20. Tätigkeitsbericht 2012/2013

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Tätigkeitsbericht 2012/2013
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 2012 und 31. März 2013 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. 410.020.d/f

Inhaltsverzeichnis

Vorwort – Bilanz und Ausblick

Durchbruch beim Personenidentifikator und im Gesundheitsdossier – Big Data und Augmented Reality, die neuen Herausforderungen

Vor 10 Jahren befassten wir uns intensiv mit dem geplanten Personenidentifikator. Entwickelt wurde er im Zusammenhang mit der Registerharmonisierung und der Absicht, künftig die Volkszählung über die Einwohnerregister zu ermöglichen. Wir kritisierten, dass der Verwendungszweck dieses eineindeutigen Identifikators nicht klar genug definiert werde und die Nummer namentlich auch nicht näher bezeichneten administrativen Zwecken dienen soll. Unser Vorschlag, bereichsspezifische Nummern zu schaffen, wurde leider nicht weiter verfolgt. In der Zwischenzeit wurde die neue AHV-Nummer kreiert, deren Verwendungszweck im Gesetz sehr weit gefasst worden ist (Art. 50e AHVG). Seither hat sie sich weiter verbreitet: Ganze kantonale Verwaltungen verwenden sie, und laufend werden neue Bedürfnisse angemeldet. So war es zunächst selbstverständlich, dass die AHV-Nummer auch für das E-Patientendossier verwendet werden sollte. Der damalige Departementsvorsteher Pascal Couchepin hatte bereits einen entsprechenden Grundsatzentscheid gefällt, obwohl wir deutlich Bedenken angemeldet hatten: Angesichts ihrer grossen Verbreitung (Arbeitsplatz, Bildungswesen, Steuern usw.) und der in Aussicht stehenden noch breiteren Verwendung konnte und kann kaum mehr von einer anonymen Nummer, wie sie ursprünglich beabsichtigt gewesen war, gesprochen werden. Im Gefolge des Wechsels an der Departementsspitze konnten wir trotz des erwähnten Grundsatzentscheids die Problematik dieser Nummer nochmals thematisieren und einen Durchbruch erzielen: Der Bundesrat ist nun damit einverstanden, dass die Zentrale Ausgleichsstelle (ZAS) nach dem Zufallsprinzip eine E-Patientennummer kreiert und sie mit der AHV-Nummer bei sich ablegt. Wir sind der Auffassung, dass die ZAS nach diesem Modell in Zukunft auch für andere heikle Bereiche – zum Beispiel das E-Voting – bereichsspezifische Nummern produzieren könnte.

Hervorstreichen möchte ich eine wichtige Verbesserung im Gesundheitswesen. Jahrelang haben wir moniert, dass zwischen den Leistungserbringern und den Versicherern auch viele Patientendaten fliessen, die nicht unbedingt benötigt werden. Deshalb haben wir von den Krankenversicherungen wiederholt verlangt, uns im Detail zu erläutern, wie die Rechnungskontrolle konkret abgewickelt werde. Statt detaillierter Informationen kam dann jeweils der stereotype Dreiklang: Für die Beurteilung der Wirksamkeit, der Zweckmässigkeit und der Wirtschaftlichkeit einer Massnahme brauchten die Kassen alle verfügbaren Patientendaten. Dabei war uns

bekannt, dass der überwiegende Teil der Rechnungen in einem automatisierten Verfahren kontrolliert und dann ohne weitere Überprüfung bezahlt wird. Mit Blick auf die Einführung der Fallkostenpauschalen (SwissDRG) war der Gefahr zu begegnen, dass sich in den Versicherungen riesige Berge mit digitalisierten medizinischen Daten auftürmen. Der von uns seit Jahren postulierte Vorschlag, zwischen dem Leistungserbringer und dem Versicherer eine unabhängige und zertifizierte Datennannahmestelle einzurichten, die mittels automatisierter Triage bestimmt, welche Rechnung näher begutachtet werden soll, stand dank der Unterstützung von Bundesrat Alain Berset plötzlich im Zentrum der Diskussion und wurde schliesslich in der bundesrätlichen Verordnung verankert. Auch wenn das neue System noch nicht flächendeckend implementiert ist und nach wie vor diverse Punkte einer Klärung bedürfen, sind wir überzeugt, dass mit diesem Systemwechsel der Persönlichkeitsschutz im Gesundheitswesen deutlich verbessert werden konnte.

Froh sind wir, dass im Verlaufe des 2012 – sechs Jahre nach Inkraftsetzung des Öffentlichkeitsgesetzes (BGÖ) – das in der Botschaft in Aussicht gestellte Personal endlich zugeteilt worden ist. Natürlich kann damit der entstandene Pendenzenberg nicht auf einen Schlag eliminiert werden – wir hoffen aber, dass die rund 75 Fälle, die bis Ende 2012 nicht innert der gesetzlichen Frist behandelt werden konnten, im Verlaufe dieses Jahres massgeblich abgebaut werden. Im Bereich des BGÖ fand letztes Jahr eine wichtige Klärung statt: Immer wieder versuchen einzelne Bundesstellen, sich aus dem Geltungsbereich des Gesetzes herauszunehmen, mit der Begründung, sie könnten sonst ihre Aufgabe nicht ausreichend wahrnehmen. Auch die Finanzkontrolle (FK) verlangte dies, weil sie befürchtete, nicht mehr an wichtige Informationen zu kommen, wenn die Informanten Transparenz erwarten mussten. Wir haben uns dagegen gewehrt mit dem Argument, es könne nicht sein, dass eine Aufsichtsbehörde, die Transparenz über allfällige Fehlleistungen der Verwaltung herzustellen habe, ihr Handeln selber nicht transparent machen müsse. Der Bundesrat hat sich inzwischen dieser Auffassung angeschlossen und den Revisionsantrag der FK abgelehnt. Weitere vergleichbare Anstrengungen stehen im Raum, gegen die wir uns aussprechen werden mit der Begründung, dass gerade auch der Nachrichtendienst oder die Wettbewerbskommission gegenüber der Bevölkerung zu Transparenz verpflichtet sind.

Im Berichtsjahr führten wir zahlreiche Sachverhaltsabklärungen zu zentralen Fragen durch (so etwa über Videoüberwachung in Garderoben oder Kreditauskunfteien) und nahmen im Rahmen von Ämterkonsultationen zu wichtigen Gesetzen Stellung (wie BÜPF, BWIS, das Handelsregister im Internet und die Postverordnung). Unsere Hinweise und Kritiken wurden bei der Regelung des Staatstrojaners und bei der Frage, wie die Eingriffe des Nachrichtendienstes in die Privatsphäre gesetzlich

geregelt und begrenzt werden können, weitgehend berücksichtigt. Nach wie vor hoffen wir, dass einige offene Punkte im Rahmen der Gesetzesberatung im Parlament verbessert werden. Die Änderung der Postverordnung gab uns die Gelegenheit, ein uraltes Anliegen einzubringen: Die Post darf seit Ende letzten Jahres den Kundinnen und Kunden, die nicht damit einverstanden sind, dass ihr Nachsendeauftrag auch Dritten weiter gegeben wird, keine Gebühr von 30 Franken mehr verrechnen. Transparenter ist nun auch die Kommunikation rund um den Nachsendeauftrag: Künftig listet die Post detailliert auf, wem sie im Einzelnen die Adresse weiter gibt, also Adresshändlern, Wirtschaftsauskunfteien, Versicherungen, Banken usw. Es genügt nicht, die Weitergabe an Dritte ganz generell zu erlauben.

Schliesslich haben wir auch wieder Erläuterungen und Informationen zu verschiedenen Themen auf unserer Webseite veröffentlicht, so zum Phänomen der Internetpranger, zu Datenschutz bei Breitensportanlässen oder zum Einsatz von Webanalysetools in der Bundesverwaltung. Anlässlich des Datenschutztages haben wir eine Broschüre zum Datenschutz am Arbeitsplatz produziert.

Wirtschaftsauskunfteien und Adresshandel haben den EDÖB im vergangenen Jahr besonders herausgefordert und sich als Grossbaustelle entpuppt. Ausgangspunkt war die Tatsache, dass Bürgerinnen und Bürger über die Google-Suche erfuhren, dass sie mit zahlreichen Informationen bis hin zur Nennung ihrer Wohnungspartner und Angabe ihrer Bonität verzeichnet waren. Der Schock war vor allem für jene Ratsuchenden gross, die sich trotz Sperrung ihrer Adresse beim Telefonanbieter oder bei der Post mit ihrer vollständigen Anschrift im Netz wiederfanden. Wir reagierten sofort und setzten als vorsorgliche Massnahme durch, dass der Schutz derjenigen Betroffenen, die ihre Adresse aus Sicherheitsgründen gesperrt hatten, unverzüglich verbessert wurde. In einer umfangreichen Sachverhaltsabklärung konnten wir die Datenflüsse der Wirtschaftsauskunftei im Adresshandel erhellen und haben der betroffenen Firma mit einer Reihe von Empfehlungen ein Verfahren abverlangt, das die Respektierung der Persönlichkeitsrechte von Betroffenen garantiert. Die Empfehlungen gelten natürlich für alle Akteure, die in diesem Bereich tätig sind. Wir werden sehr genau beobachten, wie die Empfehlungen im Einzelnen umgesetzt werden, und nötigenfalls mit ergänzenden Massnahmen eingreifen. Diese erste Abklärung fokussierte lediglich auf den Umgang mit gesperrten Adressen und spülte eine Menge von Problemen und Fragen an die Oberfläche, die nach einer weitergehenden Untersuchung rufen. Im Zentrum steht die Frage, inwieweit aus verschiedenen Quellen zu unterschiedlichen Zwecken zur Verfügung gestellte Daten zusammengefügt, neu kombiniert und analysiert werden und deren Ergebnis ohne Einwilligung der Betroffenen im Netz publiziert werden dürfen. Auf jeden Fall herrscht spürbares Unverständnis unter jenen, die bei uns Rat

suchen, wenn sie eine derart detaillierte Online-Publikation ohne Weiteres akzeptieren sollen. Ohne dem Ergebnis unserer weiteren Abklärungen vorgreifen zu wollen, kann ich eine wichtige Erkenntnis bereits vorwegnehmen: Die Rechtslage ist im Bereich der Wirtschaftsauskunfteien, des Adresshandels und namentlich der Veröffentlichung von Personendaten im Internet heute derart bruchstückhaft, dass sich nur schon in diesem Punkt eine gründliche Überarbeitung des Datenschutzgesetzes aufdrängt.

Nicht nur mit dem Internet wird der Datenschutz auf eine harte Probe gestellt. In Zukunft werden wir uns mit technischen Entwicklungen und Produkten auseinandersetzen müssen, die auf eine vollständige Kontrolle und Überwachung unseres sozialen Lebens hinauslaufen, und zwar von staatlicher wie von privater Seite. Der New Yorker Bürgermeister redet dem Einsatz von militärischen Drohnen das Wort, die aus grosser Höhe in der Lage sind, zur Überwachung der Metropole jedes Detail wahrzunehmen. So wird, wer künftig auf einer Parkbank ein Buch liest, damit rechnen müssen, dass die Drohne (bzw. die Person dahinter) mitliest. Der Einsatz kleinster Fluggeräte mit smarter Technologie für wenig Geld wird es auch jedem Neugierigen ermöglichen, in der näheren und weiteren Umgebung Erkundungsflüge durchzuführen, in Räume zu schauen und vielleicht auch mal durch ein offenes Fenster zu schlüpfen. Die durch verschiedene computergestützte Technologien ermöglichte «augmented reality» wird uns nicht nur in die Lage versetzen, die Realität durch unsere Brille zu beobachten und zu hinterfragen, sondern sie auch mit allen auf dem Netz verfügbaren Informationen anzureichern und zu interpretieren. Vielleicht werden Sie demnächst von einem mit «Google Glass» bebrillten Passanten mit Ihrem Namen begrüsst, wenn Sie sich mit Ihrer Freundin auf einem Wochenendbummel in Londons Strassen befinden: Seine Brille hat nämlich ein Foto von Ihnen geschossen, mit dem vorhanden Bildmaterial auf dem Netz abgeglichen und Sie, Gesichtserkennung sei Dank, identifiziert. Diese persönliche Ansprache ist doch sympathisch, oder?

Zunehmend rückt auch das Thema «Big Data» ins Zentrum unserer Aufmerksamkeit. Grosse Mengen von Daten fallen an

- durch maschinelle Erzeugung (Telekommunikationsverbindungen, Webzugriffe, Logdateien),
- durch automatische Erfassung von RFID-Lesern, Kameras, Mikrofonen und sonstigen Geräten,
- durch Finanztransaktionen und
- im Gesundheitswesen, im Energiesektor usw.

Angesichts der technischen Entwicklung, der riesigen Speicherkapazitäten, der Möglichkeit der raschen Übermittlung grosser Datenbestände über grosse Distanzen und der Möglichkeit der präzisen Analyse solcher Bestände werden die Daten zum Rohstoff (zum «neuen Kapital») einer künftigen «data-driven-society» (Alex Pentane, Informatikprofessor am Massachusetts Institute of Technology). Diesen Datenmengen werden mit Hilfe von Algorithmen bahnbrechende Erkenntnisse abgerungen, die eine massive Gefährdung der Privatsphäre zur Folge haben können. Beispiele gefällig? Wenn die Analyse vorhandener Big Data die Erkenntnis zulässt, dass eine verheiratete Frau, die plötzlich teuren Schmuck kauft, in der Regel vor einer Trennung steht, oder die Analyse der Transaktionsdaten eines Bankkunden zur Erkenntnis führt, dass der Betreffende demnächst sterben könnte, ist das Missbrauchspotential evident. Vor diesem Hintergrund stellt sich mit Blick auf die zur Diskussion stehende Gesetzesrevision die Frage, ob Big Data bzw. deren mögliche Nutzung mit Gesetzen umfassend gebändigt werden kann.

Ganz generell stellt sich die Frage, wie diese Entwicklung, die dank der zur Verfügung stehenden grossen Datenmengen auch zu immer mehr internetbasierten Dienstleistungsangeboten führt, auf dem Boden einer nationalen Gesetzgebung in den Griff zu kriegen ist.

Abkürzungsverzeichnis

AFAPDP	Association francophone des autorités de protection des données personnelles (Französischsprachige Vereinigung der Datenschutzbehörden)
AFV	Automatische Fahrzeugfahndung und Verkehrskontrolle
AHVG	Bundesgesetz über die Alters- und Hinterlassenenversicherung
AHVN13	13-stellige AHV-Nummer
A-IS	Ausschuss Informatiksicherheit
AllgGebV	Allgemeine Gebührenverordnung
AVE	Allgemeinverbindlicherklärung
BA	Bundesanwaltschaft
BAFU	Bundesamt für Umwelt
BAG	Bundesamt für Gesundheit
BAV	Bundesamt für Verkehr
BAZL	Bundesamt für Zivilluftfahrt
BFE	Bundesamt für Energie
BFM	Bundesamt für Migration
BFS	Bundesamt für Statistik
BGE	Bundesgerichtsentscheid
BGer	Bundesgericht
BGÖ	Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung
BInfV	Bundesinformatikverordnung
BJ	Bundesamt für Justiz
BK	Bundeskanzlei
BPG	Bundespersonalgesetz
BPV	Bundespersonalverordnung
BStatG	Bundesstatistikgesetz
BSV	Bundesamt für Sozialversicherungen
BÜPF	Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs

BVGer	Bundesverwaltungsgericht
BWIS	Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit
BWO	Bundesamt für Wohnungswesen
DRG	Diagnoses Related Groups
DSG	Bundesgesetz über den Datenschutz
EDA	Eidgenössisches Departement für auswärtige Angelegenheiten
EDI	Eidgenössisches Departement des Innern
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDSB	Europäischer Datenschutzbeauftragter
EFD	Eidgenössisches Finanzdepartement
EFK	Eidgenössische Finanzkontrolle
EJPD	Eidgenössisches Justiz- und Polizeidepartement
ENSI	Eidgenössisches Nuklearsicherheitsinspektorat
EPA	Eidgenössisches Personalamt
EPDG	Bundesgesetz über das elektronische Patientendossier
ESTI	Eidgenössisches Starkstrominspektorat
ESTV	Eidgenössische Steuerverwaltung
ETHZ	Eidgenössischen Technischen Hochschule Zürich
Eurodac	Informationssystem zum Vergleich von Fingerabdrücken zum Zwecke der effektiven Anwendung des Dubliner Übereinkommens
EVD	Eidgenössisches Volkswirtschaftsdepartement
EZV	Eidgenössische Zollverwaltung
fedpol	Bundesamt für Polizei
FinDel	Finanzdelegation
FINMA	Eidgenössische Finanzmarktaufsicht
FOGIS	Formell-gesetzliche Grundlage für den Informationsschutz
GAV	Gesamtarbeitsvertrag
GEVER	Elektronische Geschäftsverwaltung
GEWA	Datenverarbeitungssystem zur Bekämpfung der Geldwäscherei, des organisierten Verbrechens und der Terrorismusfinanzierung

GKI	Gemeinsame Kontrollinstanz von Schengen
GPK-N	Geschäftsprüfungskommission des Nationalrates
HSPD-6	Homeland Security Presidential Directive 6
IKT	Informatik- und Kommunikationstechnologien
IRB	Informatikrat des Bundes
ISAS	Informationssystem Äussere Sicherheit
ISB	Informatiksteuerungsorgan des Bundes
ISIS	Staatsschutz-Informationssystem
JANUS	Informationssystem der Bundeskriminalpolizei
KVG	Bundesgesetz über die Krankenversicherung
KVV	Verordnung über die Krankenversicherung
MWSTG	Mehrwertsteuergesetz
NDB	Nachrichtendienst des Bundes
NDG	Nachrichtendienstgesetz
N-SIS	Nationaler Teil des Schengener Informationssystems
PBG	Personenbeförderungsgesetz
PCSC	Cooperation in Preventing and Combating Serious Crime
RAB	Revisionsaufsichtsbehörde
RAV	Revisionsaufsichtsverordnung
RIPOL	Automatisiertes Polizeifahndungssystem
RogF	Informationssystem Reisende ohne gültigen Fahrausweis
SDÜ	Schengener Durchführungsübereinkommen
SECO	Staatssekretariat für Wirtschaft
SIS	Schengener Information System
SNF	Schweizerischer Nationalfonds
SpoFöG	Bundesgesetz über die Förderung von Sport und Bewegung
Swissmedic	Schweizerisches Heilmittelinstitut
UVEK	Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation

VASR	Verordnung über die anerkannten Standards zur Rechnungslegung
VBGÖ	Verordnung über das Öffentlichkeitsprinzip der Verwaltung
VBS	Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport
VDSG	Verordnung zum Bundesgesetz über den Datenschutz
VDSZ	Verordnung über die Datenschutzzertifizierungen
VIS	Visa-Informationssystem
WADA	World Anti-Doping Agency
WBF	Eidgenössisches Departement für Wirtschaft, Bildung und Forschung
WEKO	Wettbewerbskommission
ZAS	Zentrale Ausgleichsstelle
Zefix	Zentraler Firmenindex
ZEMIS	Zentrales Migrationsinformationssystem
ZNDG	Bundesgesetz über die Zuständigkeiten im Bereich des zivilen Nachrichtendienstes
ZPG	Zugpersonalgerät

1. Datenschutz

1.1 Grundrechte

1.1.1 Aspekte der Datenbearbeitung im Rahmen von statistischen Erhebungen

Anfang 2012 gaben wir im Rahmen eines Entwurfs zur Änderung der Verordnung über die Durchführung eidgenössischer statistischer Erhebungen und der Ausarbeitung eines Reglements über die Datenverknüpfungen im Bundesamt für Statistik unsere Meinung ab und nahmen an mehreren Sitzungen teil. Insgesamt wurden unsere Bemerkungen positiv aufgenommen. Die laufenden Gesetzesarbeiten dürften für grössere Transparenz und die Einbeziehung der Datenschutzaspekte sorgen, doch sollten gewisse Themen noch genauer präzisiert werden.

Im Jahr 2012 hat das Bundesamt für Statistik (BFS) einen Revisionsentwurf zur Verordnung über die Durchführung eidgenössischer statistischer Erhebungen sowie einen Entwurf für ein Bearbeitungsreglement für die Datenverknüpfungen ausgearbeitet. Die Verordnung enthält namentlich ein neues Kapitel über die Verknüpfung der Daten sowie genauere Angaben zu ihrer Bearbeitung. Um sich zu vergewissern, dass der Schutz der Personendaten in diesem Entwurf gewährleistet ist, lud uns das BFS zu mehreren Sitzungen ein.

Wir haben dem BFS unseren Standpunkt dargelegt und dabei generell die von ihm geleistete juristische Arbeit sowie die Bemühungen um eine Einbeziehung der Datenschutzaspekte begrüsst. Wir stellten auch die bei der Datenverarbeitung vorgesehene Transparenz sowie den Verweis auf Pseudonymisierungs- und Anonymisierungsmassnahmen fest. Unseres Erachtens wäre es insbesondere ratsam, im Verordnungstext auszuführen, welches Material tatsächlich vernichtet wird (grundsätzlich das Material, das der Datenbeschaffung zugrunde liegt, wie etwa Fragebögen und andere Umfragedokumente), und innerhalb welchen Zeitraums dies zu geschehen hat. Ebenso müssen genauere Angaben zu dem Zeitpunkt gemacht werden, zu dem die Anonymisierung der statistischen Daten erfolgt (gegebenenfalls mit einer Unterscheidung nach Kategorien).

Wir begrüssen auch die Ausarbeitung eines Bearbeitungsreglements zur Datenverknüpfung, in dem namentlich wichtige Datenschutzaspekte behandelt werden, etwa der Zweck dieser Bearbeitung, die Pseudonymisierung der Daten, die Angaben zum Verknüpfungsverfahren oder der Zugriff auf die Daten. In der vorliegenden

Fassung enthält das Reglement hingegen nur wenig detaillierte Informationen über die anzuwendenden Mechanismen. Das BFS beabsichtigt, die verschiedenen darin behandelten Punkte weiter auszuarbeiten. Es wird uns unserem Wunsch entsprechend in erster Linie das Kapitel über das «Key Management» (Schlüsselverwaltung) vorlegen, das unseres Erachtens einer unabhängigen Instanz übertragen werden müsste, die über die notwendigen Ressourcen und Kompetenzen verfügt und dessen Betrieb unter dem Gesichtspunkt des Datenschutzes ein zentrales Anliegen darstellt, ebenso wie die Anonymisierung und die Löschung der verknüpften Daten.

Wir unterstützen das BFS bei der Bereitstellung zusätzlicher Mittel für interne Kontrollen der Datenbearbeitung im Rahmen der Umsetzung der Bestimmungen des Bundesstatistikgesetzes und der eidgenössischen Datenschutzgesetzgebung.

Wir nahmen auch das Interesse des BFS an einer Zertifizierung des Key Management zur Kenntnis. Allerdings wiesen wir darauf hin, dass ein solcher Prozess bedeutende Investitionen erfordert. Darüber hinaus handle es sich im vorliegenden Fall nur um eine Zertifizierung bezüglich Organisation und Verfahren im Zusammenhang mit dem Key Management im Sinne von Artikel 4 der Verordnung über die Datenschutzzertifizierungen (VDSZ) und nicht um die Zertifizierung des Produkts selbst.

1.1.2 Einführung der AHV-Nummer ins Grundbuch

Die AHV-Versichertennummer wird ins Grundbuch eingeführt. Sie ist allerdings nur intern sichtbar.

Die AHV-Nummer soll als zusätzlicher Personenidentifikator in das Grundbuch eingeführt werden. Wir haben im Rahmen einer Ämterkonsultation dazu Stellung genommen. Dabei haben wir begrüsst, dass die AHV-Nummer nur verwaltungsintern ersichtlich ist, um die Möglichkeit einer unerwünschten Erstellung von Vermögensprofilen durch Private zu verhindern. Wir haben allerdings auch darauf hingewiesen, dass der Kreis der Nutzungsberechtigten in der uns vorgelegten Fassung des Gesetzesentwurfs zu unbestimmt formuliert worden ist.

Generell kann gesagt werden, dass die AHV-Nummer durch die Schaffung entsprechender gesetzlicher Grundlagen auch in diesem Berichtsjahr in diversen Bereichen eingeführt werden soll, unter anderem ins Handelsregister, in Infostar und in den Mehrwertsteuerbereich (vgl. Ziff. 1.1.3 des vorliegenden Tätigkeitsberichts). Im Bereich E-Patientendossier wurde diesbezüglich ein anderer Weg eingeschlagen (vgl. Ziff. 1.5.2 des vorliegenden Tätigkeitsberichts).

1.1.3 Verwendung der AHV-Nummer im Mehrwertsteuergesetz

Die eidgenössische Steuerverwaltung hat von sich aus die Gelegenheit ergriffen, uns eine datenschutzrechtlich verbesserte Gesetzesgrundlage für die Bearbeitung der AHV-Versichertennummer und für ein Abrufverfahren zur Stellungnahme vorzulegen.

Wir haben uns in der Vergangenheit bereits mehrfach in Ämterkonsultationen dahingehend geäussert, dass die Gesetzesgrundlagen im Bereich der Mehrwertsteuer dringend verbessert werden müssen. Einerseits wurde die Verwendung der AHV-Nummer nur auf Verordnungsstufe geregelt, was wir in unserem letzten Tätigkeitsbericht (vgl. unseren 19. Tätigkeitsbericht 2011/2012, Ziff. 1.9.3) ausführlich dargelegt haben. Andererseits hatten wir die ungenügende Bestimmtheit von Artikel 76 des Mehrwertsteuergesetzes (MWSTG) bemängelt, in dem das Abrufverfahren geregelt wird. Die eidgenössische Steuerverwaltung ist im Berichtsjahr aktiv auf uns zugekommen und hat uns einen Entwurf für einen überarbeiteten Artikel 76 MWSTG vorgelegt. Dabei wurden unsere früher gemachten Vorbehalte korrigiert: So wurde das Abrufverfahren bestimmter geregelt und eine Grundlage auf Stufe Gesetz für die Verwendung der AHV-Nummer erstellt.

1.1.4 Thinkdata.ch: Aktualisierung und Entwicklung

Nach der Einführung des Dienstes Thinkdata.ch – eines Instruments für Organisationen zur Sensibilisierung für den Datenschutz und das Öffentlichkeitsprinzip – im Januar 2012 wurden die Tätigkeiten der Arbeitsgruppe im vergangenen Jahr fortgeführt. Die zweite Version der Webseite, die nunmehr in vier Sprachen verfügbar ist, konnte in Produktion gehen.

Wir unterstützen Thinkdata.ch weiterhin durch eine aktive Mitwirkung an der Arbeitsgruppe, die diesen Dienst entwickelt. Schon gleich nach der Inbetriebnahme der Webseite im Januar 2012 hatte sie grossen Erfolg. Im Mai 2012 wurde in Genf eine Tagung zur Webseite und ihrer Zukunft organisiert. Rund dreissig Personen aus verschiedenen Bereichen nahmen daran teil. Diese Veranstaltung gab nicht nur den Anstoss zu einem Gedankenaustausch über die künftigen Versionen, sondern brachte der Arbeitsgruppe auch Verstärkung durch den Einbezug neuer Mitglieder.

Der Dienst wurde um mehrere neue Szenarien erweitert, was der Mitwirkung der Webseiten-Nutzer zu verdanken ist. Sie haben die Möglichkeit, ihre eigenen Beispiele für Problemstellungen im Zusammenhang mit dem Datenschutz und dem Öffentlichkeitsprinzip beizusteuern. Seit Juli 2012 ist eine deutsche Version der Webseite verfügbar, und seit Januar 2013 sind auch die italienische und die englische Version online geschaltet. Kurz vor dieser letzten Erweiterung wurde die Schwelle von 10 000 Zugriffen überschritten. Im Durchschnitt dauert jeder Zugriff über drei Minuten.

Derzeit befasst sich die Arbeitsgruppe mit der künftigen Entwicklung des Dienstes, wobei sie sich im Wesentlichen darauf konzentriert, ihn für verschiedene internationale Rechtssysteme auszugestalten. Parallel dazu legen wir die Richtlinien für den künftigen Betrieb fest.

1.2 Datenschutzfragen allgemein

1.2.1 Videoüberwachung in Garderoben von Freizeitanlagen

Wie wir aufgrund von Bürgeranfragen feststellen mussten, überwachen immer mehr Betreiber von Freizeitanlagen sensible Bereiche wie Umkleidekabinen oder Toiletten mit Videokameras. Dieser Trend ist aus Sicht des Datenschutzes höchst bedenklich, wird so doch in die Intimsphäre der betroffenen Personen eingegriffen.

Das Filmen in Toiletten- oder Umkleidekabinen greift in die Intimsphäre der betroffenen Personen ein und verletzt damit ihre Persönlichkeit schwer. Wenngleich hinter solchen Überwachungsmassnahmen zumeist nachvollziehbare Motive stehen, in der Regel die Verhinderung bzw. Ahndung von Diebstählen, lassen sich derart schwere Persönlichkeitsverletzungen kaum rechtfertigen. Der datenschutzkonforme Betrieb von Überwachungskameras in Toiletten- und Umkleidekabinen von Freizeitanlagen ist folglich nicht möglich.

Dennoch wurden wir vermehrt mit Anfragen und Presseberichten konfrontiert, die sich auf Videoüberwachung in Toiletten oder Umkleidebereichen etwa von Schwimmbädern, Fitnessstudios oder Restaurants beziehen. Das Thema war denn auch im Herbst prominent in den Medien vertreten: In diversen Schwimmbädern wurde der Garderobenbereich zur Verhinderung von Diebstählen mit Videokameras überwacht. Aufgrund von Bürgeranfragen haben wir im Falle eines Schwimmbades eine Sachverhaltsabklärung durchgeführt und dessen Videoüberwachungsanlage im Garderobenbereich einer vertieften Überprüfung unterzogen.

Wie wir feststellen konnten, wurde im überprüften Bad nicht in den Umkleidekabinen selbst gefilmt. Vielmehr befanden sich die Kameras im allgemeinen Umkleidebereich bei den Schliessfächern, da es dort oft zu Einbrüchen und Diebstählen gekommen ist. Diese Vorfälle wurden durch die schlechte Übersichtlichkeit der Anlage noch verschärft. Aufgrund der baulichen Gestaltung des Umkleidebereichs (insbesondere die nach Geschlechtern getrennten Räume und die Bänke vor den Schliessfächern) suchen aber viele Badegäste nicht die weiter entfernten Einzelumkleidekabinen auf, sondern kleiden sich direkt vor den videoüberwachten Schliessfächern um. So erfassten die Kameras einen Grossteil der sich umkleidenden Gäste. Dieser Umstand war den wenigsten Betroffenen bewusst, da die Überwachung in diesem Bereich nicht speziell gekennzeichnet war. Damit hatte die Videoüberwachung denselben Effekt, wie wenn direkt in den Einzelkabinen gefilmt würde: Sie griff in die Intimsphäre der betroffenen Personen ein.

Um solche Situationen zu verhindern, müssen Videoüberwachungen in Garderoben und Toilettenanlagen nebst den allgemeinen Anforderungen (vgl. Merkblatt «Videoüberwachung durch private Personen», zu finden auf unserer Webseite www.derbeauftragte.ch unter Datenschutz – Videoüberwachung) folgende Voraussetzungen erfüllen, um datenschutzkonform betrieben werden zu können: Kameras dürfen nicht in den einzelnen Toiletten- oder Umkleidekabinen installiert werden.

Im Umkleidebereich oder im Vorraum einer Toilettenanlage können Kameras montiert werden, wenn sie nicht den gesamten Bereich erfassen, so dass die betroffenen Personen die Möglichkeit haben, sich umzukleiden, ohne dabei gefilmt zu werden (z.B. in separaten Einzelkabinen oder von den Kameras nicht erfassten Nischen). Die Einzelkabinen dürfen nicht mit erfasst werden. Diese alternativen Umkleidemöglichkeiten müssen in genügender Anzahl oder Grösse zur Verfügung stehen, so dass deren Benützung für die Betroffenen zumutbar ist. Gut sichtbare Hinweisschilder müssen die betroffenen Personen zudem darüber informieren, in welchen Bereichen gefilmt wird und in welchen nicht.

Genaueres hierzu kann auf unserer Webseite www.derbeauftrage.ch unter Datenschutz – Videoüberwachung in unseren Erläuterungen zur Videoüberwachung in Garderoben und Toilettenanlagen nachgelesen werden.

Die Betreiber des überprüften Bades haben die Bedenken der Badegäste und unsere Einwände gegen die Videoüberwachung im Garderobenbereich ernst genommen. Sie werden ein neues Konzept erarbeiten und verzichten zurzeit auf die Überwachung im Umkleidebereich. Wir konnten uns bei einem Besuch vor Ort davon überzeugen, dass die fraglichen Kameras umgehend entfernt worden sind und die Überwachungsanlage des Bades nun den datenschutzrechtlichen Anforderungen entspricht.

1.2.2 Zentrale Speicherung von Kundenfotos bei Skistationen

Das in der Schweiz von vielen Skistationen verwendete Zutrittskontrollsystem muss im Bereich der Datensicherheit verbessert werden. Der Systemhersteller hat sich bereit erklärt, die von uns verlangten Verbesserungen schnellstmöglich technisch umzusetzen.

Wie eine unserer Kontrollen in den Vorjahren ergab (vgl. unseren 18. Tätigkeitsbericht 2010/2011, Ziff. 1.2.5, sowie unseren 19. Tätigkeitsbericht 2011/2012, Ziff. 1.2.9), muss das von vielen Skistationen in der Schweiz verwendete Zutrittskontrollsystem

im Bereich der Datensicherheit verbessert werden. So werden die zentral gespeicherten Fotos der Kundinnen und Kunden zwar in einem grundsätzlich nur mit der systemeigenen Software lesbaren Format gespeichert, eine Massnahme, welche eine missbräuchliche Verwendung der Fotos erschwert. Da in der Fotodatenbank aber auch besonders schützenswerte Personendaten gespeichert sein können, reicht dieser Schutz nicht aus.

Wir haben mit dem Systemhersteller geprüft, welche Verbesserungsmöglichkeiten im Bereich der Datensicherheit bestehen. Es hat sich hierbei gezeigt, dass eine sofortige Anpassung der bestehenden Systeme technisch nicht ohne Weiteres umsetzbar ist. Der Systemhersteller hat sich jedoch dazu verpflichtet, schnellstmöglich entsprechende Massnahmen zu entwickeln und in seine Produkte einzubauen. Wir werden die Entwicklung beobachten und zu gegebenem Zeitpunkt darüber informieren.

1.2.3 Reisende ohne gültigen Fahrausweis – Kontrolle der SBB-Datenbank

Wir führten bei der SBB eine Kontrolle der Datenbearbeitungen der Reisenden ohne gültigen Fahrausweis durch. Dabei stellten wir fest, dass für das Informationssystem selbst noch eine formellgesetzliche Grundlage geschaffen werden muss. Das Bundesamt für Verkehr hat sich bereit erklärt, die entsprechenden gesetzgeberischen Schritte in die Wege zu leiten. Zum Zeitpunkt unserer Kontrolle vor Ort hatte die SBB die geplante Löschung der Daten in ihrem Informationssystem noch nicht umgesetzt. Wir sind daran, das inzwischen erstellte Konzept für die Löschung samt Umsetzung zu prüfen.

Wir erhielten verschiedene Anfragen in Zusammenhang mit der Datenbearbeitung, welche die SBB zu Reisenden ohne gültigen Fahrausweis vornimmt. Die Presse berichtete verschiedentlich darüber. Da auch die Passagiere erfasst werden, die ihr Abonnement vergessen haben, sind von dieser Datenbearbeitung viele Personen betroffen. Deshalb führten wir bei der SBB eine entsprechende Kontrolle durch.

Die Daten der Reisenden ohne gültigen Fahrausweis werden von der SBB in ihrem Informationssystem RogF bearbeitet. Es stützt sich insbesondere auf das Personenbeförderungsgesetz (PBG) und die Tarife der schweizerischen Transportunternehmen. Tarif 600 enthält die allgemeinen Bedingungen zum Personenverkehr, Tarif 600.5 Richtlinien für die Behandlung von Reisenden ohne gültigen Fahrausweis. Auch letzterer stützt sich hauptsächlich auf das Personenbeförderungsgesetz, gemäss welchem Personen, die keine gültige Fahrkarte vorweisen, einen

Zuschlag bezahlen müssen. Dieser kann erhöht werden, wenn die reisende Person zum wiederholten Mal kein gültiges Billet vorweist. Weiter besitzt die SBB eine Konzernweisung zum Datenschutz. Die SBB konnte uns zwar darlegen, welche Daten in RogF zu welchem Zweck bearbeitet werden; die Details (wie Zweck, Datenkategorien, Zugriffe, Datenbearbeitungen, Löschung der Daten usw.) sind jedoch weder in einer gesetzlichen Grundlage noch in einem Papier der SBB genau umschrieben.

Nach Angaben der SBB läuft die Datenbearbeitung wie folgt ab: Der Zugbegleiter führt seine Kontrollen mit seinem Zugpersonalgerät (ZPG) durch. Zwischen dem Gerät und RogF besteht keine Onlineverbindung, vielmehr werden die im ZPG erfassten Datensätze der Reisenden ohne gültigen Fahrausweis jeweils nach Dienstschluss in die RogF-Datenbank übermittelt. Stösst der Zugbegleiter auf einen Passagier ohne gültige Fahrkarte, füllt er zudem das Formular 7000 aus, das als Fahrausweis dient und von den SBB gescannt wird. Dieses Formular wird ausgestellt, wenn eine Person ihr persönliches Abonnement (z.B. GA) vergessen hat und sich nicht ausweisen kann, oder wenn sie eine Fahrkarte besitzt, aber ihr Halbtax-Abonnement nicht dabei hat. In beiden Fällen hat die betroffene Person zehn Tage Zeit, ihr vergessenes Abonnement vorzuweisen, womit der Vorfall abgeschlossen ist.

