Version folgen im Laufe des Jahres 2012).

3.3 Publikationen des EDÖB im laufenden Geschäftsjahr

Bürgerinnen und Bürger finden Informationen zu unseren Tätigkeiten in den Bereichen Datenschutz und Öffentlichkeitsprinzip auf unserer Webseite. Im aktuellen Geschäftsjahr wurden u.a. Erläuterungen zu Cloud Computing, zur E-Privacy-Richtlinie der EU sowie ein Lehrmittel zum Thema «Elementare Datensicherheit» aufgeschaltet.

Immer mehr Unternehmen, Behörden und Institutionen lagern ihre bisher typischerweise intern erledigten Datenverarbeitungen an externe Unternehmen aus und setzen dafür auf Cloud Computing («Rechnen in der Wolke»). Unsere Erläuterungen dazu zeigen die Risiken des Cloud Computings für die Privatsphäre auf und geben Empfehlungen im Hinblick auf den Datenschutz ab. Sie sind auf unserer Webseite www.derbeauftragte.ch unter Themen – Datenschutz – Unternehmen zu finden.

Auch haben wir Erläuterungen zur E-Privacy-Richtlinie der EU für mehr Transparenz im Internet publiziert. Das EU-Parlament hatte Ende 2009 eine Revision dieser Richtlinie beschlossen, um den Anforderungen der digitalen Technologien gerecht zu werden. Ihr Ziel ist es, mehr Transparenz und Sicherheit für die Verbraucher zu schaffen. Unsere Erläuterungen behandeln u.a. die Umsetzung der in der Richtlinie enthaltenen Vorgaben und nennen allfällige Konsequenzen für die Schweiz. Sie befinden sich unter Themen – Datenschutz – Unternehmen (siehe auch Ziff. 1.3.2 des vorliegenden Tätigkeitsberichts).

Eine Einführung in die Gefahren, welche moderne Informationssysteme aus der Sicht des Datenschutzes mit sich bringen, bietet unser überarbeiteter Leitfaden zu den technischen und organisatorische Massnahmen. Er soll dabei helfen, Massnahmen zu realisieren, die einen optimalen und angemessenen Schutz der Personendaten sicherstellen. Die wichtigsten Themen des Datenschutzes werden ebenso dargestellt wie die damit verbundenen technischen und organisatorischen Massnahmen Verschlüsselung, Anonymisierung und Authentifizierung.

Im Bereich Videoüberwachung durch Private wurde das bisherige Merkblatt überarbeitet sowie ein neues zu Aufnahmen im öffentlichen Raum aufgeschaltet (Dokumentation – Datenschutz – Merkblätter – Videoüberwachung; siehe auch Ziff. 1.2.6 des vorliegenden Tätigkeitsberichts).

Zum Thema «Elementare Datensicherheit» haben wir ein Lehrmittel publiziert, welches jungen Erwachsenen Wissenswertes und Tipps zum sicheren Umgang mit ihren Daten in den Neuen Medien vermittelt (siehe Ziff. 3.4 des vorliegenden Tätigkeitsberichts). Die Unterlagen können unter Themen – Datenschutz – Internet – Kinder&Jugendliche – Lehrmittel für 16-19 Jährige heruntergeladen werden.

3.4 Datenschutzlehrmittel für junge Erwachsene

Die Sensibilisierung von Jugendlichen für den Umgang mit ihren persönlichen Daten bildete auch in diesem Jahr einen Schwerpunkt unserer Tätigkeiten im Bereich Ausbildung und Sensibilisierung. Um jungen Erwachsenen Knowhow zur Datensicherheit bei der Nutzung der Neuen Medien zu vermitteln, lancierten wir ein Lehrmittel, welches online und kostenlos verfügbar ist. Lehrerinnen und Lehrer können die Lektionen seit Januar dieses Jahres im Schulunterricht einsetzen.

