21. Tätigkeitsbericht 2013/2014

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Tätigkeitsbericht 2013/2014 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 2013 und 31. März 2014 ab.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dieser Bericht ist auch über das Internet (www.derbeauftragte.ch) abrufbar.

Vertrieb:

BBL, Verkauf Bundespublikationen, CH-3003 Bern

www.bbl.admin.ch/bundespublikationen

Art.-Nr. 410.021.d/f

Inhaltsverzeichnis

Vorwort – Bilanz und Ausblick

Letztes Jahr beendete ich das Vorwort mit dem Hinweis, dass das Thema «Big Data» zunehmend ins Zentrum unserer Aufmerksamkeit rücke. Angesichts der technologischen Entwicklung, der riesigen Speicherkapazitäten, der Möglichkeit der raschen Übermittlung grosser Datenbestände über weite Distanzen und ihrer präzisen Analyse werden die Daten zum Rohstoff (zum neuen Kapital?) einer künftigen «data-driven-society». Diese Entwicklung bringt eine massive Gefährdung der Privatsphäre mit sich.

Wenn es eines sinnfälligen, von der ganzen Welt wahrgenommenen Beispiels bedurft hätte, haben die Enthüllungen von Edward Snowden das geleistet und beeindruckendes Anschauungsmaterial geliefert. Die von ihm aufgedeckten skandalösen Überwachungspraktiken der NSA und ihrer Partner haben eine weltweite Debatte über das gewaltige Ausmass der heute möglichen und auch praktizierten globalen Überwachung der Bürger in Gang gesetzt. Der so oft zitierte Satz «Wer nichts zu verbergen hat, braucht auch nichts zu befürchten» ist in seiner Naivität gründlich entlarvt. Was erstaunt, ist die grosse Indifferenz, mit der Bürger und Politiker den Skandal ertragen.

Ein sorgfältigeres Hinschauen über die Möglichkeiten staatlicher Überwachung und allfälliger Gegenstrategien ist jedoch dringend erforderlich. Denn so viel ist klar: Der gläserne Mensch ist keine Chimäre mehr, sondern längst Realität. Die Digitalisierung unserer Lebenswelt hat mit erbarmungsloser Konsequenz dazu geführt, dass früher oder später alles öffentlich wird, ob wir das nun wollen oder nicht. Dieser Konsequenz ist es zu verdanken, dass der Geheimdienst im Fall Snowden selber Opfer jener Untaten wurde, die er im Geheimen veranstalten wollte.

Wer aber, wie viele Kommentatoren, in der Frage der allumfassenden Überwachung nur auf die geheim agierenden staatlichen Behörden fokussiert, greift zu kurz. Denn es sind gerade auch privatwirtschaftliche Akteure, die im Geschäft mit Big Data mitmischen: Daten sind Business, Geld und Macht. Die auf privater Basis entstandenen und laufend weiter wachsenden Datenberge sind das Material, mit dessen Hilfe jeder Einzelne bis ins Detail in seinen Vorlieben, Eigenschaften, Stärken und Schwächen von der Wirtschaft ausgeforscht werden kann. Wenn der private Sektor diese Aufgabe von sich aus erledigt, liegt es auf der Hand, dass staatliche Behörden – da ist die NSA nur eine von vielen – via Facebook und andere Dienste auf das verfügbare Datenmaterial zugreifen.

Dieser Datenberg gibt deshalb Anlass zur Sorge, weil die heute zur Verfügung stehenden immensen Rechnerkapazitäten und automatisierten Analyseverfahren präzise Aussagen über das gegenwärtige und künftige Verhalten der Menschen ermöglichen. Die so entdeckten Muster können zuweilen aufsehenerregende

Erkenntnisse zu Tage fördern. Dabei müssen die gefundenen Korrelationen in keinem logischen Zusammenhang stehen. Ist der Datenberg gross genug, kann vielleicht der Algorithmus zu einem Muster führen, das mit hoher Wahrscheinlichkeit voraussagt, dass eine Glatze hat, wer gelbe Schuhe trägt. Man mag hier einwenden: Mit welcher Wahrscheinlichkeit und unter welchen Umständen jemand eine Glatze und gelbe Schuhe trägt, ist auf den ersten Blick eine harmlose Erkenntnis.

Ich würde erwidern: Gefährlich kann es immer werden, weil auf diesem Weg kompromittierende Handlungen oder Eigenschaften von Menschen entdeckt werden können. Gefährlich deshalb, weil der Algorithmus keine gesicherte Erkenntnis darstellt und schon gar keine gesicherte Kausalität ausdrückt. Es sind immer Aussagen, die mehr oder weniger wahrscheinlich zu- bzw. eintreffen können. Wenn der zu einem Muster führende Algorithmus Aussagen zu einem möglichen kriminellen Verhalten von Menschen macht, kann dies für den Einzelnen verheerend sein. Mit Sicherheit ungemütlich wird es für Herrn X dann, wenn ein Geheimdienst aufgrund der Datenlage einen Algorithmus entdeckt, der ihn als Terroristen identifiziert. Kommt hinzu, dass das Ergebnis des Algorithmus auf viele andere Personen ebenfalls zutreffen kann, wenn eine grosse Menschenmenge unter die Lupe genommen wird. Genau so operieren Geheimdienste wie die NSA, welche die Unschärfe ihrer Analyse nicht weiter stört.

In diesen Kontext passt der Umstand, dass sich zunehmend Haushaltsgeräte und sonstige technische Geräte oft ohne Wissen ihrer Nutzer über das Netz verbinden und miteinander kommunizieren. Man spricht vom Internet der Dinge: Haushaltsgeräte verschicken im Verborgenen Daten an ihre Hersteller, die ihrerseits die Informationen Dritten weiter geben. So informieren Fernsehgeräte TV-Sender, wenn der Zuschauer den Kanal wechselt. Smarte TVs sollen sogar heimlich Festplatten durchsucht haben, wenn diese angeschlossen wurden und verschickten ein Inhaltsverzeichnis der Dateien an die Hersteller. Das Internet der Dinge als künftig grosser Lieferant von Big Data.

Auch die Diskussion um die Weiterverwendung von Informationen des öffentlichen Sektors gehört in diesen Zusammenhang (open government data). Die öffentliche Hand könnte so zu einem Lieferanten von Big Data werden. Wenngleich unbestritten ist, dass damit für Wirtschaft und Gesellschaft beachtliche Mehrwerte generiert werden können, birgt die Nutzung dieser Daten das Risiko, dass sie mit entsprechendem Zusatzwissen bestimmten Personen zugeordnet werden können.

Was heisst dies mit Blick auf die bereits angelaufenen Arbeiten zur Revision des Datenschutzgesetzes?

Spezialisten sind sich einig: Big Data wird für den Datenschutz zu einer grossen Herausforderung, weil damit enorme Risiken einhergehen. Grundlegende technische

und rechtliche Mechanismen des Datenschutzes werden untergraben und ausgehöhlt. Oder wie es Viktor Mayer-Schönberger und Kenneth Cukier in ihrem Buch «Big Data» formulieren: «Big Data kann uns zu lebenslangen Gefangenen unserer vergangenen Handlungen machen, die gegen uns verwendet werden, indem Systeme meinen, unser zukünftiges Verhalten vorhersagen zu können.» Ich gehen davon aus, dass es eine grundlegende Überprüfung braucht, wie die zentralen Grundsätze der Zweckbindung, der Einwilligung und der Transparenz bei der Nutzung von Big Data gewährleistet werden können. Beantwortet werden muss auch die Frage, ob die Auswertung grosser Datenbestände und deren schrankenlose Verknüpfung zulässig sein soll, namentlich, wenn auf der Basis von Wahrscheinlichkeiten Entscheide gefällt werden, die für den Einzelnen Nachteile zur Folge haben.

Fest steht, dass bis heute keine einigermassen verlässlichen Konzepte bestehen, wie dieser Herausforderung begegnet werden kann. Zu prüfen wäre beispielsweise, ob das von der Juristin und Autorin Juli Zeh postulierte digitale Grundrecht ein Weg sein könnte. Sie fordert, dass personenbezogene Daten unter die alleinige Verfügungsgewalt des Einzelnen zu stellen sind; ein Zugriff von privater Seite auf die digitale Identität solle nur mit Einverständnis des Betroffenen möglich sein. Staatliche Eingriffe seien auf die engen Grenzen notwendiger Strafverfolgungsmassnahmen zu beschränken.

Mayer-Schönberger und Cukier verfolgen einen andern Ansatz: Sie schlagen unter anderem die Durchführung einer förmlichen Datenschutzprüfung von Big-Data-Anwendungen vor, bei gleichzeitiger Lockerung der Anforderungen an Zweckbindung und Einwilligung werden. Der Gefahr, dass Big-Data-Vorhersagen und die Algorithmen und Datenbestände, auf denen sie beruhen, zu einer Black Box ohne klare Verantwortlichkeiten werden, würde er mit der Etablierung einer neuen Kontrollinstanz begegnen. Ein «Algorithmiker» würde als unabhängige Instanz, ähnlich wie ein Wirtschaftsprüfer, die Wahl der Daten, die Qualität der Werkzeuge zur Analyse und Vorhersage – einschliesslich der Algorithmen und mathematischen Modelle – und die Interpretation der Ergebnisse überprüfen und gegebenenfalls einschreiten.

Die Revision des Datenschutzgesetzes (DSG) drängt, da die Nutzung von Big Data längst begonnen hat und dadurch grundlegende Bestimmungen des DSG in Frage gestellt sind. Es braucht dringend den Auftrag an eine interdisziplinäre Expertenrunde, welche die Situation umfassend analysiert und Lösungsansätze vorschlägt. Das Parlament hat mit der Überweisung der Motion Rechsteiner einen ersten Schritt in diese Richtung getan. Eines ist klar: Der verfassungsmässige Anspruch auf Schutz der Privatsphäre ist in seiner Substanz gefährdet, wenn die Politik nicht rasch reagiert!

Noch ein Wort zum Öffentlichkeitsgesetz: Das Bundesamt für Justiz hat eine Evaluation des Gesetzes in Auftrag gegeben, nachdem von verschiedenen Seiten der

Bundesverwaltung Kritik daran laut geworden war. In der Vergangenheit wurde wiederholt argumentiert, dass zahlreiche Bestimmungen die Arbeit der Verwaltung behindern würden. Zum Teil verlangen ganze Verwaltungseinheiten, dass sie vom Geltungsbereich des Gesetzes ausgenommen werden. Wir verfolgen diese Entwicklung mit Sorge. Das Gesetz wurde vom Parlament mit dem klaren Ziel erlassen, die Tätigkeit der Verwaltung transparenter zu machen und damit das Vertrauen der Bürgerinnen und Bürger in die staatlichen Institutionen zu stärken. Gerade bei der Vergabe von staatlichen Aufträgen und Subventionen erleben wir grosse Widerstände, wenn die Offenlegung einschlägiger Dokumente verlangt wird. Wie wichtig gerade auch in diesem Bereich eine grössere Transparenz ist, hat der Korruptionsskandal beim SECO drastisch vor Augen geführt.

Abkürzungsverzeichnis

AFAPDP	Association francophone des autorités de protection des données personnelles (Französischsprachige Vereinigung der Datenschutzbehörden)
AHVN13	13-stellige AHV-Nummer
ArGV3	Verordnung zum Arbeitsgesetz
BA	Bundesanwaltschaft
BAFU	Bundesamt für Umwelt
BAG	Bundesamt für Gesundheit
BAV	Bundesamt für Verkehr
BAZL	Bundesamt für Zivilluftfahrt
BBL	Bundesamt für Bauten und Logistik
BFE	Bundesamt für Energie
BFM	Bundesamt für Migration
BFS	Bundesamt für Statistik
BGE	Bundesgerichtsentscheid
BGÖ	Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung
BJ	Bundesamt für Justiz
BK	Bundeskanzlei
BLW	Bundesamt für Landwirtschaft
BR	Bundesrat
BSV	Bundesamt für Sozialversicherungen
BÜPF	Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs
BVG	Bundesgesetz über die berufliche Alters-, Hinterlassenen- und Invalidenvorsorge
BVGer	Bundesverwaltungsgericht
BWO	Bundesamt für Wohnungswesen
CNIL	Commission nationale de l'informatique et des libertés
DAS	Datenannahmestelle
DBA CH-USA	Abkommen zwischen der Schweizerischen Eidgenossenschaft und den Vereinigten Staaten von Amerika zur Vermeidung der Doppelbesteuerung auf dem Gebiete der Steuern vom Einkommen

DEZA	Direktion für Entwicklung und Zusammenarbeit
DRG	Diagnoses Related Groups
DSG	Bundesgesetz über den Datenschutz
DSMS	Datenschutz-Managementssystem
EAZW	Eidgenössisches Amt für Zivilstandswesen
EDA	Eidgenössisches Departement für auswärtige Angelegenheiten
EDI	Eidgenössisches Departement des Innern
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EFD	Eidgenössisches Finanzdepartement
EFK	Eidgenössische Finanzkontrolle
EGMR	Europäischer Gerichtshof für Menschenrechte
EHRA	Eidgenössischer Handelsregisteramt
EJPD	Eidgenössisches Justiz- und Polizeidepartement
ENSI	Eidgenössisches Nuklearsicherheitsinspektorat
EPA	Eidgenössisches Personalamt
EPDG	Bundesgesetz über das elektronische Patientendossier
ESTI	Eidgenössisches Starkstrominspektorat
ESTV	Eidgenössische Steuerverwaltung
Eurodac	Informationssystem zum Vergleich von Fingerabdrücken zum Zwecke der effektiven Anwendung des Dubliner Übereinkommens
EVD	Eidgenössisches Volkswirtschaftsdepartement
EZV	Eidgenössische Zollverwaltung
FIFG	Bundesgesetz über die Förderung der Forschung und der Innovation (Forschungs- und Innovationsförderungsgesetz)
FINMA	Eidgenössische Finanzmarktaufsicht
FOGIS	Formell-gesetzliche Grundlage für den Informationsschutz
GAFI	Groupe d'action financière
GAV	Gesamtarbeitsvertrag
GKI	Gemeinsame Kontrollinstanz von Schengen
GwG	Geldwäschereigesetz
HFG	Humanforschungsgesetz
IPV	Individuelle Prämienverbilligung
IRS	Internal Revenue Service

ISchV	Informationsschutzverordnung
ISO/IEC	ISO/International Electrotechnical Commission
KVG	Bundesgesetz über die Krankenversicherung
KVV	Verordnung über die Krankenversicherung
NDB	Nachrichtendienst des Bundes
NDG	Nachrichtendienstgesetz
NFP	Nationales Forschungsprogramm
NKVF	Nationale Kommission zur Verhütung von Folter
N-SIS	Nationaler Teil des Schengener Informationssystems
OKP	Obligatorische Krankenpflegeversicherung
PBG	Personenbeförderungsgesetz
PIN	Personal Identification Number
POS	Point of Sale
PublG	Publikationsgesetz
RAB	Revisionsaufsichtsbehörde
RAD	Regionale ärztliche Dienste
RFID	Radio Frequency Identification
RTVG	Bundesgesetzes über Radio und Fernsehen
SAS	Schweizerische Akkreditierungsstelle
SCHEVAL	Ständiger Schengener Bewertungs- und Anwendungs-ausschuss des EU-Rats
SECO	Staatssekretariat für Wirtschaft
SIF	Staatssekretariat für internationale Finanzfragen
SIS	Schengener Information System
SIS II	Schengener Information System II
SNF	Schweizerischer Nationalfonds
SUVA	Schweizerische Unfallversicherungsanstalt
Swissmedic	Schweizerisches Heilmittelinstitut
UVEK	Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation
VBGÖ	Verordnung über das Öffentlichkeitsprinzip der Verwaltung
VBS	Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport

VIS	Visa-Informationssystem
VöV	Verband öffentlicher Verkehr
VwVG	Bundesgesetz über das Verwaltungsverfahren
WBF	Eidgenössisches Departement für Wirtschaft, Bildung und Forschung
WEKO	Wettbewerbskommission
ZAS	Zentrale Ausgleichsstelle
ZStV	Zivilstandsverordnung

1. Datenschutz

1.1 Grundrechte

1.1.1 Begleitung von Audits zur Reakkreditierung der Datenschutz-Zertifizierungsstellen

Anlässlich der Zertifizierung von Datenannahmestellen eines Krankenversicherers führte die Schweizerische Akkreditierungsstelle (SAS) mit unserer Beteiligung Reakkreditierungsaudits durch. So bot sich für uns die Gelegenheit, die Gültigkeit der Organisationszertifizierung in diesem besonderen Kontext festzustellen. Zudem erläuterten wir den Zertifizierungsstellen unsere spezifischen Forderungen bezüglich Bereich und Umfang, Qualifikation des Personals, Teamzusammensetzung und Inhalt der Prüfungsberichte.

Im Rahmen des Verfahrens zur Reakkreditierung der Organisations- oder Verfahrenszertifizierungsstellen im Bereich des Datenschutzes begleitete die SAS die Zertifizierung der Datenannahmestellen (DAS) zweier Krankenversicherer, die von den beiden derzeit für den schweizerischen Markt akkreditierten Zertifizierungsstellen durchgeführt wurden. Die Verordnung über die Krankenversicherung (KVG) schreibt nämlich vor, dass ab 1. Januar 2014 gemäss Übergangsbestimmungen jeder Versicherer über eine zertifizierte Datenannahmestelle verfügen muss. Nur die DAS erhält Zugang zu den medizinischen Informationen, die der Leistungserbringer mit der Rechnung und anderen administrativen Daten übermittelt. Sie bestimmt sodann, für welche Rechnungen eine eingehendere Prüfung erforderlich ist, und leitet die dafür notwendigen Informationen an den Versicherer weiter.

Entsprechend der Verordnung über die Datenschutzzertifizierungen wurden wir für diese Nachkontrollen der Reakkreditierung hinzugezogen und konnten dabei feststellen, dass die gegenwärtige Organisationszertifizierung geeignet ist, zu garantieren, dass die Grundprinzipen des Datenschutzes bei der gesamten Tätigkeit der Annahmestellen der Versicherer eingehalten werden. Allerdings haben wir diese Gelegenheit auch genutzt, um den Zertifizierungsstellen, mit Unterstützung der SAS, unsere spezifischen Erwartungen an die nunmehr obligatorische Zertifizierung der DAS der Krankenversicherer zu erläutern:

- Der Prüfungsbereich muss, beim Versicherer wie bei etwaigen Dienstleistern, sämtliche Prozesse abdecken, die zur Ausführung der Aufgaben der DAS erforderlich sind, einschliesslich all ihrer Schnittstellen mit den Umgebungssystemen.
- Der Prüfungsumfang umfasst die Gesamtheit der Kontrollen, die wir für das Datenschutz-Managementsystem (DSMS) definiert haben. Die Norm

ISO/IEC 27006 «Anforderungen an Stellen, die Informationssicherheits-Managementsysteme prüfen und zertifizieren» liefert im Übrigen wertvolle Hinweise bezüglich der Einschätzung des erforderlichen Zeitaufwands, der Qualifikation des beteiligten Personals und des Inhalts der Auditdokumente und -berichte.

- Das Auditteam muss die Kompetenzen eines erfahrenen Hauptauditors, eines auf Krankenversicherungsfragen spezialisierten Datenschutzexperten und eines Experten für Informationssicherheit auf sich vereinen.

Abschliessend sind wir der Ansicht, dass diese Schritte zweifellos zu einer verbesserten Einhaltung der Datenschutzanforderungen in den zertifizierten Annahmestellen beitragen werden (vgl. die auf unserer Webseite publizierte Liste; www.derbeauftragte.ch, Datenschutz – Zertifizierung – Swiss DRG).

1.1.2 Teilrevision der Statistikerhebungsverordnung

Der Bundesrat hat die Teilrevision der Verordnung über statistische Erhebungen genehmigt. In den Vernehmlassungsverfahren begrüssten wir die unternommenen Bemühungen um eine möglichst grosse Klarheit und Transparenz des Textes. Wir erinnerten indes auch an die Notwendigkeit eines Bearbeitungsreglements und der Aufnahme von Gesetzgebungsarbeiten zum Bundesstatistikgesetz, damit die Verwendung der AHV-Nummer in den statistischen Erhebungen einheitlich und transparent geregelt wird.

Am 18. Dezember 2013 genehmigte der Bundesrat die Teilrevision der Statistikerhebungsverordnung. Die Änderungen sind am 15. Januar 2014 in Kraft getreten. Die revidierte Verordnung bestimmt, unter welchen Voraussetzungen und in welcher Form Datenverknüpfungen erlaubt sind. Die verschiedenen Statistiken sind im Anhang der Verordnung über die Durchführung von statistischen Erhebungen aufgelistet. Mit der jährlichen Überarbeitung dieses Anhangs wird die erforderliche Rechtsgrundlage für die regelmässige Anpassung und Aktualisierung der Statistiken geschaffen. Im Rahmen der Revision der Verordnung wurden aus Transparenzgründen jeweils für jede Statistik die vorgesehenen Datenverknüpfungen angegeben.

Im Vernehmlassungsverfahren äusserten wir uns zur besagten Verordnung sowie zu ihrem Anhang. Wie wir feststellen konnten, berücksichtigten der in die Vernehmlassung gegebene Entwurf und die diesbezüglichen Erläuterungen die meisten Bemerkungen aus unserer Stellungnahme von 2012 (vgl. unseren 20. Tätigkeitsbericht 2012/2013, Ziff. 1.1.1), darunter namentlich die Phasen der Pseudonymisierung/Anonymisierung, die Vernichtung des Erhebungsmaterials.

Wir begrüssten zugleich die Bemühungen, die unternommen worden waren, um die Datenverknüpfung möglichst klar und transparent zu machen.

Wir erinnerten indes an die Notwendigkeit eines Bearbeitungsreglements, in dem namentlich der Prozess des Key Management beschrieben wird; auch sei eine Revision des Bundesstatistikgesetzes erforderlich, um eine einheitliche und transparente Regelung der AHV-Nummer in den statistischen Erhebungen zu ermöglichen. Ferner müssten im Rahmen dieser gesetzgeberischen Arbeiten Methoden zur Verschlüsselung bzw. Pseudonymisierung der AHV-Nummer geprüft werden.

Im Vernehmlassungsverfahren wurde deutlich, dass manche Bundesämter sehr daran interessiert wären, ihre Daten selbst mit denen das Bundesamtes für Statistik (BFS) zu verknüpfen. Nach dem heutigen Stand des Bundesstatistikgesetzes ist eine extensive Auslegung nicht gestattet; das BFS und die kantonalen und kommunalen Dienststellen für Statistik sind als Einzige befugt, zur Erfüllung ihrer Aufgaben im Statistikbereich die Daten des BFS zu verknüpfen. Für eine Ausweitung auf andere Bundesorgane wäre eine Änderung der gesetzlichen Grundlage unerlässlich.

1.1.3 Das Projekt MARS des Bundesamtes für Statistik

Wir haben vom Start des Projekts MARS beim Bundesamt für Statistik Kenntnis genommen. Ziel des Projekts ist die Einrichtung eines integralen statistischen Informationssystems über die Gesundheitsversorgung, das Daten zu den Einrichtungen, Leistungserbringern und Patienten liefert. Wir verfolgen das Projekt weiterhin aufmerksam.

Das Projekt MARS (Modules ambulatoires des Relevés sur la Santé; Statistiken der ambulanten Gesundheitsversorgung) des BFS entstand aus der Abänderung der Verordnung über die Krankenversicherung (KVV), die im Anschluss an die Teilrevision des Gesetzes über die Krankenversicherung (KVG) erfolgte. Darin wird das Bundesamt für Statistik beauftragt, bei den Leistungserbringern Daten zur ambulanten Gesundheitsversorgung zu erheben.

Die derzeit im ambulanten Sektor verfügbaren Daten sind unvollständig. Ziel des Projekts ist deshalb die Einrichtung eines integralen statistischen Informationssystems über das Gesundheitswesen, das Daten zu den Einrichtungen, Leistungserbringern und Patienten liefert. Das System soll den statistischen Bedürfnissen gemäss dem Bundesstatistikgesetz sowie den Vollzugsaufgaben des Bundes und der Kantone im Sinne des KVG gerecht werden. So sollen die bisher verfügbaren Daten im Sektor der stationären Gesundheitsversorgung um Daten über die Leistungen im ambulanten Sektor ergänzt werden.