Die SBB handelt im Rahmen ihrer konzessionierten Tätigkeit als Bundesorgan im Sinne des Datenschutzgesetzes und braucht für die Bearbeitung von Personendaten eine gesetzliche Grundlage. Bei besonders schützenswerten Personendaten muss es sich um eine gesetzliche Grundlage im formellen Sinn (etwa ein vom Parlament verabschiedetes Bundesgesetz) handeln. Das PBG regelt die Erhebung des Zuschlags, nicht dagegen das Informationssystem selbst. Gleichzeitig hält das Datenschutzgesetz fest, dass besonders schützenswerte Personendaten ohne gesetzliche Grundlage bearbeitet werden dürfen, wenn es ausnahmsweise für eine in einem Gesetz im formellen Sinn klar umschriebene Aufgabe unentbehrlich ist. Wir kamen zum Schluss, dass die SBB ein Informationssystem führen muss, um ihre gesetzlichen Aufgaben, insbesondere die Erhöhung des Zuschlags für Wiederholungstäter, überhaupt erfüllen zu können. Allerdings darf eine solche Datenbearbeitung nur ausnahmsweise gestützt auf das Datenschutzgesetz erfolgen. Eine solche Ausnahme liegt hier nicht vor.

Aufgrund der im PBG klar umschriebenen gesetzlichen Aufgabe konnten wir von einem Verbot des Informationssystems RogF bis zur Schaffung der gesetzlichen Grundlage dennoch absehen. Allerdings bleibt die Grundlage mangelhaft, weshalb das System nur für eine beschränkte Dauer weitergeführt werden kann. Die fehlende gesetzliche Grundlage muss so rasch als möglich geschaffen werden. Die Schwierigkeit für uns bestand darin, dass wir dies von der SBB nicht verlangen

konnten, da die Bahn einen Gesetzgebungsprozess nicht direkt auslösen kann. Sie kann aber beispielsweise beim Bundesamt für Verkehr (BAV) vorstellig werden, damit dieses den Prozess auslöst. Aus diesem Grund schlugen wir der SBB vor, uns in Zusammenarbeit mit dem BAV mitzuteilen, ob die notwendigen Schritte zur Schaffung einer gesetzlichen Grundlage für die Führung solcher Informationssysteme unternommen würden. Gleichzeitig behielten wir uns vor, der SBB zu empfehlen, die Datenbearbeitung in RogF zu unterlassen, falls diese Schritte ausblieben. Weiter schlugen wir der SBB vor, bis zur Schaffung der gesetzlichen Grundlagen die genauen Datenbearbeitungen in Weisungen oder Richtlinien festzuhalten.

Die SBB hatte ursprünglich geplant, die Daten in RogF grundsätzlich nach zwei Jahren zu löschen. Bei unserer Kontrolle vor Ort mussten wir jedoch feststellen, dass noch gar keine Daten gelöscht worden waren. So waren auch Angaben aus den Jahren 1999 und 2000 darin enthalten. Eine so lange Aufbewahrung verstösst gegen das Verhältnismässigkeitsprinzip. Zum Zeitpunkt unserer Kontrolle war die SBB daran, ein Konzept für die Löschung der Daten auszuarbeiten. Darin soll geklärt werden, welche Daten für welche Zwecke wie lange aufbewahrt werden sollen, und wie die Löschung umgesetzt werden kann. Wir empfahlen der SBB, das Konzept bis Ende 2012 auszuarbeiten, uns zu unterbreiten und gleichzeitig die Löschung der nicht mehr erforderlichen Daten sicherzustellen. Auch die gescannten Formulare 7000 waren zum Zeitpunkt unserer Kontrolle nicht gelöscht worden. Wir fanden Dokumente, die bis auf das Jahr 2006 zurückgingen. Auch hier empfahlen wir das gleiche Vorgehen wie für die Löschung der Daten in RogF. Weitere Empfehlungen betrafen das Ausarbeiten eines Bearbeitungsreglements für die Datenbank und die Generierung eines Passwortes.

Die SBB hat unsere Vorschläge und Empfehlungen angenommen, und das BAV hat uns gegenüber festgehalten, die nötigen Schritte zur Schaffung der fehlenden gesetzlichen Grundlagen zu unternehmen. Wir haben das Konzept für die Löschung und das Bearbeitungsreglement erhalten und werden diese Dokumente sowie die effektive Löschung der Daten prüfen. Desgleichen werden wir die gesetzgeberischen Schritte verfolgen.

1.2.4 Ausführungsbestimmungen zur Gesetzgebung im Bereich Sport

Das Parlament hat am 17. Juni 2011 zusammen mit dem Bundesgesetz über die Förderung von Sport und Bewegung auch ein neues Gesetz über die Informationssysteme des Bundes im Bereich Sport verabschiedet. Mit diesen am 1. Oktober 2012 in Kraft getretenen Bestimmungen werden gesetzliche Grundlagen für die Dopingbekämpfung in der Schweiz geschaffen. Zu den dafür notwendigen Ausführungsbestimmungen haben wir Stellung genommen. Unsere Einwände, welche die Aufbewahrungsdauer von Personendaten betrafen, wurden berücksichtigt.

Die Verordnung zum Gesetz über die Informationssysteme des Bundes im Bereich Sport regelt unter anderem die Bearbeitung von Personendaten. Im Rahmen der Ämterkonsultation haben wir insbesondere zur Aufbewahrungsdauer der Daten Stellung genommen. Diese Dauer ergibt sich aus dem Grundsatz der Verhältnismässigkeit: Die Daten sind nur solange zu speichern, wie es für den Bearbeitungszweck notwendig ist. Unsere Anmerkungen wurden berücksichtigt, indem die Dauer der Speicherung je nach Art der Daten und Bearbeitungszweck unterschiedlich definiert wurde. So werden nach Ablauf der Fristen die Daten entweder archiviert und im System gelöscht oder anonymisiert.

Mit dem Inkrafttreten des Bundesgesetzes über die Förderung von Sport und Bewegung (SpoFöG) besteht jetzt eine gesetzliche Grundlage zur Dopingbekämpfung in der Schweiz. Bisher basierte dieser Kampf auf der Einwilligungserklärung der Athletinnen und Athleten zu entsprechenden Kontrollen. Jedoch war die Abgabe dieser Einwilligung nicht freiwillig, da im Falle einer Verweigerung keine gleichwertige Alternative existierte. Besteht anstelle der Einwilligung in die Datenbearbeitung einzig die Möglichkeit, auf die Ausübung des wettkampfmässigen Sports zu verzichten, kann jedenfalls nicht von einer gleichwertigen Alternative gesprochen werden. Daher konnten die so abgegebenen Erklärungen nicht als Einwilligungen im Rechtssinne verstanden werden. Mit der von uns angeregten gesetzlichen Grundlage können nun Sportlerinnen und Sportler, die regelmässig an Wettkämpfen teilnehmen, jederzeit Dopingkontrollen unterzogen werden, ob sie eine Einwilligung abgegeben haben oder nicht (vgl. unseren 15. Tätigkeitsbericht 2007/2008, Ziff. 1.5.3).

Weiter bringt das Inkrafttreten des SpoFöG die Rechtsgrundlagen, um den notwendigen Datenaustausch mit nationalen und internationalen Anti-Doping-Stellen zu gewährleisten. Weil jedoch auch besonders schützenswerte Daten betroffen sein

können, dürfen die Daten nicht vorbehaltlos an andere internationale Anti-Doping-Stellen übermittelt werden. Die übermittelnde Stelle darf keine Daten weitergeben, wenn eine Verletzung von Persönlichkeitsrechten droht, insbesondere wenn der Empfänger den angemessenen Schutz der Daten nicht gewährleisten kann. Angemessener Schutz ist erreicht, wenn das Empfängerland über ein genügendes Datenschutzniveau verfügt oder eine vertragliche Regelung abgeschlossen wird (vgl. Ziff. 1.2.6 des vorliegenden Tätigkeitsberichts).

1.2.5 Bearbeitung von Personendaten anlässlich von Sportveranstaltungen

Die Sachverhaltsabklärung bei einem Dienstleistungsanbieter für Sportveranstaltungen konnten wir ohne Erlass einer Empfehlung abschliessen. Jedoch mangelt es ebenso an Information über die durchgeführten Datenbearbeitungen von Seiten des Veranstalters wie an Freiwilligkeit bei der Einwilligung in die Datenbearbeitung von Seiten der Betroffenen.

Die im letzten Tätigkeitsbericht erwähnte Sachverhaltsabklärung bei einem Dienstleistungsanbieter für Breitensportveranstaltungen konnten wir ohne Erlass einer Empfehlung abschliessen. Der Dienstleistungsanbieter hat unsere Verbesserungsvorschläge in seinem System umgesetzt (vgl. unseren 19. Tätigkeitsbericht 2011/2012, Ziff. 1.2.10).

Wir stellen jedoch fest, dass bezüglich der von den Veranstaltern durchgeführten Datenbearbeitungen seitens der davon Betroffenen nach wie vor ein Mangel an Information sowie an Freiwilligkeit der Einwilligung besteht. Die Veröffentlichung von Start- und Ranglisten im Internet ist für die Durchführung der Veranstaltung nicht notwendig. Daher muss den Teilnehmerinnen und Teilnehmern eine Opt-Out-Möglichkeit angeboten werden. Die von diversen Veranstaltern in ihren Reglementen resp. Datenschutzerklärungen gewählte Formulierung «Diese Zustimmung ist Voraussetzung für die Teilnahme» erfüllt die Vorgaben des Datenschutzgesetzes nicht. Wie in anderen Bereichen ist die Abgabe der Einwilligung nicht freiwillig, wenn im Falle ihrer Verweigerung keine gleichwertige Alternative besteht, zumal die Datenbearbeitung für den verfolgten Zweck nicht notwendig ist. Die Sportverbände und Veranstalter werden diesbezüglich angehalten, eine einheitliche datenschutzkonforme Datenbearbeitung umzusetzen.

1.2.6 Dopingbekämpfung und Bekanntgabe von Personendaten ins Ausland

Seit Inkrafttreten des Bundesgesetzes über die Förderung von Turnen und Sport besteht für Datenlieferungen an die World Anti Doping Agency eine gesetzliche Grundlage. Dennoch muss, da Daten ins Ausland geliefert werden, ein genügendes Datenschutzniveau durch vertragliche Vereinbarungen sichergestellt werden.

Im neuen Bundesgesetz über die Förderung von Turnen und Sport (SpoFöG) sind unter dem Titel «Massnahmen gegen Doping» die Erfassung, die Bearbeitung und der Austausch von Personendaten zur Dopingbekämpfung geregelt. Wir haben Anfragen von Sportverbänden erhalten, ob aufgrund dieser neuen Rechtslage Gesundheitsdaten von Sportlerinnen und Sportlern ohne weitere Massnahmen an die World Anti Doping Agency (WADA) auf deren in Montreal stehenden Server übermittelt werden dürfen. Wir haben die Situation analysiert und Stellung genommen.

Unter altem Recht bestanden für die Datenlieferung von Sportlerdaten an die WADA auf deren Server in Montreal zwei Schwierigkeiten: Erstens bestand für die Erhebung, die Bearbeitung und den Austausch von Personendaten zur Dopingbekämpfung keine rechtliche Grundlage. Dementsprechend hat man sich auf eine Einwilligungserklärung der Sportlerinnen und Sportler gestützt. Da diese Einwilligungen jedoch nach datenschutzrechtlichem Verständnis nicht freiwillig erfolgt sind, war deren Rechtsgültigkeit höchst zweifelhaft (vgl. unseren 15. Tätigkeitsbericht 2007/2008, Ziff. 1.5.4, sowie unseren 17. Tätigkeitsbericht 2009/2010, Ziff. 1.2.7). Zweitens untersteht die WADA weder der kanadischen Datenschutzgesetzgebung noch derjenigen der Provinz Quebec, da sie keiner kommerziellen, sondern einer ideellen Tätigkeit nachgeht. Dementsprechend besteht für Datenlieferungen an die WADA in Montreal kein genügendes Datenschutzniveau, so dass eine solche Lieferung aufgrund von Artikel 6 DSG nur dann zulässig ist, wenn das Datenschutzniveau anderweitig, z.B. vertraglich, sichergestellt wird (vgl. unseren 15. Tätigkeitsbericht 2007/2008, Ziff. 1.5.3).

Mit dem neuen SpoFöG wurde für die erste Problematik eine Lösung geschaffen. Sowohl die Erhebung und Bearbeitung von Personendaten zur Dopingbekämpfung als auch der Austausch dieser Daten mit nationalen oder internationalen Anti-Doping-Stellen wurden gesetzlich verankert und setzen damit keine Einwilligung der betroffenen Personen mehr voraus (vgl. Ziff. 1.2.4 des vorliegenden Tätigkeitsberichts). Damit wird nicht nur die Arbeit für die Anti-Doping-Stellen erleichtert,

sondern für die Sportlerinnen und Sportler auch Klarheit geschaffen über ihre Rechte und Pflichten bei Dopingkontrollen.

Nicht vereinfacht wurde jedoch die Anforderung, bei Datenlieferungen ins Ausland sicherzustellen, dass im Empfängerstaat ein angemessenes Datenschutzniveau besteht. Vielmehr hält Artikel 25 Absatz 4 SpoFöG nun ausdrücklich fest, dass eine Datenweitergabe zu verweigern ist, wenn der Empfänger keinen angemessenen Schutz der Daten gewährleisten kann. Die Bestimmung wiederholt die allgemeine Regel des Datenschutzgesetzes und macht damit klar, dass auch der gerechtfertigte Kampf gegen Doping nicht dazu führen darf, dass die betroffenen Personen des Schutzes ihrer Persönlichkeit beraubt werden.

Wir haben den anfragenden Verbänden mitgeteilt, dass auch unter dem neuen SpoFöG das Datenschutzniveau vertraglich sichergestellt werden muss und entsprechende Vereinbarungen mit der WADA abgeschlossen respektive aufrecht erhalten werden müssen.

1.2.7 Übersicht über die biometrischen Technologien

Im Rahmen der regelmässig initiierten technischen Projekte haben wir uns einen Überblick über die bestehenden biometrischen Technologien verschafft. Mit Hilfe unserer Technologiebeobachtung behalten wir den aktuellen Stand dieses in stetigem Wandel begriffenen Bereichs im Blick. Mit dem Test verschiedener Produkte konnte dieses Projekt durch einen praktischen Teil ergänzt werden.

Bei unseren Kontroll- und Beratungstätigkeiten werden wir regelmässig mit Fragen zu den biometrischen Technologien konfrontiert, da diese wachsendes Interesse wecken. Angesichts dieser stetigen Entwicklungen haben wir eine interne Studie eingeleitet, die uns eine Übersicht über die bisher bekannten und genutzten Technologien in der Forschung sowie in der Praxis vermittelt hat.

Dank der Anschaffung oder der Bereitstellung mehrerer Lesegeräte für biometrische Fingerabdrücke konnten wir auch verschiedene Erkennungssysteme praktisch testen. Unser Ansatz in dieser Studie richtete sich hauptsächlich auf den durch die verschiedenen Technologien gebotenen Schutz der Privatsphäre und die Rückverfolgbarkeit biometrischer Merkmale. Demnach sind die Technologien am besten geeignet, welche die geringsten Risiken für den Schutz der Personendaten mit sich bringen und am wenigsten Spuren hinterlassen. Wir haben diese Studie mit der Feststellung abgeschlossen, dass es heute biometrische Technologien gibt, wie etwa die Venen- oder Tastendruckerkennung, welche die Privatsphäre schützen und zugleich leicht zu nutzen sind.

1.2.8 Schulung für die Erstellung eines Bearbeitungsreglements

Wir haben zusammen mit dem Datenschutzberater des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport (VBS) ein Bearbeitungsreglement erstellt. Ziel war es aufzuzeigen, wie dabei vorgegangen werden kann und welcher Aufwand benötigt wird, um die erforderliche Transparenz zu erreichen. Basierend auf den Erkenntnissen haben wir in der Folge die weiteren Datenschutzberater der verschiedenen Ämter des VBS geschult.

Der Datenschutzberater des VBS hat uns gebeten, bei ihnen eine Schulung bezüglich der Erstellung eines Bearbeitungsreglements durchzuführen. Wir haben zugesagt und im Vorfeld der Ausbildung gemeinsam mit dem Datenschutzberater und dem Inhaber der Datensammlung anhand einer konkreten Anwendung ein solches Reglement erstellt. Bereits bei der ersten Frage zum Ziel bzw. Zweck der Anwendung gab es einige Diskussionen. Dieser Punkt beantwortet die Frage, was mit der Anwendung erreicht werden soll bzw. warum. In vielen Fällen werden bei diesen Umschreibungen aber eher die Aufgaben bzw. Funktionen aufgeführt, welche die Anwendung erfüllen soll, dabei sollten sich diese am Ziel orientieren.

Bei der Betrachtung des Systems mit seinem Umsystem (Dokumentation der vom System bzw. der Anwendung betroffenen Organisationseinheiten) ging es darum, die Anwendung grob zu erfassen bzw. zu verstehen. Warum werden welche Daten in welchen Organisationseinheiten zu welchem Zweck wie bearbeitet? Warum (zu welchem Zweck) werden die Personendaten an andere Organe übermittelt? Ist diese Datenübermittlung auch aus Sicht des Datenschutzes sinnvoll, oder könnte man die Aufgaben allenfalls mit anonymen oder pseudonymisierten Daten ebenfalls erfüllen?

Nachdem wir uns aufgrund der oben aufgeführten Analyse eine Übersicht über die Anwendung erarbeitet hatten, begannen wir gemeinsam mit der Dokumentation der Prozesse, die nun detaillierter aufzeigen sollte, wie die Aufgaben innerhalb der Organisationeinheiten erfüllt werden. Der Datenschutzberater analysiert die Prozesse insbesondere aus Sicht der Betroffenen. Diese Betrachtung ist nicht gleich wie diejenige des Inhabers, der eher auf eine möglichst effiziente Datenbearbeitung fokussiert. In der Projektorganisation befinden sich meist Vertreter der Anwenderseite als auch der Informatik sowie der Projektleiter, meist aber keine Datenschutzberater. Der Projektauftraggeber tut aber namentlich bei sensitiven Projekten gut daran, auch den Datenschutzberater der jeweiligen Projektorganisation einzubeziehen, um nicht Gefahr zu laufen, die Aspekte des

Datenschutzes zu wenig zu berücksichtigen. Dies kann nämlich in der Folge zu erheblichen Unannehmlichkeiten führen.

Damit der Datenschutzberater überhaupt weiss, was in Sachen Anwendungen passiert, und mitdenken und Feedback geben kann, muss er über neue Projekte oder Änderungen an bestehenden Systemen (Anwendungen) auf dem Laufenden gehalten werden. Die Analyse anhand einer bestehenden Anwendung hat unter anderem aufgezeigt, wie aufwendig es ist, ein System technisch und organisatorisch zu verstehen. Im Weiteren hat die Erstellung des Bearbeitungsreglements auch gezeigt, dass sinnvolle und abschliessende Regelungen erst dann möglich sind, wenn die entsprechende Transparenz vorhanden ist.

1.3 Internet und Telekommunikation

1.3.1 Erläuterungen zum Internetpranger

Internetpranger erfreuen sich wachsender Beliebtheit: Kunden, die ihre Rechnungen nicht bezahlen, Behördenmitglieder, die nicht im Sinne des Verfassers entscheiden, oder Personen mit einer bestimmten politischen Meinung werden auf einer schwarzen Liste im Internet aufgeschaltet und so in der Öffentlichkeit einem bestimmten Vorwurf ausgesetzt. Mit solchen Internetprangern werden die Persönlichkeitsrechte der Betroffenen in der Regel widerrechtlich verletzt.

Internetpranger sind aus Sicht des Persönlichkeitsschutzes problematisch: Personen, die nicht im Sinne des Verfassers gehandelt oder entschieden haben, werden im Internet veröffentlicht und mit reisserischen Worten einem bestimmten Vorwurf ausgesetzt. Der Pranger ist dabei weltweit und rund um die Uhr zugänglich, die darin veröffentlichten Informationen auch noch nach Jahren abrufbar. Da diese Angaben weder journalistisch sorgfältig aufbereitet sind noch ein differenziertes Bild über die angeprangerten Vorgänge erlauben, erfüllen solche Veröffentlichungen kein allgemeines Informationsbedürfnis. Vielmehr verfolgen solche Pranger eher das Ziel, die aufgeführten Personen zu stigmatisieren und herabzusetzen. Für die betroffenen Personen kann dies schwerwiegende Konsequenzen haben, ein von den Verfassern gewollter Effekt, der auch eine abschreckende Wirkung haben soll. Ein Rechtfertigungsgrund für die so verursachte Persönlichkeitsverletzung besteht in der Regel nicht.

Entgegen der landläufigen Meinung können die betroffenen Personen auch dann widerrechtlich in ihren Persönlichkeitsrechten verletzt werden, wenn ausschliesslich bereits veröffentlichte Daten verwendet werden. Werden solche Daten miteinander verknüpft und in einem vollkommen anderen Kontext publiziert, so hat dies nichts mehr mit der ursprünglichen Veröffentlichung zu tun. Sie rechtfertigt damit auch nicht die Verwendung der fraglichen Daten zum neuen Zweck, dem Internetpranger.

Auch bei sogenannten Behördenprangern, also schwarzen Listen mit angeblich fehlbaren Behördenmitgliedern, ist Vorsicht geboten. Zwar muss bei Personen, die ein öffentliches Amt ausüben, öffentliche Kritik erlaubt sein. Dies gilt aber nur so lange, als es sich um sachliche Kritik handelt, die sich auf die Tätigkeit als Behördenmitglied beschränkt. Diese Voraussetzung ist bei Internetprangern in der Regel nicht erfüllt, da eine verkürzte und einseitige Darstellung kaum als sachlich

bezeichnet werden kann. Keinesfalls dürfen Angaben aus dem Privatbereich, wie beispielsweise private Adresse, Telefonnummern, E-Mail-Adressen oder nicht öffentliche Fotografien, veröffentlicht werden. Unnötig herabsetzende Kommentare oder gar Aufrufe, die fragliche Person ausserhalb ihrer behördlichen Tätigkeit zu kontaktieren, dürfen ebenfalls nicht veröffentlicht werden.

Weitere Informationen zum Internetpranger finden sich auf unserer Webseite www.derbeauftragte.ch unter Datenschutz – Internet und Computer.

1.3.2 Strassenansichten im Internet – Bundesgerichtsentscheid

Das Bundesgericht hat am 31. Mai 2012 über die datenschutzrechtlichen Aspekte in Sachen Google Street View entschieden. Zentrale Punkte waren die Anwendbarkeit des Schweizer Datenschutzgesetzes, die Anforderungen beim Einsatz einer automatischen Anonymisierung, die Anonymisierung im Bereich von sensiblen Einrichtungen und die Aufnahme von Privatbereichen, welche für gewöhnliche Passanten nicht einsehbar sind.

Das Bundesgericht hat sich im Urteil (BGE 138 II 346) vorab über die Zuständigkeit der schweizerischen Behörden und Gerichte für die Beurteilung des Sachverhalts geäussert. Eine Datenbearbeitung beurteilt sich demnach nach schweizerischem Datenschutzrecht und fällt in unsere Zuständigkeit, wenn ein genügender Bezug zur Schweiz besteht – dies gilt auch, wenn die Server im Ausland stationiert sind. Bei Google Street View werden zum Beispiel die Informationen über Personen, Strassen und Plätze in der Schweiz erhoben und so veröffentlicht, dass sie hier abrufbar sind. Die Bedeutung des Entscheids liegt darin, dass das schweizerische Datenschutzgesetz auch für eine Datenbearbeitung anwendbar ist, die zu Teilen im Ausland stattfindet, wenn ein ausreichender Bezug zur Schweiz besteht.

Ein wichtiger Punkt des gesamten Verfahrens war, ob Google die Gesichter und Autonummern im Dienst Street View vor der Aufschaltung vollständig zu anonymisieren habe. Das Bundesgericht gewährte eine Fehlertoleranz von ca. einem Prozent bei der automatischen Anonymisierung. Jedoch müssen dabei folgende fünf Bedingungen erfüllt werden:

- Mit allen zur Verfügung stehenden technischen Mitteln soll eine vollständige Anonymisierung angestrebt und die automatische Anonymisierung laufend dem Stand der Technik angepasst werden.

- Den Benutzerinnen und Benutzern muss ein gut sichtbarer Link – etwa mit dem klaren Hinweis «Anonymisierung verlangen» – angeboten werden, mit welchem die hinreichende Anonymisierung unzulässiger Inhalte veranlasst werden kann.
- Personen und Fahrzeuge im Bereich von sensiblen Einrichtungen – insbesondere vor Frauenhäusern, Altersheimen, Gefängnissen, Schulen, Gerichten und Spitälern – sind vor der Publikation im Internet vollständig zu anonymisieren. Dies auf eine Weise, dass nebst den Gesichtern auch weitere individualisierende Merkmale wie Hautfarbe, Kleidung, Hilfsmittel von körperlich behinderten Personen etc. nicht mehr feststellbar sind.
- Der Privatbereich (umfriedete Höfe, Gärten usw.) ist zu respektieren. Daher dürfen Einblicke, die von einer Kamerahöhe von über 2 Meter aufgenommen wurden und dem gewöhnlichen Passanten verschlossen bleiben, nicht in Street View veröffentlicht werden. Soweit die Einwilligung der Betroffenen fehlt, sind bereits publizierte Bilder solcher Privatbereiche zu entfernen.
- Wenn neue Aufnahmefahrten durchgeführt oder neue Aufnahmen in Street View aufgeschaltet werden, ist dies in den Medien bekannt zu machen und dabei deutlich auf die Widerspruchsmöglichkeit hinzuweisen.

Wir stehen mit Google betreffend die Umsetzung der vom Bundesgericht gemachten Auflagen in Kontakt und werden diese laufend kontrollieren.

1.3.3 Internet-Tauschbörsen – Rechtslage nach dem Logistep-Urteil

Nach dem Urteil in Sachen Logistep besteht eine gewisse Unsicherheit darüber, ob die Verfolgung von Urheberrechtsverletzungen nach geltendem Recht noch möglich ist. In der Zwischenzeit sind jedoch Bemühungen im Gange, Massnahmen zur Erleichterung der Durchsetzung von Urheberechten im Internet gesetzlich zu verankern und damit in der Sache Klarheit zu schaffen.

Mit dem Logistep-Urteil (vgl. unseren 18. Tätigkeitsbericht 2010/2011, Ziff. 1.3.5) ist Unsicherheit über die Tragweite dieses Entscheids für die Verfolgung von Urheberrechtsverletzungen im Internet entstanden. Insbesondere die Staatsanwaltschaften verstehen das Urteil dahingehend, dass die Beschaffung von IP-Adressen im Internet für die Verfolgung von Urheberrechtsverletzungen generell widerrechtlich ist und die so erlangten Beweismittel einem Verwertungsverbot unterliegen. Wir

hingegen vertreten die Auffassung, dass die Beschaffung und Bearbeitung solcher Personendaten unter Beachtung folgender Grundsätze auch nach dem Urteil weiterhin möglich sein soll (vgl. unseren 19. Tätigkeitsbericht 2011/2012, Ziff. 1.3.7):

- Es muss sichergestellt sein, dass die Datenerhebung und -speicherung nicht über das hinausgeht, was absolut notwendig ist, um Strafanzeige gegen mutmassliche Urheberrechtsverletzer zu erstatten.
- Es muss sichergestellt sein, dass Verhandlungen zwischen den Rechteinhabern und dem (mutmasslichen) Urheberrechtsverletzer über Schadenersatzforderungen nur auf dessen Initiative hin oder aber nach rechtskräftigem Abschluss des Strafverfahrens stattfinden.
- Die Rechteinhaber müssen die Beschaffung der Personendaten und den Zweck ihrer Bearbeitung für die betroffenen Personen möglichst erkennbar machen, indem sie insbesondere auf ihrer Webseite an leicht zugänglicher und auffindbarer Stelle ihre Vorgehensweise (insbesondere detaillierte Angaben zu Art und Umfang der von ihnen gesammelten Daten) vollständig offen legen und dabei deutlich machen, dass Schadenersatzansprüche nur gegen rechtskräftig strafrechtlich verurteilte Urheberrechtsverletzer verfolgt werden.

Der Nachweis darüber, ob eine derartige Datenbeschaffung nach geltendem Recht möglich ist, würde am besten durch eine von den Rechteinhabern herbeizuführende höchstrichterliche Klärung der Anforderungen an eine datenschutzkonforme Beweiserhebung bei Urheberrechtsverletzungen im Internet erbracht.

Wir haben indessen auch wiederholt auf den Geschäftsbericht 2010 des Bundesgerichts hingewiesen, in dem es in seinen seltenen «Hinweisen an den Gesetzgeber» auf die als ungenügend empfundenen gesetzlichen Regelungen im Bereich Urheberrecht aufmerksam macht. Im Rahmen eines parlamentarischen Postulats führte nicht zuletzt unsere Intervention zu ersten Schritten in diesem Bereich. Im Auftrag von Frau Bundesrätin Sommaruga prüft nun eine Arbeitsgruppe bis Ende 2013 Möglichkeiten zur Anpassung des Urheberrechts an die technische Entwicklung. Dieser Auftrag schliesst die Prüfung von Massnahmen zur Erleichterung der Rechtsdurchsetzung im Internet mit ein.

1.3.4 Immobilienplattform im Internet

Auf Anfrage haben wir eine Internetplattform, welche Mieterinnen und Mietern die Möglichkeit bietet, sich ein elektronisches Bewerbungsdossier zusammenzustellen, aus datenschutzrechtlicher Sicht beurteilt.

Zwei Unternehmen haben uns ihr Projekt der Erweiterung einer Immobilienplattform vorgestellt und um datenschutzrechtliche Beurteilung derselben gebeten. Die Plattform soll interessierten Mieterinnen und Mietern die Möglichkeit bieten, ihr Dossier in strukturierter Form online erfassen zu können. Das eine Unternehmen liefert dabei auf Bestellung des Mieters eine Einschätzung der Bonität oder Betreibungsauszüge. Beim Aufbau der Plattform beachteten die Unternehmen die auf unserer Webseite publizierten Vorgaben. Der Mieter soll transparent über die Datenbearbeitungen informiert werden und die Herrschaft über seine Daten behalten. Beide Unternehmen erhalten keine Einsicht in das Dossier. Der Mieter alleine entscheidet darüber, an welche Liegenschaftsverwaltung das Dossier übermitteln werden soll. Wir stellten fest, dass das geplante Projekt den wesentlichen Datenschutzanforderungen entspricht, und haben zusätzlich Verbesserungsvorschläge unterbreitet.

1.3.5 Datenschutzkonformes Social Media Monitoring

Unternehmen und Behörden wollen vermehrt in Erfahrung bringen, wie sie in den Sozialen Medien dargestellt werden. Daraus hat sich die Dienstleistung Social Media Monitoring entwickelt.

Soziale Medien wie Facebook, Google+, XING, Twitter oder Blogs haben im Vergleich zu herkömmlichen Medien (Zeitungen, Radio, Fernsehen) in letzter Zeit auch für Firmen, Behörden und Organisationen zunehmend Bedeutung erlangt. Denn diese möchten zum einen wissen, was über sie in diesen Medien berichtet wird, und zum anderen adäquat reagieren können. Damit sich ein Unternehmen einen raschen und umfassenden Überblick verschaffen kann, wie es in den sozialen Medien dargestellt wird, haben sich spezialisierte Anbieter auf dem Markt etabliert, die geeignete Tools und Dienstleistungen zur Beobachtung dieser Seiten entwickelt haben. Man spricht dabei von «Social Media Monitoring».

Beim Einsatz von Social Media Monitoring sind allerdings die Anforderungen des Datenschutzes zu beachten: Werden nämlich bestimmte oder bestimmbare Personen (natürliche oder juristische) beobachtet, liegt eine Datenbearbeitung im Sinne des Datenschutzgesetzes vor. Dies kann etwa die Inhalte der verbreiteten

Wortmeldungen, aber auch deren Autorinnen und Autoren betreffen. Letztere veröffentlichen ihre Texte als Meinungsäusserung oder als Diskussionsbeitrag zwar bewusst auf Social-Media-Plattformen. Dieser ursprüngliche Zweck der Datenbearbeitung schliesst ein Monitoring nicht zwingend ein; das bedeutet, nicht jede technisch mögliche Bearbeitung dieser Daten ist ohne Weiteres gesetzlich gedeckt. Auch veröffentlichte Daten dürfen laut Datenschutzgesetz nicht durchwegs für andere Zwecke verwendet werden.

Der EDÖB empfiehlt namentlich, sich beim Einsatz von Social Media Monitoring auf das für die Auswertungszwecke nötige Minimum zu beschränken. Die Resultate dürfen keine Rückschlüsse auf Personen mehr erlauben. Zudem müssen die Benutzer von Social-Media-Plattformen darüber informiert sein, dass Monitoring-Tools eingesetzt werden.

Ausführlichere Informationen finden sich auf unserer Webseite www.derbeauftragte.ch unter Datenschutz – Internet und Computer – Onlinedienste.

1.3.6 Einsatz von Webanalysetools für Bundesorgane

Der Betreiber einer Webseite hat ein Interesse daran, die Zugriffe von Nutzerinnen und Nutzern zu analysieren, um zu wissen, wie sie sich auf der Seite bewegen oder um sein Onlineangebot zu optimieren. Für Webseiten des Bundes kann der Einsatz solcher Tools jedoch besondere Tücken haben.

Webanalysetools bieten typische Funktionen wie das Aufzeichnen der geografischen Herkunft der Besucherinnen und Besucher, ihre Verweildauer und eingegebene Suchmaschinenbegriffe. Mittels eines speziellen Bildelements sowie eines Skripts wird das Analysetool in der Webseite des Betreibers integriert. Werden keine besonderen Vorkehrungen getroffen, können solche Dienste Zugriffe auf die Webseite erfassen, da beim Abruf des Bildelements die IP-Adresse der zugreifenden Nutzer registriert wird. Da IP-Adressen als personenbezogene Daten betrachtet werden müssen, ist das Datenschutzgesetz (DSG) anwendbar.

Mit Hilfe der Analysesoftware können detaillierte Nutzerprofile bis hin zu den Aktivitäten der User auf der Seite erfasst und ausgewertet werden. Solche Nutzerprofile können Persönlichkeitsprofile im Sinne des DSG darstellen. Für Bundesorgane gilt es nun zu beachten, dass sie Personendaten nur bearbeiten dürfen, wenn hierfür eine gesetzliche Grundlage besteht; bei besonders schützenswerten Personendaten sowie Persönlichkeitsprofilen muss dies ein Gesetz im formellen Sinn sein.

Bei der Analyse der Zugriffe auf die Webseite werden Randdaten des Internetnutzers an den Anbieter des Auswertungstools weitergeleitet. Die Bearbeitung der Daten durch solche Anbieter ist als Datenbearbeitung durch Dritte zu qualifizieren. Auch hierfür braucht es grundsätzlich eine gesetzliche Grundlage.

Befindet sich der Server des Anbieters des Auswertungstools im Ausland, sind darüber hinaus die Regelungen zum grenzüberschreitenden Datentransfer zu beachten. Die Übermittlung von Personendaten ins Ausland birgt die Gefahr, dass dortige Behörden aufgrund nationaler Gesetzgebungen auf die Daten zugreifen könnten. Für Bundesorgane ist dieser Punkt besonders heikel, obliegt ihnen doch die Pflicht, sorgsam mit den Personendaten ihrer Bürgerinnen und Bürger umzugehen und sie insbesondere vor dem unbefugten Zugriff einer ausländischen Behörde zu sichern.

Daher empfiehlt es sich für Bundesorgane, auf den Einsatz von solchen Tools zu verzichten und Alternativen zu prüfen. Wenn hingegen mittels spezieller Vorkehrungen sichergestellt werden kann, dass bei der Analyse keine personenbezogenen Daten erhoben werden, findet das DSG keine Anwendung. Es bietet sich jedoch auch die Lösung an, die Webstatistik über entsprechende, direkt auf dem Server des Bundesorgans installierte Programme durchzuführen. So wird sichergestellt, dass keine Personendaten an einen Dritten ausserhalb der Bundesverwaltung bekannt gegeben werden.

1.3.7 Revision des Publikationsgesetzes

Die Veröffentlichung von amtlichen Publikationen stützt sich auf das Publikationsgesetz. Mit der Revision des Gesetzes soll das System den technischen und gesellschaftlichen Entwicklungen angepasst werden. Wir haben dazu in der Ämterkonsultation Stellung genommen.

Das Publikationsgesetz regelt die Veröffentlichung der Sammlungen des Bundesrechts und des Bundesblatts. Neben der gedruckten Version war bereits bisher auch die elektronische Publikation vorgesehen, jedoch genoss allein die gedruckte rechtliche Verbindlichkeit. Mit der Revision des Gesetzes findet nun ein Primatwechsel statt, und die Massgeblichkeit geht auf die elektronische Version über. Im Rahmen der Ämterkonsultation haben wir zum revidierten Gesetz Stellung genommen. Wir haben darauf hingewiesen, dass amtliche Publikationen auch sensible Personendaten enthalten können, beispielsweise in Notifikationen. Das Datenschutzgesetz sieht für die Veröffentlichung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen durch ein Bundesorgan vor, dass eine solche Publikation in einem formellen Gesetz ausdrücklich geregelt werden muss.

Auf unser Begehren hin wurde im revidierten Publikationsgesetz nun eine entsprechende Rechtsgrundlage geschaffen.

1.3.8 Revision der GEVER-Verordnung

Die Geschäftsverwaltungssysteme des Bundes sollen in Zukunft nur noch elektronisch geführt werden. Die rechtliche Grundlage dazu bildet die GEVER-Verordnung. Da mit dieser Umstellung ein gewisses Gefahrenpotenzial verbunden ist, müssen Sicherheitsvorkehrungen getroffen werden. Wir haben bezüglich datenschutzrechtlicher Aspekte beraten und in der Ämterkonsultation zur Verordnung Stellung genommen.