Jüngere Erhebungen wie die James-Studie der Zürcher Hochschule für Angewandte Wissenschaften von 2010 belegen, wie intensiv junge Menschen heutzutage die Möglichkeiten der neuen Technologien nutzen. Soziale Netzwerke, Video- und Spiele-Plattformen oder Surfen über das Mobiltelefon nehmen in ihrer Lebenswelt einen festen Platz ein. Dabei sind sie allerdings häufig sich selbst überlassen. Die Begleitung durch die Erziehungsberechtigten erfolgt besonders bei Personen aus tieferen Bildungsschichten kaum oder nur oberflächlich, weshalb den Schulen eine umso wichtigere Rolle bei der Vermittlung von Medienkompetenz zukommt. Um die Lehrerinnen und Lehrer dabei zu unterstützen, haben wir 2010 ein dreiteiliges, mehrjähriges Ausbildungsprojekt gestartet, dessen Ziel es ist, Kindern und Jugendlichen Wege zu einer sicheren und vernünftigen Nutzung der Neuen Technologien aufzuzeigen, mit Fokus auf den Schutz der eigenen Privatsphäre (vgl. unseren 18. Tätigkeitsbericht 2010/2011, Ziff. 3.3 und 3.4).

Das aktuelle Lehrmittel richtet den Fokus auf die Datensicherheit, also auf die Frage, wie man seine Personendaten und damit auch seine Privatsphäre in den Medien wirkungsvoll schützen kann. Zur Zielgruppe zählen Schüler der Sekundarstufe II. Die Inhalte wurden zusammen mit der Agentur Kik erarbeitet, welche auf die Erstellung von Unterrichtsunterlagen spezialisiert ist. Lehrerinnen und Lehrer können das umfangreiche Arbeitsdossier und die neun – voneinander unabhängigen – Lektionen im Unterricht einsetzen. Abgedeckt werden u.a. die Themen Soziale Netzwerkseiten, mobile Kommunikation und Onlineportale. Inhaltlich und konzeptionell ergänzt das Lehrmittel bereits bestehende Sensibilisierungsangebote.

Die zurzeit nur auf Deutsch verfügbaren Unterlagen stehen allen Interessierten kostenlos auf unserer Webseite www.derbeauftragte.ch unter Themen – Datenschutz – Internet – Kinder und Jugendliche zur Verfügung. Die französische und italienische Fassung folgen voraussichtlich im Herbst 2012.

3.5 Lehrgang für die Studenten der Universität Neuenburg

Auf Wunsch des kantonalen Datenschutzbeauftragten von Neuenburg haben wir einen Lehrgang für Master-Studenten an der Universität Neuenburg ausgearbeitet. Dieser Kurs befasste sich mit der Arbeit des eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten und stellte in Form eines konkreten Beispiels einen von unserer Dienststelle bearbeiteten Datenschutzfall im Arbeitsbereich vor.

Im Rahmen des unter seiner Verantwortung durchgeführten Seminars an der Universität Neuenburg veranstaltete der Neuenburger Datenschutzbeauftragte, Herr Christian Flückiger, einen Kurstag in unseren Räumlichkeiten in Bern. Er hatte uns gebeten, an diesem Tag einen etwa zweistündigen Kurs zu erteilen, der den Datenschutz im Arbeitsbereich unter rechtlichen und technischen Aspekten zum Thema haben sollte.

Wir haben diesen Kurs in mehrere Teile gegliedert. Zunächst einmal stellten wir die Organisation unserer Dienststelle und die beiden Hauptachsen unserer Arbeit vor: die Beratung und die Aufsicht. Eine ausführlichere Beschreibung des Prozesses der Sachverhaltsabklärung vermittelte den Studenten ein besseres Verständnis des Aufsichtsmechanismus; ihn konnten wir durch die Darstellung eines von uns behandelten realen Falls veranschaulichen. Schliesslich gaben wir den Studenten einen kurzen Überblick über die modernen Technologien, die bei Fragen des Datenschutzes im Arbeitsbereich zur Anwendung kommen, wie beispielsweise biometrische Erkennungssysteme oder Geolokalisierungssysteme.