In Anbetracht der besonderen Schutzwürdigkeit der erhobenen Personendaten werden wir das Projekt weiterhin aufmerksam verfolgen. Dazu ist festzuhalten, dass der Bundesrat die Erhebung, die Bearbeitung, die Weitergabe und die Veröffentlichung der Daten, unter Einhaltung des Verhältnismässigkeitsprinzips, noch in detaillierten Bestimmungen regeln muss. Zudem muss ein Bearbeitungsreglement erstellt werden, das die Bearbeitungsprozesse präzisiert.

Verschiedene Unterprojekte sind vorgesehen und müssen schrittweise verwirklicht werden. Für 2014 sind erste Pilotversuche geplant. Wir verfolgen das Projekt weiterhin aufmerksam, gerade auch weil einige rechtliche als auch technische Punkte im jetzigen Stadium noch offen sind.

1.1.4 Thinkdata: Arbeiten der Projektgruppe

Im Rahmen unserer Sensibilisierungstätigkeiten beteiligen wir uns weiterhin aktiv am Projekt Thinkdata. Das Projekt ist nun in seine operative Phase eingetreten, die von uns beaufsichtigt wird. Gleichzeitig lässt die Arbeitsgruppe, die sich mit der strategischen Fortführung des Projekts befasst, ihre Aktivitäten ruhen.

Um Thinkdata, den Dienst zur Sensibilisierung für den Datenschutz und das Öffentlichkeitsprinzip weiter zu entwickeln, haben wir die Führung einer operativen Gruppe übernommen, die sich aus mehreren Vertretern der kantonalen Datenschutzbehörden sowie Mitgliedern aus dem Privatsektor, der Politik und weiteren Bereichen zusammensetzt. Die Projektgruppe ist im Laufe des Jahres mehrmals zusammengetreten, um die Zukunft des Dienstes zu erörtern, aber auch um gewisse Funktionen der Webseite den Bedürfnissen der Nutzer wie auch der Dienstanbieter anzupassen.

Mehrere neue Szenarien sind entwickelt und auf der www.thinkdata.ch aufgeschaltet worden (hauptsächlich auf Französisch). Die Zahl der Besucher ist gleich geblieben, und über das Kontaktformular auf der Internetseite treffen regelmässig neue Vorschläge für weitere Szenarien ein.

In Zusammenarbeit mit den kantonalen Beauftragten möchten wir Thinkdata zu einem Dienst der Datenschutzbehörden machen und die Zusammensetzung der Projektgruppe neu definieren.

1.2 Datenschutzfragen allgemein

1.2.1 Zentrale Speicherung von Kundenfotos bei Skistationen – Abschluss des Verfahrens

Die von uns überprüfte Skistation hat sämtliche für einen datenschutzkonformen Betrieb des Zutrittkontrollsystems notwendigen Änderungen vorgenommen. Das Verfahren zur Sachverhaltsabklärung konnte damit abgeschlossen werden.

Da die in vielen Skistationen praktizierte Zugangskontrolle mittels Fotoabonnementskarten bei einigen Kundinnen und Kunden auf Widerstand gestossen ist, haben wir die Datenschutzkonformität solcher Systeme überprüft (vgl. 18. Tätigkeitsbericht 2010/2011, Ziff. 1.2.5). Zunächst haben wir bei einer betroffenen Skistation eine Sachverhaltsabklärung durchgeführt und mehrere Mängel bei der Umsetzung der datenschutzrechtlichen Bearbeitungsgrundsätze festgestellt. Einige dieser Mängel lagen im von den meisten Schweizer Skistationen verwendeten System selbst (vgl. 19. Tätigkeitsbericht 2011/2012, Ziff. 1.2.9). Der Systemhersteller erklärte sich daraufhin bereit, die von uns verlangten Verbesserungen schnellstmöglich technisch umzusetzen (vgl. 20. Tätigkeitsbericht 2012/2013, Ziff. 1.2.2).

Andere Mängel lagen an der konkreten Handhabung des Systems durch die kontrollierte Skistation. So wurden die betroffenen Personen zu wenig genau über die erfolgten Datenbearbeitungen informiert. Es fehlten z.B. Löschfristen für die gespeicherten Daten, und die Vergabe von Zugangsberechtigungen war zu wenig klar geregelt. Die Skistation hat die für einen datenschutzkonformen Betrieb des Systems notwendigen Änderungen in der Zwischenzeit vorgenommen und damit alle unsere Forderungen erfüllt. Das Verfahren zur Sachverhaltsabklärung konnte somit abgeschlossen werden.

1.2.2 Videoüberwachung zu Forschungszwecken

Werden bei einem Forschungsprojekt Teilnehmerinnen und Teilnehmer gefilmt, so ist der Schutz ihrer Persönlichkeit recht einfach umzusetzen. Werden hingegen nicht direkt beteiligte Drittpersonen im Zuge eines solchen Projekts aufgenommen, sind einige Vorkehrungen zu treffen, damit der Datenschutz gewahrt bleibt.

Videoaufnahmen im Rahmen von Forschungsprojekten ermöglichen es, das Verhalten bestimmter Personen festzuhalten und auszuwerten. Die daraus gewonnenen Daten sind oft viel genauer als solche, die z.B. mit Hilfe eines Fragebogens erhoben wurden. Erfassen die Kameras nur die an einem Forschungsprojekt teilnehmenden Personen, sind die datenschutzrechtlichen Bearbeitungsprinzipien verhältnismässig

einfach umzusetzen, so dass die Gefahr einer Persönlichkeitsverletzung gering gehalten werden kann. Die betroffenen Personen nehmen in der Regel freiwillig am Forschungsprojekt teil, wissen, dass sie gefilmt werden und was mit ihren Daten anschliessend geschieht oder können zumindest nachträglich umfassend über das Forschungsprojekt informiert werden.

Schwieriger stellt sich die Situation dar, wenn die Forscher in öffentlich zugänglichen Zonen filmen und die Kameras dabei auch Personen erfassen, die nicht direkt in das Forschungsprojekt involviert sind. Es wäre ein Irrtum davon auszugehen, dass z.B. Bilder von zufälligen Passanten keine Personendaten sind, nur weil die Abgebildeten nicht namentlich bekannt sind. Solche Bilder können auch ohne Namen bestimmten Personen zugeordnet werden, weshalb sie klar als Personendaten gelten und die datenschutzrechtlichen Bearbeitungsgrundsätze auch hier einzuhalten sind.

Zwar dürfen Personendaten zu Forschungszwecken auch ohne die Einwilligung der Betroffenen bearbeitet werden, sofern die Studie keinem personenbezogenen Zweck dient und in den publizierten Forschungsergebnissen keine Personen erkennbar sind. Trotz dieses Forschungsprivilegs besteht aber die Pflicht, über die Datenbearbeitung zu informieren, was sich beim Filmen im öffentlichen Raum als schwer umsetzbar erweisen kann. Zufällig in den Aufnahmebereich eintretende Passanten zum Beispiel erfahren in der Regel erst dann von der Datenbearbeitung, wenn sie die Kamera sehen und die Aufzeichnung bereits stattfindet oder stattgefunden hat.

Um die Persönlichkeitsrechte dieser Personen zu wahren, sollte daher Folgendes beachtet werden:

Die Anwendung des Forschungsprivilegs setzt voraus, dass Videobilder, auf denen Personen erkennbar sind, entweder nicht veröffentlicht oder vorgängig so verfremdet werden, dass niemand mehr identifiziert werden kann. Hierbei gilt es zu beachten, dass es oft nicht ausreicht, wenn z.B. nur die Augen der Betroffenen abgedeckt werden, da Personen auch an ihrem Gang, ihrer Kleidung usw. erkannt werden können.

Wenn möglich sollte mit gut sichtbaren Hinweistafeln auf die Videoaufnahmen aufmerksam gemacht und angeben werden, an wen man sich für weitere Informationen sowie zur Geltendmachung des Auskunfts- und Löschungsrechts wenden kann. Ist dies nicht möglich, so ist standardisiertes Informationsmaterial (z.B. Flyer, Broschüre) zu erstellen, dass vor Ort abgegeben werden kann. Die Broschüre sollte nebst allen wichtigen Punkten der Datenbearbeitung auch die erwähnten Kontaktangaben enthalten. Die Betroffenen müssen das Auskunfts- und Löschungsrecht einfach und kostenlos geltend machen können.

Das Forschungsprivileg vermag keinesfalls Videoaufnahmen des Intimbereichs zu rechtfertigen. Aufnahmen in Toiletten, Umkleidekabinen usw. sind daher, ohne die Einwilligung der betroffenen Personen, auch im Bereich der Forschung unzulässig.

1.2.3 Herausgabe von Videobildern an Strafverfolgungsbehörden

Werden Bilder von Überwachungskameras gestützt auf eine behördliche Verfügung heraus verlangt, ist ihre Herausgabe gerechtfertigt. Stützt sich die Anfrage hingegen nicht auf eine Verfügung, sollte der Betreiber der Videoüberwachungsanlage die Aufnahmen nur nach sorgfältiger Abwägung der Situation herausgeben. Er ist für die Rechtmässigkeit der Herausgabe verantwortlich.

Verlangt eine Strafverfolgungsbehörde im Rahmen eines Strafverfahrens Videobilder heraus und stützt sie sich dabei auf eine Verfügung, die den Betreiber der Überwachungsanlage zur Herausgabe verpflichtet, so ist das Herausgeben der Bilder gerechtfertigt. Stellt die Behörde die Anfrage ausserhalb eines Strafverfahrens, kann ein überwiegendes öffentliches Interesse die Herausgabe auch ohne Verfügung rechtfertigen. Ob ein solches vorliegt, muss der Betreiber der Überwachungsanlage aufgrund einer Interessenabwägung beurteilen. Dieser Entscheid kann heikel sein und sollte sich stets auf die nachfolgenden Überlegungen stützen:

- Zunächst wird geprüft, wer die Herausgabe verlangt. Ohne Verfügung sollten Bilder nur an Strafverfolgungsbehörden heraus gegeben werden. Bei anderen Behörden oder Privaten sollte immer eine Verfügung verlangt werden.
- Anschliessend muss der Betreiber prüfen, zu welchem Zweck die Bilder benötigt werden. Daher sollte die schriftliche Anfrage stets eine Begründung enthalten. Eine Herausgabe ohne Verfügung ist nur dann gerechtfertigt, wenn damit schwerwiegende Interessen geschützt werden sollen; bei Anfragen ohne Begründung oder zu Bagatellzwecken sollte der Betreiber die Herausgabe verweigern. Da er verantwortlich gemacht werden kann, wenn er Videobilder ohne Verfügung oder überwiegendes Interesse herausgibt, sollte er im Zweifel eine Verfügung verlangen.
- Gelangt der Betreiber einer Videoüberwachungsanlage zur Ansicht, dass eine Herausgabe gerechtfertigt ist, muss er das Material sichten und die für die Anfrage relevanten Bilder aussondern. Die Herausgabe hat sich auf diese zu beschränken.

Genaueres zum Thema kann auf unserer Webseite www.derbeauftragte.ch, Datenschutz – Videoüberwachung in unseren «Erläuterungen zur Herausgabe von Videobildern an Strafverfolgungsbehörden» nachgelesen werden.

1.2.4 Erfassung von Hausverboten in einer zentralen Datenbank

Nachtclubs dürfen Personendaten grundsätzlich in einer internen Schwarzen Liste erfassen, um die von ihnen erteilten Hausverbote durchzusetzen. Die Bekanntgabe solcher besonders schützenswerter Personendaten an Drittclubs ist nur im Einzelfall gerechtfertigt. Problematisch ist die systematische Bekanntgabe von Daten, die im Rahmen eines erteilten Hausverbotes erfasst wurden, an andere Clubs mittels einer zentralen Datenbank.

Im Rahmen unserer Beratungstätigkeit haben wir eine zentralen Datenbank im Bereich Diskotheken hinsichtlich ihrer Datenschutzkonformität überprüft. Wir kamen zum Schluss, dass Anpassungen erforderlich sind und haben den Verantwortlichen entsprechende Vorschläge unterbreitet.

Betriebe wie Nachtclubs oder Diskotheken dürfen im Rahmen des Hausrechts sogenannte Hausverbote erteilen. Um die erteilten Verbote in den Einzelbetrieben durchzusetzen, erfassen sie die Personendaten der unerwünschten Gäste in einer Schwarzen Liste oder Blacklist und führen Ausweiskontrollen durch. Eine solche Datenbearbeitung wird grundsätzlich durch ein überwiegendes privates Interesse rechtfertigt, soweit die allgemeinen Grundsätze des Datenschutzgesetzes (DSG) beachtet werden. Da das fehlbare Verhalten von Clubbesuchern, die in einer solchen Datenbank erfasst werden, auch strafrechtliche Konsequenzen nach sich ziehen kann, muss davon ausgegangen werden, dass diese Blacklist besonders schützenswerte Personendaten enthält. Folglich sind an die Bearbeitung solcher Daten erhöhte Anforderungen zu stellen, insbesondere betreffend Datensicherheit und Informationspflicht.

Wollen die einzelnen Betriebe im Rahmen eines Vereins die betreffenden Personendaten nun in einer zentralen Datenbank erfassen, auf welche alle Betriebe Zugriff haben, stellt dies eine Bekanntgabe von Personendaten an Dritte im Sinne des DSG dar. Da der Zweck der Weitergabe nicht mehr das Durchsetzen eines erteilten betrieblichen Hausverbots ist, braucht es hierzu einen eigenen Rechtfertigungsgrund. Es muss somit im Einzelfall geprüft werden, ob ein überwiegendes privates bzw. öffentliches Interesse die Weitergabe an Dritte rechtfertigt. Dies ist in der Regel (nur) der Fall, wenn das fehlbare Verhalten der betroffenen Person eine gewisse Schwere aufweist und wenn man davon ausgehen kann, dass sie das fragliche Verhalten auch an anderen Orten wiederholen wird. Nicht gerechtfertigt ist die Weitergabe, wenn es sich etwa um ein persönliches Problem mit einem konkreten Mitarbeiter handelt.

Es kann somit problematisch sein, wenn Daten, die im Rahmen eines erteilten Hausverbotes erfasst wurden, mittels einer zentralen Datenbank Drittclubs zugänglich

gemacht werden. Ein solches Vorgehen führt zu einer automatisierten Bekanntgabe von Personendaten an Dritte. Es kann in diesem Fall nicht bei jeder Abfrage geprüft werden, ob ein Rechtfertigungsgrund besteht.

Für die rechtmässige Datenbearbeitung bzw. für die Interessenabwägung ist jeweils der einzelne Betrieb verantwortlich. Die Übertragung der Datenbearbeitung an Dritte im Rahmen eines Outsourcing-Vertrags ist jedoch möglich. Der Dritte darf in diesem Fall die Daten nur so bearbeiten, wie der Auftraggeber selbst es tun dürfte. Für den Fall, dass der Auftragnehmer für mehrere Clubs tätig ist, muss er organisatorische und technische Massnahmen treffen, damit die Datensammlungen nicht für die anderen Clubs zugänglich sind. Die Schwarze Liste muss intern bleiben und darf nicht in einer zentralen Datenbank mit Listen von Drittclubs geführt werden. Liegt im Einzelfall ein Rechtfertigungsgrund für die Bekanntgabe an Dritte vor, kann der Auftragnehmer die betreffenden Daten an die anderen Clubs weitergeben, z.B. über eine zentrale Datenbank.

Wir haben technische und organisatorische Anpassungen für die Umsetzung der datenschutzrechtlichen Anforderungen verlangt: Insbesondere muss eine klare Trennung zwischen den internen Schwarzen Listen, wozu nur der jeweilige Club Zugang haben darf, und der gemeinsamen Datenbank bestehen. Ein Bearbeitungsreglement muss für die interne Blacklist erstellt werden, ein anderes für die gemeinsame Liste. Für die Aufnahme eines Hausverbots in letztere müssen strenge Anforderungen gelten. Es muss sich namentlich um Vorfälle handeln, die eine gewisse Schwere aufweisen. Zudem ist eine Prüfung der Wiederholungsgefahr im Einzelfall erforderlich. Bei Datenbearbeitungen durch Dritte ist eine Outsourcing-Vereinbarung abzuschliessen.

1.2.5 Einführung einer elektronischen Karte für den öffentlichen Verkehr

An einer Sitzung mit dem Verband öffentlicher Verkehr und den SBB liessen wir uns die ab 2015 geplante Einführung der elektronischen Karte für den öffentlichen Verkehr (ÖV-Karte) vorführen. Die Einführung ist schrittweise vorgesehen, wobei verschiedene Punkte noch offen sind. Wir werden die Entwicklung weiter verfolgen.

Wie wir einer vom Verband öffentlicher Verkehr (VöV) und den SBB herausgegebenen Medienmitteilung entnehmen konnten, soll die elektronische ÖV-Karte, die RFID enthalten wird, per Mitte 2015 eingeführt werden. In der Medienmitteilung wurde ebenfalls darauf hingewiesen, dass die Anforderungen des schweizerischen Datenschutzes eingehalten würden. Um dies zu überprüfen, liessen wir uns das Projekt vom VöV und den SBB an einer Sitzung vorführen. In einem ersten Schritt

werden die Abonnemente mit einem RFID-Chip ausgerüstet. Der Chip selbst wird eine Referierungsnummer, jedoch weder Vor- noch Nachnamen enthalten. Diese Daten werden vor allem Kontrollzwecken dienen. Der VöV und die SBB haben uns zugesichert, uns über die weiteren Entwicklungen auf dem Laufenden zu halten. Wir werden die weiteren Schritte verfolgen und laufend zu datenschutzrechtlichen Aspekten Stellung nehmen.

1.2.6 Reisende ohne gültigen Fahrausweis

Im Nachgang zu unserer Kontrolle bei den SBB betreffend Reisende ohne gültigen Fahrausweis führten wir eine Nachkontrolle durch. Dabei prüften wir die Löschung der Daten. Weiter haben wir zum Entwurf einer gesetzlichen Grundlage für das entsprechende Informationssystem Stellung genommen.

In Zusammenhang mit unserer Kontrolle betreffend Reisende ohne gültigen Fahrausweis hatten wir festgestellt, dass die SBB gar keine Daten gelöscht hatten, obwohl sie für diese Daten eine Aufbewahrungsdauer von zwei Jahren vorgesehen hatten (vgl. unseren Tätigkeitsbericht 2012/2013, Ziff. 1.2.3). Nachdem die SBB unsere Empfehlungen angenommen und uns ein Konzept für die Löschung und das Bearbeitungsreglement unterbreitet hatten, führten wir eine Nachkontrolle durch. Dabei konnten wir feststellen, dass sämtliche Daten, deren Aufbewahrungsdauer abgelaufen war, im Informationssystem gelöscht worden waren. Gelöscht wurden rund 1.85 Millionen Reisen, rund 0.72 Millionen Reisende sowie rund 2.7 Millionen Datensätze der Zugbegleitergeräte. Desgleichen wurden auch die zu lange aufbewahrten eingescannten «Formulare 7000» vernichtet.

Anlässlich unserer Kontrolle hatten wir weiter festgestellt, dass das Personenbeförderungsgesetz (PBG) zwar die Erhebung des Zuschlags für Reisende ohne gültigen Fahrausweis, nicht aber das Informationssystem selbst regelt. Das Bundesamt für Verkehr (BAV) hatte uns gegenüber erklärt, die entsprechenden Schritte zur Schaffung der fehlenden gesetzlichen Grundlage in die Wege zu leiten. Das BAV baute diese darauf in ein bereits bestehendes Gesetzgebungspaket («Strassenzulassung und Verkehrsstrafrecht») als neuen Artikel 20a PBG ein. Wir haben zum Entwurf Stellung genommen und einige Änderungsvorschläge gemacht, die mehrheitlich übernommen wurden. Das gesamte Gesetzgebungspaket wurde im September 2013 vom Bundesrat behandelt und wird demnächst im Parlament beraten werden.

1.2.7 Drohnen und Datenschutz

Zum Thema Drohnen und Videoüberwachung hatten wir eine Sitzung mit dem Bundesamt für Zivilluftfahrt und wurden von der Kommission für Verkehr und Fernmeldewesen des Nationalrats angehört. Wir sind der Auffassung, dass die datenschutzrechtliche Situation der Drohnen näher geprüft und allenfalls spezielle Regelungen und/oder Bewilligungen vorgesehen werden müssten.

Auf dem Markt werden vermehrt Drohnen zu erschwinglichen Preisen und mit einfacher Bedienung angeboten. Drohnen sind ferngesteuerte, meist kleinere Fluggeräte, die rechtlich den Modellflugzeugen gleichgestellt sind. Bis zu einem Gewicht von 30 Kilogramm wird grundsätzlich keine Bewilligung benötigt, sofern der «Pilot» jederzeit Sichtkontakt zu seiner Drohne hat. Drohnen sind vermehrt mit einer Kamera ausgestattet und werden immer häufiger, sowohl zu privaten als auch zu gewerblichen Zwecken, eingesetzt.

Es ist sehr einfach, mit einer Drohne private Gärten und Gebäude oder Büros zu überfliegen und zu filmen. Es können Videoaufnahmen an Orten gemacht werden, zu denen man zu Fuss gar keinen Zutritt hätte. Betroffene Personen erfahren nicht immer, dass sie oder ihr Haus/Büro gefilmt wurden. In manchen Fällen wird die Drohne erst entdeckt, wenn sie bereits Videoaufnahmen macht. Zudem kann nicht immer ermittelt werden, welche Person dahinter steckt. Zum Teil sind sich die Benutzer nicht bewusst, dass sie etwas Unrechtmässiges (evtl. auch Strafbares) machen, teils nehmen sie es in Kauf. Die aufgenommenen Bilder können sehr leicht im Internet veröffentlich werden, was die Datenschutz-Problematik verschärft.

Vor diesem Hintergrund haben wir die datenschutzrechtlichen Anforderungen an solche Aufnahmen formuliert und Erläuterungen zum Thema publiziert (www.derbeauftragte.ch, Datenschutz – Technologien – Videoüberwachung).

Ferner hatten wir in dieser Sache eine Besprechung mit dem Bundesamt für Zivilluftfahrt (BAZL) und dem Bundesamt für Justiz (BJ). Auch wurden wir von der Kommission für Verkehr und Fernmeldewesen des Nationalrats angehört. An der Sitzung waren sich alle Teilnehmer einig, dass eine grosse Schwierigkeit in Zusammenhang mit Drohnen bei der Durchsetzung der Rechte der betroffenen Personen liegt. Die Kommission hat entschieden, die Situation vorerst nur zu beobachten.

Wir sind der Auffassung, dass die datenschutzrechtliche Situation des Einsatzes von Drohnen näher geprüft werden müsste. Es stellt sich insbesondere die Frage, ob spezielle Regelungen und/oder Bewilligungsverfahren geschaffen werden müssten und wie man die Öffentlichkeit für einen verantwortungsvollen Umgang mit dieser Technologie sensibilisieren könnte.

1.2.8 Teilrevision des Bundesgesetzes über Radio und Fernsehen

Der Entwurf des teilrevidierten Bundesgesetzes über Radio und Fernsehen sieht die Schaffung einer gesetzlichen Grundlage vor für den Bezug der Daten zu den Haushalten und den zugehörigen Personen, inklusive Versichertennummer (AHVN13), von den Einwohnerregistern. Wie wir im Rahmen der Ämterkonsultation betonten, birgt die Verwendung der Versicherungsnummer in diesem Zusammenhang das Risiko der Verknüpfung von Datenbanken.

Im letzten Jahr konnten wir uns zum Entwurf des teilrevidierten Bundesgesetzes über Radio und Fernsehen (RTVG) äussern. Wir haben einerseits Anmerkungen zur Datenbearbeitung durch die Erhebungsstelle gemacht, insbesondere bezüglich der besonders schützenswerten Daten, sowie zur Verschlüsselung dieser Daten. Diese Anmerkungen wurden in den Gesetzestext übernommen.