Auch dieses Jahr beschäftigten wir uns mit der GEVER-Verordnung. Ihr zugrunde liegt ein Beschluss des Bundesrates, wonach die Departemente und die Bundeskanzlei elektronische Geschäftsverwaltungssysteme (GEVER) einführen sollen. Dokumente des Bundes sollen dabei – wo immer möglich – elektronisch bearbeitet werden. Die gesetzliche Grundlage dazu wird mit der GEVER-Verordnung geschaffen, welche sich auf das Regierungs- und Verwaltungsorganisationsgesetz stützt.

Wir haben im Rahmen der Ämterkonsultation zur überarbeiteten Verordnung Stellung genommen. Die Anforderungen an den Schutz der Dokumente, insbesondere durch technische und organisatorische Massnahmen, bilden dabei einen Schwerpunkt. Die Einheiten der Bundesverwaltung müssen ein Informationssicherheitskonzept erarbeiten, welches sich an den erforderlichen Sicherheitsstandards orientiert. Besonders schutzwürdige elektronische Geschäftsdokumente sollen verschlüsselt übermittelt und abgelegt werden. Für sämtliche Dokumente in einem GEVER-System ist sicherzustellen, dass sie vor der Kenntnisnahme durch Unberechtigte geschützt sind. Für den Austausch von GEVER-Daten zwischen solchen Systemen ist ein gesicherter Kommunikationskanal zu verwenden. Wer über umfassende Zugriffsberechtigungen verfügt (sowohl beim Leistungsbezüger als auch beim Leistungserbringer), soll der Personensicherheitsprüfung unterstellt werden. Zudem werden bestimmte Handlungen, die im GEVER-System ausgeführt werden, protokolliert. Dies erlaubt es, die Rechtmässigkeit der Bearbeitung der GEVER-Daten nachzuvollziehen und zu kontrollieren. Unsere Begehren wurden berücksichtigt, und aus datenschutzrechtlicher Sicht konnten die Differenzen in der Ämterkonsultation bereinigt werden.

1.4 Justiz/Polizei/Sicherheit

1.4.1 Umsetzung Schengen: Datenschutz-Evaluation der baltischen Staaten

Im Oktober 2012 nahmen wir zum ersten Mal an einer Schengenevaluation im Bereich Datenschutz teil. Ein kleines Expertenteam evaluierte die drei baltischen Staaten. Die dort gewonnenen Erfahrungen werden für die Evaluation der Schweiz, die demnächst stattfinden sollte, wertvoll sein.

Zum ersten Mal nahmen wir an einer Schengenevaluation im Bereich Datenschutz teil. Vom 14. bis 20. Oktober 2012 waren die drei baltischen Staaten Litauen, Lettland und Estland an der Reihe. Alle drei Staaten waren im Jahr 2006 zum ersten Mal evaluiert worden und hatten verschiedene Empfehlungen erhalten. Eine Evaluation findet grundsätzlich alle fünf Jahre statt. Sobald das Evaluationsprogramm bestimmt ist, werden die Experten, idealerweise acht bis zehn Personen, ernannt. Jeder Mitgliedstaat kann maximal einen Experten stellen.

Das Team für die vorliegende Evaluation bestand aus sechs Personen. Im Vorfeld der Kontrolle vor Ort mussten die drei betroffenen Staaten zur Umsetzung der früheren Empfehlungen Stellung nehmen sowie Fragen beantworten und verschieden Unterlagen liefern. Die Kontrolle vor Ort fand bei den Datenschutz- und bei den Polizeibehörden statt. Dort konnten wir Experten auch zusätzliche Fragen stellen. Hauptsächlich während des Aufenthalts in den baltischen Staaten tauschten die Experten ihre Meinungen aus und verfassten die ersten Entwürfe der Evaluationsberichte. Sie beleuchten unter anderem die Umsetzung von früheren Empfehlungen, die Unabhängigkeit und Tätigkeiten der Datenschutzbehörde, die Umsetzung der Datenschutzrechte der betroffenen Personen und der Datensicherheit in Schengenangelegenheiten.

Gleichzeitig werden gegenüber den evaluierten Staaten auch Empfehlungen gemacht. Diese Entwürfe wurden nach der Kontrolle vor Ort zwischen den Experten konsolidiert und die betroffenen Staaten konsultiert. Anschliessend fand eine Bereinigung der Berichte zwischen den evaluierten Staaten und den Experten statt. Die Berichte wurden dann in der für die Schengenevaluationen zuständigen SCHEVAL-Arbeitsgruppe in Brüssel präsentiert, diskutiert und von dieser verabschiedet. Nach der Evaluation findet immer ein Follow-up statt, bei dem die betroffenen Staaten aufzeigen können, ob und inwieweit sie die Empfehlungen umsetzen konnten.

Die Schweiz selbst wurde im Jahr 2008 evaluiert. Unsere nun gemachten Erfahrungen werden bei der nächsten Evaluation der Schweiz, die demnächst anstehen sollte, wertvoll sein.

1.4.2 Umsetzung Schengen: Ausschreibungen im SIS mit dem Ziel der Auslieferung

Im Rahmen der koordinierten Kontrolle der Ausschreibungen im SIS nach dem Schengener Durchführungsübereinkommen (SDÜ) erhielten wir zu unserem Fragebogen eine gemeinsame Stellungnahme des Bundesamts für Polizei und des Bundesamts für Justiz. Bei einer Kontrolle vor Ort kamen wir zum Schluss, dass die Datenbearbeitungen in der Schweiz die Voraussetzungen von Artikel 95 SDÜ erfüllen. Der Schlussbericht der Gemeinsamen Kontrollinstanz zur koordinierten Kontrolle steht noch aus.

Die Gemeinsame Kontrollinstanz Schengen (GKI) beschloss, die Ausschreibungen von Personen im SIS, um deren Festnahme mit dem Ziel der Auslieferung ersucht wird (Art. 95 SDÜ), zu überprüfen. Diese Ausschreibungen entsprechen einem Haftbefehl und in den meisten Fällen liegt ebenfalls ein europäischer Haftbefehl vor. Die GKI arbeitete einen Fragebogen aus, der von den verschiedenen Mitgliedstaaten, so auch von uns, an die zuständigen nationalen Behörden verschickt wurde. Das Bundesamt für Polizei (fedpol) und der Direktionsbereich Internationale Rechtshilfe in Strafsachen des Bundesamtes für Justiz (BJ) haben gemeinsam zum Fragebogen Stellung genommen. Die GKI hat daraufhin die Datenschutzbehörden aller Schengenstaaten aufgefordert, eine Kontrolle vor Ort vorzunehmen. Diese führten wir am 5. Juli 2012 beim genannten Direktionsbereich des BJ durch. Dabei überprüften wir insbesondere das für die Ausschreibungen nach Artikel 95 SDÜ aufgestellte Verfahren sowie die Datenbekanntgabe.

Nach Prüfung des beantworteten Fragebogens und aufgrund unserer Kontrolle vor Ort kamen wir zum Schluss, dass die vorliegenden Ausschreibungen die Voraussetzungen von Artikel 95 SDÜ erfüllen. Wir haben unseren Bericht der GKI zukommen lassen, die einen Schlussbericht der koordinierten Kontrolle verfassen wird. Diesen werden wir auf unserer Webseite publizieren.

1.4.3 Umsetzung Schengen: Information an die Nutzer und Rechtsvermerk beim Zugriff auf RIPOL, SIS und ZEMIS

Im Zusammenhang mit der Koordinationsgruppe Schengen haben wir uns mit dem Bundesamt für Polizei in Verbindung gesetzt, um die bei Nachforschungen in den Systemen RIPOL, SIS und ZEMIS verwendeten Such- und Resultatmasken zu prüfen. Dabei untersuchten wir auch, ob die mit den abgefragten Datenbanken zusammenhängenden Informationen ausreichend sind und ob ein rechtlicher Warnhinweis eingefügt werden müsste.

Wie die «Koordinationsgruppe der schweizerischen Datenschutzbehörden im Rahmen der Umsetzung des Schengen-Assoziierungsabkommens» bei ihrer Sitzung vom 10. Mai 2012 betonte, ist es wichtig, dass sich die Nutzer der Systeme RIPOL, SIS und ZEMIS im Klaren darüber sind, aus welchen Systemen die bei ihrer Suche abgefragten Daten stammen. Es wurde Besorgnis bezüglich der Rechtmässigkeit der Abfragen laut, und die Gruppe erwog die Möglichkeit, einen rechtlichen Warnhinweis in die Suchmasken einzubauen. Wir haben uns zur Beantwortung der Fragen der Koordinationsgruppe an das Bundesamt für Polizei (fedpol) gewandt.

Anhand der Auskünfte von fedpol, ergänzt durch Bildschirmaufnahmen zur Veranschaulichung der verschiedenen Resultatmasken, konnten wir feststellen, dass die Informationen über die von den Nutzern abgefragten Datenbanken in den verschiedenen Masken sehr gut sichtbar sind. Überdies wurde uns bestätigt, dass die Suchmasken direkt von den Dienstanbietern der Kantone entwickelt werden, während fedpol die Resultatmasken erstellt. Wenn die Kantone also einen rechtlichen Warnhinweis direkt in die Suchmasken aufnehmen möchten, können sie sich an ihre Dienstanbieter wenden. Auf unseren Wunsch wurde diese Thematik von der Gemeinsamen Kontrollinstanz Schengen (GKI) bei ihrer Sitzung vom 4. Oktober 2012 behandelt. Die Reaktionen der Mehrheit der Mitgliedstaaten deuten darauf hin, dass in den verschiedenen verwendeten Systemen kein rechtlicher Warnhinweis eingeführt wurde. Die GKI hält es somit nicht für zweckmässig, die Einführung solcher Warnhinweise zu empfehlen. Sie betont hingegen, vor allem die Schulung der Nutzer müsse mit Nachdruck gefördert werden.

Somit konnten wir die Koordinationsgruppe Schengen bei ihrer Sitzung vom 15. November 2012 über die Ergebnisse unserer Nachforschungen informieren. Wir kamen zum Schluss, dass es wichtig ist, das Schwergewicht auf die Ausbildung der Nutzer der Systeme RIPOL, SIS und ZEMIS zu legen, um den von der Koordinationsgruppe geäusserten Bedenken Rechnung zu tragen.

1.4.4 Abkommen mit den Vereinigten Staaten über den Verbleib der Schweiz im Visa-Waiver-Program

Die Unterzeichnung des PCSC-Abkommens mit den USA zum Austausch von Fingerabdruck- und DNA-Daten und des Memorandum of Understanding HSPD-6 über den Austausch von Daten zu mutmasslichen und bekannten Terroristen ermöglicht der Schweiz den Verbleib im amerikanischen Programm für eine visumsfreie Einreise (Visa-Waiver-Program). In diese beiden Urkunden sind Datenschutzregeln aufgenommen worden.

Das PCSC-Abkommen (Cooperation in Preventing and Combating Serious Crime) sieht den Austausch von Fingerabdruck- und DNA-Daten zur Bekämpfung von Schwerkriminalität vor. Der Austausch findet in zwei Phasen statt. Zuerst erfolgt eine Abfrage der Datenbank des ersuchten Staates, um festzustellen, ob das entsprechende Profil dort vorhanden ist oder nicht («Hit-/No-Hit-Verfahren»). Ergibt die Abfrage einen Treffer («Hit»), können in einem zweiten Schritt Personendaten und weitere Informationen ausgetauscht werden. Die Übermittlung dieser Daten ist dem nationalen Recht des ersuchten Staates unterworfen. Dank der Datenschutzbestimmungen des PCSC-Abkommens können die Rechte der betroffenen Personen gewährleistet werden. Die allgemeinen Datenschutzprinzipien sind klar aufgeführt. Besonders schützenswerte Daten werden einem zusätzlichen Schutz unterstellt. Privatpersonen können ihre Rechte (Auskunft, Berichtigung, Blockierung und Löschung) in Anwendung der nationalen Gesetzgebungen geltend machen. Die Datenschutzbehörde kann auch bei der Behörde des anderen Staates intervenieren.

Das Memorandum of Understanding (MoU) mit dem sperrigen Titel «Homeland Security Presidential Directive 6» (HSPD-6) sieht den Austausch von Daten über Personen vor, die mit terroristischen Aktivitäten in Zusammenhang gebracht werden. Diese Urkunde schafft keine neuen Rechte und Pflichten. Ihr Ziel ist die Optimierung der bestehenden Zusammenarbeit auf der Grundlage geltenden Rechts. Sie besagt auch, dass im Bereich des Datenschutzes die innerstaatlichen gesetzlichen Grundlagen gelten.

Wir haben das Bundesamt für Polizei (fedpol) mit der Prüfung der verschiedenen Dokumente im Rahmen der Verhandlungen mit den amerikanischen Behörden unterstützt. Die Unterzeichnung des PCSC-Abkommens und des MoU HSPD-6 ermöglicht der Schweiz den Verbleib im Programm für eine visumsfreie Einreise (Visa-Waiver-Program) in die USA. Schweizerinnen und Schweizer können weiterhin ohne Visum für einen Kurzaufenthalt (maximal 90 Tage) in die USA einreisen.

Risiken einer Persönlichkeitsverletzung für die betroffenen Personen, also für Personen, deren Fingerabdruckdaten und DNA-Profile bearbeitet werden, sind nicht ausgeschlossen. Es ist indes festzuhalten, dass diese Risiken auch in der bisher geltenden Gesetzgebung bestehen, und dass die in den beiden Dokumenten enthaltenen Datenschutzbestimmungen einen Schutz der Rechte der betroffenen Personen sicherstellen.

1.4.5 Totalrevision des Bundesgesetzes zur Überwachung des Post- und Fernmeldeverkehrs

Im Rahmen der Ämterkonsultation haben wir zum Entwurf des totalrevidierten Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs Stellung genommen. Neu soll eine gesetzliche Grundlage für den Einsatz von Informatikprogrammen eingeführt werden. Eine solche forderten wir auch für die Herausgabe von Inhaltsdaten bei Dienstleistungen, welche sich auf Fernmeldedienste stützen.

Nachdem wir bereits in den letzten Jahren zu den diversen Entwürfen der Gesetzgebung betreffend die Überwachung des Post- und Fernmeldeverkehrs Stellung genommen hatten, bekamen wir auch die Möglichkeit, uns zum neusten Entwurf des totalrevidierten Bundesgesetzes zu äussern. Aus unserer Sicht soll der Datenschutz eine effiziente und effektive Verbrechensbekämpfung nicht verhindern. Mit der Überwachung des Post- und Fernmeldeverkehrs wird jedoch in ein verfassungsmässig geschütztes Grundrecht eingegriffen. Dafür braucht es formell und materiell gesetzliche Grundlagen, die zudem genügend bestimmt sind.

Nachdem wir uns früher zu den fehlenden gesetzlichen Bestimmungen für den Einsatz von Informatikprogrammen (auch «Staatstrojaner» genannt) geäussert hatten (vgl. unseren 19. Tätigkeitsbericht 2011/2012, Ziff. 1.4.8), soll mit dem uns vorgelegten Gesetzesentwurf unter anderem eine solche Bestimmung geschaffen werden.

Eine ähnliche gesetzliche Grundlage forderten wir auch für die Herausgabe von Inhaltsdaten (z.B. Gerätebackups, Adressbücher oder von Benutzern erstellte Dokumente) durch Anbieter von abgeleiteten Kommunikationsdiensten wie Clouddienstleister oder Speicherplatzanbieter. Die Herausgabe von im Internet gespeicherten Inhaltsdaten soll nach unserer Auffassung explizit in einem Gesetz im formellen Sinn geregelt werden.

1.4.6 Nachrichtendienstgesetz

Der Entwurf zum Nachrichtendienstgesetz in seiner im zweiten Vernehmlassungsverfahren überwiesenen Fassung wurde unter dem Gesichtspunkt des Datenschutzes in mehreren Punkten verbessert. Andere Elemente, wie etwa gewisse Mittel zur Informationsbeschaffung oder auch der Ausschluss des Nachrichtendienstes des Bundes vom Geltungsbereich des Öffentlichkeitsgesetzes sind hingegen immer noch problematisch.

Der Entwurf zum Nachrichtendienstgesetz war Gegenstand von zwei Ämterkonsultationen. Der im April 2012 vorgelegte Gesetzesentwurf enthielt unter dem Aspekt des Datenschutzes mehrere sehr problematische Elemente. Die Rechtsvorschriften betreffend die verschiedenen Datenbanken des Nachrichtendienstes des Bundes (NDB) waren unzulänglich. Der Entwurf sah sogar ein für die betroffenen Personen noch nachteiligeres indirektes Auskunftsrecht vor als die vor dem 16. Juli 2012 geltende Regelung. Der im Oktober 2012 in die Vernehmlassung geschickte überarbeitete Entwurf bringt datenschutztechnisch einige Verbesserungen. So beziehen sich die Massnahmen zur Beschaffung bewilligungspflichtiger Informationen auf eine begrenzte Anzahl Fälle und müssen vom Bundesverwaltungsgericht genehmigt werden. Die Bestimmungen über die Datenbanken sind sehr viel detaillierter als die im Rahmen der ersten Vernehmlassung vorgeschlagenen Vorschriften. Bezüglich des Auskunftsrechts sieht der neue Entwurf eine Regelung vor, die mit derjenigen des Bundesgesetzes über die polizeilichen Informationssysteme des Bundes vergleichbar ist.

Mehrere Punkte des Entwurfs sind indes nicht befriedigend. Unseres Erachtens darf der NDB nicht über mehr Ermittlungsmöglichkeiten verfügen als die Strafverfolgungsbehörden. Der Entwurf muss daher entsprechend den Normen angepasst werden, die im Rahmen der Revision des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs erlassen werden sollen. Es stellt sich auch die Frage nach der Vereinbarkeit einer in der Schweiz vorgenommenen Bearbeitung von im Ausland unrechtmässig beschafften Personendaten mit der schweizerischen Datenschutzgesetzgebung. Die vorgesehenen neuen Zugriffsmöglichkeiten online auf Datensammlungen der Bundesverwaltung sind nicht oder nicht ausreichend begründet. Schliesslich sind wir gegen den Vorschlag, den NDB vom Geltungsbereich des Bundesgesetzes über das Öffentlichkeitsprinzip der Verwaltung auszunehmen (vgl. Ziff. 2.5.4 des vorliegenden Tätigkeitsberichts).

Der Entwurf zum Nachrichtendienstgesetz ist in der externen Vernehmlassung bei den interessierten Kreisen, und wahrscheinlich wird noch im Jahr 2013 eine Botschaft an die Eidgenössischen Räte gehen.

1.4.7 Automatische Fahrzeugfahndung und Verkehrskontrolle

Die von den Systemen der Automatischen Fahrzeugfahndung und Verkehrskontrolle der Eidgenössischen Zollverwaltung durchgeführten Überprüfungen beruhen auf angemessenen gesetzlichen Grundlagen. Die Bereitstellung eines Indexes der im System RIPOL ausgeschriebenen Fahrzeugnummernschilder durch das Bundesamt für Polizei und der Zugang der Kantonspolizeien zu diesem Index entsprechen dem geltenden Bundesrecht. Es ist Sache der kantonalen Datenschutzbehörden, die durch die Kantonspolizeien in diesem Zusammenhang durchgeführten Überprüfungen zu beurteilen.

Zusammen mit dem Rechtsdienst des Bundesamtes für Polizei (fedpol) haben wir die Systeme der automatischen Fahrzeugfahndung und Verkehrskontrolle (AFV) einer Beurteilung unterzogen. Wir prüften insbesondere die Konformität mit der geltenden Gesetzgebung. Die Beurteilung stützte sich auf das AFV-Gesamtkonzept der Schweizerischen polizeitechnischen Kommission und beschränkte sich auf die anhand der Daten des Systems RIPOL vorgenommenen Überprüfungen. Die Zugriffsrechte auf RIPOL sind im Bundesgesetz über die polizeilichen Informationssysteme des Bundes und in der Verordnung über das automatisierte Polizeifahndungssystem geregelt. Diese Bestimmungen erteilen den Kantonspolizeien und der Eidgenössischen Zollverwaltung (EZV) ausdrücklich ein Online-Zugriffsrecht zu Fahndungszwecken.

Die Bereitstellung eines Verzeichnisses mit den in RIPOL ausgeschriebenen Autonummern durch fedpol ist ebenfalls rechtskonform. Auch das Verhältnismässigkeitsprinzip wird eingehalten. Die Datenabfrage wird nämlich nur zu Fahndungszwecken verwendet, und die AFV-Anlagen decken nicht das gesamte Staatsgebiet ab (die festen Anlagen sind auf die Verkehrsknotenpunkte des Strassennetzes begrenzt, und die mobilen Anlagen betreffen nur eine beschränkte Anzahl Dienstwagen). Überdies werden die Daten unverzüglich gelöscht, wenn sich kein Treffer ergibt. Im Falle eines Treffers hingegen werden die Daten spätestens nach 30 Tagen gelöscht. Es ist auch zu erwähnen, dass der RIPOL-Index nur die unbedingt notwendigen und nicht die Gesamtheit der Daten enthält. Wir konnten weiter feststellen, dass die Kantonspolizeien und die EZV die Datensicherheitsvorschriften

einhalten. Die Übermittlung des Indexes erfolgt über eine chiffrierte Verbindung, und er wird in den AFV-Systemen in verschlüsselter Form aufbewahrt. Die Bereitstellung eines Indexes mit den ausgeschriebenen Autonummern im System RIPOL durch fedpol und der Zugriff der Kantonspolizeien auf diesen Index sind damit im Einklang mit dem geltenden Bundesrecht.

Wir haben auch die Überprüfungen untersucht, welche die EZV ausgehend von anderen Daten des Bundes durchführt. So enthält der Index der AFV-Systeme der EZV die ausgeschriebenen Fahrzeuge aus RIPOL und die Nummern der Kontrollschilder von Fahrzeugen, die mit Ermittlungen der Zollstellen und des Grenzwachtkorps in Verbindung stehen. Die Autonummer sowie ein Bild des Kontrollschildes und des Fahrzeugs oder eines Fahrzeugteils werden 30 Tage in der Datenbank für die Personenfahndung aufbewahrt. Die gesetzlichen Grundlagen für die Bearbeitung durch die EZV im Rahmen der AFV-Systeme sind das Zollgesetz, die Verordnung über den Einsatz von Bildaufnahme-, Bildaufzeichnungs- und anderen Überwachungsgeräten durch die EZV und die Verordnung über die Bearbeitung von Personendaten bei der EZV. Die Überprüfungen, die von den AFV-Systemen aufgrund des Indexes der ausgeschriebenen Fahrzeuge im System RIPOL und der Kontrollschilder von Fahrzeugen im Zusammenhang mit Ermittlungen der Zollstellen und des Grenzwachtkorps durchgeführt werden, beruhen damit auf ausreichenden Gesetzesgrundlagen.

Es ist Sache der kantonalen Datenschutzbehörden, über die Bearbeitung von Personendaten durch die Kantonspolizeien und namentlich über die Überprüfungen der Kantonspolizeien aufgrund des Indexes der im System RIPOL ausgeschriebenen Fahrzeuge und aufgrund von kantonalen Daten zu entscheiden.

1.4.8 Auskunftsrecht über Daten des Informationssystems ISIS: altes und neues Verfahren

Vom 1. Januar bis zum 15. Juli 2012 behandelten wir noch 13 Auskunftsgesuche betreffend das Informationssystem ISIS nach der alten Regelung. Seit dem 16. Juli 2012 gehen Gesuche direkt an den vom Nachrichtendienst des Bundes, während der EDÖB seinerseits für die Bearbeitung der Überprüfungsgesuche zuständig ist.

Das Informationssystem ISIS war die letzte Datensammlung, für die noch der Mechanismus des sogenannten indirekten Auskunftsrechts bestand. Am 16. Juli 2012 wurde dieses Verfahren durch das direkte Auskunftsrecht ersetzt, das für die Gesamtheit der von den Bundesorganen geführten Datensammlungen gilt (vgl. unseren 19. Tätigkeitsbericht 2011/2012, Ziff. 1.4.4 und 1.4.5). Seit diesem Datum

werden die Auskunftsgesuche zu ISIS direkt durch den Inhaber der Datensammlung, den Nachrichtendienst des Bundes (NDB), behandelt. Zwischen dem 1. Januar und dem 15. Juli 2012 haben wir noch 13 Auskunftsgesuche bearbeitet. Seit dem 16. Juli 2012 leiten wir die dem neuen Recht unterstellten Gesuche an den NDB weiter. Nachdem die betroffene Person die Antwort des NDB erhalten hat, hat sie nach dem neuen Recht die Möglichkeit, ein Überprüfungsgesuch bei uns einzureichen.

Bezüglich des N-SIS und der Datensammlungen JANUS und GEWA des Bundesamtes für Polizei (fedpol) hatten wir im Jahr 2012 sieben Fälle von Überprüfungsgesuchen zu bearbeiten.

1.4.9 Pilotversuch mit dem Informationssystem ISAS

Der Bundesrat hat vom Evaluationsbericht über den Pilotversuch ISAS Kenntnis genommen und die Fortführung der Bearbeitung bewilligt. In einer Stellungnahme in diesem Rahmen erklärten wir, dass wir nichts gegen eine Fortsetzung des Pilotversuchs einzuwenden hätten, soweit die Zahl der Teilnehmer weiterhin begrenzt bleibt. Auf eine spezifische Anfrage des NDB zu diesem Punkt hin haben wir indes eine punktuelle Erhöhung dieser begrenzten Teilnehmerzahl akzeptiert.

Gemäss Artikel 17a DSG legte uns der Nachrichtendienst des Bundes (NDB) im Mai 2012 den Entwurf eines Evaluationsberichts zum Pilotversuch ISAS zuhanden des Bundesrats zur Stellungnahme vor. Dieses Dokument beschreibt nach zweijähriger Testphase den Ablauf des Pilotversuchs. Es erwähnt auch die Ausarbeitung der Gesetzesgrundlage im formellen Sinn für das Informationssystem ISAS im Rahmen einer Teilrevision des Bundesgesetzes über den zivilen Nachrichtendienst (ZNDG). Im Entwurf des Evaluationsberichts schlägt der NDB dem Bundesrat die Fortführung der Bearbeitung vor.

In der Vernehmlassung schlug der NDB vor, völlig auf eine Einschränkung der Anzahl der in den Pilotversuch einbezogenen Mitarbeiter zu verzichten. Die begrenzte Anwendung eines Pilotversuchs (Abstecken der betroffenen Bereiche und Mitarbeiter) ist Teil der Massnahmen, mit denen Persönlichkeitsverletzungen eingeschränkt werden sollen. Die Abschaffung der Maximalzahl betroffener Mitarbeiter würde praktisch einem definitiven Betrieb des Informationssystems ISAS ohne ausreichende gesetzliche Grundlage gleichkommen. Aus diesem Grunde stellten wir uns dagegen.

Wir haben, im Lichte dieser Ausführungen, den Entwurf des Evaluationsberichts und seine Anhänge geprüft und uns für eine Fortführung der Datenbearbeitung in ISAS ausgesprochen, vorausgesetzt, dass sie so lange im begrenzten Rahmen des Pilotversuchs erfolgt, bis eine formelle Gesetzesgrundlage in Kraft tritt und damit der definitive Betrieb des Informationssystems ISAS möglich wird. Der Bundesrat hat vom Bericht Kenntnis genommen und die Fortführung der Bearbeitung bewilligt.

In Anwendung von Artikel 27 VDSG, der ein Bundesorgan verpflichtet, uns über jede wichtige Änderung eines Pilotversuchs zu informieren, ersuchte uns der NDB im September 2012 um Stellungnahme zur Erhöhung der Zahl der daran beteiligten Mitarbeiter. Obwohl der begrenzte Rahmen des Pilotversuchs wesentlich ist und beibehalten werden muss, wie wir das in unserer Stellungnahme zum Evaluationsbericht des NDB betont hatten, ist doch zu erwähnen, dass sich das Pilotprojekt ISAS in einer neuen Phase, nämlich in der Entwicklung des Informationssystems im Hinblick auf seinen definitiven Betrieb befindet. In diesem Kontext und angesichts der im Gesuch des NDB angeführten Gründe hat eine vernünftige Erhöhung der Anzahl der am Pilotversuch ISAS beteiligten Mitarbeiter keine erheblichen Auswirkungen auf die Risiken einer Persönlichkeitsverletzung der betroffenen Personen. Aus diesem Grund haben wir uns zur Erhöhung der Obergrenze der Anzahl der im Pilotversuch ISAS aktiven Mitarbeiter positiv geäussert.

1.4.10 Informationssicherheitsgesetz: Mitarbeit bei der Arbeitsgruppe FOGIS

Die Informationsschutzverordnung soll längerfristig durch ein Gesetz über die Informationssicherheit abgelöst werden, das den Geltungsbereich erweitern wird. Zu diesem Zweck wurde eine departementsübergreifende Arbeitsgruppe eingesetzt. Ihr Ziel war es, die Informationsschutzmassnahmen mit den Anforderungen des Datenschutzes, dem Öffentlichkeitsprinzip in der Verwaltung und der physischen, elektronischen und persönlichen Sicherheit in Einklang zu bringen.

Der Bundesrat hat am 12. Mai 2010 beschlossen, die Verordnung über den Schutz von Informationen des Bundes (Geltungsdauer bis zum 31.12.2014) abzuändern. Er beauftragte das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS), eine departementsübergreifende Arbeitsgruppe, bestehend aus Rechts- und Technikexperten, für die Ausarbeitung eines Gesetzesentwurfs zur Informationssicherheit einzusetzen. Dieser Gesetzesentwurf soll die

geltenden Informationsschutzvorschriften auf die Umsetzung der vom Bundesrat 2009 beschlossenen Massnahmen zur Verbesserung der Informationssicherheit ausdehnen. Diese Massnahmen umfassen naturgemäss auch Aspekte des Datenschutzes, die wiederum von den Bedingungen des Öffentlichkeitsprinzips in der Verwaltung abhängen. In diesem pluri- und interdisziplinären Kontext haben rund zwanzig Rechts- und Technikexperten aus mehreren eidgenössischen Departementen unter der Leitung von Markus Müller, Rechtsprofessor an der Universität Bern, mehrfach getagt.

Zahlreiche Themen wurden in diesem Rahmen erörtert. Bezüglich der Klassifizierung der Informationen ist festzuhalten, dass eine Variante mit drei Stufen (intern/vertraulich/geheim) und eine mit zwei Stufen (vertraulich/geheim) gewählt wurden. Unter dem Gesichtspunkt der Öffentlichkeit der Verwaltung ist das Zwei-Stufen-Modell am besten geeignet, während auf der Ebene der technischen Massnahmen eine Parallele zwischen dem Drei-Stufen-Modell und der «üblichen» Hierarchie des Datenschutzes von Personendaten (normal/sensibel/lebenswichtig) gezogen werden konnte. Das Drei-Stufen-Modell scheint auch für den Austausch von klassifizierten Informationen mit dem Ausland besser geeignet zu sein. Die zur Bearbeitung von klassifizierten oder sensiblen Informationen eingesetzten Informations- und Kommunikationstechnologien (IKT) werden ihrerseits nach generellem, hohem oder sehr hohem Schutzbedarf eingeteilt. Die Sicherheitsprüfungen bei Personen, die regelmässig vertrauliche oder geheime Informationen bearbeiten, folgen im Wesentlichen den geltenden Bestimmungen des BWIS, das eine Grundsicherheitsprüfung, eine erweiterte Prüfung und eine erweiterte Prüfung mit Befragung vorsieht. Bezüglich des Betriebssicherheitsverfahrens schreibt es Unternehmen, die Zugang zu vertraulichen (oder geheimen) Informationen oder zu IKT-Mitteln mit (sehr) hoher Schutzwürdigkeit haben, vor, dass sie über eine Sicherheitserklärung verfügen müssen, die sowohl die operativen als auch die personellen Risiken über allfällige Sicherheitsprüfungen abdeckt.

Der aus all diesen Überlegungen hervorgegangene Gesetzesentwurf, der noch einem Vernehmlassungsverfahren unterzogen wird, soll auch die interne Organisation und die Koordination der zahlreichen beteiligten Bundesämter regeln. Insbesondere die Ausarbeitung der Informationssicherheitsstrategie des Bundes, der Erlass technischer Vorgaben im Bereich der Informationssicherheit, die Durchführung der Personensicherheitsprüfungen und der Betriebssicherheitsverfahren, die Standardisierung gewisser Mittel, Ausrüstungen, Produkte oder Dienstleistungen im Bereich der Sicherheit, und eine jährliche Berichterstattung an den Bundesrat sind noch anstehende Aufgaben. Schliesslich wird der Vollzug auch externe Stellen betreffen, wie etwa die Kantone, die Kontakt zu vom Bund klassifizierten

Informationen haben, oder ausländische Staaten, mit denen wir klassifizierte Daten austauschen, wenn entsprechende internationale Verträge existieren. Auch die Koordination zwischen internen und externen Organen wird sichergestellt werden müssen.

Wir werden weiterhin an den laufenden Arbeiten mitwirken, damit dem Datenschutz, der Datensicherheit sowie dem Öffentlichkeitsprinzip Rechnung getragen wird.

1.5 Gesundheit und Forschung

1.5.1 SwissDRG: Zertifizierung der neuen Datenannahmestellen

Für die Entgegennahme von DRG-Rechnungen müssen die Krankenversicherer sogenannte Datenannahmestellen einrichten. Diese müssen zwingend über eine Datenschutzzertifizierung verfügen. Damit wird in der Schweiz erstmals das Obligatorium einer Datenschutzzertifizierung eingeführt.

Kernstück der neuen Spitalfinanzierung bilden die Fallpauschalen («Diagnoses Related Groups», kurz DRG). Die Leistungen der Spitäler im akut-somatischen Bereich werden nach qualifizierten Kriterien wie Hauptdiagnose, Nebendiagnosen und Behandlungen (Prozeduren) sowie weiteren Aspekten abgegolten. Damit die Leistungen durch die Krankenversicherer korrekt vergütet werden können, sind spezielle Rechnungen notwendig. Sie beinhalten neben den administrativen Daten auch die notwendigen medizinischen Angaben in codierter Form. Mit jeder DRG-Rechnung erhalten die Krankenversicherer also sehr detaillierte Gesundheitsdaten über die versicherten Personen.

Gleichzeitig ist aber klar, dass nur ein kleiner Anteil der Rechnungen durch die Versicherer tatsächlich detailliert geprüft wird. Deshalb musste zur Wahrung der Verhältnismässigkeit ein Prozess installiert werden, der sicherstellt, dass die Versicherer nur dann Zugang zu den Gesundheitsdaten auf der DRG-Rechnung erhalten, wenn sie diese tatsächlich einer vertieften Überprüfung unterziehen. Um dies zu erreichen hat der Bundesrat in der Krankenversicherungsverordnung (KVV) festgehalten, dass die Krankenversicherer für die Entgegennahme von DRG-Rechnungen über eine nach Datenschutzgesetz zertifizierte Datenannahmestelle verfügen müssen. Sie ist dem Versicherer vorgelagert und hat die automatisierte Triage der eingehenden DRG-Rechnungen zur Aufgabe.

Nach einem definierten Regelwerk werden die Rechnungen plausibilisiert. Je nach Resultat wird die Rechnung durch die Datenannahmestelle an die zuständige Stelle des Versicherers übermittelt. Eine unauffällige Rechnung wird ohne Weiteres zur Zahlung freigegeben. Der Versicherer erhält keine Kenntnis der codierten Gesundheitsdaten. Eine für den Vertrauensarzt bestimmte Rechnung wird durch die Datenannahmestelle direkt an diesen übermittelt. Auch hier bearbeitet die Stelle die codierten Gesundheitsdaten nicht; sie stellt lediglich fest, dass die Rechnung für den Vertrauensarzt bestimmt ist, und leitet sie unverzüglich weiter. Der Versicherer erhält selbstverständlich ebenfalls keine Kenntnis über Gesundheitsdaten.

Eine auffällige Rechnung wird durch die Datenannahmestelle an den Versicherer übermittelt und dort detailliert geprüft. Der Versicherer erhält den ganzen medizinischen Datensatz und kann, falls das zur Prüfung der Rechnung notwendig ist, vom Leistungserbringer zusätzliche Informationen einfordern. Konkret handelt es sich dabei um Austritts- und Operationsberichte. Nur so kann eine DRG-Rechnung wirklich überprüft und nicht nur plausibilisiert werden. Auch eine Überprüfung der Codierung ist nur so möglich. Fordert der Versicherer zusätzliche Informationen ein, so hat er zwingend die versicherte Person darüber zu informieren. Diese kann dann die Übermittlung der zusätzlichen Informationen an den Vertrauensarzt verlangen.

Zusammenfassend kann also festgehalten werden, dass die Datenannahmestelle eine automatisierte Triage der DRG-Rechnungen vornimmt, nur die auffälligen Rechnungen an den Versicherer übermittelt und damit die Wahrung des Grundsatzes der Verhältnismässigkeit garantiert. Damit diese wichtige Aufgabe durch die Datenannahmestelle tatsächlich wahrgenommen wird und nicht übermässig Rechnungen an den Versicherer übermittelt werden, und auch aufgrund des Umstands, dass die Stelle durch den Versicherer oder in dessen Auftrag betrieben wird, kam der Bundesrat zum Schluss, die Datenannahmestelle müsse zwingend gemäss Datenschutzgesetz zertifiziert sein. Da der Aufbau einer solchen Stelle und deren Zertifizierung eine gewisse Zeit beanspruchen, hat der Bundesrat eine Übergangslösung vorgesehen. Solange der Versicherer über keine zertifizierte Datenannahmestelle verfügt, dürfen DRG-Rechnungen von den Spitälern nur an den Vertrauensarzt übermittelt werden. Ab dem 1. Januar 2014 müssen dann aber alle Krankenversicherer über eine zertifizierte Datenannahmestelle verfügen. Die Übermittlung an den Vertrauensarzt ist ab dann nicht mehr zulässig.