Wir konnten bei den Studenten ein echtes Interesse für das Thema des Datenschutzes feststellen, bei dem technische und rechtliche Aspekte eng miteinander verflochten sind.

3.6 Tag des Datenschutzes im Zentrum CEDIDAC

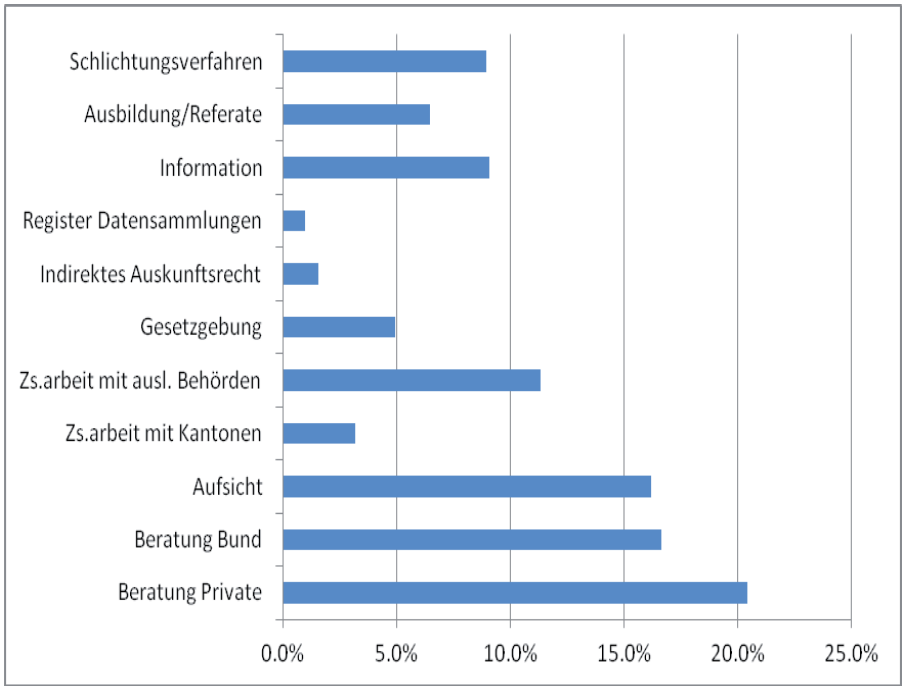
Auf Ansuchen des Zentrums für Unternehmensrecht (Centre du droit d'entreprise, CEDIDAC) der Universität Lausanne beteiligten wir uns an seinem Kolloquium vom 11. Oktober 2011 mit aktuellen Erläuterungen aus der Praxis. Diese halbtägige Lehrveranstaltung war einigen ausgewählten Aspekten des Datenschutzrechts gewidmet.

Im Rahmen der halbtägigen Veranstaltung «Datenschutz: Praktische Fragen für die Unternehmen und die Abfassung von Verträgen», die gemeinsam mit dem Master in Rechtswissenschaften, Sicherheit und Kriminalität im Zusammenhang mit neuen Technologien organisiert wurde, wurden vier wichtige Themen aus praktischer Sicht behandelt. Der erste Referent befasste sich mit den Aspekten der Bearbeitung von Personendaten des Arbeitnehmers; der zweite sprach über den Datenschutz in Bankinstituten, der dritte beschrieb den rechtlichen Rahmen für Kundendateien und Kundenkarten und der vierte stellte vorbildliche Praktiken im Bereich der Geheimhaltungspolitik vor. Über einhundert Anwälte und Unternehmensjuristen aus der Westschweiz nahmen an dieser Veranstaltung teil.