Eine Differenz konnte jedoch mit dem für die Revision zuständigen Bundesamt nicht bereinigt werden. Sie betrifft die Verwendung der Versichertennummer (AHVN13) aus den Einwohnerregistern: Wir sind in der Beurteilung des Gesetzesentwurfes zum Schluss gekommen, dass die Verwendung der AHV-Nummer zur Gebührenerhebung nicht notwendig ist, sie nicht das mildeste Mittel darstellt und die Verhältnismässigkeit im engeren Sinne nicht gegeben ist. Daher ist auf die Verwendung der Versichertennummer durch die Gebührenerhebungsstelle zu verzichten. Insbesondere schafft der flächendeckende Einsatz eines Personenidentifikators in der Verwaltung (Bund, Kantone, Gemeinden) die technischen Voraussetzungen zur Zusammenführung personenbezogener Informationen aus Datenbanken, welche die unterschiedlichsten Lebensbereiche betreffen. Die unerwünschte oder verbotene Verknüpfung kann aber erhebliche Persönlichkeitsverletzungen zur Folge haben. Daher muss jede systematische Verwendung der Versichertennummer ausserhalb der Sozialversicherung notwendig und verhältnismässig sein.

Wir haben vorgeschlagen, stattdessen eine bereichsspezifische bzw. sektorielle Nummer zu verwenden, welche auf Basis der AHVN13 errechnet wird (gehashte AHV-Nummer). Diese Umwandlung mittels einer Einwegfunktion würde dazu führen, dass die ursprüngliche Nummer nicht mehr errechnet werden könnte, was das Problem der Verknüpfung von verschiedenen Datenbanken erheblich reduzieren würde.

1.2.9 Totalrevision des Bundesgesetzes über die Informationssysteme des Bundes im Bereich Sport

Im Rahmen der Ämterkonsultation zur Totalrevision des Gesetzes über die Informationssysteme des Bundes im Bereich Sport haben wir zu den Entwürfen Stellung genommen. Insbesondere haben wir uns zur notwendigen Einwilligung durch die betroffenen Sportler sowie zur Ergänzung der Kategorien von Personendaten im Informationssystem der nationalen Agentur zur Bekämpfung von Doping geäussert.

Im Oktober 2012 wurde das Gesetz über die Informationssysteme des Bundes im Bereich Sport in Kraft gesetzt. Hinzugekommen sind seither das System zur Bearbeitung leistungsdiagnostischer Daten, das System zur systematischen Evaluation von Kursen und Lehrgängen und das System der nationalen Agentur zur Bekämpfung von Doping. Sie alle bedürfen einer formell-gesetzlichen Grundlage. Wir haben zum Gesetzesentwurf und zur Botschaft Stellung genommen.

Einerseits haben wir erwirkt, dass die Bestimmung bezüglich der Bekanntgabe leistungsdiagnostischer Daten und Ergebnisse in den Erläuterungen dahingehend ergänzt wurde, dass für jede Datenbekanntgabe die Einwilligung der betroffenen Sportler nach vorgängiger Information vorliegen muss.

Andererseits wurden aufgrund unserer Eingabe alle im Informationssystem der nationalen Agentur zur Bekämpfung von Doping geführten Kategorien von Personendaten aufgeführt. Im Prinzip bedarf es nur für die Bearbeitung von Persönlichkeitsprofilen und besonders schützenswerten Personendaten einer formell-gesetzlichen Grundlage. Für alle anderen Kategorien wäre eine gesetzliche Grundlage auf Verordnungsstufe ausreichend. Die Auflistung aller im System geführten Kategorien von Personendaten trägt zum besseren Verständnis des Informationssystems bei.

1.2.10 Veröffentlichung von Zivilstandsdaten im Internet

Wir haben das eidgenössische Amt für Zivilstandswesen betreffend die datenschutzrechtliche Problematik der Veröffentlichung von Zivilstandsdaten im Internet beraten. Dabei haben wir auf den Kontrollverlust, die unverhältnismässig lange Bearbeitung dieser Daten durch Dritte und die möglichen Zweckänderungen bei den Datenbearbeitungen hingewiesen.

Das eidgenössische Amt für Zivilstandswesen (EAZW) hat uns im Vorfeld der geplanten Änderungen von Artikel 57 der Zivilstandsverordnung (ZStV) um Beratung gebeten. Der Verordnungsartikel regelt die Veröffentlichung von Zivilstandsdaten durch die Kantone. Diese können in Eigenkompetenz die Publikation von Geburten,

Todesfällen, Trauungen und eingetragenen Partnerschaften regeln. Die Kantone haben die rechtlichen Vorgaben für die Veröffentlichung dieser Daten in der Folge unterschiedlich ausgestaltet. Wir haben das EAZW vor allem auf die mit der Publikation im Internet verbundenen Gefahren hingewiesen. So geht dabei etwa die Kontrolle über die Daten verloren. Auch werden sie länger als ursprünglich vorgesehen und zu verschiedensten Zwecken bearbeitet und mit weiteren Daten zu Persönlichkeitsprofilen verknüpft, um nur einige der Aspekte zu erwähnen, die wir erläutert haben. Aus denselben Gründen erachten wir auch die zeitlich unlimitierte Veröffentlichung von Handelsregisterdaten über das Internet als problematisch (vgl. Ziffer 1.8.4 dieses Tätigkeitsberichts).

1.2.11 Publikation von Massnahmen des Erwachsenenschutzes

Wir haben auf Anfrage der Rechtskommission des Nationalrates erläutert, wie die Bekanntgabe von Erwachsenenschutzmassnahmen datenschutzkonform ausgestaltet und die Rechtssicherheit im Geschäftsverkehr gewahrt werden kann.

Die Rechtskommission des Nationalrates bat uns um eine Stellungnahme zur parlamentarischen Initiative von Rudolf Joder. Die Initiative will die Publikation von Erwachsenenschutzmassnahmen ändern. Das neue Erwachsenenschutzrecht, das seit 2013 in Kraft ist, sieht im Unterschied zu früher aus Persönlichkeitsschutzgründen keine Publikation derselben mehr vor. Gemäss Artikel 451 des Zivilgesetzbuches kann zwar gegen Geltendmachung eines Interessensnachweises bei der Erwachsenenschutzbehörde Auskunft darüber verlangt werden, ob eine solche Massnahme vorliegt. Grundsätzlich gilt aber das Prinzip der Geheimhaltung. Der Initiant macht geltend, dass durch diese Regelung die Rechtssicherheit im alltäglichen Geschäftsverkehr gefährdet werde. Die Erwachsenschutzbehörde sei demzufolge neu zu verpflichten, das Betreibungsregister am Wohnsitz der betroffenen Person über die Ergreifung oder die Aufhebung einer Massnahme zu informieren. Auch soll das Betreibungsamt zur Weitergabe dieser Information ermächtigt werden.

Wir haben die Bedingungen für eine datenschutzkonforme Bearbeitung dieser Daten formuliert. Unserer Meinung nach dürfen nur Informationen eingetragen werden, die die Vertragsfähigkeit einer Person betreffen. Die Betreibungsämter ihrerseits dürfen diese nicht ohne Interessensnachweis (bspw. Vertragsverhandlungen) weitergeben; allfällige Datenweitergaben an Wirtschaftsauskunfteien sind gesetzlich klar zu regeln.

1.3 Internet und Telekommunikation

1.3.1 Internet-Tauschbörsen und Urheberrecht – aktueller Stand

Da nach dem Urteil Logistep Unsicherheit über die Verfolgbarkeit von Urheberrechtsverletzungen im Internet entstanden ist, hat eine Arbeitsgruppe im Auftrag von Bundesrätin Simonetta Sommaruga die Möglichkeiten zur Anpassung des Urheberrechts an die technischen Entwicklungen geprüft. Deren Schlussbericht liegt seit Anfang Dezember 2013 vor.

Nach dem Urteil Logistep kam Unsicherheit darüber auf, ob Urheberrechtsverletzungen im Internet nach geltendem Recht noch verfolgt werden können. Während die Staatsanwaltschaften das Urteil so verstehen, dass die Beschaffung von IP-Adressen im Internet für die Verfolgung von Urheberrechtsverletzung generell widerrechtlich ist, stellen wir uns nach wie vor auf den Standpunkt, dass die Beschaffung und Bearbeitung solcher Daten unter Beachtung gewisser Grundsätze möglich ist (vgl. unseren 20. Tätigkeitsbericht 2012/2013, Ziff. 1.3.3). Eine höchstrichterliche Klärung der Frage ist noch ausstehend.

Unterdessen hat die von Bundesrätin Sommaruga eingesetzte Arbeitsgruppe AGUR12 ihre Vorschläge für mögliche Anpassungen des Urheberrechts an die technischen Entwicklungen in ihrem Schlussbericht veröffentlicht (abrufbar auf www.ige.ch unter Urheberrecht – AGUR12). Der Bericht verweist direkt auf die von uns entwickelte Best Practice zum Vorgehen für eine korrekte Beschaffung und Bearbeitung von Personendaten zur Verfolgung von Urheberrechtsdelikten im Internet (vgl. unseren 19. Tätigkeitsbericht 2011/2012, Ziff. 1.3.7) und fordert, falls nötig, die Schaffung entsprechender rechtlicher Grundlagen. Wir begrüssen diese Forderung und verfolgen die weiteren Entwicklungen in diesem Gebiet eingehend.

1.3.2 Erläuterungen zu Webtracking

Webseitenbetreiber oder Werbetreibende nutzen Webtracking-Dienste, um ihre Internetangebote effizienter und wettbewerbsfähiger zu platzieren. Die Seitenbesucher merken jedoch meistens nichts davon. Aus datenschutzrechtlicher Sicht werden die Persönlichkeitsrechte der Betroffenen durch das Tracking in der Regel widerrechtlich verletzt.

Webtracking-Dienste eröffnen vielfältige Möglichkeiten: Sie dienen beispielsweise zur Analyse einer Webseite oder zur gezielten Werbeansprache, oder werden im Zusammenhang mit «Social Plug-ins» eingesetzt. Die Hauptfunktion der

Nutzerverfolgung ist es, Besucherbewegungen auf einer Webseite oder das Surfverhalten von Internetnutzern zu erfassen. Die solcherart erhobenen Daten ermöglichen es, Rückschlüsse auf die Interessen, Vorlieben oder Gewohnheiten der Userinnen und User zu ziehen. Je nach Surfverhalten entstehen so schon in kurzer Zeit detaillierte Profile.

Aus datenschutzrechtlicher Sicht sind viele der bekannten Webtracking-Dienste problematisch. Obwohl die eigentliche Datenspeicherung und -analyse in den meisten Fällen durch den Anbieter im Hintergrund erfolgt, steht der Betreiber der Internetseite genauso in der Verantwortung. Er bindet den Trackingcode in die Seite ein und veranlasst hierdurch erst eine dem Seitenbesucher nicht bewusste Weiterleitung, das Setzen von Cookies und eine Datenerhebung.

Bei der Verwendung von Webtracking muss der Webseite-Betreiber den Seitenbesucher gemäss dem Grundsatz der Transparenz umfassend über den Einsatz von Tracking-Diensten informieren, beispielsweise in einer Datenschutzerklärung. Hier muss zudem erwähnt sein, wie sich der Internetnutzer gegen das Tracking wehren kann. Da beim Webtracking in der Regel Persönlichkeitsprofile beschafft werden, braucht es die ausdrückliche Zustimmung des Seitenbesuchers bevor die Daten gesammelt werden – beispielsweise indem er seine Einwilligung mit einem Mausklick kundtut. Beim Einsatz von Social Plugins bietet sich die sogenannte «Zwei-Klick-Lösung» an: Erst durch die Betätigung eines Schiebereglers aktiviert der Seitenbesucher die Plugins und kann die Seite anschliessend «sharen».

Auch der Internetnutzer kann einiges tun, um sich gegen Webtracking zu schützen. Zunächst ist es ratsam, die gespeicherten Cookies und den Browserverlauf nach jeder Onlinesitzung zu löschen. Zudem haben viele Browser eine sogenannte Do-not-track-Funktion, welche der Internetnutzer einstellen kann. Sie signalisiert der aufgerufenen Seite, dass er das Tracking zu unterlassen hat.

Weitere Informationen zum Thema Webtracking finden sich auf unserer Webseite www.derbeauftragte.ch, Datenschutz – Internet und Computer.

1.3.3 Verordnungen zum Fernmeldegesetz

Im Rahmen einer Ämterkonsultation haben wir zu den Verordnungsentwürfen zum Fernmeldegesetz Stellung genommen. Insbesondere haben wir die erhöhten Anforderungen an die Identifikation im Bereich der Domainnamen-Registrierung kritisiert, zumal die verlangten Daten auch im Ausland gespeichert werden.

Wir wurden eingeladen, zu den Verordnungen zum Fernmelderecht Stellung zu nehmen. Dabei haben wir kritisiert, dass neu sehr umfangreiche Angaben und

Dokumente für die Domainnamen-Registrierung erforderlich sind. Im entsprechenden Entwurf wird nicht ausgeführt, warum in diesem Bereich erhöhte Anforderungen an die Identifikation notwendig und somit verhältnismässig sein sollen. Aus unserer Sicht wird die Erhöhung der Datensicherheit eine Konsequenz dieser neuen Anforderungen sein (insb. bei Einreichung, Zugriff und Speicherung). Geht man jedoch davon aus, dass verschiedene weltweit tätige Registrare (Organisationen, die Domainnamen vergeben dürfen) für die «.ch»- und «.swiss»-Domains auftreten können, werden die verlangten Identifikationsdokumente zur Bearbeitung und insbesondere zur Speicherung auch ins Ausland transferiert werden müssen. Der Zugriff von Behörden auf diese Daten richtet sich nach dem jeweiligen Landesrecht am Sitz des Registrars und nicht nach den schweizerischen Gesetzen. Dasselbe gilt auch für die Aufsicht über die Datenbearbeitung der Registrare.

1.3.4 Ämterkonsultation zum Bericht des Bundesrates zu Open Government Data

Wir haben im Rahmen der Ämterkonsultation betreffend den Berichtsentwurf des Bundesrates in Erfüllung des Postulats Wasserfallen «Open Government Data als strategischer Schwerpunkt im E-Government» Stellung genommen und unter anderem auf die Risiken der Datenverknüpfung hingewiesen.

In unserer Stellungnahme weisen wir auf das Risiko hin, dass eine künftige Verknüpfung von heute an und für sich anonymen Daten mit weiteren Daten zu einer Deanonymisierung führen kann. Um diesem Problem zu begegnen, wird zurecht erwähnt, dass die Daten konsequent hinsichtlich der datenschutzrechtlichen Anforderungen überprüft werden müssen. Des weiteren soll die Veröffentlichung von Daten restriktiv gehandhabt werden; im Zweifelsfall ist auf die Publikation zu verzichten. In der Praxis sind Vorkehrungen gegen missbräuchliche Datenverknüpfungen mittels verwaltungsinterner Vorschriften und Verfahren zu treffen.

1.3.5 Recht auf Vergessen im Rahmen der digitalisierten Zeitungsarchive

Die digitalisierte Archivierung von Zeitungen wirft aus datenschutzrechtlicher Sicht zahlreiche Fragen auf. Das Recht auf Vergessen hat schon immer bestanden, erhält aber mit der Entwicklung der modernen Technologien eine neue Aktualität. Da bei uns regelmässig Fragen zu diesem Thema eingehen, haben wir auf unserer Website entsprechende Erläuterungen aufgeschaltet.

Wir wurden namentlich von einem Journalistenverband zum Recht auf Vergessen im Rahmen der digitalisierten Zeitungsarchive angesprochen. Zahlreiche Zeitungen

haben nämlich damit begonnen, ihre Archive zu digitalisieren, was aus datenschutzrechtlicher Sicht viele Fragen aufwirft.

Die digitalisierte Archivierung von Zeitungsartikeln stellt eine Bearbeitung von Personendaten im Sinne des Datenschutzgesetzes (DSG) dar. Im Falle einer Persönlichkeitsverletzung muss die Datenbearbeitung durch einen Rechtfertigungsgrund, im Prinzip durch ein überwiegendes öffentliches Interesse, legitimiert werden. Es geht also im Wesentlichen um eine Frage der Verhältnismässigkeit. Der Verhältnismässigkeitsgrundsatz verlangt, dass Personendaten nach einer gewissen Zeit, soweit ihre Aufbewahrung nicht mehr gerechtfertigt ist, gelöscht oder anonymisiert werden.Es ist demnach angebracht, eine Interessenabwägung vorzunehmen und zu prüfen, ob das Interesse des Einzelnen an der Löschung seiner Personendaten aus den elektronischen Archiven einer Zeitung oder aus dem Index einer Suchmaschine stärker zu gewichten ist als das öffentliche Interesse an der Aufbewahrung der Daten in den elektronischen Archiven oder in den Suchmaschinen. In einem Rechtsstreit hat der Richter im Rahmen einer auf Artikel 15 DSG oder auf Artikel 28 des Zivilgesetzbuchs gestützten Zivilklage diese Interessenabwägung vorzunehmen.

Wir behalten die Entwicklung bei der Umsetzung des Rechts auf Vergessen, namentlich auf europäischer Ebene, weiterhin im Auge und haben auf unserer Website Erläuterungen zu diesem Thema publiziert (www.derbeauftragte.ch, Datenschutz – Internet).

1.3.6 Ämterkonsultation zur Revision des Publikationsgesetzes

Im Rahmen einer Ämterkonsultation haben wir uns zur Revision des Publikationsgesetzes geäussert und auf die Risiken elektronischer Publikationen aufmerksam gemacht. Das Publikationsgesetz (PublG) regelt die Veröffentlichung der Sammlungen des Bundesrechts (amtliche und systematische Sammlung) und des Bundesblatts.

Bei der Ämterkonsultation haben wir zur Revision des Gesetzes Stellung genommen. Sie sieht den Primatwechsel, d.h. den Übergang der Massgeblichkeit von der gedruckten auf die elektronische amtliche Veröffentlichung, vor. Wir haben insbesondere darauf hingewirkt, dass in den Ausführungen zum PublG Massnahmen vorgesehen werden, um Missbräuche im Zusammenhang mit den elektronischen Publikationen im Internet (z.B. das Erstellen von Persönlichkeitsprofilen) zu vermeiden. Diese Massnahmen sollen laufend den technischen Möglichkeiten und Entwicklungen angepasst werden können.

1.4 Justiz/Polizei/Sicherheit

1.4.1 Schengen-Umsetzung: Datenschutzevaluation im Vereinigten Königreich

Im Oktober 2013 haben wir zum zweiten Mal an einer Schengen-Evaluation auf dem Gebiet des Datenschutzes teilgenommen. Ein Expertenteam beurteilte den Datenschutz im Vereinigten Königreich. Die dort gemachten Erfahrungen sind bei der Evaluation der Schweiz im Mai 2014 berücksichtigt worden.

Zum zweiten Mal haben wir an einer Schengen-Evaluation auf dem Gebiet des Datenschutzes teilgenommen. Der Besuch im Vereinigten Königreich war für die Zeit vom 21. bis 24. Oktober 2013 anberaumt. Dort fand ein erstes Mal im Jahr 2004 eine Evaluation statt, die damals Anlass zu verschiedenen Empfehlungen gegeben hatte.

Bei dieser Evaluation bestand der Evaluationsausschuss aus sechs Personen, darunter eine Mitarbeiterin des EDÖB als Vertreterin der Schweiz. Im Vorfeld der Evaluation hatte das Vereinigte Königreich einen Fragebogen zu beantworten und verschiedene Dokumente vorzulegen. Die Kontrolle vor Ort wurde bei den Datenschutzbehörden und bei den Polizeibehörden durchgeführt. Der daraus entstandene Evaluationsbericht zieht Bilanz über die Umsetzung der früheren Empfehlungen, über die Unabhängigkeit und die Aktivitäten der Datenschutzbehörde, über die Umsetzung der Datenschutzrechte der betroffenen Personen und der Datensicherheit im Rahmen von Schengen und gibt Empfehlungen an das Vereinigte Königreich ab.

Nachdem der Bericht einer Konsolidierung zwischen den verschiedenen Experten unterzogen worden war, wurde er dem Vereinigten Königreich zur Konsultation unterbreitet, bevor er schliesslich im Dezember 2013 der für die Schengen-Evaluationen (SCHEVAL) verantwortlichen Ratsarbeitsgruppe vorgelegt wurde, wo er erörtert und verabschiedet worden ist. Die Evaluation ist jeweils Gegenstand einer Nachbearbeitung, in deren Verlauf der betroffene Staat aufzeigen kann, in welchem Ausmass er die Empfehlungen umsetzen konnte.

Die Schweiz ist im Jahr 2008 ein erstes Mal evaluiert worden. Die im vorliegenden Fall erworbenen Erfahrungen sind bei der Evaluation der Schweiz im Mai 2014 berücksichtigt worden.

1.4.2 Kontrolle beim Generalkonsulat der Schweiz in Dubai

Im Rahmen der Umsetzung der Schengen-Assoziierungsabkommen haben wir die fünfte Kontrolle bei einer schweizerischen Vertretung im Ausland bezüglich der Datenbearbeitung im Vergabeverfahren für Schengen-Visa durchgeführt. Wegen der erheblichen Anzahl ausgestellter Visa und der Einführung von biometrischen Visa seit Oktober 2012 haben wir das Generalkonsulat der Schweiz in Dubai für diese Kontrolle ausgewählt. Wir besuchten auch die Räumlichkeiten des externen Unternehmens, dem das Konsulat einen Teil des Verfahrens übertragen hat.

Nach den Kontrollen bei den schweizerischen Vertretungen in Kairo, Kiew, Istanbul und Moskau haben wir auch beim Generalkonsulat der Schweiz in Dubai die Bearbeitung der Visumsanträge kontrolliert. Die Kontrolle wurde dem Konsulat im August 2013 angekündigt und fand, nach Eingang und Prüfung der verlangten Dokumentation, im November 2013 vor Ort statt. Der gesamte Kontrollprozess erfolgte in enger Zusammenarbeit mit dem Datenschutzberater des EDA. Das Konsulat von Dubai stellte 2013 rund 19 000 Visa für in Dubai, Oman und Bahrain wohnhafte Personen aus. Aufgrund der hohen Zuwanderungsrate des Emirats besitzen die Antragsteller, die beim Konsulat vorsprechen, sehr unterschiedliche Staatsangehörigkeiten.

Anlässlich der Kontrolle besuchten wir neben den Räumlichkeiten des Konsulats auch das externe Unternehmen, das mit einem Teil des Bearbeitungsverfahrens beauftragt wird und dessen Räumlichkeiten sich auf derselben Etage wie das Konsulat befinden. Das Konsulat lässt nämlich den ersten Teil des Prozesses, das heisst die Terminvereinbarung für die Einreichung der Anträge sowie die Überprüfung der Antragsdossiers, extern abwickeln. Die Mitarbeiter des externen Unternehmens prüfen somit den Inhalt der Antragsdossiers und vergewissern sich, dass sämtliche erforderlichen Informationen und Dokumente im Dossier enthalten sind. Dank dieser ersten Sichtung braucht das Konsulat die Antragsteller erst zu empfangen, wenn ihr Gesuch vollständig ist. Das Vergabeverfahren kann auf diese Weise optimiert werden.

Aufgaben, die zum Zeitpunkt unserer Kontrolle ausschliesslich vom Konsulat wahrgenommen wurden, sind die Entgegennahme der Dossiers, die Erfassung der biometrischen Daten (Gesicht und Fingerabdrücke), das Inkasso der Gebühr, die Analyse des Antragsdossiers, die zur Erteilung oder Verweigerung eines Visums führt, und schliesslich die Rückgabe der Pässe. Seit März 2014 wird ein grosser Teil des Verfahrens ausgelagert: das Konsulat hat nicht mehr direkt mit den Antragstellern zu tun, sondern übernimmt nur noch die Analyse der Dossiers sowie die Vergabe und Ausstellung der Visa.

Parallel zum Kontrollbesuch hatten wir die Möglichkeit, die Räumlichkeiten des externen Unternehmens aufzusuchen, wo seit März die Antragsteller empfangen werden. Diese Räume befinden sich ebenfalls in Dubai, aber nicht im selben Gebäude wie das Konsulat. Auch wenn dieser Besuch nicht in den Rahmen der Kontrolle fiel, gab er uns doch die Gelegenheit, uns ein Bild von den Bedingungen für die Bearbeitung der Anträge und von den getroffenen Massnahmen zur Gewährleistung der Sicherheit der Personendaten zu verschaffen.