Aus der Sicht des Datenschutzes bedeutet diese Lösung einen wichtigen Schritt. Einerseits konnten wir bei der Ausarbeitung der Verordnungsregelung massgeblich mitarbeiten und so die Datenschutzmassnahmen der Krankenversicherer konkret mitgestalten. Andererseits hat die Datenschutzzertifizierung durch das Obligatorium einen neuen Stellenwert erhalten. In einem Bereich, in dem riesige Mengen von besonders schützenswerten Personendaten bearbeitet werden, müssen die Datenbearbeiter zwingend über ein Zertifikat gemäss Datenschutzgesetz verfügen. Wie genau die Datenannahmestelle aufgebaut wird, liegt in der Verantwortung der Versicherer und ist auch von deren bestehenden Struktur abhängig. Zweifellos werden sich zahlreiche Versicherer eines Dienstleisters bedienen, da sich der Betrieb einer eigenen Datenannahmestelle für sie nicht lohnt oder weil schon bisher Datenbearbeitungen im Bereich der Leistungsabrechnungen ausgelagert durchgeführt worden sind. Schon jetzt zeigt sich, dass die grossen

Krankenversicherer die Übergangsfrist nicht beanspruchen werden. Sie verfügen schon seit dem 1. Januar 2013 über eine zertifizierte Datenannahmestelle.

Für uns wird durch die neue Regelung ein erheblicher Mehraufwand entstehen. Wir müssen die Datenannahmestellen und ihre Zertifizierungen kontrollieren. Da diese Stellen entsprechend den tatsächlichen Verhältnissen durchaus unterschiedlich aufgebaut sein können, werden auch die Zertifizierungsprozesse variieren. Wir werden auch die Dienstleister, welche sich als Datenannahmestelle haben zertifizieren lassen, kontrollieren, wobei hier die durch die Auftragsdatenbearbeitung entstehenden spezifischen Ansprüche an die Zertifizierungen von grosser Bedeutung sein werden. Diese komplexe Aufgabe wird der EDÖB nur mit zusätzlichen Personalressourcen erfüllen können.

Im Sinne der Transparenz für die versicherten Personen und für die Branche publizieren wir, wie in der KVV vorgegeben, seit dem 1. Januar 2013 das Verzeichnis der nach Datenschutzgesetz zertifizierten Datenannahmestellen.

1.5.2 eHealth Schweiz und ePatientendossier: Stand der Dinge

Viele Ideen aus den eHealth-Projekten konkretisieren sich im Bundesgesetz über das elektronische Patientendossier, welches langsam Gestalt annimmt. Wir haben uns an den Entwurfsarbeiten des Bundesamtes für Gesundheit beteiligt. Einige wichtige Punkte konnten wir in unserem Sinne beeinflussen.

Wir haben uns im Berichtsjahr wiederum intensiv mit eHealth und insbesondere mit wichtigen Fragen betreffend das Bundesgesetz über das elektronische Patientendossier beschäftigt. Wichtig erscheint uns hier, dass an der Freiwilligkeit für die Patientinnen und Patienten festgehalten wird, dass ihre informationelle Selbstbestimmung gewährleistet ist und dass ein sektorieller Identifikator für eHealth geschaffen wird.

Gemäss unserer Auffassung ist es für das Gelingen von eHealth in der Schweiz ausschlaggebend, dass die Patientinnen und Patienten sich freiwillig für ein elektronisches Patientendossier entscheiden können. Ein Zwang im besonders heiklen Gesundheitsbereich würde das Gesamtprojekt gefährden. Glücklicherweise wird diese Freiwilligkeit von allen Interessengruppen anerkannt.

Entscheiden sie sich für ein elektronisches Patientendossier, soll die informationelle Selbstbestimmung für die Patientinnen und Patienten gewährleistet sein. Einträge in das Dossier sollen deshalb nur mit ihrer Zustimmung erfolgen können.

Mittels eines geeigneten Rollen- und Berechtigungkonzepts sollen die Patienten zudem die Möglichkeit haben, die sie betreffenden Informationen gezielt den Personen zugänglich zu machen, die gemäss ihrem Willen Zugang haben sollen. Auch diese Forderung wird von den Interessengruppen grundsätzlich anerkannt. Allerdings wird hier zum Teil darauf hingewiesen, dass das elektronische Patientendossier seinen praktischen Nutzen verlieren könnte, wenn sich Behandelnde nicht auf die Vollständigkeit der darin enthaltenen Informationen verlassen können. Hierzu halten wir fest, dass eine behandelnde Ärztin nie sicher sein kann, dass der Patient alle Informationen preisgibt. Viel entscheidender ist unseres Erachtens die Korrektheit der im elektronischen Patientendossier enthaltenen Informationen.

Bezüglich des Patientenidentifikators stellen wir die klare Forderung, dass in eHealth die Sozialversicherungsnummer (AHVN13) nicht in Verbindung mit Gesundheitsdaten verwendet wird (vgl. unseren 19. Tätigkeitsbericht 2011/2012, Ziff. 1.5.2). Wir sind zu diesem Thema in ständigem Kontakt mit den wichtigsten Organen. Das genaue Verfahren stand zum Ende des Berichtsjahres noch nicht fest. Eine gute Lösung zeichnet sich allerdings ab, welche die von uns geforderte sektorielle Nummer zur Identifikation der Patienten nutzen wird.

1.5.3 Datenschutzaspekte bei Versandhandelsapotheken

Im Rahmen einer Sachverhaltsabklärung im Bereich der nicht-rezeptpflichtigen Medikamente bei einer Versandhandelsapotheke stellten wir fest, dass mittels AGB das Auskunftsrecht eingeschränkt wird. Wir erachten dieses Vorgehen als sehr problematisch. Die Zulässigkeit müsste aber durch ein Gericht geklärt werden.

Der Versandhandel mit Medikamenten ist in der Schweiz grundsätzlich nicht zulässig. Eine Ausnahmebewilligung kann aber erteilt werden, wenn bestimmte Voraussetzungen zur Gewährleistung der Patientensicherheit gegeben sind. Eine dieser Voraussetzungen lautet, dass alle Medikamente nur abgegeben werden dürfen, wenn ein Rezept vorliegt. Dies führt dazu, dass Patientinnen und Patienten, welche auf diesem Weg ein nicht-rezeptpflichtiges Medikament beziehen wollen, vorgängig eine Ärztin oder einen Arzt konsultieren müssen, damit sie der Versandhandelsapotheke ein entsprechendes Rezept vorlegen können. Vor diesem Hintergrund liegt natürlich der direkte Gang in die Apotheke nahe.

Eine Versandhandelsapotheke verlangt jetzt von der Kundschaft bei der Bestellung eines nicht-rezeptpflichtigen Medikaments, wenn nicht schon ein Rezept vorhanden ist, das Ausfüllen eines Gesundheitsfragebogens, anhand dessen eine nicht-involvierte Arztperson ein Rezept ausstellen und an die Versandhandelsapotheke

übermitteln kann, worauf das Medikament ausgeliefert wird. Die Bestellerinnen und Besteller müssen dabei den AGB der Apotheke zustimmen und sich damit auch einverstanden erklären, dass sie auf die Herausgabe der intern erstellten Dokumente (also auch des Rezepts) und die Bekanntgabe des Namens der rezeptierenden Arztperson verzichten.

Wir haben im Rahmen der Sachverhaltsabklärung den Bestellungsablauf und die AGB der Versandhandelsapotheke geprüft. Das Vorgehen muss als sehr problematisch bezeichnet werden, da hier das Auskunftsrecht, das als zentraler Pfeiler des Datenschutzrechts bezeichnet werden kann, massiv eingeschränkt wird. Letztlich stellt sich aber die Frage, ob im Rahmen der privatrechtlichen Vertragsautonomie die beschriebene Einschränkung des Auskunftsrechts mittels Anerkennung der AGB rechtsgültig Bestandteil des Vertrages geworden ist. Diese Frage müsste durch ein Gericht entschieden werden.

1.5.4 Bearbeitungsreglemente der Krankenkassen: Pflicht zur Übermittlung an den EDÖB

Seit Januar 2012 sieht das Bundesgesetz über die Krankenversicherung vor, dass die ihm unterstellten Versicherer Datenbearbeitungsreglemente erstellen, uns zur Beurteilung vorlegen und öffentlich zugänglich machen. Diese Bestimmung nimmt den Artikel 21 der Verordnung zum Bundesgesetz über den Datenschutz auf und erweitert ihn. Im Laufe des Jahres 2012 haben wir den Versicherern, die uns ihr Bearbeitungsreglement noch nicht übermittelt hatten, eine Mahnung zukommen lassen.

Artikel 84b des Bundesgesetzes über die Krankenversicherung (KVG) schreibt unter dem Titel «Sicherstellung des Datenschutzes durch die Versicherer» Folgendes vor: Die Versicherer treffen die erforderlichen technischen und organisatorischen Massnahmen zur Sicherstellung des Datenschutzes und erstellen insbesondere die gemäss Verordnung zum Bundesgesetz über den Datenschutz (VDSG) notwendigen Bearbeitungsreglemente. Diese werden uns zur Beurteilung vorgelegt und sind öffentlich zugänglich.

Diese Bestimmung übernimmt damit die bereits seit 1993 aufgrund von Artikel 21 VDSG geltende Verpflichtung, verlangt aber zusätzlich, dass uns die Bearbeitungsreglemente zur Beurteilung vorzulegen und öffentlich zugänglich zu machen sind. Gemäss der neuen Bestimmung müssen uns somit die Versicherer ab dem 1. Januar 2012 ihre Bearbeitungsreglemente automatisch übermitteln und sie öffentlich machen, beispielsweise im Internet oder in anderer Form, um interessierte

Personen zu informieren. Die Ausarbeitung eines solchen Bearbeitungsreglements und seine Veröffentlichung durch den Versicherer sind obligatorisch, unabhängig von unserer Beurteilung.

Das Bundesamt für Gesundheit wies die KVG-Versicherer schon in seinem Rundschreiben 7.1 vom 25. August 2011 auf die gesetzliche Verpflichtung unter diesem neuen Artikel des KVG hin. Nachdem wir jedoch festgestellt hatten, dass uns zahlreiche Versicherungen ihr Reglement nicht übermittelt hatten, richteten wir am 23. Oktober 2012 eine schriftliche Mahnung an alle betroffenen Versicherungen. Darin setzten wir den Versicherern, die ihrer Verpflichtung noch nicht nachgekommen waren, eine Frist bis zum 30. November 2012 für die Einreichung der erwähnten Bearbeitungsreglemente.

Inzwischen haben uns die meisten betroffenen Versicherer ihre Bearbeitungsreglemente zukommen lassen.

1.5.5 Bundesgesetz über ein Krebs- und Krankheitenregister

Das Bundesgesetz über die Registrierung von Krebs und anderen Erkrankungen soll die umfassende Erfassung von Krebs flächendeckend für die ganze Schweiz unter Berücksichtigung der Persönlichkeitsrechte der Patienten regeln. Mit den gesetzlichen Grundlagen sollen ausserdem die Voraussetzungen für die Förderung der Registrierung anderer sehr verbreiteter oder gefährlicher Krankheiten geschaffen werden. Ein solches Register muss sehr hohen Datenschutzanforderungen Rechnung tragen. Dem entsprechend haben wir uns in die Arbeitsgruppe eingebracht und zu dem genannten Gesetzesentwurf Stellung genommen.

Eine Arbeitsgruppe prüft die Schaffung der für die Führung eines Krebsregisters durch den Bund erforderlichen eidgenössischen Gesetzesgrundlagen. Die Einrichtung eines Krebsregisters stellt unter dem Gesichtspunkt des Datenschutzes eine grosse Herausforderung dar; wir haben uns daher an der unter der Führung des Bundesamtes für Gesundheit (BAG) eingesetzten Arbeitsgruppe beteiligt. Der Bundesrat hatte nämlich das Eidgenössische Departement des Inneren beauftragt, bis zum Frühjahr 2012 einen Entwurf dieses Gesetzes auszuarbeiten. Das neue Gesetz wird die Grundlage für eine Harmonisierung der verschiedenen kantonalen Gesetzgebungen über die Krebsregistrierung bilden (Krebsregistrierungsgesetz). Zudem bietet es die Möglichkeit, neue Krankheitsfälle vollständig und auf nationaler Ebene

zu erfassen und einschlägige Daten zur Entwicklung der Krebserkrankungen zu beschaffen.

So ist vorgesehen, dass die in den bestehenden Registern erfassten Daten in verschlüsselter Form an eine nationale Krebsmeldestelle übermittelt werden, die mit der Zusammenstellung, Auswertung und Veröffentlichung dieser Daten betraut wird. Überdies sollte die Erfassung der Daten in den Kantonen künftig den gleichen rechtlichen und organisatorischen Rahmenbedingungen unterstellt werden. Dank der im Gesetzesentwurf vorgeschlagenen Bestimmungen kann die Qualität der erfassten Daten verbessert und damit die Auswertung auf nationaler Ebene vereinfacht werden. Forscher oder Verwaltungsdienste des Bundes und der Kantone können auf Anfrage Zugang zu den anonymisierten Daten erhalten.

Im Rahmen der Ämterkonsultation zu diesem Gesetzesentwurf hatten wir die Gelegenheit, unsere Meinung zu äussern. Der Gesetzesentwurf sieht für jede onkologische Erkrankung die Beschaffung eines minimalen Datensatzes vor, bestehend namentlich aus der genauen Diagnose, dem Datum, an dem sie gestellt wurde, und dem Datum des Behandlungsbeginns. Die Patienten sind berechtigt, sich der Weitergabe der sie betreffenden Daten an das zuständige kantonale Tumorregister zu widersetzen. Machen sie von diesem Recht keinen Gebrauch, sind die an der Diagnose und der Behandlung der Erkrankungen beteiligten Gesundheitsfachpersonen und Institutionen verpflichtet, die Daten dem zuständigen kantonalen Register zu übermitteln.

Der Gesetzesentwurf sieht ausserdem vor, dass für gewisse onkologische Erkrankungen zusätzliche Daten beschafft werden können (z.B. Krankheitsentwicklung, Behandlungsverlauf, Früherkennungsmassnahmen, Lebensqualität). Diese Daten können nur mit der Einwilligung der betroffenen Personen an das Krebsregister übermittelt werden. Wir haben dazu den Standpunkt vertreten, dass diese zusätzlich beschafften Daten besonders schützenswerte Personendaten darstellen, Daten also, anhand derer die Krankheitsentwicklung und der Behandlungsverlauf beurteilt und auch das Lebensumfeld der betroffenen Personen ermittelt werden können. Aus diesen Angaben, gekoppelt mit den minimalen Daten, lassen sich sehr detaillierte Informationen über den Gesundheitszustand einer Person ableiten; sie bedeuten demnach eine besonders schwerwiegende Verletzung des Persönlichkeitsrechts. Aus diesem Grund muss der Arzt die ausdrückliche Zustimmung seines Patienten zur Beschaffung solcher Daten einholen.

Generell haben wir erneut die systematische Verwendung der AHV-Versichertennummer zur eindeutigen Kennung kritisiert. Sie birgt nämlich grosse Risiken für die Privatsphäre der betroffenen Personen aufgrund der unerwünschten

Verbindungen, die infolge dieser Erweiterung zwischen verschiedenen Datenbanken hergestellt werden können. Deswegen vertreten wir den Standpunkt, dass eine sektorspezifische Kennung für den jeweiligen Bereich eingeführt werden müsse. Wir äusserten erneut unsere Bedenken bezüglich der Aufnahme der AHV-Nummer in die kantonalen Tumorregister. Eine Vermischung zwischen den Bereichen der Statistik, der Verwaltung und des Gesundheitswesens ist unbedingt zu vermeiden, da die für diese Bereiche geltenden Erfordernisse sowohl betreffend die Menge als auch die Qualität der Daten unterschiedlich sind. Die Verwendung spezifischer Nummern für jeden Bereich vermindert das Risiko, dass Informationen miteinander verbunden werden, was umso wichtiger ist, als die Daten der Tumorregister besonders schützenswert sind und sich daraus Persönlichkeitsprofile ergeben können. Der Vollständigkeit halber haben wir auch daran erinnert, dass der Bundesrat das BAG am 18. April 2012 beauftragt hatte, namentlich in Zusammenarbeit mit der Zentralen Ausgleichsstelle, im Rahmen des Vorentwurfs zum Bundesgesetz über das elektronische Patientendossier Alternativen für die Verwendung der AHV-Nummer zur Patientenidentifikation zu prüfen. Es erscheint uns daher notwendig, die Arbeiten in diesem Kontext auch im Zusammenhang mit dem Projekt für ein Krebsregister zu berücksichtigen.

Wir haben zudem deutlich gemacht, dass die Verknüpfung von Daten der kantonalen Tumorregister mit den statistischen Daten des Bundesamts für Statistik (BFS) den Bestimmungen von Artikel 14a Absatz 2 Bundesstatistikgesetz (BstatG) gerecht werden muss. Hier geht es um die Vermeidung jeglicher unerlaubter Zusammenstellungen, hat doch der Gesetzgeber das Datenverknüpfungsrecht auf das BFS und auf die statistischen Ämter der Kantone und Gemeinden beschränkt, um den Datenschutz zu gewährleisten und zu verhindern, dass Persönlichkeitsprofile entstehen. Im Übrigen sollen Datenverknüpfungen einem statistischen und nicht, wie hier, einem administrativen Zweck dienen. Zudem müssen sich die Datenverknüpfungen durch das BFS an die Bedingungen in Artikel 14a BstatG halten, was bedeutet, dass die Daten anonymisiert werden müssen. Davon abgesehen muss für die Verwendung der AHV-Versichertennummer durch das BFS die Gesetzgebung angepasst werden (in Form einer Teilrevision des BStatG), um eine einheitliche Regelung der AHV-Nummer in den statistischen Erhebungen herbeizuführen.

Das BAG hat unseren Bemerkungen im Wesentlichen Rechnung getragen. Unsere bei der Ämterkonsultation zum Ausdruck gebrachte Divergenz in Bezug auf die Verwendung der AHV-Nummer wurde im Vorschlag des Bundesrates aufgegriffen. Bei seiner Sitzung vom 7. Dezember 2012 hat der Bundesrat den Gesetzesentwurf genehmigt und das externe Vernehmlassungsverfahren eröffnet. Wir werden diese Gesetzesarbeiten weiterhin aufmerksam verfolgen.

1.5.6 Aufsichtstätigkeit in der medizinischen Forschung

Bei der Forschung mit medizinischen Personendaten werden die Betroffenen nicht immer um Einwilligung gefragt. Viele Betroffene sind sich nicht bewusst, dass sie ein Vetorecht haben.

Grundsätzlich dürfen Daten von Patienten nur für die Forschung verwendet werden, wenn die Betroffenen nach entsprechender Information und Bedenkzeit eingewilligt haben. Es gibt aber Fälle, in denen die Patienten nicht mehr auffindbar sind, beispielsweise dann, wenn sie ins Ausland abgereist oder gar verstorben sind. In solchen Fällen kann die Einwilligung meist nicht mehr eingeholt werden. Wird eine gewisse Anzahl von Betroffenen in einem Forschungsprojekt überschritten, muss die Einwilligung nicht eingeholt werden. Im Weiteren kann es für einen (ehemaligen) Patienten unzumutbar sein, auf eine solche Einwilligung angesprochen zu werden, etwa wenn es um eine schwere vergangene Krankheit geht, die den Betroffenen erheblich emotional belastet. Für solche Fälle, in denen keine Einwilligung eingeholt werden kann (oder muss), ist es möglich, bei der Expertenkommission für das Berufsgeheimnis in der medizinischen Forschung eine Bewilligung einzuholen.

Die Betroffenen haben im Weiteren ein Veto- und Widerrufsrecht. Sie müssen darauf aufmerksam gemacht werden, dass ihre Daten zu Forschungszwecken verwendet werden können, dass sie das Recht haben, diese Daten sperren zu lassen (Vetorecht), und dass sie die Einwilligung zu einem späteren Zeitpunkt widerrufen können. Spitäler machen die Bevölkerung beziehungsweise Patienten etwa mit Inseraten in Tageszeitungen und meist in den Patienteninformationen auf den Einsatz der Patientendaten für Forschungszwecke aufmerksam. Als man aber mögliche Betroffene danach fragte, wie ihre Patientendaten auch noch verwendet werden, war sich keine der befragten Personen bewusst, dass ihre Daten auch für Forschungszwecke verwendet werden können. Offenbar werden diese Informationen von den Patienten nicht ausreichend zur Kenntnis genommen. Dies ist bedenklich, weil die Betroffenen ja insbesondere bei sensitiven Personendaten so aufgeklärt bzw. informiert werden müssen, dass sie sich ein klares Bild über die Datenbearbeitung machen können; nur so können sie überhaupt in die Bearbeitung einwilligen. Die Information muss bei der Erhebung der Personendaten beginnen und endet bei deren Anonymisierung oder Löschung. Macht sich der Betroffene aufgrund der Information ein falsches Bild über die Datenbearbeitung, so besteht die Gefahr, dass die Einwilligung nicht rechtens ist.

Bezüglich des Vetorechts ist festzuhalten, dass sich die Patienten in einem Dilemma befinden. Sofern sie wissen, dass sie ein Vetorecht haben, und sie dieses

wahrnehmen, gilt dies meist für alle Forschungsvorhaben. Der Patient ist sich aber in vielen Fällen bewusst, dass ein grosser Teil der Forschungsvorhaben wichtig ist, und er möchte sich vielleicht nicht jeglicher Forschung verweigern. Somit wird er eher nicht von diesem Vetorecht Gebrauch machen. Er nimmt damit aber in Kauf, dass seine Daten aufgrund der oben aufgeführten Bedingungen ohne seine Kenntnisse zu Forschungszwecken verwendet werden können. Ein unseres Erachtens besseres Vorgehen wäre die Pseudonymisierung der Patientendaten, so dass diese den Forschern in nicht personenbezogener Form zur Verfügung stünden. In diesem Fall müsste die Einwilligung der Betroffenen erst eingeholt werden, wenn weitere Daten bei ihnen erhoben werden müssten. Ein solches Verfahren wäre einfacher und auch transparenter. Lösungsansätze dazu wurden schon erarbeitet und finden sich, wie bereits in unserem 16. Tätigkeitsbericht 2008/2009, Ziff. 1.5.4 erwähnt, auf den Internetseiten der Technologie- und Methodenplattform für die vernetzte medizinische Forschung http://www.tmf-ev.de/. Im Weiteren finden sich auf derselben Seite unter «Schriftenreihe» auch Bücher wie «Generische Lösungen zum Datenschutz für Forschungsnetze in der Medizin».

1.6 Versicherungen

1.6.1 Sachverhaltsabklärung bei einem Krankenversicherer

Krankenversicherer müssen Mitarbeitenden für die Leistungsabrechnung Zugriff auf medizinische Daten der Versicherten gewähren. Im Idealfall hat der Mitarbeitende Zugriff auf diejenigen Daten, die er für den konkreten Fall benötigt. Nach Abschluss sollte die Berechtigung wieder entzogen werden. Der Idealfall wird aber selten erreicht. Das zeigte eine Sachverhaltsabklärung bei einem grossen Krankenversicherer.

Uns wurde ein mutmasslicher Verstoss gegen das Datenschutzgesetz bei einem grossen Krankenversicherer gemeldet: Nahezu alle Mitarbeitenden hätten Zugriff auf besonders schützenswerte Versichertendaten. Träfe der Vorwurf zu, würde es sich um eine gravierende Verletzung der Persönlichkeitsrechte der Versicherten handeln. Deshalb haben wir uns entschieden, den Sachverhalt detailliert abzuklären.

Eine schriftliche Stellungnahme des Versicherers beantwortete nicht alle Fragen. Klarheit brachte in der Folge eine Abklärung vor Ort. Es zeigte sich, dass der erhobene Vorwurf gerechtfertigt war. Mehrere hundert Personen hatten Zugriff auf die Versichertendaten, darunter auch Mitarbeitende, die mit dem eigentlichen Fall nicht beauftragt waren. Wir konnten den Versicherer davon überzeugen, dass das Zugriffskonzept dringend den datenschutzrechtlichen Anforderungen angepasst werden muss. Diese Anpassung der Software für die Leistungsabrechnung ist für den Versicherer jedoch sehr aufwendig. Deshalb hat er sich entschieden, sich mit anderen Versicherern, die dasselbe System anwenden, zu koordinieren. So könnte in Zukunft erreicht werden, dass mehrere grosse Versicherer bei der Vergabe der Zugriffsberechtigungen auf dem gleichen und vor allem adäquaten Stand sind. Für uns ist das ein begrüssenswertes Vorgehen. Im Verlauf des ersten Semesters 2013 legt uns der Versicherer das Grobkonzept für seine zukünftige Lösung vor. Dieses werden wir kritisch prüfen und die Umsetzung kontrollieren.

1.6.2 Meinungsumfrage einer Versicherung zur Organspende

Wir wurden auf die Praxis einer Versicherung im Zusammenhang mit einer Meinungsumfrage zur Organspende aufmerksam gemacht und führten eine Sachverhaltsabklärung durch. Dabei stellten wir fest, dass die Versicherung die notwendigen Schritte unternommen hatte, um die Anforderungen der Datenschutzgesetzgebung zu erfüllen. Wir haben indes auf gewisse Punkte hingewiesen, die im Rahmen etwaiger künftiger Meinungsumfragen zu berücksichtigen wären.

Im Rahmen unserer Beratungs- und Informationstätigkeiten sind wir regelmässig mit zahlreichen Anfragen von interessierten Bürgerinnen, Bürgern und Medien konfrontiert, die erfahren möchten, wie wir zu gewissen Datenbearbeitungspraktiken von Unternehmen, Privatpersonen oder Bundesinstanzen stehen. Unsere Stellungnahmen in diesen Situationen sind grundsätzlich genereller Art und dienen dazu, die Öffentlichkeit für die potentiellen Gefahren einer Datenbearbeitung zu sensibilisieren, ohne dabei über einen konkreten Einzelfall zu entscheiden.

Vorliegend wurden wir von mehreren Seiten angesprochen, die unsere Meinung zu den Teilnahmebedingungen an der von einem Versicherer organisierten Umfrage erfahren wollten, insbesondere betreffend die Beschaffung gewisser Personendaten (wie etwa die AHV-Versichertennummer der Teilnehmenden) und ihre Weitergabe auf der Webseite einer amerikanischen Gesellschaft, welche die Hostingdienste der Umfrage anbietet.

Unabhängig von dem konkreten Fall äusserten wir unsere grundsätzlichen Bedenken zur Problematik der Datenübermittlung an Länder wie die USA, deren Gesetzgebung kein angemessenes Schutzniveau gewährleistet und mit denen keine ausreichenden Garantien vereinbart worden sind. Im Rahmen unserer Tätigkeit stellen wir häufig fest, dass diese Problematik von zahlreichen Personen oder Unternehmen nicht beachtet wird, wenn sie die Übermittlung gerade von besonders schützenswerten Personendaten (wie etwa Daten zur Gesundheit einer Person) in diese Länder planen. Damit ist der Schutz der Privatsphäre der betroffenen Personen oft nicht mehr gewährleistet, und die Risiken einer Persönlichkeitsverletzung sind erhöht.

Angesichts des Umfangs der Meinungsumfrage und in Anbetracht unserer Erfahrung mit den potentiellen Risiken einer Datenbearbeitung in den Vereinigten Staaten haben wir gemäss Artikel 29 des Bundesgesetzes über den Datenschutz (DSG) den Sachverhalt näher abgeklärt, um uns ein konkretes Bild von den durch die

Versicherung getroffenen Massnahmen zur Gewährleistung des Datenschutzes zu verschaffen.

Die Analyse der Erklärungen und der vorgelegten Dokumentation des Versicherers sowie die auf der Umfrage-Webseite durchgeführte Kontrolle ergaben, dass die Versicherung die notwendigen Schritte unternommen hatte, um die Vorschriften des DSG bezüglich des Rechtfertigungsgrundes (Einwilligung der Teilnehmenden zur Bearbeitung ihrer Personendaten im Rahmen der Umfrage) einzuhalten. Zudem war sie im Rahmen einer grenzüberschreitenden Bekanntgabe vertraglich Garantien eingegangen, die ein angemessenes Schutzniveau im Ausland sicherstellen sollen, namentlich durch den Beitritt des amerikanischen Anbieters der Umfrage-Webseite zum US-Swiss Safe Harbor Framework.

Wir machten die Versicherung indes darauf aufmerksam, dass die systematische Verwendung der AHV-Nummer ausserhalb der Sozialversicherungen laut Bundesgesetz über die Alters- und Hinterlassenenversicherung (AHVG) nur in Bereichen, die in engem Zusammenhang mit den Sozialversicherungen stehen, zulässig ist. Die Verwendung der Nummer ausserhalb dieses Kontextes ist möglich, wenn ad hoc eine gesetzliche Grundlage auf Bundesebene beziehungsweise auf kantonaler Ebene geschaffen wird. Die Ermächtigung zur Verwendung der Versichertennummer wird direkt vom Gesetzgeber erteilt, der ihren Geltungsbereich mit folgender Erläuterung in der Botschaft zur Änderung des AHVG klar regeln wollte: «Fest steht, dass die AHV-Nummer heute von zahlreichen Nutzern systematisch verwendet wird. Ein vollständiger Überblick über die Einsatzgebiete besteht aber nicht und kann auch nicht mit Sicherheit gewonnen werden. Diese Situation ist mit der datenschutzrechtlichen Forderung nach Kontrolliertheit und Kontrollierbarkeit nicht im Einklang. Eine klare Regelung für den Einsatzbereich der Versichertennummer scheint daher unverzichtbar. Rein private systematische Nutzungen sollen künftig nicht mehr möglich sein.» Mit der Festlegung strenger Nutzungsbedingungen wurde dieses Gesetz in der Absicht erlassen, den Risiken vorzubeugen, die mit einer unkontrollierten Verwendung der AHV-Nummer für die Privatsphäre der betroffenen Personen verbunden sind, da so unerwünschte Verknüpfungen zwischen verschiedenen Datenbanken entstehen können.

Überdies haben wir zur Kenntnis genommen, dass die amerikanische Anbieter-Gesellschaft der Umfragewebseite dem Vertrag U.S.-Swiss Safe Harbor Framework beigetreten ist und sich auf der Webseite des amerikanischen Handelsministeriums registriert hat; dennoch haben wir daran erinnert, dass Artikel 6 DSG nur die Frage des grenzübergreifenden Charakters der Bekanntgabe regelt. Diese muss auf jeden Fall den allgemeinen Grundsätzen des DSG entsprechen (Art. 4, 5 und 7). Wie aus unserer Prüfung hervorgeht, erhalten die Teilnehmer im Rahmen der

Umfrage zwar in angemessener Form Informationen über den Zweck der Umfrage und die diesbezügliche Datenbearbeitung, doch müsste die Versicherung sie auch eindeutig darüber aufklären, dass ihre Personendaten in die USA weitergegeben werden. Nur ein besonders umsichtiger und aufmerksamer Nutzer kann erkennen, dass die Umfrage über die Webseite der amerikanischen Gesellschaft durchgeführt wird, ohne dass er deswegen auch erfährt, dass seine Personendaten auf dem Hostrechner dieser Gesellschaft in den Vereinigten Staaten liegen.

Im Lichte der vorangehenden Erwägungen sind wir zu dem Schluss gelangt, dass die Umfrage die vom DSG aufgestellten Bedingungen betreffend ihren Rechtfertigungsgrund und die Garantien für ein angemessenes Schutzniveau im Ausland erfüllt. Wir haben jedoch darauf hingewiesen, dass in einer solchen von einem privaten Unternehmen durchgeführten Umfrage die AHV-Versichertennummer nicht verwendet werden darf, und dass die Teilnehmer über die Bekanntgabe ihrer Personendaten ins Ausland klar informiert werden müssen. Da die betreffende Umfrage abgeschlossen ist, waren wir der Auffassung, dass sich eine Empfehlung im Sinne von Artikel 29 Absatz 3 DSG erübrigt, dass die Versicherung aber verpflichtet ist, den oben stehenden Ausführungen bei etwaigen künftigen Umfragen Rechnung zu tragen.

1.7 Arbeitsbereich

1.7.1 Anforderungen an ein Whistleblowingsystem

In der Schweiz existieren keine spezifischen gesetzlichen Vorgaben für den Betrieb eines Whistleblowingsystems in privaten Unternehmen. Im Rahmen der telefonischen Beratung haben wir mehrere Anfragen zu diesem Thema beantwortet. Oftmals ging es auch um die Frage, ob eine Anmeldepflicht für die Datensammlung des Whistleblowingsystems besteht. Wir hielten fest, dass eine Anmeldung angezeigt ist.

Mehrmals haben sich Unternehmen oder deren rechtliche Vertreter bei uns telefonisch erkundigt, ob es in der Schweiz spezifische gesetzliche Grundlagen für die Einrichtung und den Betrieb eines Whistleblowingsystems gibt. Innerhalb der Bundesverwaltung gilt seit Januar 2011 der Artikel 22a des Bundespersonalgesetzes. Für den privaten Bereich bestehen keine spezifischen Regelungen, es sind aber insbesondere die Bestimmungen des Datenschutzgesetzes zu beachten.

Bei praktisch jeder Anfrage wurde auch nachgefragt, ob eine Anmeldepflicht der zugehörigen Datensammlung besteht. Private Personen müssen Datensammlungen bei uns anmelden, wenn regelmässig besonders schützenswerte Personendaten oder Persönlichkeitsprofile bearbeitet oder Personendaten an Dritte bekannt gegeben werden. Beim Betrieb eines Whistleblowingsystems ist nicht auszuschliessen bzw. sogar sehr wahrscheinlich, dass aufgrund der eingehenden Meldungen regelmässig besonders schützenswerte Personendaten bearbeitet werden. Dies entspricht vielleicht nicht dem Willen des Betreibers, aber er kann es auch nicht wirklich steuern. Aufgrund dieses Umstands haben wir den anrufenden Personen regelmässig das Anmelden der Datensammlung empfohlen.

1.7.2 Zustellung von Pensionskassenausweisen – Urteil des Bundesverwaltungsgerichts und Nachkontrolle

Am 12. April 2012 hat das Bundesverwaltungsgericht entschieden, dass die Pensionskassenausweise künftig so zuzustellen sind, dass ausschliesslich die jeweilige versicherte Person, und damit keine Dritten, Kenntnis vom Inhalt ihres Ausweises erlangen kann. Die Umsetzung des Urteils wurde von uns im Rahmen einer Nachkontrolle überprüft.

Wir haben bereits mehrmals (vgl. unseren 17. Tätigkeitsbericht 2009/2010, Ziff. 1.7.8, und unseren 18. Tätigkeitsbericht 2010/2011, Ziff. 1.7.3) die Art und Weise der Zustellung der Pensionskassenausweise kritisiert. Nun folgt die neuste Entwicklung in diesem Bereich. Zur Erinnerung: Im Jahr 2009 hatten wir eine Sachverhaltsabklärung in dieser Angelegenheit eröffnet und der betroffenen Vorsorgestiftung insbesondere empfohlen, sie solle beim Versand der Ausweise gewährleisten, dass die Dokumente direkt und ausschliesslich an die versicherte Person gelangen. Die Vorsorgeeinrichtung lehnte die Empfehlung jedoch ab. Dies führte dazu, dass wir beim Eidgenössischen Departement des Innern (EDI) einen Antrag auf Entscheid gemäss aufsichtsrechtlichem Verfahren betreffend Bundesorgane stellten. Das EDI hiess das Vorgehen der Pensionskasse gut, worauf wir beim Bundesverwaltungsgericht Beschwerde einreichten, welche am 12. April 2012 gutgeheissen wurde (vgl. unseren 19. Tätigkeitsbericht 2011/2012, Ziff. 1.7.2). Dieses Urteil A-4467/2011, das mittlerweile in Rechtskraft getreten ist, hat zur Folge, dass die Ausweise künftig so zuzustellen sind, dass ausschliesslich die jeweilige versicherte Person und kein Dritter – insbesondere nicht der Arbeitgebende – Kenntnis vom Inhalt ihres Ausweises erlangen kann.

Im Rahmen einer Nachkontrolle haben wir am 19. Dezember 2012 die Umsetzung dieses Urteils in den Räumlichkeiten der Vorsorgeeinrichtung geprüft. Dabei haben wir festgestellt, dass sie den Vorgaben des Urteils entspricht. Alle beteiligten Parteien im Vorsorgewesen (berufliche Vorsorgestiftungen der Arbeitgeber, Mitarbeitende, Broker usw.) wurden von der Pensionskasse darüber informiert, dass die Zustellung der Pensionskassenausweise neu in verschlossenen Couverts mit dem Vermerk «Persönlich» erfolgt.

Wir begrüssen dieses Urteil des Bundesverwaltungsgerichts, denn damit wird die Rechtssicherheit innerhalb der Branche, was die Übermittlung von Personendaten anbelangt, gestärkt.

1.7.3 Übermittlung von Mitarbeiterdaten an US-Behörden

Verschiedene Banken haben Dokumente an US-Behörden übermittelt, welche Namen, E-Mail-Adressen und Telefonnummern von aktuellen und ehemaligen Mitarbeitenden sowie Drittpersonen enthielten. Wir haben deshalb bei fünf betroffenen Banken eine Sachverhaltsabklärung durchgeführt und danach Empfehlungen erlassen, die die Banken zu einer transparenteren Vorgehensweise verpflichten.

Mehrere Schweizer Banken hatten im Rahmen von laufenden Verhandlungen mit den US-Behörden Dokumente, die das Geschäft mit US-Kunden betreffen, an die dortigen Behörden übermittelt. In den Unterlagen waren auch die Namen von aktuellen und ehemaligen Mitarbeitenden sowie Dritten enthalten. Mehrere dieser betroffenen Personen haben sich an uns gewandt, und nachdem bekannt wurde, dass weitere Datenübermittlungen bevorstehen, haben wir zur Klärung der datenschutzrechtlichen Fragen im August 2012 eine Sachverhaltsabklärung eingeleitet. Ziel dieses Verfahrens war, einen Überblick über die erfolgten Übermittlungen zu erhalten, um beurteilen zu können, ob es zu Persönlichkeitsverletzungen gekommen war bzw. wie die betroffenen Personen zu mehr Schutz gelangen können.