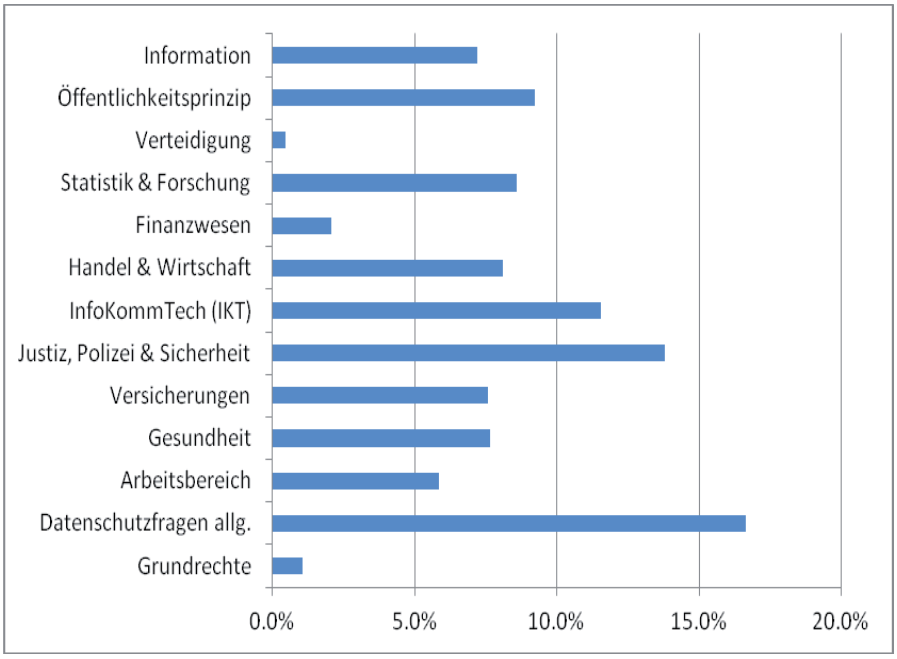
Zum Abschluss dieses Thementages hielten wir ein Referat mit dem Titel «Die heutige Praxis des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten». Wir gliederten diesen Vortrag in zwei Abschnitte. In einem ersten Teil beschrieben wir die Organisation und den Prozess der Sachverhaltsermittlung, um den Teilnehmern den im Datenschutzgesetz vorgesehenen Aufsichtsmechanismus besser verständlich zu machen. In einem zweiten Teil vermittelten wir ein anschauliches Bild unserer Arbeit anhand von konkreten Fällen, die bei uns bearbeitet werden. Diese Erläuterungen unserer Arbeitsweise und unserer Praxis stiessen auf grosses Interesse.

3.7 Statistik über die Tätigkeit des EDÖB vom 01. April 2011 bis 31. März 2012

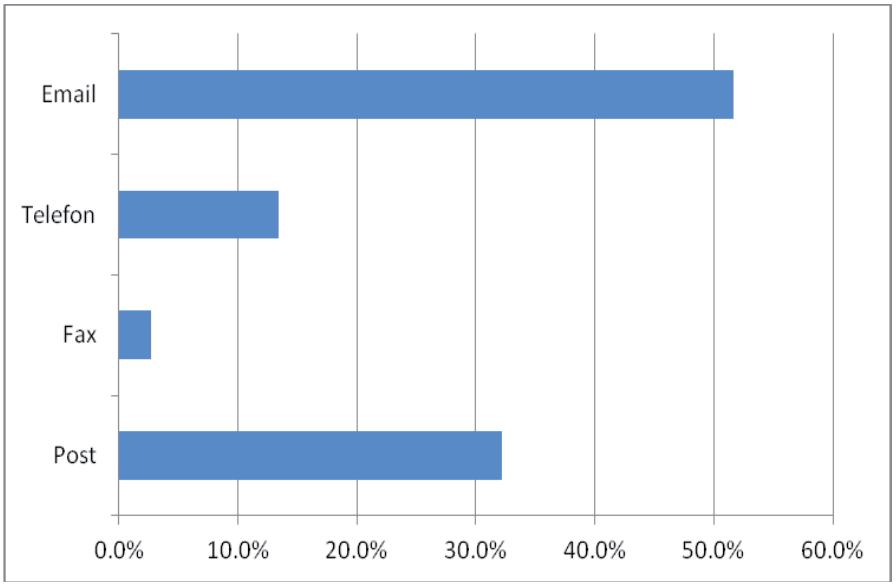
Aufwand nach Aufgabengebiet



Aufwand nach Sachgebiet



Herkunft der Anfragen



3.8 Statistik über die bei den Departementen eingereichten Zugangsgesuche nach Art. 6 des Öffentlichkeitsgesetzes (Zeitraum: 1. Januar 2011 bis 31. Dezember 2011)