Aufgrund der vom Konsulat vorgelegten Dokumentation (insbesondere der internen Weisungen für die Bearbeitung der Visumsanträge) sowie des Besuchs vor Ort war es uns möglich, die vom Konsulat durchgeführte Datenbearbeitung zu verstehen und zu analysieren. Wir konnten feststellen, dass die zur Gewährleistung der Datensicherheit getroffenen Massnahmen in Anbetracht der Schutzwürdigkeit der bearbeiteten Daten, insbesondere der biometrischen Daten, verhältnismässig und angemessen sind.

1.4.3 Auslagerungsprojekt in Zusammenhang mit der Erteilung von Schengenvisa

Für die Erteilung von Schengenvisa arbeiten verschiedene Schweizer Auslandsvertretungen mit externen Dienstleistungsanbietern zusammen. Das eidgenössische Departement für auswärtige Angelegenheiten (EDA) will diese Zusammenarbeit ausdehnen. Wir haben die Vertragsentwürfe geprüft und Änderungsvorschläge gemacht. Das EDA hat diese übernommen.

Verschiedene schweizerische Auslandsvertretungen arbeiten für die Erteilung von Schengenvisa mit externen Dienstleistungsanbietern zusammen (vgl. unseren 19. Tätigkeitsbericht 2011/2012, Ziff. 1.4.1). Das EDA will diese Zusammenarbeit nun ausdehnen. Neu sollen nicht nur die Terminvergabe, sondern auch weitere Aufgaben, wie die Zusammenstellung der Dossiers und die Erhebung von biometrischen Daten, ausgelagert werden. In diesem Zusammenhang verlangten wir vom EDA, uns die entsprechenden Vertragsentwürfe zur Prüfung zu unterbreiten. Wir prüften diese auf ihre Datenschutzkonformität hin und stellten insbesondere sicher, dass diese die Bestimmungen des europäischen Visakodex, der die Zusammenarbeit mit externen Dienstleistungserbringern ausführlich regelt, enthielten. Die Vertragsentwürfe enthielten den grössten Teil der datenschutzrechtlich relevanten Punkte. Wir baten das EDA allerdings, verschiedene Punkte in den Verträgen zu ergänzen. Es hat uns mitgeteilt, dass es unsere Bemerkungen in die definitiven Verträge übernehmen werde.

1.4.4 Entwurf des Nachrichtendienstgesetzes

Der an das Parlament überwiesene Entwurf des Nachrichtendienstgesetzes (NDG) enthält aus datenschutzrechtlicher Sicht einige problematische Elemente: die Verwendung von Luftfahrzeugen oder Satelliten ohne spezifische Bewilligung, die Möglichkeit, sich in Informatiksysteme oder -netze einzuschalten und die Nichtanwendung des Öffentlichkeitsgesetzes auf Dokumente betreffend die Nachrichtenbeschaffung im Sinne des NDG.

Wir haben mehrmals darauf hingewiesen, dass der Entwurf des NDG aus datenschutzrechtlicher Sicht in einigen Punkten Schwierigkeiten bereitet (vgl. unseren Tätigkeitsbericht 2012/2013, Ziff. 1.4.6). Wir erwähnen nachstehend die drei problematischsten Elemente:

- Nach dem Entwurf soll es möglich sein, Luftfahrzeuge oder Satelliten zu Beobachtungszwecken an öffentlichen oder frei zugänglichen Orten einzusetzen. Es kommt bei einem solchen Einsatz automatisch zur Beobachtung und zu Bild- und Tonaufzeichnungen von Sachverhalten, die zur Privatsphäre gehören. Aus diesem Grunde und unter Berücksichtigung der jüngsten Ereignisse im Bereich der Überwachung auf internationaler Ebene muss man sich fragen, ob ein solcher Mitteleinsatz nicht in die Liste der bewilligungspflichtigen Beschaffungsmittel aufgenommen werden sollte. Nicht zuletzt auch, weil es schwierig ist, den Einsatz solcher Mittel klar abzugrenzen.
- Der Entwurf sieht über die Massnahmen zur Informationsbeschaffung hinaus auch die Möglichkeit vor, sich in Informatiksysteme und -netze einzuschalten, um den Zugang zu Informationen zu stören, zu verhindern oder zu verlangsamen. Wir sind der Ansicht, dass diese Mittel nicht verhältnismässig sind. Solche Massnahmen verletzen die Grundrechte in schwerwiegender Weise und gehen weit über die Möglichkeiten hinaus, die den Strafverfolgungsbehörden zur Verfügung stehen.
- Gemäss Entwurf sollen Dokumente betreffend die Informationsbeschaffung im Sinne des NDG aus dem Geltungsbereich des Öffentlichkeitsgesetzes ausgenommen werden. Mit dieser Forderung sind wir nicht einverstanden (vgl. Ziffer 2.5.1 des vorliegenden Tätigkeitsberichts).

Wir werden unseren Standpunkt im Rahmen der Arbeiten in den parlamentarischen Kommissionen verteidigen.

1.4.5 Totalrevision des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs

Im Berichtsjahr konnten wir vor der Kommission für Rechtsfragen des Ständerats Stellung nehmen zur Totalrevision des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs. Thema war dabei auch die Herausgabe von Randdaten bei rückwirkender Überwachung.

Im zweiten Semester des vergangenen Jahres lud uns die Kommission für Rechtsfragen des Ständerats zu den Sitzungen zum Entwurf des totalrevidierten Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) ein. Dabei riefen wir unsere bereits bei der Ämterkonsultation geäusserte Haltung in Erinnerung, dass es für den Eingriff in ein verfassungsmässig geschütztes Grundrecht formelle und materielle gesetzliche Grundlagen braucht, die zudem genügend bestimmt sind. Auch betonten wir, dass die geplante Vorratsdatenspeicherung in zeitlicher Hinsicht zum verfolgten Zweck verhältnismässig sein muss (vgl. 20. Tätigkeitsbericht 2012/2013, Ziff. 1.4.5 und 19. Tätigkeitsbericht 2011/12, Ziff. 1.4.8).

In diesem Zusammenhang bat uns die Kommission um unsere Einschätzung zum Bundesgerichtsurteil vom 22. Januar 2013 betreffend die Herausgabe von Randdaten bei rückwirkender Überwachung. Unserer Auffassung nach haben die Fernmeldedienstanbieter die Randdaten grundsätzlich nicht über die im BÜPF verlangten sechs Monate hinaus aufzubewahren, wenn kein weiterer Rechtfertigungsgrund (z.B. geschuldetes Entgelt) existiert. Daher müssen sie ihre Verwaltungssysteme so konfigurieren, dass nicht mehr benötigte Rand- und Verkehrsdaten automatisch gelöscht werden. Andernfalls haben die Strafverfolgungsbehörden gemäss Bundesgericht die Möglichkeit, die nicht gelöschten Daten heraus zu verlangen.

1.4.6 Bekanntgabe von Personendaten an die Polizeibehörden

Ein Quartierverein kann den Polizeibehörden Personendaten im Zusammenhang mit Zwischenfällen in seinem Quartier bekannt geben, sofern er die allgemeinen Datenschutzprinzipien einhält.

Wir haben eine Sachverhaltsabklärung bei einem Quartierverein durchgeführt, der von seinen Mitgliedern oder von anderen Personen Informationen über quartierbezogene Vorfälle erhält (etwa Drogenhandel, Vandalismus, wildes Parkieren, Nachbarschaftsstreitigkeiten usw.). Der Verein sichtet die Informationen und gibt sie, soweit sie relevant erscheinen, an die kantonalen und kommunalen Polizeibehörden weiter. Er bewahrt keinerlei Personendaten zu diesen Vorfällen auf: sämtliche E-Mails, ob sie nun an die Polizei weitergeleitet wurden oder nicht, werden

gelöscht, und der Verein erstellt auch keine Vermerke zu den Telefonanrufen oder mündlich mitgeteilten Informationen. Die vom Verein gemeldeten Vorfälle werden von den Polizeibehörden wie jede andere in ihrer Zentrale eingegangene Meldung behandelt.

Der Verein wollte von uns wissen, ob seine Bearbeitungen mit der Datenschutzgesetzgebung konform seien. Da ein Teil davon kantonale und kommunale Organe betrifft, nahm auch der zuständige kantonale Datenschutzbeauftragte an einer Besprechung mit dem Verein und der Gemeindepolizei teil.

Gestützt auf die oben erwähnten Elemente stellten wir fest, dass der Verein Personendaten bearbeitet; in allen Fällen sind dies die Namen der Personen, die die Sachverhalte melden, und in manchen Situationen auch Daten betreffend die «verdächtigen» Personen: Namen, Autonummern, Beschreibung usw. Die als relevant erachteten Anzeigen werden an die Polizeibehörden weiter geleitet und danach vernichtet, während die übrigen Meldungen direkt gelöscht werden, sodass keine Datensammlung erstellt wird. Der Verein informiert die Personen, die Meldung erstatten, dass im Falle der Bekanntgabe an die Polizeibehörden auch ihre Namen weitergegeben werden.

Aufgrund der erteilten Auskünfte sind wir zum Schluss gelangt, dass die Beschaffung von Informationen durch den Quartiersverein über mögliche Gesetzesverstösse und deren Übermittlung an die Polizei im vorliegenden Fall mit dem Datenschutzgesetz im Einklang stehen.

1.4.7 Informationssysteme der eidgenössischen Zollverwaltung

Im Rahmen der Revision des Zollgesetzes (ZG) und zweier Verordnungen über die Informationssysteme der eidgenössischen Zollverwaltung (EZV) haben wir erneut darauf hingewiesen, dass nach dem Datenschutzgesetz die Bundesorgane nur zur Bearbeitung und Bekanntgabe von Personendaten berechtigt sind, wenn es dafür eine gesetzliche Grundlage gibt. Bei besonders schützenswerten Daten oder Persönlichkeitsprofilen ist sogar eine Gesetzesgrundlage im formellen Sinn erforderlich.

Das Gesetz im formellen Sinn hat insbesondere folgende Punkte zu regeln: Der Zweck jedes Informationssystems muss in präziser und für die betroffenen Personen erkennbarer Form umschrieben sein; das für die Bearbeitung verantwortliche Bundesorgan (Inhaber der Datensammlung) ist zu nennen; die an jedem Informationssystem Beteiligten müssen erkennbar sein; die Kategorien der bearbeiteten Daten sind zu definieren, insbesondere die Kategorien der besonders schützenswerten

Daten und die Persönlichkeitsprofile; die gegebenenfalls geltenden Einschränkungen des Zugriffsrechts der betroffenen Personen müssen erwähnt werden; die Architektur der Informatiksysteme sind in groben Zügen zu beschreiben; die Gesetzesgrundlage muss festlegen, welches Bundesorgan für die Bewilligung des Online-Zugriffs zuständig ist und welchen Behörden, ein Zugriffsrecht erteilt werden kann. Zu bestimmen sind auch die Kategorien der im Netz abrufbaren Daten und der Zweck des Zugriffs.

Unseres Erachtens entsprechen die Bestimmungen des Zollgesetzes über die Informationssysteme nicht allen oben erwähnten Anforderungen. Aus diesem Grunde haben wir die Ausarbeitung eines Gesetzes über die Zollinformationssysteme vorgeschlagen, wie es im Bereich der Armee (Gesetz über die militärischen Informationssysteme) und der Polizei (Gesetz über die polizeilichen Informationssysteme des Bundes) besteht.

Im Rahmen der Vorbereitung der Botschaft zur Teilrevision des ZG, die dem Bundesrat bis Ende 2014 vorliegen muss, hat das eidgenössische Finanzdepartement zu prüfen, ob die Bestimmungen über die Informationssysteme den datenschutzrechtlichen Anforderungen gerecht werden. Anlässlich der Ämterkonsultation werden wir unseren Standpunkt in Erinnerung rufen.

1.4.8 Totalrevision der Interpol-Verordnung

Um den an zwei Interpol-Reglementen erfolgten Änderungen Rechnung zu tragen, wurde die schweizerische Interpol-Verordnung angepasst.

Im Anschluss an technische und organisatorische Entwicklungen wurden die Bestimmungen über die Datenbearbeitungen in zwei Interpol-Reglementen angepasst. Sie sind nun in einem einzigen Reglement enthalten. Diese Anpassungen haben eine Abänderung der meisten Bestimmungen der schweizerischen Interpol-Verordnung erforderlich gemacht. Aus diesem Grund wird die Überarbeitung als Totalrevision bezeichnet; inhaltlich sind die Änderungen jedoch minimal. Im Rahmen der Ämterkonsultation haben wir einige Verbesserungen vorgeschlagen. Das Bundesamt für Polizei hat unseren Bemerkungen vollumfänglich Rechnung getragen und uns in einer Sitzung auch die im Bereich des Informationsaustauschs im Rahmen von Interpol eingetretenen Änderungen vorgestellt.

1.4.9 Expertengruppe FOGIS – Gesetzesentwurf zur Informationssicherheit

Im Rahmen der Expertengruppe FOGIS begleiten wir den Entwurf für ein Gesetz über Informationssicherheit und achten auf die Berücksichtigung der Datenschutz- und Öffentlichkeitsaspekte.

Der Bundesrat (BR) beschloss im Mai 2010, die Informationsschutzverordnung (ISchV) abzuändern und das VBS mit der Bildung einer interdepartementalen Arbeitsgruppe zu beauftragen, um einen Gesetzesentwurf zur Informationssicherheit auszuarbeiten. Dieser soll die bisher geltenden Anforderungen betreffend den Informationsschutz auf die Massnahmen zur Verbesserung der Informationssicherheit ausdehnen, die der BR am 16. Dezember 2009 beschlossen hat. Diese Massnahmen umfassen naturgemäss auch Aspekte des Datenschutzes, der wiederum von Erfordernissen des Öffentlichkeitsprinzips der Verwaltung abhängt.

In diesem pluri- und interdisziplinären Kontext sind rund zwanzig Rechts- und Fachexperten aus mehreren eidgenössischen Departementen unter der Leitung von Professor Markus Müller der Universität Bern (Expertengruppe FOGIS) zu zahlreichen Beratungen zusammengekommen.

Formal betrachtet muss dieser inzwischen schon weit fortgeschrittene Gesetzesentwurf nun noch verschiedene Vernehmlassungsverfahren durchlaufen.

Inhaltlich umfasst der Gesetzesentwurf sechs Kapitel: allgemeine Bestimmungen, allgemeine Massnahmen zur Informationssicherheit, Personensicherheitsüberprüfung, Betriebssicherheitsverfahren, Informationssicherheit kritischer Infrastrukturen sowie bei Organisation und Vollzug. Im Kapitel über die allgemeinen Massnahmen findet man einen Abschnitt betreffend die Klassifizierung der Informationen in zwei oder drei Schutzwürdigkeitsstufen: geheim, vertraulich oder intern. Aus Gründen der Einfachheit und Klarheit der Umsetzung befürworten wir das Zwei-Stufen-Modell, wobei wir durchaus Verständnis haben für das Argument der internationalen Kompatibilität, das für ein Drei-Stufen-Modell spricht. Bezüglich der geeigneten Sicherheitsmassnahmen liesse sich überdies eine Analogie zu den Kategorien von Personendaten herstellen, also zu den «hochsensiblen» Daten (deren Bekanntgabe Leib und Leben gefährden können), den besonders schützenswerten Daten und den nicht besonders schützenswerten Daten (gemäss der Definition des DSG).

Im Kapitel über die Organisation und den Vollzug ist insbesondere vorgesehen, dass die betroffenen Behörden und Organisationen Informationssicherheitsbeauftragte ernennen; diesen obliegen Aufgaben der Beratung und Unterstützung, des Sicherheits- und Risikomanagements entsprechend der technischen Entwicklung sowie der Kontrolle über die Einhaltung der Vorschriften. Eine Konferenz dieser Beauftragten würde eine gewisse Einheitlichkeit in der Durchführung gewährleisten, dem

Informations- und Erfahrungsaustausch dienen sowie die notwendige Koordination mit anderen von der Informationssicherheit betroffenen Stellen, insbesondere dem EDÖB, ermöglichen. Schliesslich sollte eine Fachstelle für Informationssicherheit auf Bundesebene unter der Leitung eines eidgenössischen Informationssicherheitsbeauftragten eingerichtet werden, um so für die korrekte Ausführung dieses Gesetzes und für die nationale und internationale Zusammenarbeit zu sorgen sowie einen regelmässigen Lagebericht an den Bundesrat zu erstellen.

Wir setzen unsere Arbeiten bei der Begleitung dieses Gesetzesentwurfs fort und achten darauf, dass die Datenschutz- und Öffentlichkeitsaspekte berücksichtigt werden.

1.5 Gesundheit und Forschung

1.5.1 Entwurf des Bundesgesetzes über das elektronische Patientendossier

Für die Umsetzung von eHealth werden die notwendigen gesetzlichen Grundlagen im Bundesgesetz über das elektronische Patientendossier geschaffen. Der nun vorliegende Entwurf nimmt wichtige Datenschutzanliegen auf. Für die Patientenidentifikation ist ein sektorielles Identifikationsmerkmal anstelle der Sozialversicherungsnummer vorgesehen. Zudem soll der Patient über den Inhalt des ePatientendossiers, die Zugriffsberechtigungen und die Vertraulichkeit der medizinischen Informationen bestimmen können.

Beim nun vorliegenden Entwurf des Bundesgesetzes über das elektronische Patientendossier (EPDG) wurden mehrere wichtige Datenschutzanliegen aufgenommen. So haben unsere Interventionen und die geleistete Überzeugungsarbeit dazu geführt, dass die Sozialversicherungsnummer als Patientenidentifikator für den eHealth-Bereich nicht mehr vorgesehen ist. Hingegen soll eine durch die Zentrale Ausgleichsstelle (ZAS) generierte und verwaltete Zufallsnummer als Patientenidentifikationsmerkmal dienen und damit die eindeutige Identifikation der Patientin oder des Patienten und die eindeutige Zuordnung der Patientendaten ermöglichen. Damit haben wir ein wichtiges datenschutzrechtliches Ziel erreicht. Auch haben wir aufzeigen können, dass sektorielle Identifikatoren oder Identifikationsmerkmale umsetzbar sind und nicht zwingend einen übermässigen zusätzlichen finanziellen Aufwand bedeuten müssen.

Weiter ist auch klar, dass das elektronische Patientendossier für die Patientin oder den Patienten freiwillig sein soll. Zudem darf es nur eröffnet werden, wenn die Person nach angemessener Information ausdrücklich eingewilligt hat. Nach der Eröffnung eines ePatientendossiers wird dann aber im Behandlungsfall vermutet, dass die Patientin oder der Patient damit einverstanden ist, dass Gesundheitsfachpersonen Daten darin erfassen. Wichtig ist, dass die Patienten dann mittels Zuteilung der Zugriffsberechtigung und Verwaltung der für die Informationen vorgesehenen Vertraulichkeitsstufen konkret darüber entscheiden können, wer insbesondere Zugang zu heiklen Gesundheitsinformationen erhält. So ist denn auch vorgesehen, dass einzelne Gesundheitsfachpersonen generell vom Zugriffsrecht ausgeschlossen werden können. Damit können wir sagen, dass der jetzt vorliegende Entwurf in seiner grundsätzlichen Ausrichtung unseren Anliegen Rechnung trägt.

Wichtige Fragen, wie das Zertifizierungsverfahren für eHealth-Gemeinschaften, die Anforderungen an die elektronische Identität der Patientinnen und Patienten sowie der Gesundheitsfachpersonen und auch die vom Bundesamt für Gesundheit betriebenen Abfragedienste werden allerdings erst im Rahmen von Ausführungsbestimmungen konkretisiert werden.

1.5.2 Zuständigkeit des EDÖB betreffend Datenschutz bei Spitälern

Die Kompetenzaufteilung zwischen kantonalen Datenschutzbehörden und dem EDÖB ist für die betroffenen Personen schon jetzt nicht immer klar. Bisher hatten wir uns für die privaten Spitäler als zuständig erachtet. Durch ein von der Vereinigung der Schweizerischen Datenschutzbeauftragten (privatim) in Auftrag gegebenes Gutachten wird diese Zuständigkeit jetzt in Frage gestellt.

Ein von privatim in Auftrag gegebenes Gutachten kommt zum Schluss, dass ein Spital unabhängig von der Rechtsform der kantonalen Datenschutzaufsichtsbehörde untersteht, wenn es im Auftrag des Kantons Leistungen erbringt. Dies ist gemäss Gutachten dann der Fall, wenn das Spital als sogenanntes Listenspital auf einer kantonalen Spitalliste geführt ist, und folgende Leistungen und Dienste erbringt:

- stationäre Leistungen aus der obligatorischen Krankenpflegeversicherung (OKP) im Rahmen eines krankenversicherungsrechtlichen Leistungsauftrages;
- stationäre Leistungen aus anderen Sozialversicherungen (Invaliden-, Unfall- und Militärversicherung, soweit diesbezüglich kantonalrechtliche Leistungsaufträge bestehen);
- ambulante Leistungen, sofern diesbezüglich kantonalrechtliche Leistungsaufträge bestehen;
- zusatzversicherte Leistungen, wenn dafür ein Sockelbeitrag aus der Grundversicherung geschuldet ist;
- Leistungen der Lehre und Forschung, soweit kantonalrechtliche Leistungsaufträge bestehen (wie vor allem im Bereich der universitären Lehre und Forschung);
- Notfalldienste im Rahmen von Leistungsaufträgen.

Zudem soll sich im Bereich der stationären OKP-Leistungen die Zuständigkeit einer kantonalen Datenschutzaufsichtsbehörde auch auf ausserkantonale Spitäler erstrecken, wenn diese Leistungsaufträge des betreffenden Kantons erfüllen. Weiter hält das Gutachten fest, dass die Spitäler ausserhalb von kantonalen Leistungsaufträgen privatwirtschaftlich tätig sind und damit grundsätzlich der Aufsicht des EDÖB unterstellt sind, sofern keine anderslautende kantonalrechtliche Bestimmung existiert.

Würde man diesem Gutachten folgen, dann hätten wir bei Spitälern, die sowohl öffentliche Aufgaben erfüllen als auch privatwirtschaftlich (also ausserhalb von Leistungsaufträgen) tätig sind, geteilte Zuständigkeiten und verschiedene Datenschutzgesetze anzuwenden. Der Verfasser des Gutachtens hält denn auch fest, dass die Situation kompliziert und unübersichtlich ist und als unbefriedigend

erachtet werden kann. Wir sind der Ansicht, dass diese Position aus juristischer Sicht zwar durchaus interessant sein mag, aber weder den Spitälern noch den Patientinnen und Patienten zugemutet werden kann. Es kann nicht sein, dass sie eine umfangreiche juristische Abklärungen durchführen müssen, um festzustellen, welches Datenschutzrecht je nach Behandlung zur Anwendung gelangt und an welche Datenschutzbehörde sie sich wenden können. Es kann auch nicht sein, dass eine private Spitalgruppe mit Standorten und Patienten in mehreren Kantonen sich damit befassen muss, welche Datenschutzbehörde für einen bestimmten Patienten oder für ein zentralisiertes Klinikinformationssystem zuständig sein könnte, wenn dieses zum Beispiel im Kanton Zürich betrieben, aber an allen Standorten eingesetzt wird.

In diesem Sinne werden wir weiterhin private Spitäler und auch Patienten beraten, welche sich in einem privaten Spital haben behandeln lassen. Weiterhin werden wir auch unsere Kontrollaufgaben gegenüber den privaten Spitälern wahrnehmen. Sollte ein privates Spital unsere Zuständigkeit anzweifeln, könnte es zu einem Gerichtsverfahren kommen. Hier müsste dann das angerufene Gericht die Frage der Zuständigkeit und des anwendbaren Rechts klären.

1.5.3 Entwurf für ein Bundesgesetz über die Registrierung von Krebserkrankungen

Der Bundesrat hat das Eidgenössische Departement des Innern beauftragt, bis zum Ende des Jahres einen Gesetzesentwurf über die Registrierung von Krebserkrankungen und die diesbezügliche Botschaft auszuarbeiten. In der Vernehmlassung erinnerten wir an die Risiken für die Privatsphäre, die mit der Verwendung der AHV-Nummer als einzigem Identifikationsmerkmal verbunden sind.