Im Rahmen der Sachverhaltsabklärung haben wir mit dem Staatssekretariat für internationale Finanzfragen, der FINMA und dem Bundesamt für Justiz Gespräche geführt. Dabei wurden uns die Überlegungen erläutert, die zu den Beschlüssen des Bundesrates betreffend Kooperation der Banken mit US-Behörden geführt haben. Wir haben auch die betroffenen Banken empfangen. In einem ersten Schritt haben wir sie zum Schutz der betroffenen Personen zu einem transparenten Verhalten gegenüber den Mitarbeitenden angehalten. Dementsprechend haben sich die Banken verpflichtet, die Mitarbeitenden während der laufenden Abklärungen vor jeder weiteren Dokumentenlieferung an US-Behörden zu informieren, falls darin ihre Namen enthalten sein sollten. Weiter mussten die Banken danach einerseits einen Fragenkatalog beantworten und uns andererseits Unterlagen zustellen, die das Verfahren der Übermittlungen und die Information der Mitarbeitenden aufzeigen. Bei einzelnen Banken haben wir auch noch einen Augenschein vor Ort vorgenommen, um uns das Verfahren zur Auswahl der Unterlagen und das Informations- und Einsichtsverfahren für die Mitarbeitenden vorführen zu lassen.

Aufgrund der eingereichten Unterlagen, der dazugehörigen Erläuterungen und der verschiedenen involvierten Bundesorgane sind wir zum Schluss gekommen, dass eine Übermittlung aufgrund überwiegender öffentlicher Interessen nachvollzogen werden kann. Es wurde uns glaubhaft dargelegt, dass den Banken ernsthafte Konsequenzen drohten, wenn sie der durch die US-Behörden geforderten

Übermittlung nicht nachkämen. Wir haben demnach in unseren Empfehlungen das überwiegende öffentliche Interesse bejaht, das als Voraussetzung für eine Bekanntgabe von Personendaten in ein Land mit ungenügendem Datenschutzniveau geltend gemacht wurde. Gleichzeitig haben wir aber klar aufgezeigt, dass die Banken bei den bisherigen Übermittlungen nicht in allen Punkten datenschutzkonform vorgegangen sind. So haben nicht alle Institute sämtliche betroffenen Personen über die bevorstehende Übermittlung informiert. Auch wurde nicht allen Personen Einsicht in die sie betreffenden übermittelten Dokumente gewährt. Aus diesem Grund haben wir in unseren Empfehlungen die Banken in Bezug auf die bereits erfolgten Datenlieferungen dazu verpflichtet, den betroffenen Personen (aktuelle und ehemalige Mitarbeitende sowie externe Dritte) das Auskunftsrecht zu gewähren. Bei jeder zukünftigen Datenlieferung an US-Behörden müssen die Banken die betroffenen Personen im Voraus über Umfang und Art der Dokumente, die übermittelt werden sollen, sowie über den Zeitraum, aus dem sie stammen, informieren. Auch ehemalige Mitarbeitende und externe Dritte sind zu informieren, sofern dies mit einem verhältnismässigen Aufwand möglich ist.

Die Banken müssen den betroffenen Personen danach eine angemessene Frist gewähren, innert der diese Auskunft über sämtliche, sie betreffenden Dokumente erhalten können. Spricht sich die Person nach dieser Auskunft gegen die Übermittlung der Dokumente aus, die ihren Namen enthalten, wird die Bank eine Interessenabwägung für den konkreten Einzelfall vornehmen. Will eine Bank die Dokumente trotzdem mit dem Namen des Betroffenen übermitteln, muss sie ihn darüber informieren und über seine Rechte aufklären.

Alle involvierten Banken haben unsere Empfehlungen angenommen. Sie sind auf unserer Webseite www.derbeauftragte.ch unter Datenschutz – Empfehlungen publiziert.

1.7.4 Überwachungs- und Kontrollsysteme am Arbeitsplatz

Die elektronische Entwicklung der letzten Jahre hat in der Arbeitswelt zu grossen Veränderungen geführt. Immer mehr technische Überwachungs- und Kontrollsysteme stehen den Arbeitgebern zur Verfügung. Es stellt sich die Frage, welche Überwachung erlaubt ist und welche Kontrolle zu weit geht.

Mit einer Projektgruppe des Staatssekretariats für Wirtschaft (SECO), welche sich der technischen Personenüberwachung am Arbeitsplatz widmete, haben wir an der Überarbeitung der Wegleitung zur Verordnung 3 zum Arbeitsgesetz mit Bezug auf Artikel 26 mitgewirkt. Danach dürfen grundsätzlich keine Überwachungs- oder

Kontrollsysteme eingesetzt werden, die das Verhalten der Arbeitnehmenden am Arbeitsplatz überwachen sollen.

Personendaten dürfen nur auf legale Weise erhoben werden. Ihre Bearbeitung unterliegt dem Grundsatz von Treu und Glauben und muss gemäss den Bestimmungen des Bundesgesetzes über den Datenschutz und dessen Verordnung erfolgen. Das Prinzip der Verhältnismässigkeit ist stets zu berücksichtigen. Es dürfen nur sachdienliche und für den angestrebten Zweck nützliche Personendaten bearbeitet werden. Diese müssen nach einer möglichst kurzen, im Voraus festgelegten Zeitspanne gelöscht werden. Der Zugang zu den bearbeiteten Personendaten (Datensammlung) ist zu regeln. Er muss auf die Personen beschränkt werden, welche zur Auswertung befugt sind.

Beim Einsatz von Überwachungs- und Kontrollsystemen ist stets darauf zu achten, dass der Schutz der Persönlichkeit von Arbeitnehmerinnen und Arbeitnehmern gewährleistet bleibt. Betroffene Personen müssen vorgängig ausführlich über Art, Ziel und Zweck der Bearbeitung informiert werden. Wenn immer möglich ist ein betriebsinternes Nutzungsreglement zu erstellen, welches Arbeitnehmerinnen und Arbeitnehmern transparent darüber Aufschluss gibt, welche Rechte und Pflichten ihnen beim Einsatz von Überwachungs- und Kontrollsystemen zustehen. Es hat sich gezeigt, dass solche Systeme nicht nur zum betriebseigenen Nutzen, sondern auch erfolgreich zum Schutz und zur allgemeinen Sicherheit der Arbeitnehmenden eingesetzt werden können. Der gewissenhafte Arbeitgeber muss sich aber stets bewusst bleiben, dass der Einsatz solcher Systeme ohne Vorankündigung zu Misstrauen führt. Eine vernünftige und nachvollziehbare Kontrolle kann durchaus gerechtfertigt sein. Vernünftig und nachvollziehbar ist sie vor allem dann, wenn Transparenz herrscht und nicht plötzlich heimliche «Schnüffeleien» bekannt werden. Wo der Grundsatz der Transparenz missachtet wird, ersuchen Mitarbeiterinnen und Mitarbeiter um Beistand.

Der Einsatz von Überwachungs- und Kontrollsystemen am Arbeitsplatz tangiert zwei verschiedene Problembereiche. Sofern schwergewichtig das Verhalten der Mitarbeitenden überwacht und kontrolliert wird, wo demzufolge deren Gesundheit gefährdet ist und der Schutz der Persönlichkeit im Mittelpunkt steht, sind vorerst die kantonalen Arbeitsinspektorate zu konsultieren. Wo dagegen hauptsächlich Personendaten gesammelt und bearbeitet werden, drängt sich zusätzlich die Konsultation der Datenschutzverantwortlichen auf.

1.7.5 Verwaltung des E-Mail-Accounts im Arbeitsbereich

Was geschieht mit dem E-Mail-Account bei unerwarteten Abwesenheiten? Inwieweit ist der Arbeitgeber berechtigt, meine E-Mails zu konsultieren? Dies sind die häufigsten Fragen aus dem Arbeitsbereich, die uns an der Telefonhotline gestellt werden. Die persönliche Integrität und die Privatsphäre im Spannungsfeld der Arbeitswelt bedürfen einer Regelung.

Der Büroalltag hat sich mit dem Siegeszug der Informatik von Grund auf geändert. Wo früher die Privatsphäre grundsätzlich ohne grossen Aufwand eingehalten werden konnte, ist die Ausgangslage heute nicht mehr eindeutig geregelt. Zu Zeiten, als Korrespondenz ausschliesslich per Post und Kurier eintrafen, galt die verbindliche Regel, dass mit dem Vermerk «Persönlich» bezeichnete verschlossene Briefumschläge durch das zuständige Kanzleipersonal nicht geöffnet werden durften. Alle Mitarbeitenden konnten ihre persönlichen Schriftstücke in dem ihnen zugewiesenen abschliessbaren Bürobehältnis aufbewahren. Ein Zugriff auf die Geschäftskorrespondenz musste dagegen auch bei Abwesenheit einer Mitarbeiterin oder eines Mitarbeiters stets gewährleistet sein, entweder an deren Arbeitsplatz oder aber in einer zentralen Ablage.

In Bezug auf Kurier und eingehende Post klappt dies für gewöhnlich immer noch anstandslos. Seitdem Mitarbeitende aber ihren eigenen E-Mail-Account besitzen, wird ein Grossteil der eingehenden geschäftlichen wie privaten Informationen über diesen abgewickelt. E-Mails verdrängen die Briefpost stetig. Die Unterscheidung zwischen geschäftlichen und privaten E-Mails lässt jedoch vielerorts zu wünschen übrig. Vielfach wird erst bei unerwarteter Abwesenheit der Mitarbeitenden – beispielsweise wegen Krankheit oder Unfall – bemerkt, dass sich hier die grundsätzliche Frage stellt, ob der Arbeitgeber den E-Mail-Account eines Mitarbeiters in dessen Abwesenheit ohne Einverständnis konsultieren darf. Dies ist eine der meistgestellten Fragen aus dem Arbeitsbereich, welche uns an der Telefonhotline gestellt wird. Wie Arbeitnehmerinnen und Arbeitnehmer ihren E Mail-Account benutzen dürfen, hat der Arbeitgeber deshalb vorzugsweise in einem Reglement für die Nutzung der betriebsinternen Informatik zu bestimmen. Das Weisungsrecht gemäss Artikel 321d Obligationenrecht bildet hierfür die gesetzliche Grundlage.

Ein solches Nutzungsreglement sorgt für Transparenz und Rechtssicherheit. Es ist der Belegschaft bekannt zu geben, welche Kompetenzen dem Arbeitgeber zustehen, damit unnötige Diskussionen zwischen ihm und den Arbeitnehmenden verhindert werden können. Beim Erlass von Regeln ist darauf zu achten, dass sie auch durchsetzbar sind. Ein Totalverbot der privaten Nutzung hat einen grossen

Kontrollaufwand zur Folge und bleibt deshalb meist Wunschdenken. Je deutlicher ein Nutzungsreglement ist, desto mehr ist sich die Belegschaft im Klaren, was erlaubt und was verboten ist. Die optimale Lösung wäre die strikte Trennung der geschäftlichen E-Mails von den privaten, die ja nie ganz ausgeschlossen werden können. Da den Mitarbeitenden neben dem geschäftlichen E-Mailaccount in den wenigsten Fällen noch ein eigener privater zur Verfügung gestellt wird, darf von allen Mitarbeitenden verlangt werden, dass sie ihre privaten E-Mails laufend und unverzüglich auf einen privaten Ordner verschieben, etwa indem sie in ihrem Account eine entsprechende Regel einrichten. Bei vereinbarten Abwesenheiten haben Mitarbeitende den Abwesenheitsassistenten ihres E-Mail-Accounts zu aktivieren. Bei unerwarteten längeren Abwesenheiten sollten die Informatikzuständigen über eine Möglichkeit verfügen, einen Abwesenheitsassistenten oder eine Weiterleitung der E-Mails zu aktivieren, ohne dabei den Account der abwesenden Mitarbeiterin öffnen zu müssen.

Weitere Lösungsmöglichkeiten sind auf unserer Webseite www.derbeauftragte.ch unter Datenschutz – Dokumentation – Leitfäden zu finden.

1.7.6 Datenschutzkonforme Qualitätssicherung bei einem Marktforschungsinstitut

Ein Marktforschungsinstitut, bei welchem wir letztes Jahr eine Sachverhaltsabklärung durchgeführt hatten, hat auf unseren Vorstoss hin eine Vorgehensweise umgesetzt, die eine datenschutzkonforme Qualitätssicherung vorsieht.

Im Rahmen einer Sachverhaltsabklärung bei einem Marktforschungsinstitut (vgl. unseren 19. Tätigkeitsbericht 2011/2012, Ziff. 1.1.1) haben wir festgestellt, dass Mitarbeitende in gewissen Fällen ungenügend darüber informiert werden, wie die Qualität ihrer Arbeit überwacht wird. So haben die Vorgesetzten Interviews mitgehört, ohne dass das interviewende Personal davon in Kenntnis gesetzt worden war. Zusätzlich war die Vorgehensweise des Mithörens für die Mitarbeitenden weder einheitlich noch transparent geregelt. Ein solches «Silent Monitoring» kann jedoch eine unverhältnismässige systematische Überwachung darstellen, was aus arbeits- sowie datenschutzrechtlicher Sicht unzulässig ist.

Während unserer Abklärungen haben wir das Unternehmen auf diese Problematik hingewiesen, worauf es eine neue, einheitliche und klar definierte Vorgehensweise zur Qualitätssicherung erarbeitete. Die Mitarbeitenden werden demnach in Zukunft grundsätzlich mit einem optischen Signal darauf aufmerksam gemacht, wenn die Vorgesetzten das Telefongespräch mithören. Ein Silent Monitoring ohne

Ankündigung ist nur noch in einzelnen, beschränkten Situationen möglich. Diese betreffen vor allem die Probezeit oder mangelnde Leistungen. Die verschiedenen Ausnahmen werden den Mitarbeitenden transparent mitgeteilt, was wir als datenschutzkonform erachten. Nachdem wir die Dokumentation dieser Vorgehensweise geprüft und eine Bestätigung der Umsetzung erhalten hatten, konnten wir die Abklärung abschliessen. Aufgrund dieser Erfahrungen gehen wir davon aus, dass auch weitere Unternehmen, die in diesem Bereich tätig sind, ihre Qualitätssicherung in Zukunft datenschutzkonform gestalten werden.

1.7.7 Verhaltenskodex zur Verhinderung von Interessenkonflikten bei Bundesangestellten

Der neue Verhaltenskodex für Bundesangestellte sieht vor, dass die Mitarbeitenden private Beteiligungen an Unternehmen ab einem gewissen Wert melden müssen. Wir wurden angefragt, ob eine solche Meldung mit den Grundsätzen des Datenschutzgesetzes vereinbar ist.

Im Nachgang zum Rücktritt des Nationalbankpräsidenten anfangs 2012 haben sich mehrere Bundesstellen veranlasst gesehen, einen Verhaltenskodex bzw. ein Reglement zu entwerfen, mit welchem Insiderdelikte und Interessenkonflikte verhindert werden sollen. Eine dieser Stellen hat uns den Entwurf ihres Kodexes mit der Bitte um eine Beurteilung aus datenschutzrechtlicher Sicht unterbreitet. Darin sollte primär eine Meldepflicht für private Beteiligungen ab einem gewissen Wert festgelegt werden. In einer ersten Stellungnahme sind wir vor allem auf die Art und Weise der Meldung bzw. der Überprüfung eingegangen.

Wir haben festgehalten, dass im Rahmen einer solchen Meldepflicht die Daten bzw. Meldungen nicht ohne Weiteres einem Dritten, zum Beispiel einer Treuhandfirma, bekanntgegeben werden dürfen, sofern dafür keine gesetzliche Grundlage besteht. Die betroffene Amtsstelle hat daraufhin auf eine solche Bekanntgabe verzichtet.

Wir haben die Verwaltungseinheit in einem zweiten Schritt um eine Stellungnahme zu den bestehenden rechtlichen Grundlagen für die geplante Meldepflicht gebeten. Die Antwort hielt fest, die Meldepflicht stütze sich vor allem auf den Artikel zur allgemeinen Treuepflicht im Bundespersonalgesetz (Art. 20 BPG). Zum Zeitpunkt der hier beschriebenen Anfrage wurde dieser Artikel in der zugehörigen Verordnung (BPV) jedoch nur zum Thema der Nebenbeschäftigung ausgeführt. Die Verwaltungsstelle hat aber angemerkt, dass mit der Revision der BPV im Herbst 2012 dieser Artikel mit Bestimmungen zum Abschluss von Nebengeschäften und

weiteren Pflichten des Personals ergänzt werde. Zudem werde darin konkretisiert, dass die Departemente und Verwaltungseinheiten ergänzende Bestimmungen erlassen können, namentlich um Interessenskonflikte und den Missbrauch von vertraulichen Informationen zu vermeiden.

Aufgrund dieser Ausführungen und im Hinblick auf die Revision der BPV in diesem Bereich kamen wir zum Schluss, dass eine Meldung von privaten Beteiligungen ab einem gewissen Wert in der betroffenen Amtsstelle durchaus verlangt werden kann. Solche Pflichten der Mitarbeitenden können denn auch neu aufgrund der bestehenden gesetzlichen Grundlage (Art. 14 BPV, in Kraft seit 15. September 2012) in ergänzenden Bestimmungen wie Weisungen, einem Verhaltenskodex oder einem Reglement datenschutzkonform festgelegt werden, und die Daten dürfen danach auch durch die Amtsstelle bearbeitet werden.

1.8 Handel und Wirtschaft

1.8.1 Warenkorbanalyse bei Kundenbindungsprogrammen

Auf Anfrage eines Grossverteilers haben wir die nachträgliche Einführung einer Warenkorbanalyse bei einer Kundenkarte aus datenschutzrechtlicher Sicht beurteilt. Eine solche Änderung der Datenbearbeitung stellt insbesondere erhöhte Anforderungen an die Transparenz und die Einwilligung der Kunden.

Kundenkarten werden im Rahmen von Kundenbindungsprogrammen von verschiedenen Firmen eingesetzt. Teilnehmende erhalten gewisse Vergünstigungen und weitere Vorteile, im Gegenzug will das Unternehmen jedoch seine Kundinnen und Kunden möglichst an sich binden. Mittels einer sogenannten Warenkorbanalyse registriert das Unternehmen die Einkäufe der Kunden, welche diese unter Vorweisen ihrer Kundenkarte bezahlt haben. Die Firma erhält so detaillierte Daten über die Einkäufe und kann weitere Marketingmassnahmen oder ähnliches planen. Die Teilnehmenden solcher Kundenbindungsprogramme müssen über diese detaillierte Datenbeschaffung transparent informiert werden. Sie können jedoch jederzeit durch Vorzeigen resp. Nichtvorzeigen ihrer Kundenkarte beim Einkauf die Sammlung ihrer Warenkorbdaten direkt beeinflussen.

Anfang Jahr bat uns ein Grossverteiler, die nachträgliche Einführung einer solchen Warenkorbanalyse aus datenschutzrechtlicher Sicht zu beurteilen. Bisher hatte der Grossverteiler die Einkaufsdaten bloss zu buchhalterischen Zwecken gespeichert. Wir haben darauf hingewiesen, dass mit der Einführung der Warenkorbanalyse zu Marketingzwecken Persönlichkeitsprofile im Sinne des Datenschutzgesetzes (DSG) beschafft werden. Dabei müssen verschiedene Voraussetzungen beachtet werden: So muss der Grossverteiler umfassend und transparent über die geplante Änderung informieren. Neben der Information direkt in den Geschäftsbedingungen zur Kundenkarte sind weitere Kanäle wie beispielweise die Webseite oder die Kundenzeitung zu nutzen. Die Kartennutzer wiederum müssen der Warenkorbanalyse ausdrücklich zustimmen, nachdem sie von den Änderungen Kenntnis genommen haben. Dabei genügt es nicht, wenn der Kunde die Karte bloss weiterhin nutzt. Die Zustimmung zur Warenkorbanalyse muss unmittelbar aus der Erklärung zum Ausdruck kommen – beispielsweise durch Ankreuzen einer vorformulierten Bestätigung. Fehlt eine solche Zustimmung, ist die Analyse des Warenkorbs der betroffenen Person zu unterlassen. Die Kundinnen und Kunden dürfen nicht dazu gezwungen werden, den neuen Bestimmungen zuzustimmen. Ebenso müssen die Teilnehmer des Kundenbindungsprogramms die Möglichkeit haben, auf gezielte

Werbeansprache aufgrund der Analyse ihres Warenkorbs zu verzichten. Der Grossverteiler hat von unseren Stellungnahmen Kenntnis genommen und zugesagt, unsere Forderungen umzusetzen.

1.8.2 Abklärungen im Bereich Kredit- und Wirtschaftsauskunfteien: Moneyhouse

Die Wirtschaftsauskunftei Moneyhouse veröffentlicht im Rahmen der von ihr angebotenen Personensuche unter anderem Adressdaten im Internet, die Betroffene anderweitig gesperrt hatten. Wir haben eine Sachverhaltsabklärung eröffnet, um diese Datenbearbeitungen genauer zu untersuchen.

Im Frühsommer 2012 stieg die Anzahl Anfragen von Bürgerinnen und Bürgern, die den Internetdienst Moneyhouse der Firma itonex AG betrafen, sprunghaft an. Es wurden insbesondere Fragen gestellt zur Veröffentlichung von andernorts gesperrten Adressen im Internet, zur umfangreichen Darstellung der sozialen Netzwerke der betroffenen Personen und zur Preisgabe von Personendaten von minderjährigen Kindern. Diese Daten erschienen in den Resultaten der von Moneyhouse angebotenen Personensuche. Nachdem sich Personen bei uns meldeten, die vergeblich versucht hatten, mit dem Unternehmen Kontakt aufzunehmen, um die Veröffentlichung ihrer Adressdaten aus Sicherheitsgründen schnellstens zu stoppen, eröffneten wir eine Sachverhaltsabklärung.

In der Folge gelang es jedoch auch uns nicht, Kontakt zu dem Unternehmen herzustellen. Deshalb ersuchten wir das Bundesverwaltungsgericht (BVGer) um Erlass einer vorsorglichen Massnahme. Wir wollten damit erreichen, dass der Dienst der Personensuche einstweilig eingestellt wird, weil Betroffenen durch die Publikation ihrer Adresse akute Gefahr drohte.

Das BVGer wies Moneyhouse in einer ersten Zwischenverfügung an, die umstrittene Personensuche vorläufig nicht mehr anzubieten. In einer weiteren Zwischenverfügung liess das Gericht später die Suchfunktion unter strengen Auflagen wieder zu. Demzufolge müssen Adressdaten auf Verlangen von Betroffenen innerhalb eines Arbeitstages gelöscht werden. Dieser Entscheid berührt die materielle Frage, ob mit der Veröffentlichung der Personendaten im Internet gegen das Datenschutzrecht verstossen werde, nicht.

Wir sind der Ansicht, dass die Zulässigkeit der Veröffentlichung von Adressdaten im Internet, die betroffene Personen gesperrt haben, rechtlich überprüft werden muss. Aus diesem Grund haben wir uns in einem ersten Teil der Sachverhaltsabklärung

auf diese Fragestellungen fokussiert und dabei auch Empfehlungen gegenüber Moneyhouse abgegeben. Die Wirtschaftsauskunftei hat die Empfehlungen akzeptiert. Die weiteren Datenbearbeitungen sind nun Thema des zweiten Teils der Sachverhaltsabklärung.

1.8.3 Versand von Belegen des Handelsregisters via Internet

Im vergangenen Sommer haben zwei Kantone im Rahmen der Umsetzung des Öffentlichkeitsprinzips eine neue Praxis für ihre Handelsregister eingeführt. Sie übermitteln nunmehr per E-Mail über eine automatische Bekanntgabe sämtliche Belege augenblicklich an jede Person, die sie beantragt. Dieser uneingeschränkte Übergang von einer Einsichtnahme, die den Gang zum Handelsregister oder zumindest einen persönlichen Kontakt erforderte, zu einer Umsetzung des Öffentlichkeitsprinzips via Internet wirft grundlegende Fragen in Bezug auf den Daten- und Persönlichkeitsschutz auf.

Die Handelsregister von Zürich und Basel-Stadt machen ihre Belege seit Juli 2012 per E-Mail zugänglich. Wir wurden von betroffenen Bürgern sowie von den Polizeibehörden auf diesen Sachverhalt aufmerksam gemacht. Gemäss den uns erteilten Auskünften können die der Öffentlichkeit mittels automatischer Bekanntgabe verfügbar gemachten Dokumente Unterschriften, Geburtsdaten, Privatadressen, Nummern von Pässen, Identitätskarten, Kreditkarten und andere unter dem Sicherheitsaspekt heikle Informationen enthalten.

Zwar ist das im Gesetz verankerte Öffentlichkeitsprinzip für eine reibungslose Geschäftsabwicklung unerlässlich. Die zu diesem Zweck eingesetzten Mittel dürfen jedoch nicht losgelöst von jeglichen Datenschutzüberlegungen verwendet werden. Tatsächlich ist es problematisch, wenn solche persönlichen Informationen per Online-Dienstleistung zugänglich gemacht werden, da sich daraus schwer kontrollierbare Risiken ergeben (Betrug, Fälschung von Dokumenten, Datenverbindungen, usw.). Für die betroffenen Personen bedeutet das überdies den Verlust der Kontrolle über ihre eigenen Daten und damit über ihr verfassungsmässiges Recht auf Selbstbestimmung über ihre Informationen. Die Verknüpfung von Daten durch Unternehmen, die auf die Beschaffung und systematische Verwertung von Personendaten spezialisiert sind, zum Beispiel Wirtschaftsauskunfteien, wird dadurch leicht gemacht. Diese Unternehmen bearbeiten in der Folge die Daten, um beispielsweise ohne Wissen der betroffenen Person Persönlichkeitsprofile zu erstellen. Hinzu kommt das internationale Element des Problems. Dieses ist nicht

zu vernachlässigen angesichts der Tatsache, dass es für einmal im Netz veröffentlichte Daten keine Grenzen gibt. Sie werden einerseits dem Geltungsbereich des schweizerischen Rechts entzogen und können andererseits in Staaten bearbeitet werden, die über kein angemessenes Datenschutzniveau verfügen.

Vom Standpunkt unserer Aufsichtstätigkeit aus weisen wir darauf hin, dass unsere Eingriffsmöglichkeiten im vorliegenden Fall begrenzt sind, namentlich weil öffentliche Register des Privatrechtsverkehrs ausdrücklich vom Geltungsbereich des Datenschutzgesetzes ausgenommen sind. Im Rahmen unserer Beratungs- und Unterstützungsaufgaben haben wir indes eine Diskussion mit der zuständigen Aufsichtsbehörde, dem Eidgenössischen Handelsregisteramt, aufgenommen. Wir wollten damit auf die oben erwähnten Risiken aufmerksam machen. Wir haben auch mehrmals im Rahmen der Vernehmlassungsverfahren zur Revision des Obligationenrechts und der Handelsregisterverordnung Stellung genommen, um den Gesetzgeber über die Probleme aufgrund der dieser Sachlage zu orientieren.

In Anbetracht dieser Ausführungen ist es ratsam, Personen, die in Zürich und Basel-Stadt eine Eintragung vornehmen wollen, schon vor dem Notar auf die Konsequenzen der in diesen Kantonen geltenden Praktiken aufmerksam zu machen. So können sie die derzeit vorhandenen Möglichkeiten nutzen, um den Inhalt der Belege auf das laut Gesetz unbedingt erforderliche Minimum zu beschränken. Umfassendere Informationen betreffend die diesbezüglich laufenden Gesetzesänderungen finden sich in Ziffer 1.8.4 des vorliegenden Tätigkeitsberichts.

1.8.4 Modernisierung des Handelsregisters – Änderung des Obligationenrechts

Das Handelsregister soll modernisiert werden. Neu vorgesehen ist eine elektronische, zentrale Datensammlung, die sich auf ein einheitliches Softwaresystem stützen soll. Aus datenschutzrechtlicher Sicht begrüssen wir vor allem die handelsregisterrechtlich konforme Einführung eines Rechts auf Vergessen.

Die Einträge im Handelsregister sollen neu in elektronischer Form direkt in der zentralen Datensammlung integriert und über das Internet veröffentlicht werden. Der zentrale Firmenindex (zefix) würde dadurch überflüssig. In die Gesetzesvorlage soll weiter eine Bestimmung für die Verwendung der AHV-Versichertennummer im Handelsregister aufgenommen werden. Damit wird eine automatische Aktualisierung der Angaben ermöglicht, die Pflicht zur Meldung von Änderungen des Namens oder der Nationalität würde entfallen. Die AHV-Versichertennummer würde weder offengelegt noch publiziert. Wir haben jedoch bemängelt, dass der

Kreis der Nutzungsberechtigten der Nummer in der Vorlage noch zu wenig genau bestimmt worden ist.

Die neue Organisation des Handelsregisters soll die Zusammenarbeit der Behörden erleichtern. So sollen via Amtshilfe, sofern keine Geheimnisschutzvorschriften dies verhindern, auch Einträge anderer Amtsstellen im Handelsregister ersichtlich sein. Zwecks besserer Identifikation wird zudem ein Personenregister dem Handelsregister angegliedert. Welche Datenfelder in diesem Personenregister zugänglich gemacht werden, war aus der Vorlage zu diesem Zeitpunkt nicht ersichtlich. Wir haben deshalb darauf aufmerksam gemacht, dass Bundesorgane besonders schützenswerte Personendaten nur im Abrufverfahren zugänglich machen dürfen, wenn dieses auf Gesetzesstufe genügend geregelt worden ist.

Im Rahmen dieser Ämterkonsultation haben wir erneut auf die Schwierigkeiten hingewiesen, welche die zeitlich unlimitierte Veröffentlichung von Handelsregisterdaten im Internet mit sich bringt. Wir vertreten seit langem die Ansicht, dass in dieser Hinsicht eine Interessenabwägung gemacht werden muss. Das öffentliche Interesse an der Publikation von alten Wirtschaftsdaten im Internet (wie z.B. Daten über eine gelöschte Unternehmung nach Ablauf aller Verjährungsfristen) sollte gegen das private Interesse der betroffenen Person an einer Entfernung dieser Daten aus dem Internet abgewogen werden. Es gibt andere Veröffentlichungskanäle, die dem Grundsatz der Verhältnismässigkeit besser entsprechen als das Internet.

Unsere Einwände wurden vom Bundesamt für Justiz entgegengenommen. In die Vorlage, die anschliessend für die Vernehmlassung ausgearbeitet wurde, ist neu ein dem Handelsregisterrecht angepasstes Recht auf Vergessen aufgenommen worden. Wir begrüssen diese Anpassung und verfolgen die weiteren Entwicklungen in diesem Bereich mit Interesse. Weitere Informationen zu diesem Thema sind in Ziff. 1.8.3 des vorliegenden Tätigkeitsberichts zu finden.

1.8.5 Bearbeitung von Personendaten im Adresshandel

Die Sachverhaltsabklärung bei einem Adresshändler konnten wir in vielen Punkten abschliessen. Einzig die Bearbeitung von Liegenschaftsdaten musste gesondert beurteilt werden. Wir kommen zum Schluss, dass deren Bearbeitung und Bekanntgabe zu unterlassen ist.

Im Berichtsjahr haben wir die Sachverhaltsabklärung bei einem Adresshändler vom letzten Jahr weitgeführt. Im Laufe der Arbeiten und Gespräche mit den

verantwortlichen Personen hat sich abgezeichnet, dass in den meisten Punkten Verständnis für unsere datenschutzrechtlichen Verbesserungsvorschläge besteht. Die Korrekturen betreffen fast alle im Wesentlichen die Grundsätze der Transparenz und der Information über die Datenbeschaffung und -bearbeitung. So hat der Adresshändler diesbezüglich alle unsere Änderungsvorschläge gemäss unserem Schlussbericht akzeptiert. Einzig die Bearbeitung von Liegenschaftsdaten mussten wir in einer separaten Stellungnahme behandeln. Darunter fallen beispielsweise das Baujahr des Gebäudes, die Anzahl Geschosse, aber auch Informationen aus Baugesuchen und weitere Details zu einer bestimmten Wohnadresse. Diese Angaben verknüpft der Adresshändler mit den Personen dieser Wohnadresse, und die Daten stellen folgedessen Personendaten im Sinne des DSG dar. Die Liegenschaftsangaben stammen zum Teil aus öffentlichen Quellen, wie etwa das Grundbuch oder Baugesuche, werden dort jedoch zweckgebunden publiziert. Eine Bearbeitung der Daten im Bereich des Adresshandels für Marketingaktivitäten oder andere Geschäfte von Dritten, stellt eine Verletzung des Zweckbindungsprinzips des DSG dar. Eine solche Verletzung kann durch die Einwilligung der betroffenen Personen gerechtfertigt sein, was vorliegend jedoch nicht der Fall ist. Deshalb kommen wir zum Schluss, dass hier die Bearbeitung von Liegenschaftsdaten aufgrund eines fehlenden Rechtfertigungsgrundes zu unterlassen ist. Der Adresshändler hat auch diesen Punkt grundsätzlich akzeptiert und wird die Daten nicht mehr personenbezogen bearbeiten und an Dritte bekannt geben. Details dazu werden im Rahmen einer Nachkontrolle von uns überprüft und beurteilt werden.

1.8.6 Öffnung des Postmarkts: Totalrevision der Verordnung

Im Rahmen der Ämterkonsultation zur Totalrevision der Postverordnung haben wir unsere Stellungnahme abgegeben. Dabei äusserten wir uns zu den Informationspflichten und zum Umgang mit Adressdaten, insbesondere zu deren Weitergabe an Dritte.

Im letzten Quartal des vergangenen Jahres sind das totalrevidierte Postgesetz und Postorganisationsgesetz samt den zugehörigen Verordnungen in Kraft getreten. Nachdem die Gesetze bereits 2010 vom Parlament verabschiedet worden waren, mussten noch die entsprechenden Verordnungen revidiert werden. Im Rahmen der Ämterkonsultation hatten wir die Möglichkeit, zu den Verordnungsentwürfen Stellung zu nehmen.

Die Totalrevision der Postgesetzgebung verfolgte zwei Hauptziele: Zum einen sollte der Verfassungsauftrag – die Sicherstellung der Grundversorgung der Bevölkerung

mit Dienstleistungen des Post- und Zahlungsverkehrs – umgesetzt, zum anderen der Postmarkt für die privaten Anbieterinnen vollständig geöffnet werden. Um Letzteres zu gewährleisten, bedarf es auch eines Austauschs von Personendaten. Wir richteten unseren Fokus bei der Beurteilung des Verordnungsentwurfes unter anderem auf die Informationspflichten der Dienstleistungsanbieterinnen über die Datenbearbeitungen und -weitergaben. Ein wichtiger Grundsatz des Datenschutzgesetzes ist nämlich die Transparenz der Datenbearbeitung; nur wenn sie gewährleistet ist, können die Betroffenen ihre Rechte auch wahrnehmen. Die neue Gesetzgebung verpflichtet daher alle Postdienstleistungsanbieterinnen mit Hauszustellung, die sich am Adressaustausch beteiligen, ihre Kundinnen und Kunden über den Umgang mit Adressdaten zu informieren.

Möchte eine Anbieterin von Postdiensten Datensätze an Dritte weitergeben, muss sie die Einwilligung der betroffenen Personen einholen. Es reicht nicht, die beabsichtigte Datenbekanntgabe in den allgemeinen Geschäftsbedingungen zu erwähnen. Vielmehr müssen die Betroffenen direkt über die Weitergabe der Daten an Dritte informiert werden, beispielsweise per Post oder prominent auf den Formularen der Kundenaufträge. Dabei müssen unter anderem auch die Kategorien der Datenempfänger genannt werden, denn nur wenn sich die Kundinnen und Kunden darüber im Klaren sind, in was sie einwilligen, können sie ihre Willenserklärung gültig abgeben. So ist es für die Betroffenen entscheidend, zu wissen, ob ihre Daten einzig an Unternehmen und Personen weitergegeben werden, mit welchen sie in einer direkten Vertragsbeziehung (Zeitschriftenverlage, Versicherungen, Banken etc.) stehen, oder aber auch an Adresshändler (Adressdienstleister) und Wirtschaftsauskunfteien.

Eine wichtige Neuerung ist zudem, dass der Widerspruch gegen die Weitergabe von Personendaten an Dritte keine Kostenfolgen haben darf. Damit wurde eine aus Sicht des Datenschutzes langjährige Forderung umgesetzt: Die Abgabe einer Willenserklärung muss nämlich nach vorgängiger Information freiwillig erfolgen, da sie sonst nicht rechtsgültig ist. Die alte Regelung erlaubte es jedoch, von den Postkundinnen und -kunden einen Zuschlag zu erheben, wenn sie sich gegen die Weitergabe ihrer Daten an Dritte entschieden. Die Reaktionen der Bürgerinnen und Bürger auf die im Frühjahr erfolgte Preiserhöhung zeigte, dass die Höhe des Zuschlags Auswirkungen auf die Abgabe der Einwilligung gehabt haben dürfte. Das war insofern problematisch, als dass die Ausübung eines Grundrechts nicht von monetären Überlegungen abhängig sein sollte.

Unsere im Rahmen der Ämterkonsultation gemachten Anmerkungen zu den Informationspflichten und zum Umgang mit Adressdaten, insbesondere zur Weitergabe von Personendaten an Dritte, wurden damit berücksichtigt. Die Betroffenen

können sich nun ohne finanzielle Nachteile für oder gegen die Weitergabe ihrer Adressdaten an Dritte aussprechen.

1.8.7 Datenbank eines Finanzdienstleisters zur Speicherung von sicherheitsrelevanten Ereignissen

Das geheime Sammeln und Verknüpfen von Daten über Mitarbeiter, Dritte und Kunden durch eine Bank ist ein datenschutzrechtlich heikles Unterfangen. Trotz allfälligen gesetzlichen Sorgfaltspflichten, die ein solches Vorgehen rechtfertigen würden, muss die Datenbearbeitung den Vorgaben und Grundsätzen des Datenschutzgesetzes entsprechen. Um dies zu prüfen, haben wir eine Sachverhaltsabklärung eröffnet.