Dep.	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt/auf-geschoben	hängig
BK	24	15	3	6	0
EDA	80	26	17	37	0
EDI	87	36	27	19	5
EJPD	51	25	10	16	0
VBS	27	15	3	9	0
EFD	45	16	23	6	0
EVD	42	10	18	10	4
UVEK	110	60	25	25	0
Total 2011 (in %)	466 (100 %)	203 (44 %)	126 (27 %)	128 (27 %)	9 (2 %)
Total 2010 (in %)	239 (100 %)	106 (45 %)	62 (26 %)	63 (26 %)	8 (3 %)
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 %)	-

Bundeskanzlei BK

Dep.	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt/auf-geschoben	hängig
BK	13	5	3	5	0
EDÖB	11	10	0	1	0
TOTAL	**24**	**15**	**3**	**6**	**0**

Departement: EDA

Dep.	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt/auf-geschoben	hängig
EDA	80	26	17	37	0
TOTAL	**80**	**26**	**17**	**37**	**0**

Departement EDI

Dep.	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt/auf-geschoben	hängig
GS EDI	5	2	1	2	0
EBG	0	0	0	0	0
BAK	7	5	1	0	1
BAR	4	2	2	0	0
METEO CH	1	1	0	0	0
NB	0	0	0	0	0
BAG	33	16	6	10	1
BFS	0	0	0	0	0
BSV	11	5	6	0	0
SBF	1	1	0	0	0
ETH Rat	0	0	0	0	0
SNM	0	0	0	0	0
SWISS MEDIC	19	4	7	5	3
SNF	3	0	2	1	0
SUVA	3	0	2	1	0
TOTAL	**87**	**36**	**27**	**19**	**5**

Departement EJPD

Dep.	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt/auf-geschoben	hängig
GS EJPD	5	2	1	2	0
BJ	8	1	2	5	0
FEDPOL	4	3	0	1	0
METAS	1	0	1	0	0
BFM	15	10	2	3	0
SIR	0	0	0	0	0
IGE	3	1	2	0	0
ESBK	11	7	0	4	0
ESchK	1	0	1	0	0
RAB	0	0	0	0	0
ISC	2	1	0	1	0
NKVF	1	0	1	0	0
TOTAL	**51**	**25**	**10**	**16**	**0**

Departement VBS

Dep.	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt/auf-geschoben	hängig
GS VBS	16	10	0	6	0
Verteidig./ Armee	5	1	2	2	0
NDB	1	0	1	0	0
armasuisse	2	1	0	1	0
BABS	1	1	0	0	0
BASPO	2	2	0	0	0
TOTAL	**27**	**15**	**3**	**9**	**0**

Departement EFD

Dep.	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt/auf-geschoben	hängig
GS	7	2	4	1	0
EFV	4	2	1	1	0
EPA	3	2	1	0	0
ESTV	4	2	2	0	0
EZV	2	2	0	0	0
EAV	0	0	0	0	0
BBL	4	0	3	1	0
BIT	1	0	0	1	0
EFK	19	6	11	2	0
SIF	0	0	0	0	0
PUBLICA	0	0	0	0	0
ZAS	1	0	1	0	0
TOTAL	**45**	**16**	**23**	**6**	**0**