Um die Daten betreffend Krebserkrankungen vollständig und einheitlich zu erfassen, möchte der Bundesrat eine Rechtsgrundlage auf Bundesebene schaffen. Das Gesetz über die Registrierung von Krebserkrankungen (KRG) stützt sich auf das bestehende dezentralisierte System und ergänzt dieses gleichzeitig. Die in den kantonalen Registern enthaltenen Daten sollen an ein vom Bund finanziertes nationales Krebsregister weitergeleitet werden, das die Aufgabe hat, diese Informationen zusammenzuführen, zu evaluieren und zu veröffentlichen. Die Finanzierung der kantonalen und regionalen Register wird weiterhin den Kantonen obliegen. In Zukunft wird für jeden Fall eine Mindestdatenmenge erhoben, namentlich die genaue Diagnose, das Datum, an dem sie gestellt wurde und der Zeitpunkt des Behandlungsbeginns. Für manche Krebsarten sollen zusätzliche Daten erfasst werden (beispielsweise Informationen zur Entwicklung der Krankheit oder der Behandlung).

In der Vernehmlassung haben wir daran erinnert, dass die systematische Verwendung der AHV-Nummer als Identifikationsmerkmal grosse Risiken für die Privatsphäre der betroffenen Personen birgt, da sich durch diese Erweiterung unerwünschte Verbindungen zwischen einzelnen Datenbanken herstellen lassen (vgl. unseren 20. Tätigkeitsbericht 2012/2013, Ziff. 1.5.5). Eine Vermischung der Statistikbereiche, der Verwaltung und des Gesundheitswesens, ist unbedingt zu vermeiden, da die in diesen Bereichen bestehenden Erfordernisse sowohl bezüglich der Menge als auch der Qualität der Daten unterschiedlich sind. Die Verwendung einer bereichsspezifischen Nummer verringert das Risiko, dass Informationen miteinander in Verbindung gebracht werden. Dies ist umso wichtiger, als die Daten des Tumorregisters besonders schützenswert sind und die Erstellung von Persönlichkeitsprofilen ermöglichen.

Nachdem wir feststellen mussten, dass im Entwurf die AHV-Nummer als Kennung beibehalten wird, erinnerten wir erneut an die Notwendigkeit von Alternativlösungen für die Verwendung der AHV-Nummer, die sich nach den Entwicklungen bei der sektorspezifischen Patientenidentifikationsnummer im Rahmen des Entwurfs zum EPDG richten könnten. Hier sollte nicht die gleiche sektorbezogene Nummer wie für das Patientendossier, sondern eine andere spezifisch für die Krebsregister geltende Nummer verwendet werden.

Am 30. Oktober 2013 hat der Bundesrat den Bericht über das Vernehmlassungsverfahren zur Kenntnis genommen. Obwohl sich die angehörten Parteien mit deutlicher Mehrheit für eine Regelung auf Bundesebene ausgesprochen haben, sind einige Punkte weiterhin umstritten. Differenzen gibt es beispielsweise betreffend den Umfang der für die Evaluation der Behandlungs- und der Versorgungsqualität notwendigen Daten. Diese Fragen werden noch mit den betroffenen Akteuren im Hinblick auf die Ausarbeitung der Botschaft zu behandeln sein.

Davon abgesehen müssen gewisse Punkte im Zusammenhang mit den Patientenrechten und dem Datenschutz überarbeitet werden. Dies betrifft namentlich die Information der Patienten und die Verwendung der erhobenen Daten durch Drittpersonen. Der Bundesrat hat daher das Eidgenössische Departement des Inneren mit der Ausarbeitung des Gesetzesentwurfs und der diesbezüglichen Botschaft bis Ende des Jahres beauftragt. Wir werden unsererseits darauf achten, dass unsere Vorbehalte zur Verwendung der AHV-Nummer berücksichtigt werden.

1.5.4 Änderung der Zuständigkeit bei der Bewilligungserteilung in der medizinischen Forschung

Im Bereich der medizinischen Forschung haben wir mehrere Kontrollen durchgeführt. Dabei sind uns verschiedene Punkte aufgefallen, die noch nicht optimal umgesetzt wurden. Insbesondere bei der Dokumentation der Projekte bestand Verbesserungsbedarf. Ziel der Kontrollen war es auch, den zuständigen Ethikkommissionen wichtige Hinweise für ihre künftigen Aufgaben mitzugeben.

Aufgrund unserer Kontrollen im Bereich der medizinischen Forschung konnten wir feststellen, dass die Prozesse bzw. Abläufe bei zahlreichen Forschungsprojekten ungenügend dokumentiert waren. Aus Transparenzgründen sind diese Prozesse aber wichtig, sowohl für die Forschung selber als auch für die Bewilligungsorgane. In der Dokumentation müssen die wesentlichen Arbeitsschritte aufgeführt sein: von der Erhebung der unverschlüsselten (nicht pseudonymisierten) Personendaten bis zu deren Pseudonymisierung, Anonymisierung oder Löschung.

Es ist auch wichtig, den anonymisierten Datensatz aufzuführen, der für das Forschungsprojekt eingesetzt werden soll. Nur so kann man beurteilen, ob dieser Datensatz tatsächlich anonym ist. Dabei gilt es zu beachten, dass nur diejenigen Daten bearbeitet werden, welche für das Forschungsprojekt notwendig sind. Bei der Verschlüsselung bzw. Pseudonymisierung ist darauf zu achten, dass sie möglichst dort erfolgt, wo die Daten erhoben werden. Dies wird meist der behandelnde Arzt sein. Erst aufgrund dieser Informationen kann man sich einen Überblick verschaffen und die Datenschutzkonformität des Forschungsprojekts beurteilen.

Bei der Einwilligung ist es gemäss dem Humanforschungsgesetz (HFG) neu so, dass je nach Situation die Einwilligung nicht nur beim Betroffenen, sondern auch bei seiner gesetzlichen Vertretung oder den nächsten Angehörigen (Einwilligungsgeber) eingeholt werden kann bzw. muss. Das ist zu begrüssen, weil bei einem solchen Vorgehen in den meisten Fällen eine Einwilligung eingeholt werden kann. Dabei gilt es zu beachten, dass die Informationen verständlich sein müssen: Es ist unerlässlich, den betroffenen Personen aufzuzeigen, wie das Forschungsprojekt abläuft und welche Schutzmassnahmen getroffen wurden. Erfolgt keine transparente Information so besteht die Gefahr, dass die Einwilligung nicht rechtens ist.

Artikel 34 des HFG nennt die Bedingungen, unter denen die Bearbeitung von Personendaten (oder biologisches Material) ohne Einwilligung bzw. ohne auf das Widerspruchsrecht aufmerksam gemacht zu haben, möglich ist. Diese Regelung lehnt sich an den früheren Artikel 321bis StGB an und besagt, dass Forschungsprojekte

durchgeführt werden dürfen, wenn die folgenden drei Bedingungen kumulativ erfüllt sind:

- Es muss unmöglich oder unverhältnismässig schwierig sein, die Einwilligung einzuholen bzw. über das Widerspruchsrecht zu informieren, oder es kann der betreffenden Person nicht zugemutet werden.
- Es liegt keine dokumentierte Ablehnung vor.
- Das Interesse der Forschung an der Nutzung der Daten überwiegt das Interesse der betroffenen Personen, über die Weiterverwendung ihres biologischen Materials und ihrer Daten zu bestimmen.

Bei unseren früheren Überprüfungen der Auflagen ist uns aufgefallen, dass das Vetorecht (Widerspruchsrecht) den Betroffenen meist nicht bekannt war, obwohl es z.B. in den Patientenbroschüren kommuniziert wurde. Dieses Recht gilt für alle Forschungsprojekte. Es stellt sich diesbezüglich u. a. die Frage, wo der Widerspruch der Patienten festgehalten werden soll, damit für alle Forschenden ersichtlich ist, dass diese Daten nicht benutzt werden dürfen. Im Weiteren müssten auch die Kontrollorgane überprüfen können, ob ein Veto vorliegt.

1.6 Versicherungen

1.6.1 Kontrolle der Datenannahmestellen der Krankenversicherer für die Rechnungen des Typus DRG

Unsere Kontrolle von zwei zertifizierten Datenannahmestellen hat gezeigt, dass die Umsetzung der automatisierten Dunkelprüfung der Rechnungen des Typus DRG aus technischen Gründen weniger schnell als erwartet voranschreitet.

Wir haben im Berichtsjahr bei zwei Krankenversicherern die zertifizierten Datenannahmestellen für Rechnungen des Typus DRG (diagnosebezogene Fallgruppen) kontrolliert. Dabei mussten wir feststellen, dass bei den Datenannahmestellen nur ein sehr kleiner Teil der Rechnungen in elektronischer Form mit allen notwendigen Angaben, insbesondere dem medizinischen Datensatz, angeliefert wird. Ausschlaggebend für diese schleppende Umsetzung ist gemäss unseren Erkenntnissen die verzögerte Einführung des standardisierten Datensatzes in den Systemen, welche die Spitäler für die Rechnungserstellung verwenden.

So konnten wir bei der Kontrolle der Datenannahmestelle eines grossen Krankenversicherers zwar feststellen, dass sie für die automatisierte Prüfung der DRG-Rechnungen bereit ist, diese aber aufgrund der grossen Anzahl an Papierrechnungen nur eingeschränkt betrieben werden kann. Allerdings hat der Versicherer auch die Abläufe und Systeme, welche für das Bearbeiten von Papierrechnungen des Typus DRG notwendig sind, zertifizieren lassen. Somit sind hier die Anforderungen an eine zertifizierte Datenannahmestelle erfüllt.

Die Kontrolle bei einem mittleren Krankenversicherer hat hingegen gezeigt, dass dieser sich wohl auf eine rechtzeitige Einführung des elektronischen Rechnungsformats verlassen und deshalb keine Zertifizierung der Prozesse für die DRG-Rechnungen in Papierform vorgenommen hat. Der Versicherer war anlässlich der Kontrolle noch der Ansicht, dass er auf eine Zertifizierung der Papierprozesse verzichten wolle, weil er ab dem 1. Januar 2014 die Entgegennahme von Papierrechnungen des Typus DRG verweigern werde. Dieser Plan wurde wahrscheinlich auch massgeblich dadurch geprägt, dass er für die Erledigung der automatisierten Dunkelprüfung mit einem Dienstleister zusammen arbeitet, der – zumindest zum Zeitpunkt der Kontrolle – ausdrücklich nur elektronische Rechnungen bearbeiten wollte.

Mittlerweile hat sich gezeigt, dass dieses Vorgehen kaum umsetzbar ist, da auch Ende 2013 der Anteil an elektronischen DRG-Rechnungen noch bei weit unter 50 Prozent lag. Aus unserer Sicht kann es für diesen und alle anderen Versicherer, die dies nicht schon gemacht haben, nur eine Lösung geben: die Zertifizierung der in den Datenannahmestellen durchgeführten Papierprozesse. Ansonsten konnten wir

bei beiden Versicherern die Verhältnismässigkeit der nach der Dunkelprüfung an den Versicherer weitergeleiteten Rechnungen nicht überprüfen, da hierfür aufgrund des beschriebenen Sachverhalts noch zu wenig elektronische Rechnungen durch die DAS bearbeitet worden waren.

1.6.2 Zertifizierung von Datenannahmestellen

Zahlreiche Krankenversicherer haben Datenannahmestellen zertifizieren lassen und bei uns angemeldet. Bei kleineren und mittleren Krankenversicherern wird die automatisierte Dunkelprüfung oft durch einen Dienstleister durchgeführt. Versicherungsgruppen betreiben hingegen lieber eine zentrale Datenannahmestelle für alle Mitglieder der Versicherungsgruppe.

Haben Krankenversicherer das Zertifikat für ihre Datenannahmestelle (DAS) erhalten, so müssen sie diese unaufgefordert bei uns anmelden. Wir publizieren eine Liste der zertifizierten Datenannahmestellen auf unserer Internetseite (www.derbeauftragte.ch, Datenschutz – Zertifizierung – Swiss DRG). Dort ist ersichtlich, ob der Versicherer die Datenannahmestelle selbst betreibt, ob dies für mehrere Krankenversicherer einer Gruppe passiert, ob ein Dienstleister die automatisierte Dunkelprüfung erledigt, durch welchen Zertifizierer die Zertifizierung erfolgt ist und auch bis wann das erteilte Zertifikat gültig ist. Bis Januar 2014 waren bei uns 39 Annahmestellen gemeldet.

Aufgrund dieser Anmeldungen können verschieden Schlüsse gezogen werden. Kleine und mittlere Krankenversicherer haben die automatisierte Dunkelprüfung mehrheitlich an einen Dienstleister ausgelagert. Hier zeigt sich eine Konzentration auf momentan zwei Dienstleister. Einige mittlere Krankenversicherer betreiben die automatisierte Dunkelprüfung aber auch im eigenen Haus. Bei den grossen Versicherungsgruppen zeigt sich, dass sie eine zentralisierte DAS für alle Mitglieder der Gruppe betreiben. Hier besteht aus ihrer Sicht allerdings eine Auslagerung an die Gruppengesellschaft.

Wichtig ist hier, dass bei der Zusammenarbeit mit einem Dienstleister alle für den Betrieb der Annahmestelle notwendigen Prozesse beim auslagernden Versicherer und beim Dienstleister zertifiziert sein müssen. Ein Dienstleister alleine kann also kein Zertifikat für eine Datenannahmestelle erhalten, weil dieses immer für einen bestimmten Versicherer oder für eine bestimmte Gruppe ausgestellt wird. Bei einem Zertifikat für eine Gruppe muss zudem klar ersichtlich sein, für welche Mitglieder dieses tatsächlich Gültigkeit hat. Selbstverständlich muss dies auch aus dem zugehörigen Auditbericht klar hervorgehen.

Im Berichtsjahr haben wir wiederum eine Fachgruppensitzung mit den akkreditierten Zertifizierungsgesellschaften KPMG AG, der Schweizerischen Vereinigung für Qualitäts- und Management-Systeme (SQS) und der Schweizerischen Akkreditierungsstelle (SAS) durchgeführt. Insbesondere wurden hier die Anforderungen an die Ausbildung der beim Zertifizierungsaudit eingesetzten Prüfer, die Anforderungen an den Auditbericht und die erforderliche Auditdauer thematisiert. Da die Datenschutzzertifizierung auf der Norm ISO/IEC 27001 basiert, wurde hier die für Audits massgebliche Norm ISO/IEC 27006 als sinngemäss für bindend erklärt.

Zudem haben wir erneut – wie bei der im Herbst des Vorjahres durchgeführten Sitzung – klargestellt, dass bei der Datenannahmestelle auch alle Papierprozesse zu zertifizieren sind. Diese Arbeitssitzungen haben sich gemäss unserer Ansicht sehr bewährt, da wir hier als Zertifizierungsschema-Inhaber direkt mit den involvierten Stellen Probleme diskutieren und Lösungen finden, aber auch unmittelbar unsere für die Zertifizierer bindenden Vorgaben abgeben und erläutern können. Entsprechend werden wir die jährliche Fachgruppensitzung weiterführen. Sollte es notwendig sein, werden wir auch Ad-hoc-Sitzungen durchführen.

1.6.3 Individuelle Prämienverbilligung – Übermittlung von Versichertendaten an kantonale Stellen

Für die Gewährung der individuellen Prämienverbilligung wird es zu umfangreichen Datenbekanntgaben von Krankenversicherern an die kantonalen Durchführungsstellen kommen. Wir bezweifeln, dass dieses Vorgehen zulässig ist.

Für die Gewährung der individuellen Prämienverbilligung (IPV) hat das Bundesamt für Gesundheit (BAG) mit einer Änderung der Verordnung über die Krankenversicherung den Weg dafür geöffnet, dass die Kantone in ihren gesetzlichen Bestimmungen die Krankenversicherer zu bestimmten Meldeprozessen verpflichten können. Wir sind aber klar der Meinung, dass nur eine gesetzliche Bestimmung des Bundesrechts für die Versicherer der Obligatorischen Krankenpflegeversicherung (OKP) als rechtsgenügliche gesetzliche Grundlage betrachtet werden kann, da die Versicherer in diesem Bereich als Bundesorgane handeln.

Besonders kritisch erachten wir in diesem Bereich den vorgesehenen Meldeprozess «Ganzer Versichertenbestand». Die Krankenversicherer sollen hier den kantonalen Durchführungsstellen den ganzen Bestand der nach Krankenversicherungsgesetz versicherten Personen übermitteln. Diese Datenbekanntgabe haben wir in mehreren Stellungnahmen gegenüber dem BAG als unverhältnismässig qualifiziert, da hier auch Angaben von Personen an die kantonale Durchführungsstelle übermittelt werden, die entweder keinen Anspruch auf eine Prämienverbilligung haben oder den bestehenden Anspruch aus irgendwelchen Gründen nicht geltend machen wollen.

Da offenbar auch nicht alle Krankenversicherer davon überzeugt sind, dass das Prozedere zulässig ist, haben sich mehrere Versicherer mit uns in Verbindung gesetzt und uns um eine Stellungnahme gebeten. Hier haben wir klar festgehalten, dass eine kantonale Bestimmung für ein Bundesorgan nicht als gesetzliche Grundlage für eine Datenbekanntgabe geeignet ist. Auch verstosse der Meldeprozess «ganzer Versichertenbestand» gegen den datenschutzrechtlichen Grundsatz der Verhältnismässigkeit, da er für die Gewährung der IPV nicht notwendig ist. Wir erwarten nun vom BAG, dass im Bundesrecht möglichst rasch eine klare gesetzliche Bestimmung für die Meldeprozesse im Rahmen der IPV geschaffen wird, welche auch den fundamentalen Grundsatz der Verhältnismässigkeit respektiert.

1.7 Arbeitsbereich

1.7.1 Übermittlung von Mitarbeiterdaten durch Banken – neue Entwicklungen

Nach den Empfehlungen an fünf Banken im Jahr 2012 haben wir dieses Jahr im Rahmen der Diskussion um eine Globallösung im Steuerstreit ein Merkblatt erstellt, dass das Vorgehen für alle Banken, die in diesem Zusammenhang Personendaten übermitteln wollen, regelt. Weiter haben wir betroffenen Personen ihre Rechte erläutert und sie beraten.

Im Herbst 2012 haben wir im Zusammenhang mit der Übermittlung von Mitarbeiterdaten an US-Behörden bei fünf Banken Sachverhaltsabklärungen durchgeführt. Diese haben wir im Oktober 2012 mit fünf Empfehlungen abgeschlossen. Während der Debatte um eine Globallösung des Steuerstreits mit den USA im Frühling 2013 wurde über Datenübermittlungen von weiteren Banken diskutiert. Wir wurden erneut kontaktiert und nahmen an verschiedenen verwaltungsinternen Sitzungen teil. Dabei haben wir unsere Position und das in den Empfehlungen skizzierte Verfahren erläutert.

Wir haben immer betont, dass auch jene Banken, die nicht zu den Adressaten unserer Empfehlungen gehörten, bei der Übermittlung von Personendaten an US-Behörden immer die datenschutzrechtlichen Prinzipien anwenden und sich in diesem Sinne auch an unsere Empfehlungen halten müssen. Nachdem das Parlament keine gesetzliche Grundlage geschaffen hat, haben wir ein Merkblatt publiziert. Dieses beschreibt das von uns geforderte Vorgehen vor einer Übermittlung von Personendaten und richtet sich an alle davon betroffenen Banken. Gleichzeitig haben wir verschiedene Banken direkt angeschrieben und über das Merkblatt informiert. Auch haben wir betroffene Personen über ihre Rechte aufgeklärt und beraten.

1.7.2 Sachverhaltsabklärung in Sachen Whistleblowing

Im Rahmen einer Sachverhaltsabklärung haben wir die Datenbearbeitung von Meldungen, die an die Meldestelle der Eidgenössischen Finanzkontrolle erfolgen, auf ihre Datenschutzkonformität untersucht. In den Bereichen Registrierungspflicht und Bearbeitungsreglement haben wir entsprechende Empfehlungen erlassen.

Seit dem Jahr 2003 gibt es bei der Eidgenössischen Finanzkontrolle (EFK) eine Meldestelle, an welche sich Mitarbeitende der Bundesverwaltung bei der Feststellung von Unregelmässigkeiten oder Korruptionsverdacht wenden können. Auf den 1. Januar 2011 ist zusätzlich ein Artikel im Bundepersonalgesetz in Kraft getreten,

der besagt, dass die Mitarbeitenden unter gewissen Voraussetzungen sogar verpflichtet sind, Unregelmässigkeiten zu melden. Mit der eingerichteten Meldestelle sollen somit einerseits strafbare Handlungen geahndet werden können (Meldepflicht), andererseits auch weiterhin die Korruption bekämpft werden (Melderecht) und schliesslich verhindert werden, dass Mitarbeiter solche Meldungen als Erstes der Presse weiterleiten.

Im Rahmen unserer Aufsichtstätigkeit haben wir im Jahr 2013 die Einhaltung der datenschutzrechtlichen Bestimmungen bei der Whistleblowing-Meldestelle für Bundesangestellte überprüft. Dazu haben wir der EFK in einem ersten Schritt einen Fragekatalog zugestellt. Aufgrund der erhaltenen Antworten haben wir einen Augenschein vor Ort durchgeführt und gestützt auf diese Informationen einen Schlussbericht erstellt.

Die EFK bearbeitet Personendaten im Sinne des DSG, auch wenn gewisse Meldungen in anonymer Form erfolgen. Die Daten werden intern bei der EFK gespeichert und nur durch die zuständigen Personen bearbeitet. Wir kamen bei unseren Abklärungen zum Schluss, dass die EFK eine Datensammlung betreibt. Gemäss DSG müssen Bundesorgane sämtliche Datensammlungen beim EDÖB zur Registrierung anmelden und im Falle der Bearbeitung besonders schützenswerter Personendaten ein Bearbeitungsreglement erstellen. Wir haben der EFK empfohlen, ihre Datenbearbeitung entsprechend unserer Ausführungen anzupassen. Da unsere Empfehlungen nicht angenommen wurden, ist das Verfahren noch hängig.

1.7.3 Aufzeichnung von Telefongesprächen beim Kundendienst der Post

Im Anschluss an die Klage einer Gewerkschaft über die Aufzeichnung von Telefongesprächen der Mitarbeiter des Kundendiensts haben wir eine Sachverhaltsabklärung bei der Schweizerischen Post eingeleitet. Die Abklärung ergab, dass die Datenschutzvorschriften, namentlich die Information der Mitarbeiter und die Verhältnismässigkeit der Kontrollprozesse, im betreffenden Fall eingehalten wurden.

Eine Gewerkschaft hat uns ihre Besorgnis angesichts der Aufzeichnung von Telefongesprächen der Beschäftigten in den Call Centers der Schweizerischen Post mitgeteilt. Wir eröffneten darauf hin eine Sachverhaltsabklärung. Dabei wurde der von der Gewerkschaft beanstandete Sachverhalt einer datenschutzrechtlichen Prüfung unterzogen. Bei diesem Verfahren ging es ausdrücklich nicht um die Überprüfung von Einzelfällen. Solche Untersuchungen liegen nämlich in der Zuständigkeit der Zivilgerichte, die in einem spezifischen Fall, das heisst auf Ersuchen eines betroffenen Mitarbeitenden, abklären können, ob Bestimmungen über den Persönlichkeitsschutz verletzt wurden.

Das Kontrollergebnis erlaubte uns den Schluss, dass die Datenschutzvorschriften, namentlich die Information der Mitarbeitenden und die Verhältnismässigkeit der Kontrollprozesse im konkreten Fall eingehalten werden. Unserer Analyse zeigte nämlich auf, dass nur von einem Teil der Anrufe Aufzeichnungen gemacht werden: auch werden einzig die während eines bestimmten Zeitraums aufgezeichneten Anrufe für die Beurteilung der Leistungen der Beschäftigten verwendet. Die fragliche Zeitspanne wird den Mitarbeitern im Voraus angekündigt.

Die Aufzeichnung der übrigen Gespräche erfolgt ausschliesslich zum Zweck der Evaluation der Branchenprozesse und nicht für die Kontrolle der Leistungen der Mitarbeitenden. Die Aufzeichnungen werden ausschliesslich aufgrund von allgemeinen und bereichsübergreifenden Kriterien verlangt. Jeder Beschäftigte wird über die Überwachung der Gespräche informiert, und dies nicht mittels eines akustischen oder optischen Signals, sondern durch eine klare und transparente Vorankündigung der Aufzeichnungsperioden, auf die er namentlich über das Intranet des Unternehmens Zugriff hat.