Im Verlauf dieses Redaktionsjahres wurden wir durch Medienberichte auf eine angeblich datenschutzwidrige und geheime Datenbank, die von einer schweizerischen Grossbank geführt werde, aufmerksam. Darin seien Personendaten über Kunden, Mitarbeitende und Dritte, zum Teil ohne ihre Kenntnis, gespeichert. Da die Persönlichkeit einer grösseren Anzahl von Personen in unverhältnismässiger Art und Weise verletzt sein könnte, stellte sich eine Prüfung dieser Bearbeitungsmethoden als unabdingbar heraus. Wir haben deshalb im Rahmen unserer Aufsichtskompetenzen über juristische Personen eine Sachverhaltsabklärung eröffnet.

In diesem Zusammenhang hat sich die Bank in einer ersten Stellungnahme dahingehend geäussert, dass diese Daten sicherheitsrelevant seien, und sich dabei auf ein überwiegendes Privatinteresse und gesetzliche Pflichten als Rechtfertigungsgrund für diese Datenbearbeitungen gestützt. Ob und wie die Bearbeitung, Zugriffe, Datenflüsse, Aufbewahrungsdauer und die Voraussetzungen der Bekanntgabe geregelt sind, werden wir im Rahmen des eröffneten Verfahrens prüfen.

Die Sachverhaltsabklärung ist noch im Gange.

1.9 International

1.9.1 Internationale Zusammenarbeit

Das vergangene Jahr war geprägt durch die Fortführung der Arbeiten zur Revision und Modernisierung des Übereinkommens 108, der Richtlinien der OECD und des europäischen Rechtsrahmens sowie durch einen intensiveren Gedankenaustausch der Datenschutzbeauftragten im Hinblick auf eine verstärkte internationale Zusammenarbeit. Wir haben an diesen Arbeiten und Überlegungen namentlich durch eine aktive Präsenz im Europarat, in der OECD, bei der europäischen und der internationalen Konferenz der Datenschutzbeauftragten und in der französischsprachigen Vereinigung der Datenschutzbehörden mitgewirkt. Auch an den Arbeiten der gemeinsamen Kontrollinstanzen Schengen, Eurodac und Visa waren wir beteiligt.

Europarat

Der beratende Ausschuss des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen 108) hat unter dem Vorsitz des stellvertretenden Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten seine Arbeiten zur Modernisierung dieses verbindlichen Rechtsinstruments fortgeführt und abgeschlossen. Auf seiner 29. Plenartagung vom 27. bis 30. November 2012 verabschiedete er in diesem Zusammenhang einen Änderungsentwurf zum Übereinkommen. Dieser soll an das Ministerkomitee des Europarates weitergeleitet werden, der einen zwischenstaatlichen Adhoc-Ausschuss mit der abschliessenden Bearbeitung beauftragen wird. Dieser Ausschuss sollte auch Nichtmitgliedstaaten des Europarates offen stehen, die für einen Beitritt zum Übereinkommen 108 in Betracht kommen.

Bei diesen Arbeiten zur Modernisierung des Übereinkommens geht es darum, den mit der Verwendung der neuen Informations- und Kommunikationstechnologien verbundenen Herausforderungen entgegen zu treten. Das Recht auf Datenschutz sollte verstärkt und gleichzeitig mit der Ausübung anderer Rechte und Grundfreiheiten in Einklang gebracht werden. Zudem sollen die Umsetzungs- und Überwachungsmechanismen des Übereinkommens verbessert werden. Der Text soll einen technologisch neutralen Ansatz verfolgen und die Kohärenz und Vereinbarkeit mit dem Rahmen der Europäischen Union sicherstellen. Schliesslich sollen diese Arbeiten auch dazu beitragen, die universelle Bestimmung und die offene Ausgestaltung des Übereinkommens zu stärken und zu fördern.

Gegenstand und Zweck des Übereinkommens ist es, für jede natürliche Person das Recht auf den Schutz personenbezogener Daten sicherzustellen, um die Wahrung der übrigen Rechte und Grundfreiheiten bei der Verarbeitung personenbezogener Daten zu gewährleisten. Der Geltungsbereich des überarbeiteten Übereinkommens wird erweitert und soll jegliche Verarbeitung von personenbezogenen Daten, ungeachtet der verwendeten Mittel und Verfahren, erfassen. Er ist nicht mehr ausschliesslich auf automatisierte Verarbeitungsformen beschränkt. Dagegen wird zu Recht die Verarbeitung durch eine natürliche Person für die Ausübung rein persönlicher oder privater Aktivitäten vom Geltungsbereich ausgenommen. Im Vergleich zum bisherigen Text sieht der Revisionsentwurf eine genauere Umschreibung des Verhältnismässigkeitsprinzips vor, das neu nicht mehr nur die Daten selbst, sondern auch die Bearbeitung und die Wahl der Mittel umfasst; andererseits führt er den Grundsatz der Datenminimierung ein.

Der Entwurf legt auch ganz allgemein die Voraussetzungen für die Zulässigkeit der Bearbeitung fest, nämlich die Einwilligung oder jede andere rechtmässige Begründung. Dieser letztere Ausdruck deckt namentlich die in Artikel 13 DSG aufgeführten Rechtfertigungsgründe und das Erfordernis der gesetzlichen Grundlage für die Bearbeitung durch Organe des Bundes im Sinne von Artikel 17 DSG ab. Betreffend die besonders schützenswerten Daten bleibt der Grundsatz des Verbots bestehen. Diese Daten dürfen nur bearbeitet werden, wenn das innerstaatliche Recht angemessene Garantien vorsieht, welche die übrigen im Übereinkommen genannten Garantien ergänzen. Mit diesen zusätzlichen Garantien soll den Risiken vorgebeugt werden, die für die betroffene Person bei der Datenbearbeitung entstehen können. Zudem wird der Katalog der besonders schützenswerten Daten um die genetischen Daten und auf die biometrischen Daten erweitert, die eine Person eindeutig identifizieren. Unterschieden wird zwischen den von Natur aus besonders schützenswerten Daten, wie etwa Gesundheitsdaten, und den Daten, die aufgrund ihrer Verwendung besonders schützenswert sind, etwa Daten, deren Bearbeitung die rassische Herkunft erkennen lässt. Mit diesem Vorgehen wird namentlich vermieden, dass Fotos automatisch als besonders schützenswerte Daten gelten.

Der vom T-PD angenommene Entwurf sieht auch die Einführung einer Meldepflicht bei Datenschutzverletzungen vor, wenn diese die Rechte und Grundfreiheiten der betroffenen Personen in schwerwiegender Weise beeinträchtigen können. Die Meldung sollte bei den Datenschutzbehörden erfolgen. Eine Information der betroffenen Personen ist nicht vorgesehen. Es wird jedoch Aufgabe der Behörden sein, über eine solche Information zu entscheiden. Der Entwurf führt auch die Pflicht ein, die betroffenen Personen anlässlich der Beschaffung von Personendaten zu informieren. Er stärkt zudem deren Rechte und beschreibt die Pflichten der für die

Bearbeitung verantwortlichen Personen. Insbesondere müssen sie die Massnahmen nachweisen können, die sie zur Gewährleistung des Datenschutzes treffen, und Folgenabschätzungen vornehmen. Die Vertragsparteien haben ausserdem darauf zu achten, dass die für die Datenbearbeitung bestimmten Produkte und Dienstleistungen schon im Planungsstadium den Auswirkungen des Rechts auf Datenschutz genügen und die Konformität der Datenbearbeitung mit dem geltenden Recht erleichtern («Privacy by design»).

Bezüglich der grenzüberschreitenden Datenströme hält der Entwurf am freien Informationsfluss zwischen den Parteien fest. Die innerhalb der Europäischen Union eingerichtete spezifische Regelung auf der Grundlage der Äquivalenz von Drittstaaten bleibt indessen bestehen. Die Anerkennung der Äquivalenz in den Vertragsstaaten, die nicht Mitglieder der Europäischen Union sind, sollte allerdings erleichtert werden. Die Übermittlung an Drittstaaten hängt vom Erfordernis eines angemessenen Datenschutzniveaus ab, das in Gesetzesbestimmungen oder auf Ad-hoc- oder Standardgarantien begründet sein kann, die in verbindlichen Rechtsurkunden verankert sind (bspw. in Verträgen oder zwingenden Unternehmensvorschriften). Die Bekanntgabe in Ermangelung eines angemessenen Schutzniveaus ist mit der entsprechenden Einwilligung weiterhin möglich, soweit sie erforderlich ist für den Schutz der spezifischen Interessen der betroffenen Person oder für die Wahrung überwiegender legitimer Interessen, namentlich gesetzlich vorgesehener bedeutender öffentlicher Interessen. Ausnahmen sind auch möglich, um die Meinungsäusserungs- und Informationsfreiheit zu gewährleisten. Die Datenschutzbehörden müssen jedoch zum Einschreiten berechtigt sein, insbesondere im Zusammenhang mit Ad-hoc-Garantien.

Der Revisionsentwurf stärkt auch die Kompetenzen der Kontrollbehörden. Diese erhalten Entscheidungs- und Sanktionsbefugnisse. Ihre Unabhängigkeit sollte besser gewährleistet sein. Sie müssen insbesondere mit angemessenen personellen, technischen und finanziellen Mitteln ausgestattet werden und über die notwendigen Infrastrukturen für die Erfüllung ihrer Aufgaben verfügen und ihre Befugnisse unabhängig und effektiv ausüben. Schliesslich muss die Zusammenarbeit zwischen den Datenschutzbehörden verstärkt werden, namentlich im Hinblick auf eine Koordinierung ihrer Interventionen und Untersuchungen oder bei der Durchführung gemeinsamer Massnahmen.

Einer der Mängel des geltenden Übereinkommens ist einerseits die fehlende Kontrolle vor der Ratifizierung oder dem Beitritt, andererseits die fehlende Überwachung der Einhaltung der daraus entstehenden Verpflichtungen. Der Entwurf sieht vor, dass die Parteien in ihrem innerstaatlichen Recht die erforderlichen Massnahmen einführen müssen, um den Bestimmungen dieses Übereinkommens Wirkung

zu verleihen und ihre effektive Durchführung zu gewährleisten. Diese Massnahmen müssen vor der Ratifizierung oder dem Beitritt getroffen werden. Ausserdem müssen die Parteien dem Vertragsausschuss die Möglichkeit geben, die Einhaltung ihrer Verpflichtungen zu beurteilen. Damit wird die Rolle des Ausschusses gestärkt. Neben den bisherigen Beratungsfunktionen kann er die Konformität des Datenschutzniveaus eines Staates mit den Bestimmungen des Übereinkommens evaluieren und dessen Umsetzung durch die Parteien periodisch überprüfen.

Der EDÖB unterstützt den vom beratenden Ausschuss verabschiedeten Entwurf. Nach dessen Annahme durch das Ministerkomitee wird eine Änderung unserer eidgenössischen und kantonalen Datenschutzgesetzgebungen erforderlich werden.

Europäische Konferenz der Datenschutzbeauftragten

Die Frühjahrskonferenz der europäischen Datenschutzbeauftragten fand vom 3. bis 4. Mai 2012 in Luxemburg statt und wurde von der luxemburgischen Datenschutzbehörde organisiert. An der Konferenz nahmen Delegierte der Datenschutzbehörden aus 38 Ländern, sowie Vertreter des Europarates, der europäischen Instanzen und der OECD teil. Im Zusammenhang mit den Erwartungen an die europäische Datenschutzreform wurden auf der Konferenz die Reformprojekte der Europäischen Union und die Pläne zur Modernisierung des Übereinkommens 108 erörtert. So hatten wir die Gelegenheit, die Arbeiten zur Revision vorzustellen (s. Europarat oben). Diese Reformen sollen den Datenschutzgesetzgebungen mehr Effizienz und Klarheit verleihen, was nicht nur denjenigen dienen soll, die Daten bearbeiten, sondern auch den Bürgerinnen und Bürger, indem ihnen zu mehr Transparenz und einer besseren Kontrolle über ihre Daten verholfen und die Wahrnehmung ihrer Rechte erleichtert wird.

In diesem Rahmen diskutierten die Beauftragten über die Stärkung der Rechte der Nutzer von Internetdiensten, über die Notwendigkeit einer Vereinfachung der administrativen Pflichten der verschiedenen Akteure zugunsten einer grösseren Eigenverantwortung sowie über die Entwicklung und Stärkung der Rolle der Datenschutzbehörden. Zur Rolle der Datenschutzbehörden erklärte Viviane Reding, Vizepräsidentin der Europäischen Kommission und europäische Kommissarin für Justiz: «Die von der Europäischen Kommission vorgeschlagene Datenschutzreform schafft ein einziges Gesamtregelwerk wirksamer Datenschutzvorschriften, die unseren Bürgern mehr Kontrolle über ihre Daten sichern und es gleichzeitig den Unternehmen leichter machen, durch regelkonformes Vorgehen die Vorteile des Binnenmarktes zu nutzen. Eine einheitliche Gesetzgebung reicht aber nicht aus. Wir brauchen auch jemanden, der darauf achtet, dass diese Vorschriften überall

in der gesamten EU und überall auf die gleiche Weise angewendet werden. Aus diesem Grunde wollen wir mit unserer Reform die Rolle der nationalen Kontrollbehörden erheblich stärken und ihre Aufgaben und Befugnisse so harmonisieren, dass sie aus diesen Regeln eine konkrete Realität für die europäischen Bürger und Unternehmen machen können.»

Die Beauftragten verabschiedeten eine Resolution über die europäische Datenschutzreform, in der sie die Bemühungen zur Stärkung der Rechte des Einzelnen und zur Verbesserung ihrer Effektivität unter Berücksichtigung des technologischen Wandels und der Globalisierung hervorheben und anerkennen. Die Beauftragten begrüssen insbesondere die Absicht, die Verantwortung der verschiedenen beteiligten Akteure und namentlich der für die Bearbeitung verantwortlichen Personen zu stärken, den Willen, den Verwaltungsaufwand zu verringern, sowie das Vorhaben, die Kohärenz des rechtlichen Rahmens zu verbessern und die Rolle der Datenschutzbehörden zu stärken. Sie machen indes auf das Risiko aufmerksam, das entstehen kann, wenn aufgrund von Ausnahmen und Abweichungen vom allgemeinen Datenschutzrahmen unterschiedliche Datenschutzregelungen gelten. Sie wünschen insbesondere im Sektor Polizei und justizielle Zusammenarbeit in Strafsachen ein ebenso hohes Datenschutzniveau wie für die dem allgemeinen Verordnungsentwurf unterstellten Sektoren.

Die Resolution ist auf unserer Webseite www.derbeauftragte.ch unter Der EDÖB – Internationale Zusammenarbeit abrufbar.

Gemeinsame Kontrollinstanz von Schengen (GKI)

Die gemeinsame Kontrollinstanz von Schengen (GKI) trat im Jahre 2012 vier Mal zusammen. Sie wählte den stellvertretenden eidgenössischen Beauftragten zu ihrem Vorsitzenden. Die GKI setzte ihre Kontrolltätigkeiten fort, namentlich ihre Inspektion der Warnsysteme betreffend gesuchte Personen, die zwecks Auslieferung festzunehmen sind. Der Schlussbericht und die damit einhergehenden Empfehlungen sollen im ersten Quartal 2013 angenommen werden. Die GKI hat ihren Bericht über die Folgemassnahmen zu den Empfehlungen fertig gestellt, die im Anschluss an die Kontrolle betreffend die im SIS integrierten Personen- oder Fahrzeugdaten zum Zweck der diskreten Überwachung oder einer spezifischen Kontrolle abgegeben wurden. Dieser Bericht wird veröffentlicht.

Eine Erhebung betreffend die Ausübung des Auskunftsrechts in den verschiedenen Schengen-Staaten ist ebenfalls im Gange und sollte 2013 abgeschlossen werden. Die GKI nahm auch Kenntnis von den Kontrollen des EDÖB bei den Schweizer Botschaften ausserhalb der Schengen-Zone und wies auf die Bedeutung solcher Kontrollen hin. Ausserdem verfolgt die GKI die Entwicklungen betreffend das SIS2

und namentlich die Migration von SIS1+ zu SIS2, die im ersten Quartal 2013 anlaufen sollte. Sie äusserte insbesondere den Wunsch, an der Einrichtung der in der Regelung des SIS2 vorgesehenen neuen Kontrollstruktur mitwirken zu können.

Auf schweizerischer Ebene erfolgt die Koordinierung der Tätigkeiten im Rahmen von Schengen in einer aus dem EDÖB und den kantonalen Datenschutzbehörden bestehenden Koordinationsgruppe. Diese tagt mindestens zwei Mal jährlich. Über sie können die Kantone über die laufenden Entwicklungen und über die Tätigkeiten der GKI informiert, die Kontrolltätigkeiten geplant und Informationen ausgetauscht werden. 2012 hatte die Gruppe namentlich die Gelegenheit zu einem Gedankenaustausch über die Kontrollmethoden.

Aufsichts-Koordinationsgruppen Eurodac und VIS

Am 24. Mai und am 21. November 2012 fanden die Sitzungen der Koordinationsgruppe Eurodac statt, an denen wir teilnahmen. Der Europäische Datenschutzbeauftragte (EDSB) berichtete über die bei der Zentraleinheit Eurodac durchgeführte Kontrolle. Thematisiert wurde auch die koordinierte Kontrolle der unlesbaren Fingerabdrücke. Weiter wurde ein Fragebogen für die Kontrollen der für den Verkehr mit der Zentraleinheit zuständigen Stellen in den einzelnen Mitgliedstaaten sowie der revidierte Vorschlag der Europäischen Kommission der Eurodac-Verordnung besprochen. Diskutiert wurde auch der Übergang der Eurodac-Daten von der Europäischen Kommission zur IT-Agentur in Tallinn (Estland). Der Server befindet sich in Strassburg (Frankreich).

Am 21. November 2012 fand die erste offizielle Sitzung der Koordinierungsgruppe VIS statt. Wie in unserem letzten Tätigkeitsbericht erwähnt, konnte das europäische Visa-Informationssystem (VIS) seinen Betrieb für die erste Region am 11. Oktober 2011 aufnehmen (vgl. unseren 19. Tätigkeitsbericht 2011/2012, Ziff. 1.10.1). Die Koordinierungsgruppe VIS ist gleich aufgebaut wie diejenige zu Eurodac und setzt sich ebenfalls aus dem EDSB und den nationalen Datenschutzbehörden zusammen. Folglich sind auch wir dort vertreten. Besprochen wurde unter anderem die Inbetriebnahme des VIS am 2. Oktober 2012 in einer weiteren Region, nämlich den Golfstaaten. Der EDSB stellte zudem seine Kontrolle bei der Zentraleinheit VIS vor.

Internationale Konferenz der Datenschutzbeauftragten

Die 34. Internationale Konferenz der Datenschutzbeauftragten fand vom 23. bis 26. Oktober 2012 in Punta del Este in Uruguay statt (www.privacyconference2012.org). Wie gewohnt kamen zu der Konferenz Datenschutzbehörden aus den vier Kontinenten, Vertreter der Industrie und der Zivilgesellschaft, Regierungsdelegierte, internationale Organisationen und Akademiker zusammen. Sie war in zwei Teile gegliedert,

von denen der eine den Datenschutzbehörden vorbehalten war und der andere den übrigen interessierten Akteuren offen stand. Das Programm der 34. Konferenz gestaltete sich um das Thema «Privatsphäre und Technologie im Gleichgewicht». Sie ermöglichte globale Beratungen über die Erwartungen der Informationsgesellschaft angesichts der Standards und Vorschriften für den Schutz von Personendaten. Es wurden auch verschiedene von den Staaten im Rahmen der Informationsgesellschaft eingerichtete Strategien geprüft, die namentlich der Entwicklung einer wirksameren, transparenteren, auf der Nutzung der neuen Technologien beruhenden Verwaltungsform dienen sollen. Die Beratungen galten insbesondere dem rechtlichen Rahmen der Online-Verwaltung. Die Konferenz verschaffte sich auch einen Überblick über die verschiedenen bestehenden oder in Vorbereitung befindlichen Rechtsmodelle im Bereich des Datenschutzes. Der Aspekt der Technologien und ihrer Auswirkung auf den Datenschutz (Geolokalisierung, Biometrie, intelligente Daten) sowie die Herausforderungen aufgrund gewisser technologischer Anwendungen (Online-Verhaltenswerbung, transparente Verwaltung) für den Datenschutz wurden ebenfalls angesprochen. Sodann ging die Konferenz auch auf gewisse spezifische Aspekte des Datenschutzrechts ein, darunter namentlich die aufgeklärte Einwilligung, der Schutz der Gesundheitsdaten, die Bekämpfung der Piraterie oder die internationale Zusammenarbeit der Datenschutzbehörden.

Bei der den Datenschutzbehörden vorbehaltenen Konferenz hatten die Beauftragten die Gelegenheit, die Frage der Verbesserung der internationalen Zusammenarbeit und der Strukturierung der Konferenz zu vertiefen. Sie pflegten auch einen umfassenden Meinungsaustausch über die Frage der Profilbildung (profiling). Zudem verabschiedeten die Beauftragten eine Resolution über die Zukunft der Privatsphäre. Darin verpflichten sie sich zu einer Intensivierung der gegenseitigen Zusammenarbeit, um koordiniert, namentlich durch gemeinsames Vorgehen, den Herausforderungen für den grenzüberschreitenden Datenschutz und den Risiken für die Privatsphäre entgegen zu treten. Sie verpflichten sich auch zu einem Informations- und Erfahrungsaustausch für einen optimalen Einsatz ihrer Ressourcen. Ausserdem wollen sie für die Förderung einer besseren Interoperabilität zwischen den verschiedenen Rechtssystemen und Regelungen zum Schutz der Privatsphäre sorgen. Des Weiteren nahmen die Beauftragten eine Resolution an, in der sie insbesondere davor warnen, dass Cloud Computing zu einer Schwächung der Datenschutzstandards führen könnte. Daher werden die für die Bearbeitung verantwortlichen Personen aufgefordert, vor dem Einsatz von Cloud Computing dessen Verträglichkeit mit der Privatsphäre zu analysieren. Die Anbieter von Cloud-Dienstleistungen müssen Transparenz gewährleisten und ausreichende Sicherheitsgarantien bieten; sie müssen insbesondere Datenverletzungen melden

können und den Nutzern weiterhin die Kontrolle über die Daten ermöglichen. Der Einsatz von Technologien zur Wahrung der Privatsphäre (privacy by design) und von Zertifizierungen ist zu fördern. Schliesslich verabschiedete die Konferenz eine Schlusserklärung in Sachen Profilbildung. Die Verwendung dieser Techniken hat im Einklang mit den Datenschutzanforderungen zu erfolgen (namentlich Transparenz, Wahrung der Verhältnismässigkeit, Evaluierung der für Profilierungen verwendeten Algorithmen, Rolle des Menschen, Kontrolle durch unabhängige Behörden).

Die Resolutionen und die Schlusserklärung befinden sich auf unserer Webseite www.derbeauftragte.ch unter Der EDÖB – Internationale Zusammenarbeit.

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

Die Arbeitsgruppe beschäftigte sich dieses Jahr insbesondere mit der Revision der Richtlinien zu Sicherheit und Datenschutz. Auch die Richtlinien zur Sicherheit der Informationsnetze werden zur Zeit überarbeitet. Schliesslich wurde die Frage der Wirtschaftlichkeit von personenbezogenen Informationen in Relation mit Datenschutz und Sicherheit untersucht.

Nachdem die für die Revision der Richtlinien zu Sicherheit und Datenschutz eingesetzte Expertengruppe in einem Dokument die Methodologie und den Rahmen des Revisionsprozesses festgelegt hatte, wurde das entsprechende Dokument nach einer Konsultationsrunde genehmigt. Die Absicht der Expertengruppe war nicht primär, alles zu ändern, sondern die Richtlinien unter Beibehaltung der noch geltenden Prinzipien im Zeitalter des Internets zu modernisieren. Dabei sollten zusätzliche begleitende Erläuterungen verfasst werden, die den heutigen technischen Gegebenheiten Rechnung tragen. Nach intensiven Diskussionen zwischen der Experten- und der Arbeitsgruppe wurden nun die Vorschläge für die Revision der Richtlinien präsentiert. Dabei werden deren acht Grundprinzipien nicht verändert, weil sie immer noch aktuell sind. Hingegen werden die Richtlinien ergänzt mit dem Ziel, Datenschutz effizienter zu gewährleisten.

Nebst kleineren redaktionellen Änderungen ist die Einführung von so genannten «privacy management programmes» massgebend. Obwohl diese noch nicht rechtlich definiert sind, würden sie Inhabern von Datensammlungen gewisse zusätzliche Verpflichtungen auferlegen. Privacy management programmes wären also gewissermassen als erweitertes Bearbeitungsreglement zu verstehen, welches für alle Datenbearbeitungen des Dateninhabers Geltung hat. Die wichtigsten Aspekte sind unter Anderem die Auflistung aller Datenschutz- und Datensicherheitsmassnahmen, die Implementierung von Massnahmen wie privacy by design, die Systemarchitektur, die Rolle des Datenschutzberaters (privacy officer) und Pläne zur

Handhabung von Datenschutz- und Datensicherheitsproblemen. Schliesslich sollten Inhaber von Datensammlungen verpflichtet werden, ihre privacy management programmes den Datenschutzbehörden auf Anfrage vorlegen zu müssen.

Es ist auch vorgesehen, dass bei Datensicherheits- oder Datenschutzverletzungen der Inhaber der Datensammlung gehalten wäre, Behörden und die Öffentlichkeit zu informieren. Eine weitere Änderung betrifft die Bestellung von explizit unabhängigen und technisch kompetenten Datenschutzbehörden. Bei Übermittlungen von Personendaten ins Ausland wird auf die Notwendigkeit von adäquaten Modellen hingewiesen, die den Datenschutz über die nationalen Grenzen hinaus gewährleisten. Hierbei wird auf das sowohl in der EU als auch in der Schweiz geltende Modell der Länderliste mit gleichwertigem Datenschutz verwiesen.

Andere Neuerungen betreffen die Verstärkung der internationalen Zusammenarbeit, die Sensibilisierung und Ausbildung, die technischen Massnahmen zu mehr Datenschutz («privacy enhancing technologies», kurz PET), die Sicherstellung des grenzübergreifenden Datenschutzes, unabhängig davon, wo sich die Daten befinden. D.h. es sollte nicht mehr möglich sein, durch die Auswahl eines bestimmten Landes zur Ablage der Daten, Datenschutzbestimmungen zu umgehen. Schliesslich wird in den Richtlinien ausdrücklich festgehalten, dass der Schutz von Personendaten ein Grundrecht ist, welches nebst anderen Grundrechten besteht.

Ein weiteres Dokument hält all jene Vorschläge fest, die im Änderungsprozess nicht vollständig berücksichtigt wurden, jedoch im weiteren Verlauf der Revision diskutiert werden sollen. Insbesondere betrifft dies das Erfordernis der Information und Einwilligung («notice and choice»), und die Notwendigkeit, die Verwendung von Personendaten zu beschränken («specification and use limitation»). Die ursprünglichen Erläuterungen zur Richtlinie bleiben bestehen, während die neuen Änderungen und Ergänzungen in einem zusätzlichen Dokument aufgelistet und entsprechend erklärt werden. Somit begleiten zwei erklärende Erläuterungen die Richtlinie und sind deren integraler Bestandteil.

Wenn man bedenkt, dass innerhalb der OECD verschiedene Rechtssysteme berücksichtigt werden müssen, sind die vorgeschlagenen Änderungen für die Schweiz und den breiteren europäischen Raum sicher ein Schritt in die richtige Richtung. Höchstwahrscheinlich wird es nicht möglich sein, alle uns in Europa bekannten Datenschutzprinzipien in der Revision zu berücksichtigen. Sie soll in der zweiten Hälfte 2013 abgeschlossen werden.

Gleichzeitig werden die Richtlinien zur Sicherheit der Informationsnetze revidiert, deren Kerngehalt jedoch nicht geändert werden muss. Hingegen sollten diese Richtlinien den heutigen technischen Gegebenheiten und Herausforderungen

angepasst werden. Insbesondere sollten Sicherheitsaspekte über kritische IT-Systeme in Verbindung mit dem Internet integriert werden. Zentraler Punkt ist die geteilte Sicherheitsverantwortung von Staat und privatem Sektor. Die Sicherheitsrichtlinien werden nicht mit den Datenschutzrichtlinien vereinigt, jedoch sollen die Synergien hervorgehoben werden, beispielsweise über eine Referenzierung der entsprechenden Bestimmungen.

Zur Studie über die Frage der Wirtschaftlichkeit von personenbezogenen Informationen in Relation mit Datenschutz und Sicherheit waren in den vorangegangenen Sitzungen vier Bereiche (soziale Netzwerke, Wirtschaftsauskunfteien, Suchmaschinen und Kundenbindungsprogramme) ausgewählt worden, anhand denen Berechnungen vorgenommen werden sollten. Verschiedene Resultate sind bemerkenswert, so etwa die Preise, die Unternehmen für einzelne Datensätze anbieten, aber auch diejenigen, die auf illegalen Märkten gelten. Weiter unterscheiden sich diese Preise stark vom Wert, den betroffene Personen für einzelne Datensätze angeben (Selbsteinschätzung), und dem weit tieferen Preis, den Individuen für deren Schutz zu bezahlen bereit wären. Diese Werte unterscheiden sich je nach Staat, abhängig von der vor Ort geltenden Wahrnehmung der Privatsphäre. Beispiele dafür sind die divergierenden Vorstellungen von US- und EU-Bürgern oder das unterschiedliche Verständnis von Privatsphäre im asiatischen Raum .

Die Studie ist nun vollendet und zeigt die verschiedenen Möglichkeiten auf, wie man den Wert resp. den Preis von Datensätzen berechnen kann.

Französischsprachige Vereinigung der Datenschutzbehörden

Die französischsprachige Vereinigung der Datenschutzbehörden (AFAPDP) führte ihre sechste Konferenz und ihre Generalversammlung vom 21. bis 23. November 2012 in Monaco durch. Die Konferenz begann mit einem den Vertretern der französischsprachigen Staaten und Behörden des afrikanischen Kontinents vorbehaltenen Teil. In diesem Rahmen konnten die Behörden dieser Staaten die Bedeutung des Schutzes von Personendaten ansprechen und spezifisch auf den afrikanischen Kontinent zugeschnittene Massnahmen vorschlagen.

Diskussionsthemen waren die in Ausarbeitung befindlichen Rechtsinstrumente, die Bedeutung der Biometrie im Bereich des Datenschutzes und die transparente Verwaltung («open data»), sowie die bei der Einsetzung von neuen Datenschutzbehörden und der Entwicklung einer «Datenschutzkultur» auftretenden Schwierigkeiten. Im zweiten Konferenzteil konnten die Arbeiten und Standpunkte der französischsprachigen Behörden aufgezeigt werden. Die Behörden gingen auf die Frage der Kontrolle der Datenschutzbehörden über die Entwicklung der elektronischen Verwaltung, die Sensibilisierungsaufgaben der Datenschutzbehörden, die digitale

Ausbildung, namentlich mit der Präsentation der Plattform www.thinkdata.ch, den Einsatz der Biometrie bei Wahlen und die Bedeutung von technischem Fachwissen bei den Datenschutzbehörden im Rahmen der Ausübung ihrer Befugnisse ein.

Bei den Diskussionen über den Einsatz der Biometrie im Rahmen von Wahlen in Afrika, namentlich zur Verhinderung von Wahlbetrug (mehrfache Stimmabgaben) stellten wir fest, dass die Verwendung der Biometrie den angestrebten Zweck bei weitem nicht erfüllt und mehr kommerziellen Zwecken gewisser europäischer Unternehmen dient. Tatsächlich können die Probleme mit Fehlabläufen, namentlich bei den Bevölkerungsregistern in den betroffenen Ländern, nicht mit der Biometrie gelöst werden. Es ist auch hervorzuheben, dass die Präsentation der Plattform Thinkdata auf grosses Interesse bei mehreren französischsprachigen Behörden gestossen ist, die diesen Dienst im Rahmen ihrer Sensibilisierungsaufgaben übernehmen könnten. Schliesslich äusserten die Teilnehmer den Wunsch nach einer Vernetzung der technologischen Kompetenzen der verschiedenen Behörden.

Anlässlich ihrer Generalversammlung nahm die AFAPDP Kenntnis von einem Zwischenbericht über die Einrichtung eines Systems, in dessen Rahmen die Angemessenheit des Schutzes bei Datenübertragungen in der Praxis beurteilt werden kann (namentlich Einführung einer verbindlichen Unternehmensklausel). Es sollte im Laufe des Jahres 2013 beschlossen werden. Die Generalversammlung nahm Kenntnis vom Fortschritt der Arbeiten zur Modernisierung des Übereinkommens 108. Sie verabschiedete eine Erklärung, in der die Annahme einer weltweit gültigen Urkunde zum Schutz von Personendaten nach dem Vorbild der im Jahre 2009 in Madrid verabschiedeten internationalen Rechtsnormen befürwortet wird (siehe unseren 17. Tätigkeitsbericht 2009/2010, Ziff. 1.10.1). Dieses Fernziel soll über Zwischenetappen erreicht werden, unter anderem über den Beitritt von Nichtmitgliedstaaten des Europarates zum Übereinkommen 108. Die AFAPDP könnte künftig auch eine Rolle bei der Verbreitung des Übereinkommens in den Schwellenländern spielen. So wird sie zu einem einflussreichen Partner im Bereich des internationalen Datenschutzes, und dies nicht nur aufgrund ihrer mit Hilfe der Internationalen Organisation der Frankophonie geleistete Unterstützung für die Schwellenländer, sondern auch durch ihre aktive Mitwirkung an den weltweiten Debatten. So hat sie zum Beispiel Beobachterstatus im Europarat und bei der Internationalen Konferenz der Datenschutzbeauftragten.

Die Erklärung von Monaco befindet sich auf unserer Webseite www.derbeauftragte.ch unter Der EDÖB – Internationale Zusammenarbeit.

2. Öffentlichkeitsprinzip

Die Anzahl der eingereichten Zugangsgesuche ist 2012 gegenüber dem Vorjahr um gut acht Prozent gestiegen. Gleich bleiben die Quoten bei der vollständigen Gewährung und der vollständigen Verweigerung des Zugangs. Eine leichte Abnahme um drei Prozentpunkte ist bei der teilweisen Gewährung (inkl. Zugangsgewährung unter zeitlichem Aufschub) zu verzeichnen. Die grösste Überraschung dürfte im massiven Einbruch der in Rechnung gestellten Gebühren liegen. Die Anzahl der eingereichten Schlichtungsanträge ist im Berichtsjahr um 20 Prozent auf 78 gestiegen.

2.1 Zugangsgesuche

2.1.1 Departemente und Bundesämter

Gemäss den uns mitgeteilten Zahlen sind im Jahr 2012 bei den Bundesbehörden insgesamt 506 Zugangsgesuche eingereicht worden. In 223 Fällen gewährten die Behörden einen vollständigen, in 120 einen teilweisen Zugang. Bei 138 Gesuchen wurde die Einsichtnahme vollständig verweigert. 19 Zugangsgesuche wurden zurückgezogen, wobei dies in mehr als der Hälfte der Fälle aufgrund der durch die Behörde veranschlagten Gebühren erfolgte. Sechs Fälle aus dem Berichtsjahr waren noch hängig. Es fällt auf, dass die Zahl der bei den Behörden eingereichten Zugangsgesuche weiter zunimmt, die anteilsmässige Verteilung der vollständigen Gewährung, der vollständigen Verweigerung und auch der teilweisen Gewährung des Zugangs hingegen sehr konstant bleibt (siehe Ziff. 3.7 des vorliegenden Tätigkeitsberichts). Die allgemeine Zunahme der Zugangsgesuche dürfte ein Zeichen für den wachsenden Bekanntheitsgrad des Öffentlichkeitsgesetzes als Instrument zur Informationsbeschaffung der Bevölkerung darstellen. Die Stabilisierung der Zahlen in Bezug auf die Zugangsgewährung bzw. -verweigerung spricht dafür, dass in den sechseinhalb Jahren seit Inkrafttreten des Öffentlichkeitsgesetzes bei den Behörden eine Sensibilisierung stattgefunden und sich im Umgang mit Zugangsgesuchen eine gewisse Routine und damit einhergehend auch eine gewisse Systematisierung eingestellt hat. Gegenüber dem Vorjahr zeigen die Prozentsätze der vollständigen Verweigerungen (27%) und der vollständig gewährten Zugänge (44%) keine Veränderung.

Am meisten Zugangsgesuche für das Jahr 2012 meldete uns die WEKO (27 Gesuche). Danach folgen das BAFU (25), das BAG (24) und das BFM (23). Bei den Departementen liegen das UVEK (100 Gesuche), das EDA (88) und das EVD (80; seit 1.1.2013 Eidgenössisches Departement für Wirtschaft, Bildung und Forschung WBF genannt)

an der Spitze. 16 von 72 Behörden meldeten uns für das Berichtsjahr, 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 2012 nicht fortgesetzt, im Gegenteil: Der bis anhin zu beobachtende Trend zu einer steten und teilweise massiven Zunahme der in Rechnung gestellten Gebühren ist im Berichtsjahr regelrecht eingebrochen. Die durch lediglich fünf Behörden erhobenen Gebühren haben sich im Vergleich zum Vorjahr auf rund 6300 Franken mehr als halbiert.

Was den Zeitaufwand für die Bearbeitung der Zugangsgesuche anbelangt, weisen wir erneut darauf hin, dass die Behörden erstens nicht verpflichtet sind, ihn zu erfassen, und dass es zweitens keine für die gesamte Bundesverwaltung geltenden Vorgaben für eine einheitliche Erfassung gibt. Die uns auf freiwilliger Basis übermittelten Angaben sind daher nur bedingt aussagekräftig. Gemäss diesen hat der gemeldete Zeitaufwand erneut zugenommen (2010: 815 Stunden; 2011: 1519 Stunden; 2012: 2155 Stunden). Der Zeitaufwand für die Mitwirkung in Schlichtungsverfahren erhöhte sich von 453 Stunden im 2011 nur leicht auf 480 Stunden im 2012.