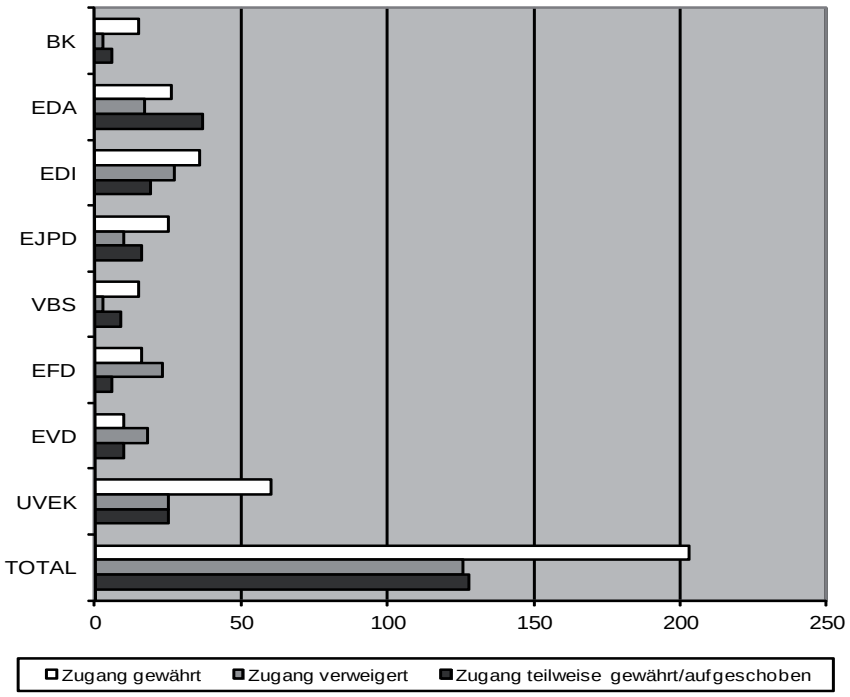
Departement EVD

Dep.	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt/auf-geschoben	hängig
GS	2	1	0	1	0
SECO	7	0	6	1	0
BBT	2	1	1	0	0
BLW	17	3	8	2	4
BVET	3	1	1	1	0
BWL	1	1	0	0	0
BWO	5	3	0	2	0
PUE	2	0	2	0	0
WEKO	3	0	0	3	0
ZIVI	0	0	0	0	0
BFK	0	0	0	0	0
TOTAL	**42**	**10**	**18**	**10**	**4**

Departement UVEK

Dep.	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt/auf-geschoben	hängig
GS	2	0	1	1	0
BAV	3	3	0	0	0
BAZL	19	10	6	3	0
BFE	18	2	7	9	0
ASTRA	5	5	0	0	0
BAKOM	6	4	0	2	0
BAFU	22	12	4	6	0
ARE	4	0	3	1	0
COMCOM	0	0	0	0	0
ENSI	22	15	4	3	0
PostReg	2	2	0	0	0
UBI	7	7	0	0	0
TOTAL	**110**	**60**	**25**	**25**	**0**

Behandlung der Zugangsgesuche



3.9 Statistik über die bei der Bundesanwaltschaft eingereichten Zugangsgesuche nach Art. 6 des Öffentlichkeitsgesetzes (Zeitraum: 1. Januar 2011 bis 31. Dezember 2011)

Bundesanwaltschaft BA

Dep.	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt/auf-geschoben	hängig
BA	3	2	1	0	0
TOTAL	**3**	**2**	**1**	**0**	**0**

3.10 Statistik über die bei den Parlamentsdiensten eingereichten Zugangsgesuche nach Art. 6 des Öffentlichkeitsgesetzes (Zeitraum: 1. Januar 2011 bis 31. Dezember 2011)

Parlamentsdienste PD

Dep.	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt/auf-geschoben	hängig
PD	1	1	0	0	0
TOTAL	**1**	**1**	**0**	**0**	**0**

3.11 Anzahl Schlichtungsgesuche nach Kategorien der Antragsteller (Zeitraum: 1. Januar 2011 bis 31. Dezember 2011)

Kategorie Antragsteller	2011
Medien	24
Privatpersonen (bzw. keine genaue Zuordnung möglich)	10
Interessenvertreter (Verbände, Organisationen, Vereine usw.)	9
Unternehmen	16
Rechtsanwälte	6
Total	**65**

3.12 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:	10 Personen
Einheit 2:	12 Personen
Einheit 3:	2 Personen
Kanzlei:	4 Personen