Wir sind der Ansicht, dass die Dauer der Aufzeichnungsperioden insofern den Datenschutzanforderungen entspricht, als die Häufigkeit dieser Perioden und die Dauer der aufgezeichneten Gespräche dem Verhältnismässigkeitsprinzip gerecht werden. Es wird weder ständig noch systematisch aufgezeichnet. Darüber hinaus ist die Abhörfunktion der laufenden Gespräche in Echtzeit durch den unmittelbaren Vorgesetzten endgültig deaktiviert. Der Zugriff auf die Aufzeichnungen ist einer begrenzten Anzahl Personen vorbehalten, die diese Möglichkeit zur Ausführung ihrer Aufgabe benötigen. Die Dauer der Datenaufbewahrung ist ebenfalls in angemessenem Verhältnis begrenzt.

Die Post hat indessen, um die Information ihrer Angestellten zu verbessern, auf unseren Vorschlag ihre internen Strukturen geändert. Diese treffen eine klarere Unterscheidung zwischen dem Prozess zur Qualitätsverbesserung bei den Leistungen der Mitarbeitenden einerseits und den Massnahmen zur Verbesserung der Branchenprozesse andererseits. Zu den beiden Zweckbestimmungen eines solchen Systems, dem Kreis der zum Abhören der Gespräche berechtigten Personen, sowie der Datenaufbewahrungsdauer wurden ebenfalls weitere Klärungen vorgenommen, die zu einem besseren Verständnis der internen Weisungen beitragen.

Die Mitarbeiterinnen und Mitarbeiter des Kundendienstes verfügen schon heute über klare Weisungen, die sie darüber aufklären, unter welchen Voraussetzungen ihre Daten rechtmässig bearbeitet werden können, und wie sie andernfalls die ihnen zur Wahrung ihrer Rechte notwendig erscheinenden Schritte unternehmen können. Falls also ein Mitarbeitender der Ansicht ist, dass die Bedingungen für ihn betreffende Aufzeichnungen nicht korrekt sind, und insbesondere wenn sie nicht

den Weisungen oder der Datenschutzgesetzgebung entsprechen, hat er die Möglichkeit, individuell dagegen vorzugehen.

Dazu ist anzumerken, dass die oben erwähnte Kontrolle die Datenschutzaspekte, nicht aber den arbeitsrechtlichen Bereich betraf. Das Staatssekretariat für Wirtschaft (SECO) hat seinerseits Kommentare zur Umsetzung von Artikel 26 der Verordnung 3 zum Arbeitsgesetz (ArGV 3) herausgegeben. Die Kontrolle der Ausführung dieser Verordnung, und damit der Art und Weise, in der die Beaufsichtigung der Beschäftigten zum Zwecke der Ausbildung, der Qualitätskontrollen oder der Leistungskontrolle erfolgt, obliegt den kantonalen Arbeitsinspektoraten.

1.7.4 Versand von Pensionskassenausweisen – Schwierigkeiten in der Praxis

Anlässlich unserer Kontrolle bei der vom Entscheid des Bundesverwaltungsgerichts vom 10. April 2012 betroffenen Pensionskasse AXA Winterthur konnten wir feststellen, dass sie ihre Praxis entsprechend dem Urteil geändert hat. Andere Akteure der beruflichen Vorsorge haben jedoch ihre Praxis offenbar noch nicht angepasst.

In seinem Entscheid vom 10. April 2012 hat das Bundesverwaltungsgericht (BVGer) für die Weitergabe der Daten durch die schweizerischen Vorsorgeeinrichtungen willkommene Grundsätze aufgestellt. So hat es namentlich der Praxis ein Ende gesetzt, die darin bestand, den Arbeitgebenden die Pensionskassenausweise in einem unverschlossenen Couvert zuzustellen. Dabei wurden die Persönlichkeitsrechte der Arbeitnehmenden verletzt. Gemäss der nunmehr gefestigten Rechtsprechung müssen die Ausweise so zugestellt werden, dass einzig die versicherte Person – unter Ausschluss von Dritten, namentlich des Arbeitgebenden – von ihrem Inhalt Kenntnis nehmen können (vgl. unseren 20. Tätigkeitsbericht 2012/2013, Ziff. 1.7.2).

Der Begriff des Dritten spielte für die Lösung des Problems eine zentrale Rolle. Obwohl er im Datenschutzgesetzhäufig verwendet wird, ist er nicht definiert. Das BVGer hat daher die Frage im Lichte der funktionsbezogenen Umschreibung geklärt. Nach dieser Theorie sind Dritte alle Personen, welche aufgrund der Art ihres Tätigkeitsbereichs in einem Unternehmen die betreffenden Personendaten für die Erfüllung ihrer jeweiligen Aufgaben nicht benötigen.

Als Beispiel zur Veranschaulichung dieses Falls erwähnt das BVGer die Situation eines Abteilungsleiters, der willentlich oder aus Nachlässigkeit Einsicht in die Personalakte eines Arbeitnehmenden nimmt, der einer anderen Abteilung angehört. Nach Auffassung des Gerichts stellt dieser Sachverhalt eine Bekanntgabe an Dritte dar, auch wenn sie innerhalb derselben Organisation erfolgt. Eine solche Verbreitung der Information ist aus Sicht des Datenschutzes nur zulässig, wenn ein

Rechtfertigungsgrund vorliegt (also ein Gesetz, die Einwilligung des Betroffenen, ein überwiegendes privates oder öffentliches Interesse); andernfalls bedeutet die Bekanntgabe der Daten eine widerrechtliche Verletzung der Persönlichkeit des betroffenen Arbeitnehmenden.

Vorliegend wurde festgehalten, dass die beruflichen Vorsorgeeinrichtungen, unabhängig von ihrer Rechtsform, öffentliche Aufgaben erfüllen. Sie gelten dann als Bundesorgane, wenn sie Verpflichtungen wahrnehmen, die ihnen vom Bundesgesetz über die berufliche Alters-, Hinterlassenen- und Invalidenvorsorge (BVG) übertragen werden. Diese Feststellung ist wichtig, denn die geltenden Bestimmungen sind unterschiedlich, je nachdem ob eine Bearbeitung von einem Privatunternehmen oder von einer öffentlichen Verwaltung vorgenommen wird. Der Gesetzgeber hat nämlich für die Datenbearbeitung durch Organe des Bundes restriktivere Bedingungen vorgesehen. In einem solchen Fall kann nur eine gesetzliche Grundlage eine Bearbeitung rechtfertigen, im Gegensatz zu Privaten, die sich auf mehrere Rechtfertigungsgründe berufen können.

Im vorliegenden Fall kam das BVGer zum Schluss, dass es keine gesetzliche Grundlage gibt, die eine Ausnahme von der im Vorsorgebereich geltenden Schweigepflicht rechtfertigen würde, und dass somit keinerlei Rechtfertigung für die Übermittlung der Ausweise an die Arbeitgebenden oder jeden anderen Dritten geltend gemacht werden kann.

Überdies ist daran zu erinnern, dass die Pensionskassenausweise Informationen enthalten, die im Arbeitsverhältnis eine strategische Bedeutung haben können. Man kann daraus namentlich folgende Angaben entnehmen: die Freizügigkeitsleistungen, die neu eintretende Mitarbeiter einbringen, die Einkäufe von Versicherungsjahren, den Vorbezug eines Teils der Pensionskassenguthaben für den Erwerb von Wohneigentum, ob und wann sich das Guthaben infolge Ehescheidung verändert hat oder Hinweise betreffend eine temporäre Erwerbsunfähigkeit. All diese Elemente können zu anderen Zwecken als der beruflichen Vorsorge genutzt werden.

Die Vorsorgeeinrichtung muss daher sämtliche notwendigen Massnahmen treffen, um sicherzustellen, dass die bisweilen besonders schützenswerten Daten der Versicherten nicht beim Versand offen gelegt werden. Die Datensicherheit muss gewahrt bleiben; sie ist eng mit der Sorgfaltspflicht der Vorsorgeeinrichtung verbunden. Diese muss folglich die Ausweise entweder direkt in einem geschlossenen Umschlag an die Privatadresse der Versicherten oder an den Arbeitgebern in einem verschlossenen Couvert zur Verteilung senden. In diesem Fall muss auf dem Umschlag der Name des Empfängers und der Vermerk «Persönlich» angebracht sein.

Trotz einer klaren Stellungnahme des BVGer in dieser Sache erhalten wir immer noch Hinweise auf Versäumnisse. Es ist daher daran zu erinnern, dass der Entscheid, wenngleich er zunächst nur die Prozessparteien betrifft, eine Präzisierung des Datenschutzrechts darstellt, die allgemeine und abstrakte Geltung hat. Die so entwickelte Rechtsprechung gilt für alle betroffenen Akteure und fördert gleichzeitig die Rechtssicherheit.

In Anbetracht der obigen Ausführungen werden wir die künftigen Entwicklungen auf diesem Gebiet weiterhin aufmerksam verfolgen.

1.7.5 Personalinformationssystem des Bundes

Im Personalinformationssystem des Bundes, BV PLUS, werden grosse Mengen an Personendaten bearbeitet. Infolge verschiedener Anfragen sowie aufgrund der verarbeiteten Datenmenge haben wir uns dieses System erläutern lassen. Dies half uns gleichzeitig, diejenigen Projekte zu verstehen, die wir im Rahmen von Ämterkonsultationen begleitet haben.

Wir sind im letzten Jahr sowohl im Rahmen unserer Beratungstätigkeit als auch im Rahmen der Begleitung von Rechtsetzungsprojekten und Ämterkonsultationen vermehrt mit Fragen über das Personalinformationssystem des Bundes, BV PLUS, konfrontiert worden. Aus diesem Grund war es für uns wichtig, dieses System näher kennenzulernen. Der Betreiber des Systems, das Eidgenössische Personalamt (EPA) hat uns in Form einer Präsentation die verschiedenen Funktionsweisen von BV PLUS erläutert. In einer gemeinsamen Sitzung wurden zudem verschiedene kommende Projekte besprochen und Detailfragen diskutiert.

Wir haben im Jahr 2013 auch weitere Gesetzgebungsprojekte begleitet, in welchen Daten aus BV PLUS betroffen waren: Das Bundesamt für Informatik und Telekommunikation etwa betreibt verschiedene Informationssysteme, die auch Daten aus BV Plus enthalten, die seit diesem Jahr eine genügende gesetzliche Grundlage haben. Weiter haben wir ein Projekt des EPA begleitet, welches sicherstellen soll, dass bei einem verwaltungsinternen Übertritt von Mitarbeitenden, nur diejenigen Daten an die neue Verwaltungsstelle übermittelt werden, die für diese notwendig sind. Bisher konnte dafür jedoch keine technische Lösung gefunden werden. Wir werden die weiteren Entwicklungen mitverfolgen.

1.8 Handel und Wirtschaft

1.8.1 Energiestrategie 2050 und Smart Metering

Zur Energiestrategie 2050 haben wir im Rahmen der Vernehmlassung Stellung genommen. Wir kritisierten die fehlende Bestimmtheit der gesetzlichen Grundlage für die Personendatenbearbeitung und haben eine Anpassung gefordert. Weiter begleiteten wir beratend die Arbeitsgruppe Smart Grid Road Map Schweiz.

Die Bestimmungen zur Personendatenbearbeitung in der Vernehmlassungsvorlage zur Energiestrategie 2050 genügten aus unserer Sicht den Anforderungen an die Bestimmtheit einer gesetzlichen Grundlage nicht. Wir haben gefordert, dass der Zweck des Systems so umschrieben werden muss, dass er für die betroffenen Personen genau erkennbar ist. Je schwerer die Eingriffe in die Persönlichkeitsrechte (also bei besonders schützenswerten Personendaten und Persönlichkeitsprofilen) sein können, umso höher muss der Detailgrad sein.

Unabhängig von der Natur der bearbeiteten Personendaten genügt es nicht, anzugeben, der Zweck des Systems bestehe darin, dem verantwortlichen Bundesorgan die Erfüllung seiner gesetzlichen Aufgaben zu ermöglichen. Vielmehr muss abschliessend aufgezählt werden, für welche Aufgaben eine Datenbearbeitung vorgesehen ist.

In Sachen Smart Metering (Digitale Stromzähler) und Datenschutz haben wir die Arbeitsgruppe des Bundesamtes für Energie «Smart Grid Road Map Schweiz» beratend begleitet. In verschiedenen Sitzungen brachten wir unsere Empfehlungen ein (siehe auch unsere Erläuterungen zum Thema unter www.derbeauftrage.ch, Datenschutz – Wohnen und Verkehr). Ein zentraler Punkt beim Einsatz solcher Stromzähler wird die Verhältnismässigkeit der Datenbearbeitung sein. Das bedeutet, dass nur die Daten bearbeitet werden dürfen, die für die Zweckerfüllung notwendig sind, und dass nicht mehr benötigte Daten zu löschen oder zu anonymisieren bzw. zu aggregieren sind.

1.8.2 Kundenkarten im Detailhandel

Der EDÖB hat dieses Jahr umfassende Nachkontrollen im Bereich Kundenkarten bei den zwei bedeutendsten Grossverteilern der Schweiz durchgeführt. Die Auswertungen dazu sind noch im Gange.

Seit unseren letzten vertieften Sachverhaltsabklärungen zum Thema Kundenkarten bei den beiden Grossverteilern Migros und Coop sind mehrere Jahre vergangen (www.derbeauftragte.ch, Datenschutz – Handel und Wirtschaft – Kundendaten). Im

Rahmen von Nachkontrollen haben wir in diesem Jahr erneut die Datenbearbeitungen in diesem Bereich untersucht. Dabei haben wir die Gelegenheit genutzt, um auch die neuen Angebote und Services im Zusammenhang mit den Kundenkarten zu prüfen. Die Kontrollen haben es uns erlaubt, die Umsetzung der Verbesserungsvorschläge aus den letzten Abklärungen zu prüfen und die seither neu dazugekommenen Datenbearbeitungen einer detaillierten Analyse zu unterziehen und damit die Einhaltung der Datenschutzbestimmungen zu überprüfen. Die Auswertungen dieser Abklärungen sind noch im Gange. Es konnte schon während den Kontrollen festgestellt werden, dass die beiden Grossverteiler keinen Handel mit den Kundendaten betreiben und dies auch für die Zukunft nicht geplant ist.

1.8.3 Wirtschaftliche Nutzung von Personentrackingsystemen

Immer häufiger werden Personentrackingsysteme dazu eingesetzt, Kundenverhalten zu analysieren und so Verkaufsräume, Produktepaletten oder Dienstleistungsangebote zu optimieren. Wir haben daher in diesem Jahr einige dieser Systeme analysiert und einige Risiken für die Persönlichkeitsrechte der betroffenen Personen festgestellt.

Wer das Verhalten seiner Kundinnen und Kunden kennt, kann daraus geldwerte Vorteile ziehen. So können die Standorte von Werbeflächen optimiert, das Sortiment angepasst oder gar personalisierte Werbung versendet werden. Immer mehr Unternehmen wollen diese Vorteile nutzen und setzen zu diesem Zweck Systeme ein, welche Personen automatisiert beobachten und deren Verhalten analysieren. Die von uns geprüften Systeme erfassen Personen, die einen bestimmten Raum (z. B. ein Einkaufszentrum) betreten und verfolgen deren Weg innerhalb dieses Raums.

Einige Systeme setzten dabei auf biometrische Daten (Gesichtserkennung), so dass unbestrittenermassen Personendaten bearbeitet werden. Sie bieten in der Regel die zusätzliche Möglichkeit, die erfassten Personen z.B. nach Alter, Geschlecht oder ethnischer Herkunft zu kategorisieren. Die Risiken einer Persönlichkeitsverletzung liegen auf der Hand, weshalb hier dem Datenschutz besondere Beachtung geschenkt werden muss (vgl. hierzu auch unseren Leitfaden zu biometrischen Erkennungssystemen, der auf unserer Webseite www.derbeauftragte.ch, Datenschutz – Biometrie nachgelesen werden kann).

Andere Systeme nutzen dagegen die von Mobiltelefonen ausgesendeten Signale und zeichnen den Weg jedes sich im fraglichen Raum befindlichen Geräts auf. Auch wenn hier auf den ersten Blick keine Personendaten erhoben werden (so können z.B. die TMSI- oder die IMSI-Nummern von Mobilfunkgeräten von den Systembetreibern keiner bestimmten Person direkt zugeordnet werden), kann ein Personenbezug in

einigen Fällen relativ einfach auf indirektem Weg hergestellt werden: Aufgrund des entstehenden Bewegungsprofils ist es unter Umständen möglich, das ursprünglich unpersönliche Profil einer bestimmten Person zuzuordnen.

So unterscheiden sich z.B. die Bewegungsprofile von Mitarbeitenden in einem Geschäft in der Regel klar von denjenigen der Kundschaft, und bei einer kleinen Belegschaft kann das Mitarbeiterprofil leicht einem bestimmten Mitarbeitenden zugeordnet werden. Auch durch die Verknüpfung mit weiteren Daten (z.B. den Aufnahmen von Überwachungskameras) können ursprünglich unpersönliche Bewegungsprofile personalisiert werden. Daher muss auch bei diesen Systemen davon ausgegangen werden, dass Personendaten bearbeitet werden und somit die allgemeinen Bearbeitungsgrundsätze des Datenschutzgesetzes einzuhalten sind.

Dies bedeutet in erster Linie, dass für die Datenbearbeitung ein Rechtfertigungsgrund vorliegen muss. Beim Betrieb solcher Systeme könnte dies ein überwiegendes Interesse oder die Einwilligung der betroffenen Personen sein:

- Ein überwiegendes Interesse ist anzunehmen, wenn solche Systeme z.B. zur Verbesserung der Sicherheit von Flughafen- oder Bahnhofsgebäuden eingesetzt werden. Ein überwiegendes Interesse liegt auch vor, wenn die Systeme zu nicht personenbezogenen Zwecken, also z.B. zu einer rein statistischen Auswertung von Kundenfrequenzen, eingesetzt werden, und in den Analyseergebnissen keine Personen erkennbar sind.
- Nicht durch ein überwiegendes Interesse gerechtfertigt sind hingegen personenbezogene Analysen zu Marketingzwecken. Die Datenbearbeitung muss in diesem Fall durch die Einwilligung der betroffenen Personen gerechtfertigt werden. Dabei ist zu beachten, dass die Einwilligung stets freiwillig zu erfolgen hat, die betroffene Personen also die Möglichkeit haben muss, sich in einem von einem Trackingsystem überwachten Gebäude aufzuhalten, ohne davon erfasst zu werden. Dies konkret umzusetzen, kann sich je nach Ausgestaltung des Systems als sehr schwierig erweisen.

Gänzlich ausgeschlossen ist der Einsatz solcher Systeme, um das Verhalten von Mitarbeitenden zu überwachen. Dies wäre gesetzeswidrig und könnte auch mit der Einwilligung der betroffenen Mitarbeitenden nicht gerechtfertigt werden.

Genaueres zum Thema kann auf unserer Webseite www.derbeauftragte.ch, Datenschutz – Technologien nachgelesen werden.

1.8.4 Recht auf Vergessen beim Handelsregister

In der Gesetzesvorlage zur Modernisierung des Handelsregisters soll kein «Recht auf Vergessen» eingeführt werden. Das Eidgenössische Amt für das Handelsregister schliesst aus dem Vernehmlassungsresultat, dass es keine speziellen Regeln für die Veröffentlichung von Daten im Internet brauche. Wir bedauern diesen Entscheid.

In unserem 20. Tätigkeitsbericht äusserten wir uns zu den geplanten Änderungen des Handelsregisters (Ziff. 1.8.4). Insbesondere begrüssten wir die Tatsache, dass das Eidgenössische Amt für das Handelsregister (EHRA) ein dem Handelsregisterrecht angepasstes Recht auf Vergessen in die Vernehmlassungsvorlage aufgenommen hatte. Die Vernehmlassung ist im Berichtsjahr abgeschlossen worden.

Gestützt auf das Resultat der Vernehmlassung will das EHRA die Möglichkeit der Unterbindung einer freien Abfrage der Handelsregisterdaten über das Internet nach Ablauf einer gewissen Zeit nicht weiter prüfen. Fünf der Teilnehmer der Vernehmlassung hätten nämlich die Auffassung vertreten, dass keine speziellen Regeln für die Internet-Öffentlichkeit gelten sollten. Wir können uns dieser Argumentation nicht anschliessen. Unserer Meinung nach muss zwischen dem physischen Führen der Daten in den Handelsregistern und der Art, wie der Inhalt veröffentlicht wird, unterschieden werden.

In diversen Sitzungen und Stellungnahmen hatten wir das EHRA auf die Problematik der zeitlich unbeschränkten Veröffentlichung von HR-Daten im Internet hingewiesen. Seit einzelne Handelsregister dazu übergegangen sind, auch die Belege rückwirkend und genauso, wie sie eingereicht wurden, im Internet zu publizieren, hat sich diese Problematik zusätzlich verschärft. So werden beispielsweise Wohnadressen von Verwaltungsräten, Protokollauszüge die u.a. besonders schützenswerte Personendaten enthalten, Pass- und ID Nummern usw. ebenfalls einer breiten Öffentlichkeit zugänglich gemacht.

Wir bedauern das Vorgehen des EHRA ausserordentlich, insbesondere da das geschilderte Problem durch die Usanzen der privaten Auskunfteien noch verschärft wird. Die Problematik der Publikation von Daten über das Internet haben wir ebenfalls in unserem aktuellen Tätigkeitsbericht in Ziffer 1.2.10 zur Veröffentlichung von Zivilstandsdaten über das Internet beschrieben.

Ebenfalls soll die AHV-Versichertennummer als Identifikator in das Handelsregister eingeführt werden. Obwohl sie nur verwaltungsintern ersichtlich sein soll, ist diese weitere Ausdehnung ihrer Verwendung aus datenschutzrechtlicher Sicht problematisch (siehe auch Ziffer 1.5.3 des vorliegenden Tätigkeitsberichts).

1.8.5 Abklärungen im Bereich Kredit- und Wirtschaftsauskunfteien

Die Begleitung der Umsetzung unserer Empfehlung in Sachen Moneyhouse hat einige Zeit beansprucht. Seitdem die Betreiberin des Dienstes, die itonex AG, die Löschungsmodalitäten geändert hat, haben sich viele Personen darüber beschwert. Wir beraten diese und sind dabei, die von der itonex AG angebotenen Dienstleistungen zu analysieren.

Im 20. Tätigkeitsbericht 2012/2013 haben wir über unsere letzte Sachverhaltsabklärung berichtet, die insbesondere die Veröffentlichung von Adressen im Internet zum Gegenstand hatte (Ziff. 1.8.2). Das Unternehmen itonex AG, das die Plattform betreibt, hatte unsere Empfehlungen akzeptiert.

Der Abschluss dieses ersten Teils unserer Sachverhaltsabklärung und die Begleitung der Umsetzung der Empfehlung erforderte dabei mehr Zeit als erwartet. Die vom Unternehmen geänderten Modalitäten für die Löschung hatten zur Folge, dass sich vermehrt Personen an uns wandten, die sich dagegen wehrten, dem Unternehmen eine Kopie eines amtlichen Ausweises zuzustellen. Man wolle dem Unternehmen, das ungefragt Personendaten über das Internet verbreite, nicht noch mehr Informationen zur Verfügung stellen, war die meist geäusserte Kritik.

Gemäss den Vorgaben des Datenschutzgesetzes müssen Unternehmen eine Authentifizierung vorsehen, d.h. sie müssen überprüfen, ob es sich tatsächlich um die Person handelt, welche hier ihr Recht auf Löschung durchsetzen will. Dabei können verschiedene Verfahren eingesetzt werden, die dem Schutzbedarf der Daten angepasst werden müssen. Wir haben betroffenen Personen geraten, zuerst festzustellen, welche Personendaten itonex AG schon hat und in einem zweiten Schritt die allfällig darüber hinausgehenden Informationen auf der Kopie des Ausweises zu schwärzen. Diese Informationen sind auch auf unserer Website abrufbar (www.derbeauftragte.ch, Datenschutz – Handel und Wirtschaft).