2.1.2 Parlamentsdienste

Die Parlamentsdienste meldeten für das Berichtsjahr kein einziges Zugangsgesuch.

2.1.3 Bundesanwaltschaft

Die Bundesanwaltschaft meldete uns für das Jahr 2012 vier Zugangsgesuche, bei welchen der Zugang in einem Fall vollständig gewährt, in einem weiteren Fall vollständig verweigert und in zwei Fällen teilweise gewährt bzw. aufgeschoben wurde.

2.2 Schlichtungsanträge

Im 2012 wurden insgesamt 78 Schlichtungsanträge eingereicht (siehe Ziff. 3.10 des vorliegenden Tätigkeitsberichts), was einer Zunahme gegenüber dem Vorjahr (65 Anträge) von exakt einem Fünftel entspricht. Am meisten Anträge reichten Medienschaffende ein (33), gefolgt von Privatpersonen (21). Insgesamt wird von der Möglichkeit zur Einreichung eines Schlichtungsantrages gerade auch von Privatpersonen vermehrt Gebrauch gemacht. Diese Zahlen lassen folgende Schlüsse und Bemerkungen zu: In 258 Fällen verweigerte die Bundesverwaltung den Zugang vollständig (138) respektive teilweise (120). Dem stehen 78 bei uns eingereichte Schlichtungsanträge gegenüber. Im Berichtsjahr wurde somit in 30 Prozent aller Fälle von ganz oder teilweise abgelehnten Zugangsgesuchen ein Schlichtungsantrag eingereicht.

Insgesamt konnten im Berichtsjahr 61 Schlichtungsanträge abgeschlossen werden. Davon stammen 20 Anträge aus dem Berichtsjahr selbst, 35 aus dem Jahr 2011 und sechs noch aus dem Jahr 2010. In sechs Fällen konnte zwischen den Beteiligten eine Schlichtung erzielt werden. Insgesamt erliessen wir 19 Empfehlungen, wo keine einvernehmliche Lösung möglich oder von vornherein ersichtlich war. Damit konnten 26 Schlichtungsanträge erledigt werden. In drei Fällen gewährten die Ämter während des laufenden Schlichtungsverfahrens von sich aus den Zugang. 16 Schlichtungsanträge wurden zurückgezogen und in 14 Fällen waren die Voraussetzungen für die Anwendung des Öffentlichkeitsgesetzes nicht gegeben. In drei Fällen wurde der Schlichtungsantrag nicht fristgerecht eingereicht. In zehn von 25 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 von der Behörde zugestanden).

Antragstellende müssen aufgrund der Zunahme der Schlichtungsanträge und der nach wie vor knappen personellen Ressourcenlage weiterhin länger als die gesetzlich vorgesehenen 30 Tage auf die Durchführung eines solchen Verfahrens warten.

2.3 Abgeschlossene Schlichtungsverfahren

2.3.1 Empfehlungen

Nachfolgend werden die im Jahr 2012 erlassenen Empfehlungen im Bereich des Öffentlichkeitsgesetzes kurz zusammengefasst. Die vollständigen Versionen sind auf unserer Webseite www.derbeauftragte.ch unter Öffentlichkeitsprinzip – Empfehlungen – 2012 zu finden.

Empfehlung Bundesanwaltschaft / Arbeitsvertrag des alt Bundesanwalts (22. Februar 2012)

Der Antragsteller verlangte Zugang zum Arbeitsvertrag, welcher die Bundesanwaltschaft (BA) mit alt Bundesanwalt Erwin Beyeler für die Zeit vom Januar 2012 bis Februar 2012 abgeschlossen hatte. Die BA verweigerte den Zugang mit der Begründung, dass sie seit dem 1. Januar 2011 nicht mehr unter den Geltungsbereich des Öffentlichkeitsgesetzes falle. Zudem müsste der Zugang zum verlangten Dokument zum Schutz der Privatsphäre von Herrn Beyeler ohnehin verweigert werden. Demgegenüber kam der Beauftragte in seiner Empfehlung zum Schluss, dass das Öffentlichkeitsgesetz im vorliegenden Fall sehr wohl anwendbar sei und dass ein überwiegendes öffentliches Interesse an der Einsichtnahme in den Arbeitsvertrag von alt Bundesanwalt Beyeler bestehe; seine Privatsphäre werde durch das Zugänglichmachen dieses Dokumentes – wenn überhaupt – nur geringfügig beeinträchtigt.

Empfehlung SECO / Betriebslisten Gesamtarbeitsvertrag (3. April 2012)

Nachdem der Bundesrat einen Gesamtarbeitsvertrag (GAV) allgemein verbindlich erklärt hatte, verlangten mehrere Antragsteller beim Staatsekretariat für Wirtschaft (SECO) Einsicht in Listen, die von einer Paritätischen Landeskommission angeblich dem SECO zugestellt worden waren und dem Bundesrat als Grundlage für die Allgemeinverbindlicherklärung gedient haben sollen. Das Amt stellte den Antragstellern einen Teil der verlangten Listen zu und wies darauf hin, dass sich keine weiteren Dokumente in seinem Besitz befänden. Daher kam der Beauftragte in seiner Empfehlung zum Schluss, dass das Öffentlichkeitsgesetz nicht anwendbar sei.

Empfehlung BAG / Liste Acrylamidmessungen (19. Juni 2012)

Der Antragsteller verlangte beim Bundesamt für Gesundheit (BAG) Einsicht in eine Datentabelle, welche das Kantonale Labor Zürich (KLZH) im Auftrag des BAG zum Zwecke der Untersuchung von Acrylamidwerten in Lebensmitteln erstellt hatte. Das BAG verweigerte den Zugang vollständig, indem es argumentierte, dass mit

der Publikation «Acrylamide monitoring in Switzerland, 2007-2009: results and conclusions» das öffentliche Informationsinteresse der Bevölkerung erfüllt sei. Weiter bestünde mit der Zugänglichmachung der Liste die Gefahr, dass Geschäfts- und Fabrikationsgeheimnisse offenbart würden. Der Beauftragte stellte in seiner Empfehlung fest, dass das subjektive Zugangsrecht des Antragstellers durch die wissenschaftliche Publikation in einer Online-Zeitschrift nicht erfüllt sei; das BGÖ verlange die Veröffentlichung in einem Publikationsorgan oder auf einer Internetseite des Bundes. Weiter enthalte die Liste seines Erachtens keine Geschäfts- und Fabrikationsgeheimnisse. Der Beauftragte empfahl daher die Zugänglichmachung der Liste in anonymisierter Form.

Empfehlung BAG / Protokoll-Beilagen Eidgenössische Arzneimittelkommission (25. Juni 2012)

Der Antragsteller verlangte beim Bundesamt für Gesundheit (BAG) Zugang zu Protokoll-Beilagen (sog. Résumés) der Eidgenössischen Arzneimittelkommission, welche das BAG bei der Erstellung der sogenannten Spezialitätenliste berät. Das Amt verweigerte den Zugang zu diesen Résumés teilweise und argumentierte, gewisse Dokumente bildeten die Grundlagen für einen noch nicht getroffenen administrativen Entscheid. Darüber hinaus enthielten die Résumés Fabrikations- und Geschäftsgeheimnisse sowie Personendaten, die nicht zugänglich gemacht werden dürften. Der Beauftragte kam in seiner Empfehlung zum Schluss, dass das Amt den Zugang zu Recht teilweise verweigert hat, zum einen weil in gewissen Fällen der administrative Entscheid noch ausstand, zum anderen weil die Résumés tatsächlich schutzwürdige Fabrikations- und Geschäftsgeheimnisse sowie Personendaten enthielten.

Empfehlung ETHZ / Vertragsdokumente (16. Juli 2012)

Der Antragsteller verlangte von der Eidgenössischen Technischen Hochschule Zürich (ETHZ) Zugang zu Dokumenten (ca. 600 Seiten) im Zusammenhang mit einem Vertrag über die Entwicklung einer Software, den die ETHZ mit einem Unternehmen eingegangen war. Die ETHZ lehnte das Gesuch vollständig ab und führte an, dass die Unterlagen als Ganzes Geschäfts- und Fabrikationsgeheimnisse enthielten und dass eine Herausgabe überdies die Datenschutz- und Persönlichkeitsrechte der Mitarbeitenden der ETHZ verletze. In seiner Empfehlung hielt der Beauftragte vorweg fest, dass erstens die Beweispflicht für das Vorliegen eines Ausnahmegrundes bei der Behörde liege und daher eine Zugangsbeschränkung ohne gute Begründung nicht rechtmässig sei. Zweitens müsse die Behörde bei der Beurteilung von Gesuchen stets das Verhältnismässigkeitsprinzip beachten, weshalb der Zugang zu Textpassagen, die nicht durch eine Ausnahmeklausel des

Öffentlichkeitsgesetzes gedeckt sind, zwingend zu gewähren sei. Angesichts der umfangreichen Unterlagen, in die der Antragsteller Einsicht verlangte, empfahl der Beauftragte der ETHZ, dem Antragsteller eine Auflistung mit den relevanten Dokumenten zuzustellen, damit dieser sein Zugangsgesuch präzisieren könne.

Empfehlung BK / Chronologie Rücktritt Philipp Hildebrand (20. Juli 2012)

Der Antragsteller verlangte von der Schweizerischen Bundeskanzlei (BK) Zugang zu einer Chronologie des Rücktritts des Präsidenten der Schweizerischen Nationalbank. Die BK verweigerte den Zugang und begründete dies u.a. damit, dass Dokumente zuhanden des Bundesrates nicht veröffentlicht würden. In seiner Empfehlung hielt der Beauftragte fest, dass die BK als Stabsstelle des Bundesrates diese Chronologie als Informationsnotiz unmittelbar in seinem Auftrag erstellt hatte. Somit gelte die Informationsnotiz als Dokument des Gesamtbundesrates. Weil der Gesamtbundesrat jedoch nicht in den Anwendungsbereich des Öffentlichkeitsgesetzes fällt, empfahl der Beauftragte der BK, an ihrem Entscheid, die Dokumente nicht herauszugeben, festzuhalten.

Empfehlung BWO / Verkauf SWAG (9. August 2012)

Der Antragsteller verlangte beim Bundesamt für Wohnungswesen (BWO) Zugang zu allen entscheidrelevanten Dokumenten betreffend den Verkauf der Sapomp Wohnbau AG (SWAG) durch die Schweizerische Eidgenossenschaft. Mit der Abwicklung des Verkaufsgeschäftes hatte das BWO ein privates Unternehmen betraut. Das Amt bejahte die Anwendbarkeit des Öffentlichkeitsgesetzes und sprach sich für den teilweisen Zugang zu den Dokumenten aus. So verneinte es einerseits das Vorliegen von Geschäftsgeheimnissen und bejahte die Bekanntgabe von Personendaten aus überwiegendem öffentlichem Interesse. Andererseits verweigerte es den Zugang zu bestimmten Dokumenten, weil einzelne Ausnahmebestimmungen des Öffentlichkeitsgesetzes vorlägen respektive die Dokumente Personendaten von Dritten enthielten. Zudem führte das BWO aus, dass sich ein Teil der gewünschten Dokumente nicht in seinem Besitz befänden. Der Beauftragte hielt in seiner Empfehlung fest, dass der Bund bei der einzelfallweisen Auslagerung von öffentlichen Aufgaben dafür zu sorgen habe, dass die Umsetzung des Öffentlichkeitsprinzips nicht beeinträchtigt werde. Im konkreten Fall ging er davon aus, dass die Departementsleitung ihren definitiven Entscheid betreffend den Verkauf der SWAG aufgrund der ihr vom BWO zugestellten Unterlagen gefällt habe und das BWO für diesen Entscheid vorgängig alle relevanten Dokumente vom beauftragten Unternehmen erhalten bzw. von diesem eingefordert hatte. Weiter verneinte der Beauftragte das Vorliegen von Geschäftsgeheimnissen und erkannte in Bezug auf

bestimmte Personendaten Dritter ein überwiegendes öffentliches Interesse am Zugang. Insgesamt empfahl der Beauftragte, die Mehrheit der Dokumente zugänglich zu machen.

Empfehlung BSV / Sitzungsprotokolle AHV/IV-Kommission (16. August 2012)

Der Antragssteller verlangte vom Bundesamt für Sozialversicherungen (BSV) Einsicht in die Sitzungsprotokolle der AHV/IV-Kommission aus den Jahren 2011 und 2012. 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 und deren Sitzungen zudem gemäss internem Kommissionsreglement vertraulich seien. Der Beauftragte verwies in seiner Empfehlung auf Urteile des Bundesverwaltungsgerichts vom 17. Juni 2011 und vom 7. Dezember 2011 (vgl. unseren 19. Tätigkeitsbericht 2011/2012, Ziff. 2.4), gemäss denen Verwaltungskommissionen spätestens seit dem 1. Januar 2009 ebenfalls der dezentralen Bundesverwaltung angehören und damit auch in den Geltungsbereich des Öffentlichkeitsgesetzes fielen. Da das BSV keine Ausnahmegründe darlegen konnte, empfahl der Beauftragte, den Zugang zu den Sitzungsprotokollen zu gewähren.

Empfehlung SECO / Änderung Allgemeinverbindlicherklärung (18. September 2012)

Der Antragssteller verlangte vom Staatssekretariat für Wirtschaft (SECO) Zugang zu Unterlagen betreffend die Änderung der Allgemeinverbindlicherklärung (AVE) des Gesamtarbeitsvertrages (GAV) für die vorzeitige Pensionierung im westschweizerischen Ausbaugewerbe. Das SECO verweigerte den Zugang mit der Begründung, dass sich während der Dauer eines AVE-Verfahrens kein Anspruch auf Zugang zu Akten ableiten liesse und es sich vorliegend um für den bevorstehenden Bundesratsbeschluss relevante Dokumente handle. In seiner Empfehlung stützte der Beauftragte die Haltung des SECO, wonach bis zum entsprechenden Bundesratsbeschluss der Anwendungsfall eines noch nicht gefällten administrativen Entscheids vorliege, weshalb die amtlichen Dokumente noch nicht zugänglich gemacht werden müssten.

Empfehlung NDB / Dossier DDR-Spion (21. September 2012)

Der Antragsteller verlangte am 22. Mai 2012 beim Nachrichtendienst des Bundes (NDB) Zugang zum Dossier eines DDR-Spions. Der NDB verweigerte den Zugang und machte geltend, die Dokumente könnten aus Gründen der inneren und äusseren Sicherheit des Landes sowie zum Schutz der betroffenen Personen nicht

zugänglich gemacht werden. Weil die vom Antragsteller bezeichneten Dokumente allesamt vor Inkrafttreten des Öffentlichkeitsgesetzes erstellt worden waren und damit überhaupt nicht in dessen Anwendungsbereich fielen, hielt der Beauftragte in seiner Empfehlung fest, dass der Antragsteller über keinen Anspruch auf Herausgabe der Dokumente verfügt.

Empfehlung ENSI / Sicherheitsbericht Kernkraftwerk Mühleberg (2. Oktober 2012)

Der Antragsteller verlangte vom Eidgenössischen Nuklearsicherheitsinspektorat (ENSI) Zugang zu amtlichen Dokumenten im Zusammenhang mit der «Sicherheitstechnischen Stellungnahme zur periodischen Sicherheitsüberprüfung des Kernkraftwerks Mühleberg». Das ENSI verweigerte den Zugang vollständig mit der Begründung, dass ein Teil der bezeichneten Dokumente gemäss der Übergangsbestimmung des BGÖ nicht in den zeitlichen Geltungsbereich des Öffentlichkeitsgesetzes falle. Daneben seien alle übrigen Dokumente Teil von Verfahrensakten eines hängigen Verwaltungsverfahrens und somit nicht vom sachlichen Geltungsbereich des Gesetzes erfasst. In seiner Empfehlung gelangte der Beauftragte ebenfalls zum Schluss, dass die vom Antragsteller bezeichneten Dokumente in der Tat zu einem Teil nicht in den zeitlichen und zum anderen Teil nicht in den sachlichen Geltungsbereich des Öffentlichkeitsgesetzes fallen. Daher stütze er die Haltung des ENSI, den Zugang zu allen Dokumenten zu verweigern.

Empfehlung ESTV / Projekt INSIEME (5. Oktober 2012)

Der Antragsteller verlangte bei der Eidgenössischen Steuerverwaltung (ESTV) Zugang zu einer Liste mit Namen und Angaben sämtlicher Unternehmen, die für das IT-Projekt INSIEME Dienstleistungen erbracht hatten oder mit denen Dienstleistungs- und Lieferantenverträge abgeschlossen worden waren. Die ESTV gewährte den Zugang nicht umgehend, sondern schob ihn bis zum Abschluss des in der Zwischenzeit eingeleiteten Strafverfahrens auf. Zum gleichen Ergebnis kam der Beauftragte in seiner Empfehlung.

Empfehlung fedpol / Dezentral getätigte Beschaffungen (19. Oktober 2012)

Der Antragssteller verlangte vom Bundesamt für Polizei (fedpol) Zugang zu einem Bericht über dezentral getätigte Beschaffungen. fedpol verweigerte den Zugang u.a. mit der Begründung, dass aus dem Bericht Rückschlüsse zum polizeitaktischen Vorgehen der Bundeskriminalpolizei gezogen werden könnten. Dies würde die gerichtspolizeilichen Ermittlungen beeinträchtigen respektive zu einer Gefährdung der eingesetzten Mitarbeitenden führen. Der Beauftragte präzisierte vorab in

seiner Empfehlung, dass es sich bei den zu beurteilenden Dokumenten insbesondere um die Korrespondenz von fedpol mit dem Bundesamt für Bauten und Logistik und der Beschaffungskommission des Bundes. Ebenfalls betroffen war eine Tabelle, welche u.a. die Beschaffungsobjekte (z.B. Artikel wie Autobahnvignetten, Schränke und Heftklammern), die Vertragspartner und Gesamtkosten auflistete.

Der Beauftragte gelangte zum Schluss, dass der Schutzauftrag respektive die polizeiliche Ermittlungstätigkeit von fedpol auch bei Offenlegung der verlangten Dokumente weiterhin problemlos erfüllt werden könne und die zielkonforme Durchführung konkreter behördlicher Massnahmen und Ermittlungserfolge durch eine breite Kenntnisnahme der erworbenen Beschaffungsobjekte nicht beeinträchtigt werde. Weiter war der Beauftragte der Ansicht, dass das Interesse der Öffentlichkeit am uneingeschränkten Zugang zu den Dokumenten gegenüber dem Schutz der Privatsphäre der Vertragspartner überwiege und die Mitarbeitenden von fedpol im Falle der Zugänglichmachung ihrer Personendaten keine nachteiligen Folgen zu erwarten hätten. Dementsprechend empfahl er den Zugang zu den verlangten Dokumenten.

BK / Bundesratsbeschluss zur Übermittlung von Mitarbeiterdaten an das amerikanische Justizdepartement (19. Oktober 2012)

Die Antragstellerin verlangte bei der Bundeskanzlei (BK) Zugang zur Kopie des Bundesratsbeschlusses betreffend die Übermittlung von Mitarbeiterdaten einiger Schweizer Banken an das amerikanische Justizdepartement. Die BK verweigerte den Zugang zum gewünschten Dokument einerseits, weil der Bundesrat den Beschluss im Rahmen eines Mitberichtsverfahrens gefällt hatte, und anderseits, weil ein Strafverfahren hängig war. Der Beauftragte kam zum Schluss, dass die BK nicht verpflichtet war, den Zugang zum gewünschten Dokument zu gewähren, da Bundesratsbeschlüsse Bestandteil des Mitberichtsverfahrens sind und dem Öffentlichkeitsgesetz nicht unterstehen.

Empfehlung EFK / Prüfbericht Immobilien (12. November 2012)

Die Antragstellerin verlangte Einsicht in den Bericht «Finanzaufsichtsprüfung armasuisse Immobilien von Ende 2010» der Eidgenössischen Finanzkontrolle (EFK). Die EFK gewährte lediglich einen teilweisen Zugang und verlangte dafür eine Gebühr von 400 Franken. Die Antragstellerin war weder mit den von der Behörde vorgenommenen Abdeckungen noch mit der Gebühr einverstanden und reichte beim Beauftragten einen Schlichtungsantrag ein. Die Behörde vertrat hingegen die Ansicht, erstens habe sie den Zugang vollständig gewährt, und zweitens sehe das Öffentlichkeitsgesetz in Bezug auf strittige Gebühren nicht die Möglichkeit

eines Schlichtungsverfahrens vor. In seiner Empfehlung kam der Beauftragte zum Schluss, dass der Umfang der Zugangsgewährung direkte Auswirkungen auf die Gebührenfrage habe, weshalb ein enger Zusammenhang zwischen Sach- und Kostenfrage bestehe. Demzufolge erachtete der Beauftragte es grundsätzlich für zulässig, in einem Schlichtungsantrag gleichzeitig mit der Zugangsbeschränkung auch die verlangte Gebühr zu beanstanden.

Weiter stellte der Beauftragte fest, dass die Gesuchbestätigung gemäss Artikel 16 Absatz 2 der Verordnung zum Öffentlichkeitsgesetz (VBGÖ) weder eine Einwilligung in den Gebührenbetrag noch eine Verzichtserklärung auf ein späteres Rechtsmittel sei. Schliesslich vertrat er hinsichtlich der Gebührenbemessung die Haltung, dass das Äquivalenzprinzip im Bereich des Öffentlichkeitsgesetzes nur modifiziert anwendbar sei. Die Gebührenhöhe darf dessen Grundsatz, Zugang zum amtlichen Dokument zu erlangen, nicht zuwiderlaufen und keine abschreckende Wirkung entfalten. So ist konkret mit Rücksicht auf die praktische Wirksamkeit des Zugangsrechts die Erhebung einer niedrigeren Gebühr angezeigt, auch wenn der Verwaltungsaufwand objektiv eine höhere Gebühr rechtfertigen würde. Zudem lässt sich die Äquivalenz zwischen Verwaltungsleistung und finanzieller Gegenleistung im Öffentlichkeitsgesetz kaum herstellen. Im Ergebnis empfahl der Beauftragte den vollständigen Zugang zum Prüfbericht und die Wiedererwägung des verlangten Gebührenbetrages.

Empfehlung Swissmedic / Überprüfung der Rechtmässigkeit von Medizinprodukten (4. Dezember 2012)

Der Antragsteller A verlangte Zugang zu amtlichen Dokumenten des Schweizerischen Heilmittelinstituts Swissmedic, die einer Überprüfung der Rechtmässigkeit betreffend Werbung und Verkauf von bestimmten Medizinprodukten zugrunde lagen. Swissmedic gewährte einen teilweisen Zugang. Dabei schwärzte es die umfangreichen Dokumente einerseits wegen Geschäfts- und Fabrikationsgeheimnissen (u.a. auf 20 Seiten) vollumfänglich, andererseits wegen Personendaten teilweise ein. In Bezug auf einige wenige Seiten schob Swissmedic den Zugang auf, weil sich ein betroffener Dritter (Antragsteller B) einer Herausgabe seiner Personendaten widersetzte. Nachdem A bereits einen Schlichtungsantrag eingereicht hatte, gelangte in der Folge auch B an den Beauftragten; er argumentierte, die betreffenden Dokumente bildeten Teil von Verfahrensakten eines Verwaltungs- bzw. Verwaltungsstrafverfahrens. Ausserdem seien die ihn betreffenden Dokumente nicht anonymisierbar, da er als Ersteller der Dokumente alleine aufgrund der firmenspezifischen Gestaltung und Schriftart in seinen Schreiben identifizierbar sei. Swissmedic schob den Zugang zu diesen Dokumenten zwar auf, stellte

sich jedoch auf den Standpunkt, dass die den B betreffenden Dokumente nicht Teil eines Verwaltungs- bzw. Verwaltungsstrafverfahrens bildeten.

In seiner Empfehlung kam der Beauftragte zum Schluss, dass Swissmedic das Öffentlichkeitsgesetz korrekt umgesetzt habe und A somit zu Recht und in angemessener Weise ein eingeschränkter Zugang zu den verlangten Dokumenten gewährt worden sei. Die von Swissmedic in Rechnung gestellten Gebühren wurden vom Beauftragten als verhältnismässig qualifiziert. In Bezug auf B hielt der Beauftragte fest, dass dessen Firmenkorrespondenz keine besonderen Merkmale aufweise, weshalb eine Identifikation des Dokumentenerstellers nicht ohne Weiteres möglich sei. Darüber hinaus schloss sich der Beauftragte der Einschätzung von Swissmedic an, wonach die amtlichen Dokumente, welche den Antragsteller B betrafen, nicht Teil eines Verwaltungs- bzw. Verwaltungsstrafverfahrens seien. Er empfahl Swissmedic, diese Dokumente ebenfalls an A herauszugeben.

Empfehlung EFK / Überprüfung der Rechtmässigkeit von Gebühren, Berechtigung zur Einreichung eines Schlichtungsantrags vor der Beurteilung des Zugangsgesuches (4. Dezember 2012)

Der Antragsteller verlangte Zugang zum «Bericht Elektronische Kriegführung; Prüfung der Wirtschaftlichkeit und des Einsatzes von Systemen des VBS, vom 30. September 2009» der Eidgenössische Finanzkontrolle (EFK). Die EFK teilte ihm mit, dass es sich bei dem fraglichen amtlichen Dokument um einen als vertraulich klassifizierten Bericht handle, weshalb u.a. noch mit der betroffenen Verwaltungseinheit geprüft werden müsse, ob er entklassifiziert werden könne. Weiter informierte sie ihn über einen voraussichtlichen Gebührenbetrag von 8000 bis 10 000 Franken. In der Folge reichte der Antragsteller beim Beauftragten einen Schlichtungsantrag ein und bat ihn zu prüfen, ob die EFK ihm zu Recht diese Gebühr für die Einsicht in das Dokument in Aussicht gestellt habe. Der Beauftragte gelangte in seiner Empfehlung zum Schluss, dass der Antragsteller aufgrund des Verdachts auf einen überhöhten Arbeitsaufwand ausnahmsweise bereits vor der materiellen Beurteilung des Zugangsgesuches zur Einreichung eines Schlichtungsantrags berechtigt sei. Die angekündigte Gebührenhöhe sei derart exzessiv, dass sie im Ergebnis einer Zugangsbeschränkung bzw. -verweigerung gleichkomme.

Empfehlung EPA / Zusammenstellung über ausbezahlte Zulagen in der Bundesverwaltung (6. Dezember 2012)

Der Antragsteller verlangte beim Eidgenössischen Personalamt (EPA) Einsicht in eine Zusammenstellung ausbezahlter Zulagen in der Bundesverwaltung. Das EPA verweigerte den Zugang mit der Begründung, die verlangten Informationen seien

im Auftrag der Finanzdelegation (FinDel) erstellt worden und daher Bestandteil der Kommissions- und Delegationsunterlagen der FinDel. Die Beratungen und Protokolle der Kommissionen sind gemäss Parlamentsgesetz vertraulich. Aus den Unterlagen, welche die FinDel dem Beauftragten zukommen liess, war ersichtlich, dass die verlangte Zusammenstellung in ihrem ausdrücklichen schriftlichen Auftrag vom EPA erstellt worden war. Weil eine spezialgesetzliche Geheimhaltungsnorm des Parlamentsgesetzes vorliegt, kommt das Öffentlichkeitsgesetz für die explizit von der FinDel verlangten Dokumente nicht zur Anwendung. Für den Antragsteller bestand somit nach Ansicht des Beauftragten kein Rechtsanspruch auf Zugang zu den verlangten Unterlagen, und er empfahl daher dem EPA, an der Verweigerung des Zugangs festzuhalten.

Empfehlung BAZL / Dokumente eines Verwaltungsstrafverfahrens gegen eine Fluggesellschaft (18. Dezember 2012)

Der Antragsteller verlangte beim Bundesamt für Zivilluftfahrt (BAZL) Zugang zu amtlichen Dokumenten betreffend ein eingestelltes Verwaltungsstrafverfahren gegen eine Fluggesellschaft. Konkret ersuchte er um Einsicht in all jene Dokumente, welche auf die Meldung eines Flugpassagiers über einen verspäteten Flug zurückgehen, sowie alle damit zusammenhängenden Dokumente, welche aus der Beurteilung dieses Sachverhalts durch das BAZL und seinem Entscheid, die Fluggesellschaft in diesem Fall nicht zu sanktionieren, hervorgingen. Das Amt verweigerte dem Antragsteller den Zugang zu den Dokumenten mit Verweis auf den fehlenden sachlichen Geltungsbereich des Öffentlichkeitsgesetzes für Dokumente aus Verfahrensakten eines (Verwaltungs-) Strafverfahrens. Im Rahmen des Schlichtungsverfahrens forderte der Beauftragte das BAZL mehrmals auf, ihm die betroffenen Dokumente zur Beurteilung einer allfälligen Zugangsgewährung zuzustellen. Die Behörde stellte sich jedoch auf den Standpunkt, dass zur Beurteilung der Grundsatzfrage, ob das Öffentlichkeitsgesetz Dritten einen Anspruch auf Zugang zu Dokumenten eines Verwaltungsstrafverfahrens einräume, keine Einsichtnahme in die betreffenden Dokumente durch den Beauftragten notwendig sei. Im Unterschied zu den Ausführungen in der Botschaft des Bundesrates zum Öffentlichkeitsgesetz, hielt der Beauftragte gestützt auf die Lehre in seiner Empfehlung fest, dass amtliche Dokumente eines bereits abgeschlossenen Verfahrens gleichwohl in den sachlichen Geltungsbereich des Öffentlichkeitsgesetzes fielen. Dies gelte jedoch nur unter der Voraussetzung, dass die Dokumente bereits vor der Verfahrenseröffnung bestanden hätten und nicht explizit für das Verfahren erstellt worden seien. Weil das BAZL dem Beauftragten die Aushändigung der Dokumente verweigerte, hatte er keine Möglichkeit zu beurteilen, ob zumindest ein Teil der betroffenen Dokumente aus der Zeit vor der Verfahrenseröffnung

stammte. Konsequenterweise – und entsprechend dem Grundsatz «im Zweifel für die Transparenz» – wies er das BAZL in seiner Empfehlung an, den Zugang zu allen vom Antragsteller bezeichneten Dokumenten zu gewähren.

2.3.2 Schlichtungen

In folgenden Fällen konnte eine Schlichtung erzielt werden:

Schlichtung EDA / Inspektionsbericht und Abgangsvereinbarung

Der Antragsteller verlangte beim EDA die Einsicht in einen internen Inspektionsbericht aus dem Jahr 2005 sowie in die Abgangsvereinbarung über die Auflösung eines Dienstverhältnisses zwischen dem Departement und einer angestellten Person. Das EDA und der Antragsteller einigten sich auf die Bekanntgabe einer Information aus der Abgangsvereinbarung, wofür noch die Zustimmung der betroffenen Drittperson einzuholen war. Diese war einverstanden, weshalb eine einvernehmliche Lösung gefunden werden konnte. Der Antragsteller anerkannte zudem, dass der Inspektionsbericht vor Inkrafttreten des BGÖ erstellt worden war und er folglich kein Zugangsrecht geltend machen konnte.

Schlichtung SNF / Projektskizzen

Die Antragstellerin verlangte den Zugang zu den Forschungsarbeiten, die im Rahmen des Nationalfondsprojekt 57 beim Schweizerischen Nationalfonds (SNF) eingereicht worden waren. Sie begehrte vollumfängliche Einsicht in die Forschungsdokumente, bevor die Ergebnisse von den Forschenden offiziell veröffentlicht wurden. Weiter ersuchte die Antragstellerin um die Übersetzung der Abstracts der Studien sowie allfällige zusammenfassende Ausführungen in Deutsch, Französisch und Italienisch. Im weiteren Verlauf stellte sie nochmals ein Zugangsgesuch. In der Schlichtungsverhandlung konnten sich die Parteien in Bezug auf die zwei Gesuche darauf einigen, dass elf Forschungsgruppen angefragt werden, ob der SNF ihre Schlussberichte herausgeben könne.

2.4 Gerichtsentscheide zum Öffentlichkeitsgesetz

2.4.1 Bundesverwaltungsgericht

Das Bundesverwaltungsgericht (BVGer) hat im Jahr 2012 drei Urteile im Zusammenhang mit dem Zugang zu amtlichen Dokumenten gefällt; zweien ging ein Schlichtungsverfahren beim Beauftragten voraus.

Das Bundesamt für Sozialversicherungen (BSV) hatte gegen die Empfehlung des Beauftragten vom 22. Dezember 2011 (vgl. unseren 19. Tätigkeitsbericht 2011/2012, Ziff. 2.3.1) eine Verfügung erlassen, die an das BVGer weitergezogen wurde. Die vom Beschwerdeführer konzernintern beauftragte Buchhaltungsabteilung verpasste die vom Gericht angesetzte Frist zur Leistung eines Kostenvorschusses. Das Begehren um Wiederherstellung der Frist lehnte das Gericht ab, da es organisatorische Unzulänglichkeiten nicht als unverschuldeten Hindernisgrund gelten liess. Die Frage, ob der Beschwerdeführer das Zugangsverfahren mit einem neuen Gesuch wieder in Gang setzen und auf diesem Weg eine gerichtliche Beurteilung erzwingen könne, oder ob diesem Verfahren die Rechtskraft der vorinstanzlichen Verfügung entgegenstehe, liess das Gericht offen (Urteil vom 12. April 2012, Ref. A-884/2012).

Das Staatssekretariat für Wirtschaft SECO ersuchte nach der Empfehlung vom 6. Juli 2011 (vgl. unseren 19. Tätigkeitsbericht 2011/2012, Ziff. 2.3.1) den Beauftragten um deren nachträgliche Anpassung, da in der Zwischenzeit in dieser Sache ein Strafverfahren hängig geworden sei. Der Beauftragte konnte diesem Begehren bereits aus formellen Gründen nicht nachkommen, da das Öffentlichkeitsgesetz keine solche Möglichkeit vorsieht. In der Folge erliess das SECO eine Verfügung, mit welcher es seinen materiellen Entscheid betreffend den Zugang zu den verlangten Dokumenten bis zum rechtskräftigen Abschluss des genannten Strafverfahrens sistierte. Dagegen reichte der Beschwerdeführer eine Rechtsverzögerungsbeschwerde bei BVGer ein. Das Gericht befasste sich eingehend mit den einzelnen Schritten im Verfahren auf Zugang zu amtlichen Dokumenten, bejahte die Rechtsverzögerung und wies die Sache zur materiellen Beurteilung an das SECO zurück (Urteil vom 15. Mai 2012, Ref. A-6037/2011).

In einem weiteren Fall befasste sich das BVGer mit der Frage, ob die im Öffentlichkeitsgesetz vorgesehene Gebührenpflicht auch für Medienschaffende gelte. Ein Journalist hatte Zugang zu Informationen über die Prüfung der Energieetiketten von Elektrogeräten durch Electrosuisse und das Eidgenössische Starkstrominspektorat (ESTI) verlangt. Das Bundesamt für Energie (BFE) informierte den Gesuchsteller nach Sichtung der Dokumente über die zu erwartende Gebührenhöhe von

etwa 200 Franken, worauf dieser dem BFE mitteilte, dass er an seinem Gesuch festhalte. Nachdem ihm nach Schwärzung einiger Stellen teilweise Einsicht in das Dokument gewährt und er auf die entstandenen Kosten von nunmehr 250 Franken hingewiesen worden war, ersuchte er das BFE um eine Verfügung über die Rechnung sowie eine Rechtsmittelbelehrung. Der Journalist focht diese Verfügung an mit der Begründung, dass sie gegen den Willen des Gesetzgebers verstosse, da die Gebührenerhebung die besonderen Bedürfnisse und die besondere Rolle der Medien ausser Acht lasse und dadurch das Öffentlichkeitsprinzip unterlaufe. Das BVGer vertrat in seinem Entscheid hingegen den Standpunkt, dass der Bundesrat in der Botschaft zum Öffentlichkeitsgesetz bei der Gebührenerhebung für Medienvertreter zwar eine Erleichterung in Betracht gezogen, letztlich jedoch in der Öffentlichkeitsverordnung keine generelle Befreiung der Medien von der allgemeinen Gebührenpflicht vorgesehen habe. Eine Gebührenbefreiung für Medienschaffende wäre daher auch mit dem Rechtsgleichheitsgebot nicht ohne Weiteres zu vereinbaren.

Ein Verzicht auf Gebührenerhebung ist in der Allgemeinen Gebührenverordnung (AllgGebV) hingegen dann vorgesehen, wenn ein überwiegendes öffentliches Interesse an der entsprechenden Verfügung oder Dienstleistung besteht. Dabei müsse im Bereich des Öffentlichkeitsgesetzes, so das BVGer, das öffentliche Interesse am Zugang zu den Dokumenten mit dem Interesse an einer rationellen und effektiven Verwaltung abgewogen werden. Daher könne ein Gebührenverzicht insbesondere dann erfolgen, wenn es um Leistungen gehe, die für den Staat oder den Einzelnen – und damit für die Öffentlichkeit – existenziell seien. Das BVGer hielt sodann fest, dass das überwiegende öffentliche Interesse nicht generell mit der Projektarbeit der Medienschaffenden, welche je nachdem einen – grösseren oder kleineren – Teil der Bevölkerung interessiert, gleichgesetzt werden könne.

Im Ergebnis hat das BVGer explizit festgehalten, dass auch gegenüber Medienschaffenden eine Gebühr für den Zugang zu amtlichen Dokumenten erhoben werden kann. In Bezug auf die konkrete Gebührenerhebung führte es aus, dass jedes Dokument – Satz für Satz – zu prüfen sei, und nicht nur die entsprechenden Bezeichnungen und Namen Dritter, was einen nicht unerheblichen Aufwand zur Folge haben könne. Das Gericht erachtete die von der Vorinstanz auferlegte Gebühr von 250 Franken als angemessen und wies die Beschwerde ab (Urteil vom 27. November 2012, Ref. A-1200/2012).