Immer noch beschweren sich auch Personen, die im Handelsregister eingetragen sind und deren Einträge ebenfalls über www.moneyhouse.ch publiziert werden. Hier müssen wir jeweils darauf verweisen, dass es diesbezüglich einen rechtskräftigen Bundesverwaltungsgerichtsentscheid gibt. Solange die itonex AG die im Handelsregister eingetragenen Informationen kostenlos und vollständig anzeigt, können diese Inhalte nicht gelöscht werden (siehe auch unseren Beitrag im vorliegenden Tätigkeitsbericht zur Modernisierung des Handelsregisters; Ziff. 1.8.4).

Wir sind zurzeit in einem zweiten Teil der Sachverhaltsabklärung dabei, die weiteren, von itonex AG angebotenen Dienstleistungen zu untersuchen. Die Analyse wird angesichts der umfangreichen Datenbearbeitungen, welche das Unternehmen vornimmt, noch einige Zeit in Anspruch nehmen.

1.8.6 Löschung von Adressen in Bonitätsdatenbanken

Inhaber von Bonitätsdatenbanken müssen bei Löschungsgesuchen geltend gemachte Sicherheitsbedürfnisse berücksichtigen.

Es melden sich bei uns immer wieder Personen, die ihre Adresse aus einer Bonitätsdatenbank löschen möchten. Nach Datenschutzgesetz kann eine Auskunftei Daten zur Prüfung der Kreditwürdigkeit auch gegen den Willen desBetroffenen bearbeiten, solange sie weder besonders schützenswerte Personendaten noch Persönlichkeitsprofile bearbeitet. Machen Personen nachvollziehbare Sicherheitsgründe für die Löschung ihrer Daten geltend, so müssen diese Argumente in der einzelfallweise vorzunehmenden Interessensabwägung berücksichtigt werden. Die Adresse sollte unserer Meinung nach gelöscht werden.

Allerdings muss der betroffenen Person bewusst sein, dass ihre Unauffindbarkeit in Bonitätsdatenbanken mit Nachteilen im Geschäftsleben verbunden ist. Kreditkäufe werden insbesondere bei unpersönlichen, über das Internet abgewickelten Massengeschäften dadurch erschwert oder verunmöglicht. Auskunfteien dürfen ihren Kunden die Nichtauffindbarkeit einer Person in einer Bonitätsdatenbank mitteilen, diesen Umstand aber nicht mit schlechter Bonität gleichsetzen.

1.8.7 Datenaustausch betreffend Ladendiebstähle

Ein Einzelhandelsunternehmen und die ihm angeschlossenen Ladengeschäfte können, unter gewissen Voraussetzungen, über Personen, die bei einem Diebstahl gefasst werden, Informationen erheben, namentlich um die Zweckmässigkeit einer Strafanzeige zu prüfen. Der systematische Austausch der Fälle von Diebstahl unter den verschiedenen Einzelhandelsunternehmen im Rahmen einer zentralisierten Datenbank verletzt indes den Grundsatz der Verhältnismässigkeit.

Eine private Sicherheitsfirma hat uns um eine Stellungnahme zur Einrichtung einer zentralisierten Datenbank ersucht, in der die in den Einzelhandelsgeschäften verzeichneten Diebstähle systematisch erfasst werden sollen. Der Austausch von Informationen über Personen, die wegen Diebstahls aufgegriffen werden, sollte es den Kaufhäusern in erster Linie ermöglichen, die Zweckmässigkeit einer Strafanzeige zu beurteilen und die Sanktionen und Massnahmen im Wiederholungsfalle anzupassen. Das vorgestellte Konzept sah auch vor, dass die Polizei- oder Strafverfolgungsbehörden im Abrufverfahren Zugriff auf die Datensammlung erhalten, um Fälle von Wiederholungstaten, gewerbsmässigem oder bandenmässigem Diebstahl leichter aufzudecken.

Was die Datenbearbeitungen durch Einzelhandelsunternehmen anbelangt, müssen diese entsprechend dem DSG die allgemeinen Datenschutzprinzipien einhalten und sich auf einen Rechtfertigungsgrund stützen können. In Ermangelung einer Einwilligung und einer spezifischen Gesetzesgrundlage zur Rechtfertigung der Erfassung und des Austauschs dieser Daten über eine gemeinsame Plattform haben wir geprüft, ob sich Einzelhandelsfirmen auf ein überwiegendes privates oder öffentliches Interesse berufen können.

Die Sicherheitsfirma machte zunächst das öffentliche Interesse der Diebstahlbekämpfung geltend. Diese ist jedoch in erster Linie eine öffentliche Aufgabe, die Sache der zuständigen Polizei- und Justizbehörden ist und eine gesetzliche Grundlage erfordert. Einzelhandelsunternehmen oder eine private Sicherheitsfirma können sich in diesem Fall nicht auf ein überwiegendes öffentliches Interesse berufen, um ohne Auftrag an Stelle der Behörden typische Polizeiaufgaben wahrzunehmen und systematisch besonders schützenswerte Daten anderen Privatpersonen bekannt zu geben. Es handelt sich hier nämlich um eher geringfügige Vermögensdelikte und nicht um Straftaten, die eine Gefahr für Leib und Leben bedeuten. Das Einzelhandelsunternehmen oder das betroffene Ladengeschäft hat ausserdem immer die Möglichkeit, der Polizei im Rahmen einer Klage oder einer Strafanzeige die Daten bekannt zu geben. Die Strafverfolgungsbehörden ihrerseits können im Rahmen eines Verfahrens die Herausgabe der in einer Datensammlung enthaltenen Daten verlangen.

Wir haben sodann geprüft, ob die Unternehmen ein überwiegendes privates Interesse geltend machen können. In dieser Hinsicht ist zu unterscheiden zwischen der Bearbeitung der Personendaten im Rahmen der internen Datensammlung und der Bekanntgabe der Daten an andere Einzelhandelsfirmen im Rahmen einer gemeinsamen Datensammlung.

Ein überwiegendes privates Interesse kann in der Regel für die Bearbeitung von Daten im Rahmen einer internen Datensammlung anerkannt werden, vorausgesetzt dass die allgemeinen Datenschutzgrundsätze beachtet werden. Das Einzelhandelsunternehmen kann die in den ihm angeschlossenen Ladengeschäften festgestellten Diebstähle registrieren, um sich die Möglichkeit zu sichern, bei der Polizei Anzeige zu erstatten oder eine andere Massnahme wie ein Ladenverbot für das einzelne Geschäft oder das Unternehmen zu verhängen. Die zu derselben Einzelhandelsfirma gehörenden Ladengeschäfte können also, unabhängig von ihrem Standort in der Schweiz, ihre Daten austauschen; auf dieser Grundlage kann das Einzelhandelsunternehmen die Situation beurteilen und die Massnahmen anpassen, indem es beispielsweise entscheidet, ob eine Strafanzeige angebracht ist oder nicht. Im Rahmen einer Klage oder einer Strafanzeige kann die Einzelhandelsfirma oder das betroffene Ladengeschäft dann diese Daten der Polizei bekannt geben.

Nach einer Interessenabwägung sind wir zum Schluss gelangt, dass abgesehen von der Bearbeitung von Diebstählen im Rahmen einer internen Datensammlung der systematische und automatisierte Datenaustausch zwischen den verschiedenen Einzelhandelsunternehmen unverhältnismässig ist. Es gibt nämlich andere, die Privatsphäre weniger beeinträchtigende Mittel: dass die Einzelhandelsfirmen aus Gründen der Zweckmässigkeit in den fraglichen Situationen nicht in jedem Fall Strafanzeige erstatten wollen, ist verständlich. Wenn sie jedoch auf dieses Mittel verzichten, können sie sich später auch nicht auf ein überwiegendes privates Interesse berufen, um, dazu noch systematisch, besonders schützenswerte Daten anderen Geschäften bekannt zu geben und so ein spezifisch für Diebstähle in (allen) Einzelhandelsgeschäften vorgesehenes privates Strafregister zu schaffen. Überdies ist darauf hinzuweisen, dass es sich hier um geringfügige Vermögensdelikte und nicht um Straftaten handelt, die Leib und Leben gefährden.

1.8.8 Tool des EDÖB zur Datenschutz-Folgenabschätzung

Im Rahmen unserer Aktivitäten zur Sensibilisierung für den Datenschutz und entsprechend dem heutigen Trend zu «Privacy by design» haben wir ein Wirkungsanalyse-Tool für den Datenschutz in Form eines dynamischen Fragebogens entwickelt. Es ermöglicht den Nutzern, sich in Bezug auf ihre Einstellung zum Datenschutz in dem von ihnen zur Auswertung gewählten Projekt anhand einer personalisierten Beurteilung zu positionieren.

Das Konzept des «Privacy by design» entspricht dem heutigen Trend, der darauf ausgerichtet ist, die Datenschutzprobleme schon bei der Planung und Entwicklung neuer Produkte zu erfassen. In diesem Kontext haben wir ein Wirkungsanalyse-Tool für den Datenschutz entwickelt. Mit diesem Instrument soll den an der Planung und der darauf folgenden Realisierung neuer Produkte oder neuer Anwendungen beteiligten Akteuren die Möglichkeit geboten werden, eine erste Beurteilung vorzunehmen und im Voraus die auftretenden Datenschutzprobleme zu erkennen, um rasch geeignete Massnahmen zu ergreifen.

Das Instrument hat die Form eines dynamischen Fragebogens: Die Fragen werden nacheinander entsprechend den zuvor erteilten Antworten aufgezeigt. Auf diese Weise passt sich der Fragebogen jedem Nutzer an: Die strategischen Schwerpunkte werden durch die Herkunft des Nutzers, der den Privatsektor oder ein Bundesorgan vertritt, und durch die Kategorien der verwendeten Personendaten, insbesondere die besonders schützenswerten Daten, definiert. Der Fragebogen ist in mehrere Kapitel unterteilt, die sich beispielsweise mit der Beschaffung, der Weitergabe und der Speicherung der Daten, aber auch mit den zu treffenden technischen und organisatorischen Massnahmen befassen.

Ist der Fragebogen ausgefüllt, wird eine passende Evaluation erstellt und dem Nutzer vorgelegt. Diese Evaluation setzt sich aus einer nach den erteilten Antworten berechneten Bewertung sowie einer Liste von Kommentaren zusammen. Für jeden Abschnitt der Evaluation erläutert ein generischer Kommentar verschiedene Aspekte des Datenschutzes. Wenn der Nutzer beim Ausfüllen des Fragebogens Antworten erteilt hat, aus denen sich schliessen lässt, dass ein besonderer Aspekt nicht berücksichtigt oder ungenügend beachtet wird, weist ihn überdies ein spezifischer Kommentar auf die möglichen datenschutzrechtlichen Versäumnisse bei der Planung seines Projekts hin.

Dieses Sensibilisierungsinstrument wurde bewusst einfach und losgelöst von den geltenden Rechtsgrundlagen gestaltet, um es möglichst vielen Personen zugänglich zu machen. Es wurde unter Einhaltung des Datenschutzes konzipiert, das heisst, dass keinerlei Nutzerdaten aufbewahrt werden. Es ist auf unserer Website abrufbar (www.derbeauftragte.ch).

1.8.9 Projekt für ein System zum Empfang von Hotelgästen

Wir sind um eine Stellungnahme zur Einrichtung eines Systems für den Gästeempfang von Luxushotels ersucht worden, mit dem der Aufenthaltsort und die Präferenzen der Kunden mit Hilfe der RFID-Technologie erfasst werden sollen. Eine derartige Profilierung erfordert eine vorgängige Information der betroffenen Personen sowie ihre ausdrückliche Einwilligung. Es muss eine Alternative angeboten werden. Insbesondere müssen die Datenerhebung und jede spätere Bearbeitung, namentlich die Evaluation der Daten, für die betroffenen Personen erkennbar sein.

Ein Start-Up-Unternehmen, das ein Gästeempfangssystem für das Luxushotelgewerbe entwickelt, mit dem der Aufenthaltsort und die Präferenzen der Kunden mit Hilfe der RFID-Technologie erfasst werden, hat sich an uns gewandt. Gemäss dem Projekt erhält jeder Kunde anstelle oder zusätzlich zu einer klassischen Schlüsselkarte einen mit einem RFID-Chip versehenen kleinen Schlüsselanhänger. Dank der RFID-Technologie kann der Kunde mittels installierter Antennen in Echtzeit im Hotel lokalisiert werden. Neben den Identifikationsdaten werden die Wünsche und Präferenzen der Gäste erhoben, wie etwa die Zimmerreinigungs-Zeiten, die Temperatur oder die Beleuchtung des Zimmers, die im Hotel aufgesuchten Räumlichkeiten oder auch die bevorzugten Speisen. Mit diesem System sollen der Empfang der Gäste durch individualisierte Dienstleistungen persönlicher gestaltet und das Personalmanagement optimiert werden.

Da die Erhebung solcher Daten dem Datenschutzgesetz (DSG) unterworfen ist, haben wir unsere Beurteilung zum Einsatz eines derartigen Systems abgegeben: Die geplanten Bearbeitungen bedürfen eines Rechtfertigungsgrunds. Besteht

weder eine gesetzliche Grundlage noch ein überwiegendes Interesse, kann einzig die Einwilligung der betroffenen Personen die Bearbeitung der Kundendaten im Rahmen des Systems für den Gästeempfang rechtfertigen. Ein Einverständnis ist nur gültig, wenn es frei und nach vorgängiger Information erfolgt: die Teilnahme an dem System muss fakultativ (freiwillig) sein, und es muss eine Alternative angeboten werden.

Der Kunde muss stets die Kontrolle über seine Daten behalten und seine Einwilligung kann jederzeit rückgängig gemacht werden. Der Gast muss zudem im Voraus über die Datenbearbeitungen sowie über ihren Zweck informiert werden. Da die erhobenen Daten ein Persönlichkeitsprofil ergeben können, braucht es eine ausdrückliche Einwilligung: diese kann in Form einer Unterschrift verlangt werden, die bei der Aushändigung des RFID-Chips nach den Erklärungen zur Datenerhebung abgegeben wird.

Darüber hinaus ist darauf zu achten, dass die grundlegenden Prinzipien des Datenschutzes eingehalten werden, was umso wichtiger ist, als die erhobenen Daten im vorliegenden Fall ein Persönlichkeitsprofil ergeben können (verstärkter Schutz). Im Besonderen müssen jegliche Datenerhebung und jede spätere Bearbeitung, wie etwa die Evaluation der Daten, für die betroffenen Personen erkennbar sein.

Entsprechend dem Grundsatz der Verhältnismässigkeit müssen sich die bearbeiteten Daten auf die Angaben beschränken, mit denen das angestrebte Ziel erreicht werden kann und die ein angemessenes Verhältnis zwischen der Persönlichkeitsverletzung und dem Zweck der Bearbeitung aufweisen. Im vorliegenden Fall wäre es insbesondere unverhältnismässig, die Gäste im gesamten Hotelkomplex auf Schritt und Tritt aufzuspüren; die von den Antennen erfassten Zonen sind zu begrenzen. Eine Meldung der Anwesenheit auf der Etage oder beim Betreten eines bestimmten Bereichs (z. B. Empfang, Restaurant, Wellness-Bereich) oder beim Verlassen des Bereichs erscheint angesichts des verfolgten Zwecks ausreichend.

Überdies dürfen einzig die Personen, welche die betreffenden Daten tatsächlich benötigen, zu einem bestimmten Zeitpunkt Zugriff darauf haben; das Reinigungspersonal beispielsweise braucht nur zu wissen, ob (oder wann) ein Zimmer gereinigt werden kann, und nicht, wo genau die Person sich aufhält. Das Erfordernis der Verhältnismässigkeit begrenzt die Datenbearbeitung auch zeitlich gesehen. Sobald die Personendaten für das angestrebte Ziel nicht mehr dienlich sind, müssen sie vernichtet oder anonymisiert werden.

Gemäss dem Grundsatz der Zweckbindung dürfen die Personendaten nur zu dem Zweck bearbeitet werden, der bei ihrer Erhebung angegeben wird oder der sich aus den Umständen ergibt. Wenn der Gast nicht seine ausdrückliche Einwilligung dazu gegeben hat, können zum Beispiel die Daten nicht an Dritte zu Marketing-Zwecken weitergegeben werden.

Gemäss dem Grundsatz der Sicherheit müssen die Personendaten durch geeignete organisatorische und technische Massnahmen gegen jegliche unbefugte Bearbeitung geschützt werden. Cloud-Computing ist hier für die Bearbeitung von Persönlichkeitsprofilen nicht geeignet. Zudem muss man sich bewusst sein, dass die privaten Daten der Kunden von Luxushotels, mehr noch als andere, die Zielscheibe von Hacker-Angriffen werden könnten, und dass ein grösseres Risiko besteht, dass Personen mit unlauteren Absichten sich unbefugt Zugang zu den Personendaten von bekannten oder vermögenden Personen verschaffen könnten. Soweit Daten auch ins Ausland weitergeben werden sollten, wird im Voraus zu überprüfen sein, ob diese Daten einer Gesetzgebung unterworfen sind, die ein angemessenes Schutzniveau gewährleistet. In Ermangelung einer gleichwertigen Gesetzgebung dürfen Personendaten nur unter gewissen klar bestimmten Voraussetzungen bekannt gegeben werden.

Neben der Einhaltung der erwähnten Grundsätze und Pflichten muss der Inhaber der Datensammlung namentlich auf die Umsetzung des Auskunftsrechts achten. Er ist auch verpflichtet, die Datensammlung beim Beauftragten zur Registrierung anzumelden.

Wir sind zum Schluss gelangt, dass die Verwendung dieses Systems für den Empfang von Hotelgästen aus datenschutzrechtlicher Sicht heikel ist. Die Kunden der Hotels, die das System einführen, müssen wählen können, ob sie daran teilnehmen wollen oder nicht. In Anbetracht der möglichen Erstellung von Persönlichkeitsprofilen erfordern die Datenbearbeitungen auf jeden Fall eine angemessene Information und die ausdrückliche Einwilligung der betroffenen Personen. Personen, die den Einsatz der RFID-Technologie ablehnen, muss eine Alternative angeboten werden.

1.8.10 Revision des Bundesgesetzes und der Verordnung über Bauprodukte

Die im Frühling 2012 begonnene Ämterkonsultation zum Thema Bauprodukte warf einige Fragen hinsichtlich des Legalitätsprinzips auf, namentlich betreffend der Anforderungen an die Normdichte bei der Bearbeitung sensibler Daten durch Bundesorgane.

Unter der Federführung des Eidgenössischen Finanzdepartements, beziehungsweise des Bundesamts für Bauten und Logistik wurde im Frühling 2012 die Ämterkonsultation zur Revision des Bundesgesetzes und der Verordnung über Bauprodukte initiiert. Um wirtschaftliche Nachteile für die Schweiz zu vermeiden, bemüht sich die Eidgenossenschaft stetig, ihre technischen Vorschriften auf das internationale Recht abzustimmen. Mit der Vorlage wird daher beabsichtigt, alle wesentlichen Unterschiede zwischen dem neuen europäischen und dem bisherigen schweizerischen Bauprodukterecht zu beseitigen.

Zu diesem Zweck wurde einerseits ein neues Konzept für das Inverkehrbringen von Bauprodukten entwickelt und andererseits eine Anpassung der Marktüberwachung vorgesehen. Um den neuen Anforderungen an die Marktüberwachung gerecht zu werden, ist die Einführung einer Vollzugsdatenbank auf Bundesebene nötig. Der Gesetzesentwurf sieht vor, dass in dieser auch besonders schützenswerte Daten bearbeitet werden, wie z.B. administrative und strafrechtliche Verfolgungen und Sanktionen, die Bauproduktehersteller im Rahmen ihrer Tätigkeit als solche betreffen. Dieser Umstand führt dazu, dass die Rechtsgrundlage, insbesondere bezüglich der Normdichte, strengeren Anforderungen genügen muss. In unseren Stellungnahmen haben wir diesbezüglich vier Hauptbemerkungen angebracht:

- Die erste betrifft die Zweckbezeichnung der Datenbearbeitung. Wir haben darauf aufmerksam gemacht, dass es unabhängig von der Natur der bearbeiteten Daten nicht genüge, eine allgemeine Bezeichnung anzubringen. Da der Zweck der Datenbank der Marktüberwachung dienen soll, muss dies im Gesetzestext auch klar zum Ausdruck kommen.
- Zweitens äusserten wir uns hinsichtlich der Einführung eines gesetzesinternen Verweises auf die im revidierten Gesetzestext aufgeführten administrativen und strafrechtlichen Bestimmungen, die eine Bearbeitung zur Folge haben könnten.
- Drittens haben wir darauf beharrt, dass ein Dateninhaber bezeichnet wird und dafür das BBL empfohlen.
- Unsere letzte Bemerkung betraf die Auflistung der Fachorganisationen, die auch mit Marktüberwachungskompetenzen betraut werden können, jedoch nirgendwo im Entwurf konkret bezeichnet sind und sich nur generisch als Marktüberwachungsorgane im Gesetzesentwurf befinden.

Von den vier aufgeführten Hauptanträgen wurden die ersten drei berücksichtigt und im Gesetzesentwurf umgesetzt. Dem letzten Punkt bezüglich der Bestimmung der an der Datenbearbeitung u.a. von sensiblen Daten beteiligten Marktüberwachungsorgane wurde nicht Rechnung getragen. Wir haben in unseren Stellungnahmen stets darauf hingewiesen, dass allfällige Differenzen, die nicht berücksichtigt werden können, auch im Bundesratsantrag auszuweisen seien.

1.9 Finanzen

1.9.1 Sachverhaltsabklärung bei einem Finanzdienstleister

Wir haben im Sommer 2012 eine Sachverhaltsabklärung bei einem Finanzdienstleister eingeleitet, um zu prüfen, ob die Erhebung und Verwaltung der Informationen den Datenschutzanforderungen gerecht werden.

Die erste Etappe des Verfahrens, in der in Zusammenarbeit mit der Bank die Tatsachen festgestellt werden sollten, ist abgeschlossen (vgl. unseren 20. Jahresbericht 2012/2013, Ziff. 1.8.7). Diese Phase, in der das kontrollierte Unternehmen nicht nur zur Mitarbeit verpflichtet ist, sondern auch die Möglichkeit zu einer Stellungnahme hat, bildet die Grundlage für den Schlussbericht, in dem die rechtlichen Erwägungen behandelt werden.

Das Verfahren ist zurzeit noch im Gange.

1.9.2 Abklärungen in Sachen kontaktlose Kreditkarten

Im Anschluss an einen Informationsaustausch mit der französischen Datenschutzbehörde und einer Kontaktaufnahme mit den wichtigsten Kreditkartenherausgebern haben wir eine Standortbestimmung bezüglich der kontaktlosen Zahlungsfunktion bei Kreditkarten vorgenommen.

Seit dem letzten Jahr haben sich einzelne Medien des Themas der Kreditkarten für kontaktloses Bezahlen angenommen. Dabei werden Analysen und Schlussfolgerungen unterschiedlicher Art entwickelt, die bezüglich der Persönlichkeitsrechte und der Datensicherheit zumeist besorgniserregend sind. Einige dieser Thesen wurden von der französischen Datenschutzbehörde (Commission nationale de l'informatique et des libertés, CNIL) in ihrer Mitteilung vom 1. Juli 2013 unter dem Titel «Sicherheit der kontaktlosen Kreditkarten: welche Fortschritte und Verbesserungen sind möglich?» erhärtet.

Wir haben auf dieser Grundlage und im Rahmen unserer gesetzlichen Aufgaben einen kurzen Informationsaustausch mit der französischen Behörde eingeleitet. So konnten wir in einem ersten Schritt die sowohl im Internet als auch in der gedruckten Presse zirkulierenden Informationen evaluieren. In der Folge wurde auch Kontakt zu den wichtigsten Kreditkartenherausgebern in der Schweiz aufgenommen, um ihnen Gelegenheit zu einer Stellungnahme zu geben.

Die seit dem letzten Jahr in der Schweiz herausgegebenen Karten sind grösstenteils bereits mit einer auf RFID basierenden Technologie versehen, die an verschiedenen, mit kompatiblen Terminals (Point of Sale, POS) ausgestatteten Verkaufsstellen

kontaktloses Bezahlen ermöglicht. Die drei grossen Lizenzgeber für Kreditkarten, MasterCard, Visa und American Express, haben ähnliche Produkte, allerdings unter verschiedenen Namen, eingeführt. Es handelt sich um die Systeme PayPass, payWave und ExpressPay.