2.5 Ämterkonsultationen und weitere Stellungnahmen

2.5.1 Inkraftsetzung des neuen Rechnungslegungsrechts

Der Beauftragte hat im Rahmen der Ämterkonsultation betreffend die Anhörung zur Inkraftsetzung des Rechnungslegungsrechts und zu den Ausführungsbestimmungen (VASR und Teilrevision RAV) Stellung genommen. Der Entwurf sah u.a. eine Ausnahme der Revisionsaufsichtsbehörde (RAB) vom persönlichen Geltungsbereich des Öffentlichkeitsgesetzes vor. Der Beauftragte anerkannte zwar einerseits, dass die Aufsichtstätigkeit der RAB in bestimmten Fällen nach einem qualifizierten Schutz verlangt. Anderseits wies der Beauftragte darauf hin, dass das Öffentlichkeitsgesetz im Einzelfall ausreichend gesetzliche Möglichkeiten zum Schutz von Berufs- und Geschäftsgeheimnissen und von Personendaten bietet. Die RAB schloss sich dieser Haltung nach einer gemeinsamen Sitzung mit Vertretern des Beauftragten und des Bundesamtes für Justiz an.

2.5.2 Dringliche Interpellation: Keine schleichende Ausdehnung von Gesamtarbeitsverträgen auf andere Branchen

Im Rahmen einer Ämterkonsultation hat sich der Beauftragte zum Antwortentwurf des Bundesrates zu einer dringlichen Interpellation betreffend die Anwendbarkeit des Öffentlichkeitsgesetzes auf Verfahren über die Allgemeinverbindlicherklärung (AVE) eines Gesamtarbeitsvertrages geäussert. Der Antwortentwurf führte zu Recht aus, dass während des AVE-Verfahrens kein Zugangsanspruch nach Öffentlichkeitsgesetz bestehe, da der politische und administrative Entscheid in der Sache noch nicht gefallen sei. Der Beauftragte schlug dazu eine Ergänzung vor, dass nach dem Entscheid der AVE subsidiär die Ausnahmen des Öffentlichkeitsgesetzes gelten.

2.5.3 Neufestsetzung der Labortarife: Verstärkte Transparenz im Verfahren

Die Geschäftsprüfungskommission des Nationalrates (GPK-N) hat im Rahmen ihrer Untersuchung der Rechtmässigkeit und Angemessenheit des Verfahrens bei der Neufestsetzung der Labortarife gemäss dem Bundesgesetz über die Krankenversicherung (KVG) sieben Empfehlungen erlassen. Nachdem der Bundesrat dazu bereits am 21. Oktober 2009 Stellung bezogen hatte, ersuchte ihn die GPK-N erneut um Bericht. Die GPK-N verlangte in einer ihrer Empfehlungen vom Bundesrat,

zu prüfen, inwiefern in besonderer Weise Betroffenen sowie der interessierten Öffentlichkeit die Zwischenergebnisse des Verfahrens im Entscheid bezüglich der Analysenliste besser zugänglich gemacht werden könnten. Namentlich geht es um die materiellen Stellungnahmen des BAG, der externen Experten sowie die Empfehlungen der Eidgenössische Kommission für Analysen, Mittel und Gegenstände zuhanden des EDI. In diesem Zusammenhang solle der Bundesrat allfällige rechtliche Hindernisse gegen eine verstärkte Transparenz des Verfahrens identifizieren und entsprechende Lösungen skizzieren.

Der Beauftragte empfahl, in der Antwort des Bundesrates ein klare Trennung zwischen aktiver und passiver Information vorzunehmen und explizit darauf hinzuweisen, dass eine Behörde Information auch dann aktiv bekannt geben kann, wenn darauf nach Öffentlichkeitsgesetz kein Anspruch besteht. Das BAG hat unsere Ausführungen berücksichtigt und die entsprechenden Änderungen vorgenommen.

2.5.4 Entwurf für ein Nachrichtendienstgesetz

Der Beauftragte hat im Rahmen der Ämterkonsultation betreffend die Vernehmlassung des Entwurfs zum Nachrichtendienstgesetz (NDG) Stellung genommen. Der Entwurf sah u.a. eine Ausnahme des Nachrichtendienstes (NDB) vom persönlichen Geltungsbereich des Öffentlichkeitsgesetzes vor. Der Beauftragte lehnte diesen Vorschlag insbesondere unter Hinweis auf die Konzeption des Öffentlichkeitsgesetzes (BGÖ) ab, welche auf drei Pfeilern beruht:

- Erstens fallen nach dieser Konzeption grundsätzlich alle Behörden des Bundes unter den persönlichen Geltungsbereich des Öffentlichkeitsgesetzes.
- Zweitens fallen grundsätzlich alle amtlichen Dokumente unter den Geltungsbereich.
- Drittens sieht das Öffentlichkeitsgesetz ein System vor, wonach der Entscheid über die Zugänglichkeit zu amtlichen Dokumenten auf einer Interessenabwägung im Einzelfall beruht.

Um dem Umstand gerecht zu werden, dass bestimmte Informationen einer Behörde einen besonderen Schutzbedarf haben können, enthalten insbesondere die Artikel 7 bis 9 BGÖ einen umfangreichen Katalog von gesetzlichen Möglichkeiten, um den Zugang zu amtlichen Dokumenten aufzuschieben, einzuschränken oder zu verweigern. Nach Ansicht des Beauftragten ist es damit ohne Weiteres möglich, im Falle besonders sensibler Informationen den konkreten Umständen Rechnung zu tragen. Der Argumentation des NDB, wonach sein besonderer Schutzbedarf

prinzipiell nicht mit dem Transparenzgedanken des Öffentlichkeitsgesetzes vereinbar sei, widersprach der Beauftragte somit entschieden.

Weiter widersprach der Beauftragte mit Blick auf die bislang vom VBS gemeldeten Jahresstatistiken dem Einwand des NDB, dass Zugangsgesuche nach dem Öffentlichkeitsgesetz zu beträchtlichem Mehraufwand führen würden. Auch gab er zu bedenken, dass gerade die jüngsten Geschehnisse innerhalb der Verwaltung (insbesondere im Zusammenhang mit «Insieme» bei der Eidgenössischen Steuerverwaltung und dem Datendiebstahl beim NDB im Berichtsjahr) einmal mehr gezeigt hätten, wie wichtig das Öffentlichkeitsgesetz und die Transparenz über Auftrag, Organisation und Tätigkeit der Verwaltung sind.

Da das VBS die Anträge des Beauftragten nicht berücksichtigte, erstellte er einen Mitbericht an den Bundesrat. Im Gegensatz zum Entwurf in der Ämterkonsultation schlug das VBS nunmehr vor, die «Informationsbeschaffung durch den NDB» – so der vorgeschlagene Wortlaut des überarbeiteten Entwurfs – gänzlich vom sachlichen Geltungsbereich des Öffentlichkeitsgesetzes auszunehmen. Der Beauftragte widersprach dem Vergleich des VBS, wonach die Informationsbeschaffung durch den NDB mit einem gerichtlichen Verfahren gleichzusetzen sei und damit vom Öffentlichkeitsgesetz ausgenommen werden sollte. Dabei gab er auch zu bedenken, dass Verfahrenserlasse ja gerade Einsichtsrechte der Parteien vorsehen, anstatt eine Einsichtnahme von vornherein auszuschliessen. Der Beauftragte kritisierte auch die sehr allgemeine Formulierung «Informationsbeschaffung durch den NDB», womit in letzter Konsequenz die Hauptaufgabe des Dienstes vollständig vom Öffentlichkeitsgesetz ausgenommen würde.

Der Bundesrat schloss sich den Bedenken des Beauftragten nicht an. Mit Blick auf Sinn und Zweck des Öffentlichkeitsgesetzes ist dies umso bedauerlicher, als dass damit der Bevölkerung jeglicher Anspruch auf minimale Transparenz genommen wird, zumal die nachrichtendienstliche Tätigkeit in nicht erkennbaren und damit verborgenen Bereichen agiert.

Siehe zum Thema auch Ziff. 1.4.6 des vorliegenden Tätigkeitsberichts.

2.6 Varia

2.6.1 Tagung zum Öffentlichkeitsprinzip

Am 24. Februar 2012 veranstaltete der Beauftragte in Zusammenarbeit mit dem Bundesamt für Justiz den «Journée de la transparence» (Tagung zum Öffentlichkeitsprinzip) für die Öffentlichkeitsberater der Bundesverwaltung. Die Veranstaltung bezweckte einerseits den Erfahrungsaustausch der rechtsanwendenden Behörden bei der praktischen Umsetzung des Öffentlichkeitsprinzips, anderseits diente sie der Beantwortung konkreter, wiederholt aufgetauchter Fragen.

Aufgrund der Ergebnisse dieser Veranstaltung überarbeiteten und aktualisierten der Beauftragte und das BJ das Dokument «Umsetzung des Öffentlichkeitsprinzips in der Bundesverwaltung: Häufig gestellte Fragen» aus dem Jahr 2010. Es ist abrufbar auf unserer Webseite www.derbeauftragte.ch unter Öffentlichkeitsprinzip – FAQ zur Umsetzung des Öffentlichkeitsprinzips.

2.6.2 Beziehungen zu kantonalen Schlichtungsstellen – Arbeitsgruppe Schlichtungswesen

Der EDÖB ist nicht die einzige Behörde in der Schweiz, welche Schlichtungsverfahren im Bereich des Öffentlichkeitsprinzips durchführt. Mehrere Kantone kennen dieses informelle Verfahren der Streitbeilegung im Zusammenhang mit der Zugänglichkeit von amtlichen Dokumenten ebenfalls. Da dem EDÖB und interessierten kantonalen Öffentlichkeitsbeauftragten die Zusammenarbeit und der Praxisaustausch wichtig sind, wurde im Herbst 2011 die «groupe d'intervision sur la gestion consensuelle des conflits transparence» gebildet. Auch im letzten Jahr ermöglichten regelmässige Zusammenkünfte den teilnehmenden Behörden einen vertieften Erfahrungsaustausch zu Fragen des Öffentlichkeitsprinzips und der Schlichtungstätigkeit.

3. Der EDÖB

3.1 Siebter Datenschutztag

Anlässlich des siebten Datenschutztags am 28. Januar 2013 haben wir eine Broschüre zum Daten- und Persönlichkeitsschutz am Arbeitsplatz herausgegeben. Zugleich wurde an einer Veranstaltung bei Lausanne die neue Version des Online-Diensts «Think Data» präsentiert, der Behörden und Unternehmen in Datenschutz- und Transparenzfragen Hilfestellung leistet.

Die Privatsphäre eines Menschen ist ein hohes Gut und geniesst einen besonderen Schutz. Das gilt natürlich auch am Arbeitsplatz und muss vom Arbeitgeber respektiert werden. Wie in der kleinen illustrierten Broschüre «Daten- und Persönlichkeitsschutz am Arbeitsplatz – mein gutes Recht» erläutert wird, findet die Privatsphäre der Arbeitnehmerin und des Arbeitnehmers jedoch dort ihre Grenzen, wo sie mit den Geschäftsinteressen des Arbeitgebers oder mit dem Gesetz in Konflikt gerät. Auch erfährt man in dem als Einführung gedachten Werk, was Arbeitgeber beim Einsatz von Videoüberwachung zu beachten haben, wie bei auffälligem Surfverhalten der Angestellten vorzugehen ist oder dass bei der Recherche nach Stellenbewerbern nur öffentliche zugängliche Quellen konsultiert werden dürfen. Die Broschüre steht allen Interessierten auf unserer Webseite www.derbeauftragte.ch unter Datenschutz – Arbeitsbereich zum kostenlosen Download zur Verfügung.

Datenbearbeitungen durch Unternehmen stehen auch beim Online-Dienst Think Data im Blickpunkt, dessen neue Version der Öffentlichkeit am diesjährigen Datenschutztag im Rahmen einer Konferenz in Chavannes-près-Renens präsentiert wurde. Auf www.thinkdata.ch finden Unternehmen, Behörden und Organisationen auf ihre jeweiligen Bedürfnisse zugeschnittene Ratschläge und Informationen zum korrekten Umgang mit den bei ihnen anfallenden Personendaten (vgl. unseren 19. Tätigkeitsbericht 2011/2012, Ziff. 3.2.). Think Data wird von einer interdisziplinären Arbeitsgruppe betreut. Seit Anfang 2013 liegt die Federführung bei uns.

Ebenfalls an der Konferenz referierte Ebrahimi Touradj, Professor der ETH Lausanne, zu den Chancen und Risiken der Videoüberwachung und erläuterte dabei insbesondere, wie sich diese Technologien datenschutzkonform einsetzen lassen. Die Perspektiven des Datenschutzes im Zeitalter der Digitalisierung standen anschliessend im Fokus einer Podiumsdiskussion unter Beteiligung von Alexis Roussel, Vizepräsident der Schweizerischen Piratenpartei, Jean-Philippe Walter, stv. Datenschutz- und Öffentlichkeitsbeauftragter, und weiteren Experten.

3.2 Publikationen des EDÖB im laufenden Geschäftsjahr

Als wichtigster Publikations- und Informationskanal dient uns die Webseite www.derbeauftragte.ch, auf der die Userinnen und User nützliche Informationen und Antworten auf ihre Fragen in den Bereichen Datenschutz und Öffentlichkeitsprinzip finden. Erweitert wurde die breite Themenpalette im Berichtsjahr u.a. um Erläuterungen zum Datenschutz bei Breitensportveranstaltungen, in Bibliotheken sowie zum Thema Internetpranger. Zudem haben wir eine Broschüre zum Daten- und Persönlichkeitsschutz im Arbeitsbereich herausgegeben.

Das Instrument des Internetprangers erfreut sich wachsender Beliebtheit. Im Internet tauchen immer häufiger schwarze Listen auf, auf denen Personen veröffentlicht werden, die nicht im Sinne des Verfassers gehandelt oder entschieden haben. Nicht selten werden dabei auch Privatadressen und Fotografien der fraglichen Personen publiziert, was verschiedene datenschutzrechtliche Fragen aufwirft (vgl. Ziff. 1.3.1 des vorliegenden Tätigkeitsberichts). Ausführliche Informationen zum Thema finden Sie auf unserer Webseite www.derbeauftragte.ch in der Rubrik Datenschutz – Internet und Computer.

An den hiesigen Breitensportanlässen wie dem Gigathlon oder den zahlreichen Volksläufen nehmen jedes Jahr tausende Hobbysportlerinnen und -sportler teil. In diesem Rahmen werden auch Personendaten bearbeitet. Oft geht diese Bearbeitung über die unmittelbare Abwicklung der Veranstaltung hinaus. Aus Datenschutzsicht sind manche dieser Dienstleitungen problematisch (vgl. Ziff. 1.2.5 des vorliegenden Tätigkeitsberichts). Unsere Erläuterungen dazu befinden sich auf unserer Webseite unter Datenschutz – Freizeit und Sport.

Auch zum Thema Datenschutz in Bibliotheken haben wir im Berichtsjahr Erläuterungen publiziert. Bibliotheken müssen Personendaten bearbeiten, damit sie die Bücherausleihe administrativ abwickeln können. Durch Zusatzdienstleistungen, wie z.B. das Anbieten von Arbeitsstationen mit Internetanschluss, fallen weitere Personendaten an. Diese Daten sind weniger harmlos, als es auf den ersten Blick erscheinen mag. Werden sie miteinander verknüpft, können sie nämlich ein aufschlussreiches Persönlichkeitsprofil ergeben (Datenschutz – Statistik, Register und Forschung).

Ebenfalls im Berichtsjahr haben wir gemeinsam mit dem Bundesamt für Justiz die häufig gestellten Fragen zur Umsetzung des Öffentlichkeitsprinzips in der

Bundesverwaltung umfangreich erweitert. Das Dokument dient den Bundesbehörden als Hilfsmittel bei der Bearbeitung von Zugangsgesuchen und ist zu finden auf unserer Webseite unter Öffentlichkeitsprinzip – Dokumentation / Hilfsmittel – FAQ für die Bundesverwaltung.

An den selben Adressatenkreis richten sich die Informationen zum Einsatz von Web-Analysetools in der Bundesverwaltung. Mit solchen Tools werten Webseitenbetreiber die Zugriffe der Besucherinnen und Besucher aus, insbesondere zur Optimierung ihres Onlineangebots. In dem Dokument (zu finden auf unserer Webseite unter Datenschutz – Internet und Computer) werden die datenschutzrechtlichen Voraussetzungen erläutert, welche die Bundesstellen dabei zu erfüllen haben.

Schliesslich veröffentlichten wir anlässlich des siebten Datenschutztages eine Broschüre zum Daten- und Persönlichkeitsschutz am Arbeitsplatz, die sich sowohl an Arbeitgeber als auch an Arbeitnehmer richtet und ihnen ihre Rechte und Pflichten in Erinnerung ruft. Videoüberwachung am Arbeitsplatz ist genauso ein Thema des kleinen, illustrierten Hefts wie die Internetnutzung zu privaten Zwecken und die Online-Recherche im Rahmen von Stellenbewerbungen. Zu finden ist sie unter Datenschutz – Arbeitsbereich.

3.3 Mitarbeit im Informatikrat und im Ausschuss Informatiksicherheit des Bundes

Seit Anfang 2012 wirken wir im Informatikrat des Bundes mit. So erhalten wir Gelegenheit, uns über die geplanten Vorgaben zu informieren und gegebenenfalls unsere Meinung zu den damit verbundenen Datenschutz- oder Öffentlichkeitsaspekten zu äussern. Wir beteiligen uns auch am Ausschuss Informatiksicherheit, da zwischen der Informationssicherheit und technischen Datenschutzmassnahmen offenkundige Synergien bestehen.

Am 01. Januar.2012 wurde die Revision der Bundesinformatikverordnung (BInfV) in Kraft gesetzt. Seither ist der Informatikrat des Bundes (IRB) das Konsultativorgan für das Informatiksteuerungsorgan des Bundes (ISB) zu Geschäften betreffend Informations- und Kommunikationstechnologien (IKT), die der Absprache mit den Departementen und der Bundeskanzlei bedürfen, insbesondere für den Erlass von Vorgaben und für die Genehmigung von Ausnahmen. Er setzt sich aus dem oder der Delegierten für die Informatiksteuerung des Bundes und je einem namentlich bezeichneten Vertreter oder einer namentlich bezeichneten Vertreterin jedes Departements und der Bundeskanzlei zusammen. Mit beratender Stimme können je ein Vertreter oder eine Vertreterin der Eidgenössischen Finanzverwaltung, des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB), der internen Leistungserbringer sowie der Parlamentsdienste teilnehmen. Nach einem Jahr ziehen wir eine positive Bilanz aus unserer regelmässigen Mitwirkung im IRB, und dies hauptsächlich in zweierlei Hinsicht: Wir werden unmittelbar über die geplanten Informatikvorgaben informiert (namentlich in den Bereichen Büroautomation, Telefonie, Geschäftsverwaltung und Standardisierung dieser Produkte) und können gegebenenfalls unsere Meinung zu den betroffenen Datenschutz- und Öffentlichkeitsaspekten äussern.

Der Ausschuss Informatiksicherheit (A-IS) ist das Konsultativorgan des ISB für alle IKT-Sicherheitsfragen. Er setzt sich aus den Informatiksicherheitsbeauftragten der Departemente und der Bundeskanzlei zusammen. Mit beratender Stimme können je ein Vertreter oder eine Vertreterin der Eidgenössischen Finanzkontrolle, des EDÖB sowie der Parlamentsdienste teilnehmen. Wir arbeiten seit mehreren Jahren in diesem Ausschuss mit, denn es besteht eine offenkundige Synergie zwischen den Problemen der Informationssicherheit und den technischen Datenschutzmassnahmen. Als Beispiel seien die Möglichkeiten genannt, welche die Verschlüsselung oder die Pseudo-Anonymisierung der Personendaten bieten. Zudem erinnern wir daran, dass die Organisationszertifizierung im Bereich Datenschutz im

Wesentlichen auf der Norm ISO/IEC 27001:2005 für die Zertifizierung von Managementssystemen im Informationssicherheitsbereich beruht. Im Rahmen der Schulung der Informatiksicherheitsbeauftragten der Departemente oder ihrer Ämter wurde sogar eine institutionelle Zusammenarbeit eingeführt, um eine Sensibilisierung für Datenschutzprobleme zu bewirken.

3.4 Sensibilisierung und Ausbildung von Studenten

Auf Wunsch der juristischen Fakultät der Universität Lausanne haben wir im November 2012 vor Studierenden im Masterstudiengang referiert und dabei die Tätigkeiten des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten vorgestellt. Auch beschrieben wir in Form konkreter Beispiele verschiedene von unserer Behörde bearbeitete Datenschutzfälle. Die Präsentation fand im Rahmen eines fachübergreifenden Kurses der Fakultät für Rechts- und Kriminalwissenschaften statt.

Die Präsentation gliederte sich in zwei Teile. Der erste galt der Organisation unserer Behörde und den beiden Hauptachsen unserer Tätigkeit: Beratung und Aufsicht. Der von unserer Behörde eingerichtete Kontrollmechanismus wurde den Studenten zur Erleichterung des Verständnisses anhand konkreter Beispiele erläutert. Auf die Präsentation folgte die Behandlung von zwei praktischen Fällen, die uns beschäftigt haben oder noch beschäftigen. So haben wir das Beispiel eines Falles aus der Rechtsprechung zum Urheberrecht unter dem Blickwinkel der in den Entscheiden des Bundesverwaltungsgerichts und des Bundesgerichts behandelten datenschutzrechtlichen Entwicklungen aufgegriffen. Danach erläuterten wir das Zugriffsrecht auf die Informationssysteme des Bundes. Schliesslich gingen wir kurz auf die möglichen Änderungen der schweizerischen Datenschutzgesetzgebung ein, welche im Zuge der Modernisierung des Übereinkommens des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen 108) notwendig werden könnten.

Unsere Vorträge für Studierende sind Bestandteil einer allgemeinen Sensibilisierungs- und Informationsarbeit im Bereich Datenschutz, die wir im Rahmen unserer Beratungs- und Schulungstätigkeiten auch in Zukunft verfolgen werden. Wir konnten uns erneut vom Interesse der Studenten für den Datenschutz überzeugen.

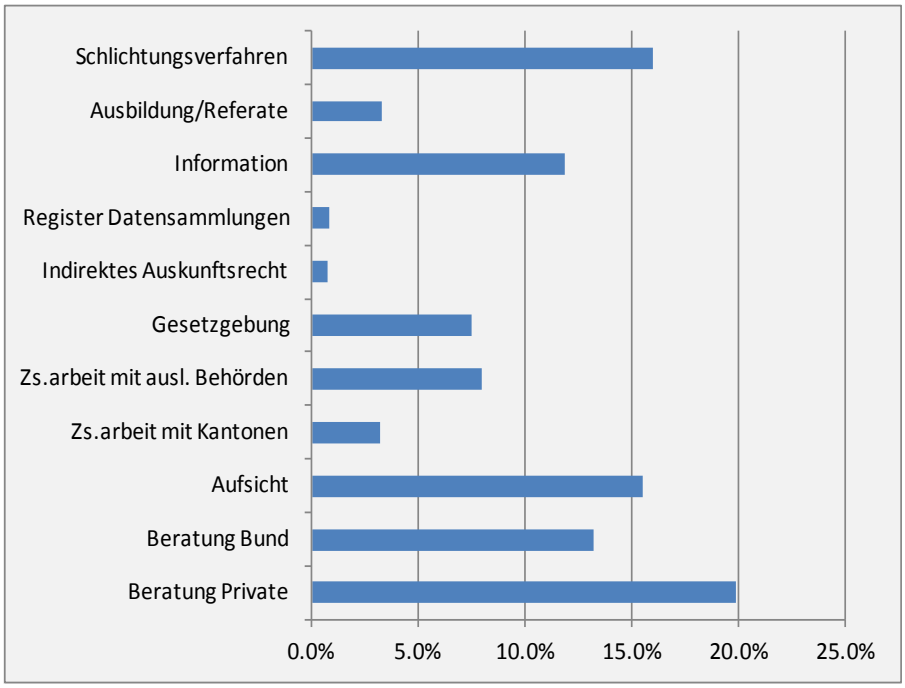
3.5 Schulung für Datenschutzberatende in der Bundesverwaltung

Unsere Präsentation zur Überwachung am Arbeitsplatz stiess bei zwei Veranstaltungen des Eidgenössischen Personalamts auf reges Interesse.

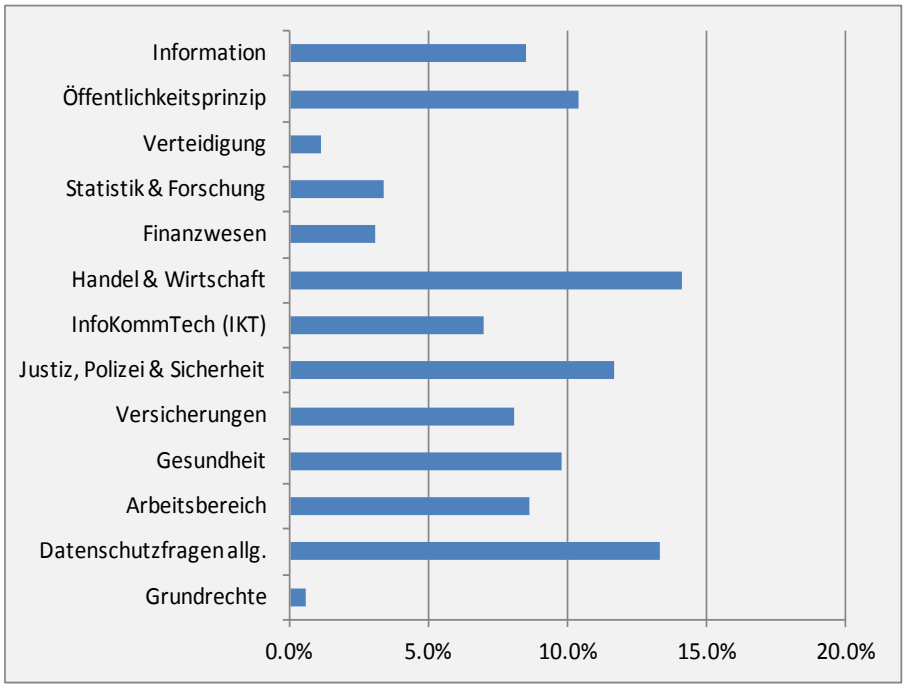
Das Eidgenössische Personalamt hat im letzen Jahr eine Weiterbildung im Bereich des Datenschutzes lanciert. Diese richtet sich an Datenschutzberatende der Bundesverwaltung. Wir haben an den beiden ersten Veranstaltungen teilgenommen sowie das Thema Überwachung am Arbeitsplatz präsentiert. Dabei haben wir den Teilnehmenden die neuen geltenden rechtlichen Grundlagen zum Aufzeichnen und Auswerten von Daten der Mitarbeitenden der Bundesverwaltung erläutert und dazu auch Beispiele präsentiert. Das Thema stiess auf reges Interesse, und es wurden zahlreiche Fragen gestellt. Die Diskussion mit den Teilnehmenden war hilfreich, um verschiedene Problematiken im Bereich des Personalrechts der Bundesverwaltung zu analysieren. Die Teilnahme an diesen Veranstaltungen zeigt uns zudem auf, dass Weiterbildung im Bereich Datenschutz sinnvoll und notwendig ist.

3.6 Statistik über die Tätigkeit des EDÖB vom 01. April 2012 bis 31. März 2013

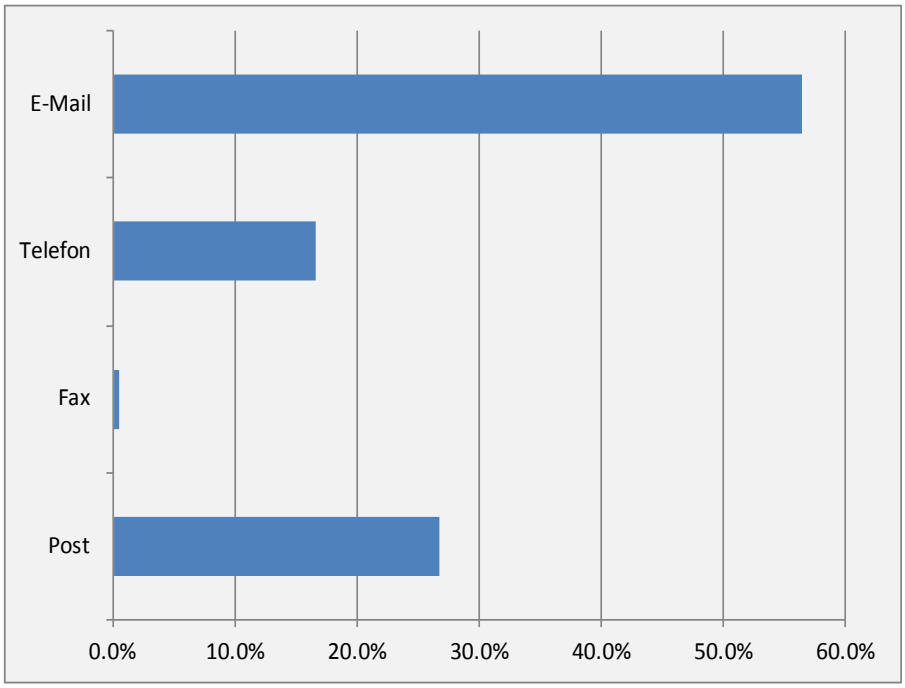
Aufwand nach Aufgabengebiet



Aufwand nach Sachgebiet



Herkunft der Anfragen



3.7 Statistik über die bei den Departementen eingereichten Zugangsgesuche nach Art. 6 des Öffentlichkeitsgesetzes (Zeitraum: 1. Januar 2012 bis 31. Dezember 2012)

Dep.	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt/ aufge-schoben	hängig	Rückzug
BK	13	2	5	5	0	1
EDA	88	57	14	17	0	0
EDI	75	28	23	18	3	3
EJPD	57	28	15	10	1	3
VBS	34	7	20	7	0	0
EFD	59	19	28	11	0	1
EVD*	80	22	17	31	2	8
UVEK	100	60	16	21	0	3
Total 2012 (in %)	506 (100 %)	223 (44 %)	138 (27 %)	120 (24 %)	6 (1 %)	19 (4 %)
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 %)	-	-

* seit 1. Januar 2013 Eidgenössisches Departement für Wirtschaft, Bildung und Forschung WBF

Bundeskanzlei BK

Dep.	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt/ aufge-schoben	hängig	Rückzug
BK	13	2	5	5	0	1
EDÖB	8	6	1	1	0	0
Total	**21**	**8**	**6**	**6**	**0**	**1**

Eidgenössisches Departement für auswärtige Angelegenheiten EDA

Dep.	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt/ aufge-schoben	hängig	Rückzug
EDA	88	57	14	17	0	0
Total	**88**	**57**	**14**	**17**	**0**	**0**

Eidgenössisches Departement des Innern EDI

Dep.	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt/ aufge-schoben	hängig	Rückzug
GS	9	4	1	4	0	0
EBG	0	0	0	0	0	0
BAK	3	1	1	1	0	0
BAR	3	3	0	0	0	0
Meteo Schweiz	0	0	0	0	0	0
NB	0	0	0	0	0	0
BAG	24	10	6	6	2	0
BFS	2	1	1	0	0	0
BSV	11	5	5	1	0	0
SBF	1	1	0	0	0	0
ETH-Rat	2	1	0	1	0	0
SNM	0	0	0	0	0	0
Swiss-medic	17	1	7	5	1	3
SNF	0	0	0	0	0	0
SUVA	3	1	2	0	0	0
Total	**75**	**28**	**23**	**18**	**3**	**3**

Eidgenössisches Justiz- und Polizeidepartement EJPD

Dep.	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt/ aufge-schoben	hängig	Rückzug
GS	7	4	1	1	0	1
BJ	2	1	1	0	0	0
FEDPOL	7	3	2	1	1	0
METAS	5	4	0	1	0	0
BFM	23	11	7	5	0	0
SIR	2	1	0	1	0	0
IGE	6	4	2	0	0	0
ESBK	5	0	2	1	0	2
ESchK	0	0	0	0	0	0
RAB	0	0	0	0	0	0
ISC	0	0	0	0	0	0
NKVF	0	0	0	0	0	0
Total	**57**	**28**	**15**	**10**	**1**	**3**

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS

Dep.	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt/ aufge-schoben	hängig	Rückzug
GS	13	3	6	4	0	0
Verteidig./ Armee	8	3	4	1	0	0
NDB	4	0	4	0	0	0
arma-suisse	6	0	4	2	0	0
BABS	0	0	0	0	0	0
BASPO	3	1	2	0	0	0
Total	**34**	**7**	**20**	**7**	**0**	**0**

Eidgenössisches Finanzdepartement EFD

Dep.	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt/ aufge-schoben	hängig	Rückzug
GS	7	5	2	0	0	0
EFV	2	1	0	1	0	0
EPA	3	2	1	0	0	0
ESTV	15	5	5	5	0	0
EZV	8	1	6	1	0	0
EAV	2	1	1	0	0	0
BBL	6	4	0	2	0	0
BIT	3	0	3	0	0	0
EFK	12	0	9	2	0	1
SIF	1	0	1	0	0	0
PUBLICA	0	0	0	0	0	0
ZAS	0	0	0	0	0	0
Total	**59**	**19**	**28**	**11**	**0**	**1**

Eidgenössisches Volkswirtschaftsdepartement EVD*

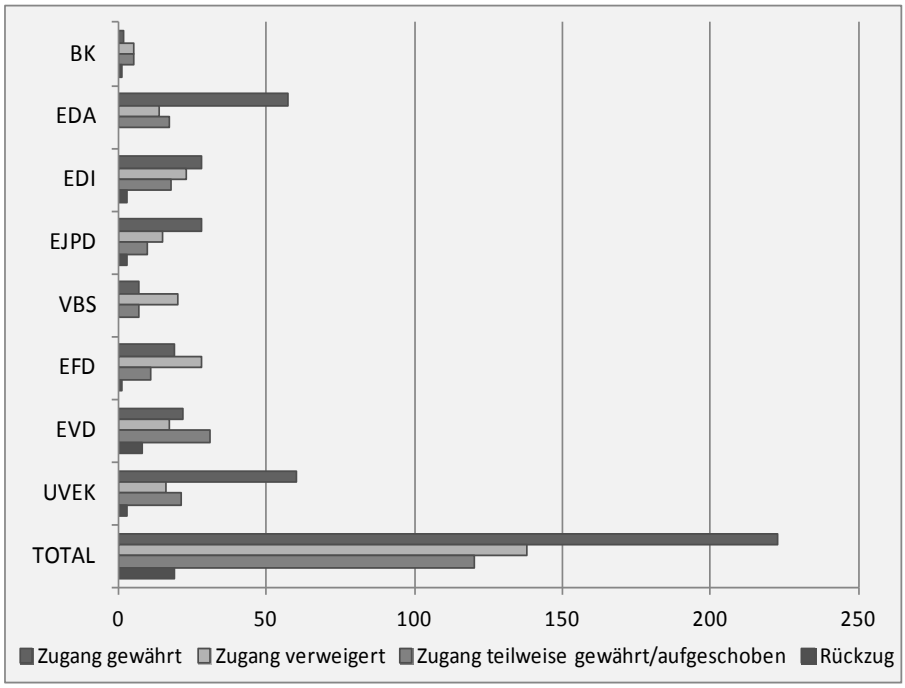
Dep.	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt/ aufge-schoben	hängig	Rückzug
GS	3	0	1	0	1	1
SECO	19	5	7	4	1	2
BBT	2	1	1	0	0	0
BLW	21	4	4	8	0	5
BVET	3	2	1	0	0	0
BWL	0	0	0	0	0	0
BWO	0	0	0	0	0	0
PUE	1	1	0	0	0	0
WEKO	27	9	2	16	0	0
ZIVI	3	0	0	3	0	0
BFK	0	0	0	0	0	0
KTI	1	0	1	0	0	0
EHB	0	0	0	0	0	0
Total	**80**	**22**	**17**	**31**	**2**	**8**

* seit 1. Januar 2013 Eidgenössisches Departement für Wirtschaft, Bildung und Forschung WBF

Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK

Dep.	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt/ aufge-schoben	hängig	Rückzug
GS	3	1	1	1	0	0
BAV	10	6	1	3	0	0
BAZL	6	0	5	1	0	0
BFE	8	2	3	3	0	0
ASTRA	4	4	0	0	0	0
BAKOM	11	9	2	0	0	0
BAFU	25	19	2	4	0	0
ARE	2	0	0	2	0	0
ComCom	1	1	0	0	0	0
ENSI	18	6	2	7	0	3
PostCom	0	0	0	0	0	0
UBI	12	12	0	0	0	0
Total	**100**	**60**	**16**	**21**	**0**	**3**

Behandlung der Zugangsgesuche



3.8 Statistik über die bei der Bundesanwaltschaft eingereichten Zugangsgesuche nach Art. 6 des Öffentlichkeitsgesetzes (Zeitraum: 1. Januar 2012 bis 31. Dezember 2012)

Bundesanwaltschaft BA

Dep.	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt/ aufge-schoben	hängig	Rückzug
BA	4	1	1	2	0	0
Total	**4**	**1**	**1**	**2**	**0**	**0**

3.9 Statistik über die bei den Parlamentsdiensten eingereichten Zugangsgesuche nach Art. 6 des Öffentlichkeitsgesetzes (Zeitraum: 1. Januar 2012 bis 31. Dezember 2012)

Parlamentsdienste PD

Dep.	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt/ aufge-schoben	hängig	Rückzug
PD	0	0	0	0	0	0
Total	**0**	**0**	**0**	**0**	**0**	**0**

3.10 Anzahl Schlichtungsgesuche nach Kategorien der Antragsteller (Zeitraum: 1. Januar 2012 bis 31. Dezember 2012)

Kategorie Antragsteller	2012
Medien	33
Privatpersonen (bzw. keine genaue Zuordnung möglich)	21
Interessenvertreter (Verbände, Organisationen, Vereine usw.)	12
Rechtsanwälte	8
Unternehmen	3
Universitäten	1
Total	**78**

3.11 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:	11 Personen
Einheit 2:	12 Personen
Einheit 3:	5 Personen
Kanzlei:	2 Personen