Diese Bezeichnungen – die übrigens im Allgemeinen auf der Karte vermerkt sind – vermitteln schon einen kleinen Eindruck von der Funktionsweise: hält man die Karte in die Nähe eines POS, wird die Zahlung ohne Eingabe eines Codes oder eine Unterschrift auf der Rechnung verbucht. Die Identifikation erfolgt in diesem Fall über Radiofrequenzen. Die für den Kauf notwendigen Daten werden auf diesem Weg von der Karte zum Terminal übertragen. Ein Authentifizierungsprozess, beispielsweise mittels einer persönlichen Identifikationsnummer (PIN), bleibt grundsätzlich aus. Die Transaktion ist indes auf einen Höchstbetrag beschränkt, um den Schaden bei Verlust oder Diebstahl in Grenzen zu halten.

Die oben beschriebene Datenübertragung ist nicht den Verkaufsterminals vorbehalten. Sie kann daher als unerwünschtes Ergebnis dazu führen, dass diese Daten von einer unbefugten Person, die über die notwendige technologische Minimalausrüstung verfügt, ohne Wissen des Karteninhabers abgefangen und gelesen werden. Insbesondere an öffentlichen Orten besteht ein erhöhtes Risiko.

Im Anschluss an die Bestandsaufnahme zum Thema der Informationssicherheit – die eng mit der Haftpflicht des Inhabers der Datensammlung (hier der Kreditkartenanbieter) zusammenhängt – muss die Frage der informationellen Selbstbestimmung aufgegriffen werden. Dieses in der Bundesverfassung verankerte Grundrecht bedeutet, dass jedermann berechtigt ist, sich einer Datenbearbeitung zu widersetzen. Dieses Recht kann wie jedes Grundrecht eingeschränkt werden, aber nur unter klar bestimmten Voraussetzungen. Für einen solchen Fall sieht das DSG Rechtfertigungsgründe für eine zulässige Bearbeitung vor: die Einwilligung, das überwiegende private oder öffentliche Interesse oder das Gesetz. Vorliegend machen die befragten Kartenherausgeber aber keinerlei überwiegende private oder öffentliche Interessen für die beschriebene Bearbeitung geltend. Die Ausstattung der Karte mit dem RFID-Chip wird überdies nicht von der Entscheidung oder der Einwilligung des Kunden abhängig gemacht.

Die Informationspolitik der befragten Kartenherausgeber entspricht zwar dem Transparenzgebot, sie genügt aber nicht, um auf eine Einwilligung seitens des Kunden zu schliessen. Nehmen wir aber an, dass eine stillschweigende Einwilligung ausreicht, da a priori keine besonders schützenswerten Daten vom Chip aus weitergegeben werden. In diesem Fall müssen die wesentlichen Elemente der Einwilligung ebenfalls gegeben sein. Dabei handelt es sich einerseits um den Aspekt der Information und andererseits um die freie Willensbildung des Betroffenen. Hier liegt der Kern des Problems mit dem freien Einverständnis.

In Tat und Wahrheit begünstigt die heutige Situation im schweizerischen Markt der kontaktlosen Kreditkarten ein strukturelles Ungleichgewicht zwischen dem Kunden und der Bank. Eine Alternative, das heisst die Wahl eines Konkurrenten, der ein gleichwertiges Ersatzprodukt ohne RFID anbieten würde, besteht nämlich a priori nicht. Eine stillschweigende Einwilligung in die die allgemeinen Geschäftsbedingungen erfüllt somit die Kriterien des freien Einverständnisses nicht.

Wir fordern den Bankensektor auf, die Massnahmen zur Wahrung der persönlichen Freiheiten anzupassen, namentlich indem sie den Kunden die Möglichkeit der freien Wahl oder der Ablehnung der Technologie bieten. In Erwartung dieser Entwicklung weisen wir die Inhaber von Kreditkarten, die ihre Daten schützen möchten, darauf hin, dass sie ihre Karten in speziellen Portemonnaies, welche die Übertragung von Radiofrequenzen blockieren, oder in Aluminiumhüllen aufbewahren können.

1.9.3 Datenbekanntgabe an ausländische Steuerbehörden

Es gab im Bereich Datenbekanntgabe an ausländische Steuerbehörden verschiedene Gesetzesvorlagen. Wir haben unsere Positionen bei den Gesetzgebungsarbeiten zum Foreign Account Tax Compliance Act (FATCA) und zum Steueramtshilfegesetz eingebracht.

Im Berichtsjahr nahmen wir zu verschiedenen Gesetzesvorlagen Stellung, die die Übermittlung von Steuerdaten an ausländische Behörden regulieren. Zum Foreign Account Tax Compliance Act (FATCA) und dem Steueramtshilfegesetz äussern wir uns wie folgt:

Foreign Account Tax Compliance Act (FATCA)

In unserem 19. Tätigkeitsbericht 2011/2012, Ziff. 1.9.1, haben wir über dieses US-Gesetz und die aus unserer Sicht problematischen Datenbearbeitungen berichtet. Das Abkommen wurde am 14.2.2013 von der Schweiz unterzeichnet und wurde zugleich mit einem Ausführungsgesetz in die Vernehmlassung geschickt. Grundsätzlich gibt es zwei Modelle dieses Abkommens, die Schweiz hat sich dafür entschieden, Modell 2 zu übernehmen. Es handelt sich bei beiden Modellen um eine Art des automatisierten Informationsaustauschs. Bei Modell 2 rapportieren die FFI (Foreign Financial Institutes, also Banken, Versicherungen usw.) im Unterschied zu Modell 1 direkt an die amerikanische Steuerbehörde (Internal Revenue Service, IRS). Damit wird, nach Meinung des Staatssekretariats für internationale Finanzfragen (SIF), das Steuergeheimnis besser gewahrt. Amerikanische Konteninhaber, welche keine Einwilligung zur Bekanntgabe dieser Daten geben, können ihre Parteirechte vor der Bekanntgabe dieser Daten an den IRS wahrnehmen. Allerdings gibt es zurzeit gesetzgeberische Bestrebungen, diese Parteirechte einzuschränken.

Wir wurden zu einer Sitzung der Kommission für Wirtschaft und Abgaben (des Ständerats eingeladen und haben die Gelegenheit genutzt, unsere Bedenken zu äussern. Insbesondere haben wir bemängelt, dass zum Zeitpunkt der parlamentarischen Diskussion der Gesetzesvorlagen noch viele Unklarheiten bestanden. So war unklar, wie die Verträge zwischen den FFI und der IRS ausgestaltet, und welche datenschutzrechtlichen Bearbeitungsprinzipien darin berücksichtigt würden (insbesondere die Möglichkeit der Berichtigung und der Grundsatz der verhältnismässigen Datenbearbeitung). Das Parlament hat das Abkommen und die Gesetzesvorlage genehmigt. Inzwischen hat die IRS die Einführung von FATCA auf Juli 2014 verschoben.

Steueramtshilfegesetz

Das Steueramtshilfegesetz ist auf den 1. Januar 2013 in Kraft getreten. Wegen diverser internationaler Entwicklungen musste es im Verlauf dieses Jahres angepasst werden. In der ordentlichen Ämterkonsultation zu den geplanten Änderungen wurden wir leider nicht begrüsst. Wir verfassten deshalb einen Bericht zuhanden des Bundesrats, der die Botschaft zur Änderung des Steueramtshilfegesetzes verabschieden sollte. Darin bemängelten wir das Verfahren der nachträglichen Information der beschwerdeberechtigten Person. Bis anhin wurde dieser jeweils vor Übermittlung von Steuerinformationen an eine ersuchende Behörde im Ausland die Möglichkeit gegeben, sich rechtlich dagegen zu wehren.

Neu soll die beschwerdeberechtigte Person erst nach der Übermittlung der Informationen durch die Eidgenössische Steuerverwaltung (ESTV) informiert werden, wenn die ersuchende (ausländische) Behörde glaubhaft macht, dass der Zweck der Amtshilfe oder der Erfolg der Untersuchung durch die vorgängige Information vereitelt würde. Wir kritisierten die zu ungenaue Formulierung der Ausnahmeregelung und die Verhinderung der Transparenz von Datenbearbeitungen. Transparenz ist notwendig, damit eine Person ihre Persönlichkeitsrechte wahrnehmen kann. Der Bundesrat hat sich unseren Antrag abgelehnt. Das Thema Übermittlung von Steuerdaten an ausländische Behörden wird auch in Ziffer 1.9.5 des vorliegenden Berichts behandelt.

1.9.4 Revidierte Empfehlungen der GAFI (Groupe d'action financière)

Das Staatssekretariat für internationale Finanzfragen hat verschiedene Gesetzesänderungen in die Ämterkonsultation gegeben, die die Empfehlungen der GAFI (Groupe d'action financière) auf nationaler Basis umsetzen sollten. Zu diversen Punkten haben wir Stellung genommen.

Im Rahmen der Gesetzgebungsarbeiten zur Umsetzung der Empfehlungen der GAFI äusserten wir uns zur Einführung von Meldepflichten für Inhaberaktionäre, zur Definition der inländischen politisch exponierten Personen, zu den Terrorlisten und zu der Schaffung einer interdepartementalen Struktur zur Bekämpfung der Geldwäscherei, der Risikoevaluation und der Sicherstellung der Kohärenz der schweizerischen Politik mit den internationalen Entwicklungen. Mit den geplanten Gesetzesänderungen soll folgendes erreicht werden:

- Verbesserung der Transparenz bei den juristischen Personen, wobei hier insbesondere Meldepflichten für Inhaberaktionäre eingeführt werden.
- Ausdehnung des Begriffs der politisch exponierten Personen (PEP) auf inländische Personen und Angehörige zwischenstaatlicher Organisationen sowie die Einführung entsprechender risikobasierter Sorgfaltspflichten für Finanzintermediäre.
- Schwere Steuerdelikte werden als Vortaten zur Geldwäscherei qualifiziert.
- Barzahlungen über 100 000 Franken müssen über einen der Geldwäschereigesetzgebung unterstellten Finanzintermediär abgewickelt werden.
- Das Verdachtsmeldesystem soll verbessert und damit die Arbeit der Meldestelle für Geldwäscherei (MROS) erleichtert werden.
- Die Umsetzung der GAFI-Empfehlung zu gezielten Sanktionen im Bereich Terrorismusfinanzierung soll verbessert werden. In diesem Bereich soll eine interdepartementale Arbeitsgruppe geschaffen werden.

Grundsätzlich ist zu bemerken, dass in diesen Vorlagen in kurzer Zeit eine Vielzahl von Gesetzesartikeln in verschiedenen Erlassen aus datenschutzrechtlicher Sicht zu beurteilen war. Wir haben uns in der Folge auf einige Punkte konzentriert, die nachfolgend aufgeführt werden. Unserer Meinung nach führt die Einführung der Meldepflichten für Inhaberaktionäre und die damit verbundenen Dokumentationspflichten der Unternehmen zu einer grossen Anzahl von weiteren Personendatensammlungen. Dadurch steigt das Risiko für mögliche Persönlichkeitsverletzungen erheblich.

Weiter wird in der Botschaft zum Geldwäschereigesetz (GwG) zwar ausgeführt, welche Personen als den politisch exponierten Personen nahe stehend zu definieren sind. Der Kreis dieser Personen ist im Gesetz aber zu ungenau formuliert worden, wodurch die Finanzintermediäre verpflichtet werden, Personendaten in unverhältnismässigem Umfang zu bearbeiten.

Betreffend die Weitergabe von Terrorlisten durch das Eidgenössische Finanzdepartement an die Finanzintermediäre haben wir darauf hingewiesen, dass die Rechte der betroffenen Personen insbesondere auf Berichtigung gewahrt bleiben müssen

und die Geltendmachung dieser Rechte durch die mangelnde Transparenz der Datenbearbeitung gefährdet ist. Letztens haben wir uns zu den unklaren Angaben betreffend die Schaffung einer interdepartementalen Arbeitsgruppe geäussert. Das Staatssekretariat für internationale Finanzfragen (SIF) hat unsere Bedenken betreffend Einhaltung des Legalitätsprinzips entgegengenommen und teilweise berücksichtigt.

1.9.5 Datenübermittlung von Versicherungspolicen an die amerikanischen Steuerbehörden

Eine Datenübermittlung an die amerikanische Steuerbehörde IRS kann auch andere Informationen als rein finanzielle Daten zum Inhalt haben, wenn es um die Aufdeckung von Steuerdelikten geht.

Das schweizerische Recht kennt einige Möglichkeiten, durch die ein Bankkredit mit Ansprüchen aus einer Lebensversicherung abgesichert werden kann. Namentlich die Sicherungsabtretung und die Verpfändung. Diese zwei Rechtsgeschäfte unterstehen strengen Formvorschriften aus dem Bundesgesetz über den Versicherungsvertrag. Eine davon ist die Übergabe der Police an den Sicherheitsgeber, in diesem Fall eine Bank. Dies ist von Bedeutung, denn im Rahmen eines Amtshilfeverfahrens zwischen der amerikanischen Steuerbehörde IRS und der Eidgenössischen Steuerverwaltung (ESTV) ist es möglich, dass die Police zur Aufdeckung von Steuerdelikten herausverlangt wird. Es stellt sich diesbezüglich die Frage, inwiefern und in welcher Form sie übermittelt werden darf, und an welche Stelle man sich wenden soll, falls man von solch einem Verfahren betroffen ist.

Als erstinstanzliche Bundesbehörde ist die ESTV dem Datenschutzgesetz unterstellt. Es kommt bei erstinstanzlichen Verwaltungsverfahren sowie bei internationalen Amtshilfeverfahren zur Anwendung. Das Abkommen zwischen der Schweizerischen Eidgenossenschaft und den Vereinigten Staaten von Amerika zur Vermeidung der Doppelbesteuerung auf dem Gebiete der Einkommensteuern (DBA CH-USA) kommt auch für Versicherungsdaten, die z.B. bei einer schweizerischen Bank hinterlegt sind, zur Anwendung. Insofern sind die Bestimmungen beider Erlasse dort parallel anwendbar, wo das DBA CH-USA keine vom DSG abweichende Bestimmung vorsieht. In denjenigen Fällen, in denen Abweichungen vorliegen, geniesst das DBA als Spezialgesetz Vorrang.

Aus Sicht des DSG können Bundesorgane Personendaten nur bearbeiten, wenn dafür eine gesetzliche Grundlage besteht. Die grenzüberschreitende Bekanntgabe an eine ausländische Behörde gilt als Datenbearbeitung. Dementsprechend ist eine gesetzliche Grundlage notwendig. Bei der Bearbeitung von besonders schützenswerten Daten sowie Persönlichkeitsprofilen sind weitere Auflagen zu beachten:

Bundesorgane dürfen sie nur bearbeiten, wenn ein Gesetz im formellen Sinn es ausdrücklich vorsieht oder wenn die betroffene Person im Einzelfall eingewilligt oder ihre Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat.

Das DBA CH-USA gilt als Gesetz im formellen Sinn und kann somit eine Datenbekanntgabe durch die ESTV an den IRS rechtfertigen, wenn die Voraussetzungen für die Bekanntgabe gemäss Artikel 26 des Abkommens erfüllt sind. Aus diesem Artikel ergibt sich, dass eine Weitergabe in Form einer beglaubigten Kopie von einer bei einer Bank hinterlegten Lebensversicherungspolice nur zulässig ist, wenn diese notwendig ist für die Durchführung der Bestimmungen des DBA CH-USA oder zur Verhütung von Betrugsdelikten und dergleichen. Zudem ist eine Weitergabe durch den IRS an weitere Behörden nur unter Berücksichtigung strenger gesetzlicher Auflagen erlaubt.

Gemäss der Verordnung über die Amtshilfe nach Doppelbesteuerungsabkommen verläuft das Verfahren folgendermassen:

Die ESTV übermittelt der ersuchenden Behörde die nach schweizerischem Recht erhältlichen Informationen, die zur Durchführung der Abkommen notwendig sind. Im Voraus muss sie die betroffene Person schriftlich über Art und Umfang der zu übermittelnden Informationen benachrichtigen sowie jede Person, die nach dem Bundesgesetz über das Verwaltungsverfahren (VwVG) zur Beschwerde berechtigt ist.

Stimmen die beschwerdeberechtigten Personen der Informationsübermittlung schriftlich zu oder antworten sie innert 30 Tagen nach Empfang der Mitteilung der ESTV nicht, so übermittelt diese die Informationen unmittelbar nach Vorliegen der Zustimmung oder nach Ablauf der Frist. In den übrigen Fällen entscheidet sie in Form einer Verfügung. In dieser Hinsicht unterliegt der Entscheid der ESTV der Beschwerde nach den allgemeinen Bestimmungen über die Bundesrechtspflege.

Daraus ergibt sich, dass man zwingend seine Widerspruchsrechte bei der ESTV in der angegebenen Frist geltend machen muss. Als Alternative sieht Artikel 25 DSG bei schon erfolgten Übermittlungen die Möglichkeit vor, weitere – ausserhalb der gemäss DBA CH-USA vorgeschriebenen Verfahren – Widerspruchsrechte geltend zu machen.

Zusammengefasst und in Anbetracht der obenerwähnten Ausführungen ist festzuhalten, dass eine Übermittlung von beglaubigten Kopien und anderen Dokumenten an die IRS im Rahmen des DBA CH-USA vorgesehen ist. Wir raten deshalb jenen Personen, die von solch einem Sachverhalt betroffen sind, Kontakt mit der ESTV aufzunehmen, um ihre Rechte fristgemäss zu wahren und das weitere Vorgehen bestimmen zu können. Weitere Informationen zu diesem Thema sind in Ziffer 1.9.3 des vorliegenden Tätigkeitsberichts zu finden.

1.9.6 Zusammenarbeit mit der FINMA betreffend operationelle Risiken im Bankensektor

Die Eidgenössische Finanzmarktaufsicht (FINMA) hat uns im Laufe des Jahres 2013 zur Änderung des Rundschreibens 2008/21 «Operationelle Risiken – Banken», bzw. zu dem Teil betreffend die Bearbeitung elektronischer Kundendaten zu Rate gezogen.

Die Finanzkrise und die aussergewöhnlichen Verluste, die sie für die Wirtschaft verursachte, hatten eine neue Herangehensweise bezüglich der von Finanzdienstleistern eingegangenen operationellen Risiken zur Folge. Eine internationale Debatte zu diesem Thema führte zur Ausarbeitung neuer Regelungen, namentlich zur Empfehlung eines Mindestanteils an Eigenmitteln, um im Falle einer Liquiditätskrise die Verluste aufzufangen, und von Richtlinien für das mit den elektronischen Aktivitäten des Sektors verbundene Risikomanagement.

Die so entstandenen neuen Anforderungen konnten jedoch nicht mehr in die Vorschläge für eine Bankenregulierung – die Basler Abkommen III – einfliessen, da diese bereits eingeführt wurden, bevor konkrete Empfehlungen ausgearbeitet werden konnten. Daher hat die Eidgenössische Finanzmarktaufsicht (FINMA) damit begonnen, diese Anforderungen in dem oben erwähnten Rundschreiben auszugestalten und es den eingetretenen Entwicklungen anzupassen.

Darüber hinaus haben die erwähnte Krise und ihre Folgen für die Wirtschaft zu einer weit reichenden Bewusstseinsbildung in Sachen Sicherheit der elektronischen Daten von Kunden der schweizerischen Banken geführt. Die dadurch geweckten verschiedenen Begehrlichkeiten haben dabei eine bedeutende Rolle gespielt. Die Vertraulichkeit dieser Daten ist nicht gewährleistet, was einen dringenden Handlungsbedarf schafft. So werden im Rundschreiben in Anhang 3 «Umgang mit elektronischen Kundendaten» die neun Grundsätze für das sachgerechte Management von Risiken im Zusammenhang mit der Vertraulichkeit elektronischer Personendaten natürlicher Personen, deren Geschäftsbeziehungen in oder von der Schweiz aus geführt werden, formuliert.

Im Rahmen unserer Zusammenarbeit bezog sich unsere Tätigkeit namentlich auf die Fragen zum dritten von der FINMA entwickelten Grundsatz, «Datenspeicherort und -zugriff». Dieser sieht in manchen Fällen eine Pflicht zur Anonymisierung oder Pseudonymisierung der Daten vor. Der wichtigste Grundbestandteil ist die Frage von Kundendaten, die ausserhalb der Schweiz gespeichert werden oder auf die aus dem Ausland zugegriffen werden kann. Gegebenenfalls müssen Kundenidentifikationsdaten angemessen geschützt werden, beispielsweise durch Verschlüsselung oder Pseudonymisierung.

In Anbetracht der vorangehenden Ausführungen stellen wir in diesem Bereich eine willkommene Entwicklung fest und erachten die Zusammenarbeit mit der FINMA als zufrieden stellend.

1.10 International

1.10.1 Internationale Zusammenarbeit

Die internationale Zusammenarbeit spielt bei unseren Tätigkeiten eine unumgängliche Rolle. So war das Jahr 2013 geprägt von der Fortführung der Arbeiten zur Modernisierung des Übereinkommens 108, der Richtlinien der OECD und des europäischen Rechtsrahmens. Die Verstärkung der Zusammenarbeit zwischen den Datenschutzbehörden stand ebenfalls im Mittelpunkt der Diskussionen, namentlich in der Französischsprachigen Vereinigung der Datenschutzbehörden, der Internationalen Konferenz der Datenschutzbeauftragten und der gemeinsamen Kontrollinstanzen von Schengen, Eurodac und VIS.

Europarat

Die Modernisierung des Übereinkommens zum Schutz des Menschen bei der Verarbeitung personenbezogener Daten (Übereinkommen 108) ist weiterhin eine vorrangige Aktivität des Europarats. So wurde der vom beratenden Ausschuss des Übereinkommens 108 (T-PD) auf seiner 29. Plenarsitzung (siehe 20. Tätigkeitsbericht 2012/2013, Ziff. 1.10) angenommene Modernisierungsentwurf an einen Adhoc-Ausschuss (CAHDATA) weitergeleitet, der aus den Regierungsvertretern der Mitgliedstaaten des Europarats, von Uruguay, der Staaten mit ständigem Beobachterstatus im Europarat und einer Anzahl Drittstaaten, die einen Beitritt zum Übereinkommen erwägen, zusammengesetzt ist. Vertreter von internationalen Organisationen, Nichtregierungsorganisationen und der Wirtschaft beteiligen sich ebenfalls an den Arbeiten. Der CAHDATA ist beauftragt, den vom T-PD vorbereiteten Text fertig zu stellen und ein Änderungsprotokoll zum Übereinkommen auszuarbeiten. Er hielt 2013 eine erste Sitzung ab und sollte seine Arbeiten bis Ende 2014 abgeschlossen haben.

Der T-PD prüfte seinerseits den Entwurf für einen erläuternden Bericht zum revidierten Übereinkommen und legte den Rahmen der im Modernisierungsentwurf vorgesehenen künftigen Überwachungsmechanismen fest. Er befasste sich auch in erster Lesung mit einer Revision der Empfehlung R (89) 2 über den Schutz persönlicher Daten, die für Beschäftigungszwecke verwendet werden. Diese Revision ist aufgrund der technologischen Entwicklungen und der immer häufigeren Verwendung von Überwachungstechnologien am Arbeitsplatz notwendig geworden. Der Ausschuss prüfte auch einen Sachverständigenbericht über die Zweckmässigkeit einer Überarbeitung der Empfehlung R (87) 15 über die Nutzung personenbezogener Daten im Polizeibereich.

Da die Empfehlung integrierender Bestandteil zwingender internationaler Abkommen, insbesondere der Schengen-Abkommen ist, kam der Ausschuss zu dem

Schluss, dass eine Änderung nicht zweckmässig sei, sondern dass vielmehr eine neue Urkunde ausgearbeitet werden sollte, die den heutigen Datenschutzerfordernissen im Rahmen der polizeilichen Tätigkeiten und der Kriminalitätsbekämpfung gerecht werde. Der Ausschuss hat sein Arbeitsprogramm für 2014/2015 verabschiedet. Er wird sich namentlich mit dem automatischen Datenaustausch zu Steuer- und Finanzzwecken befassen.

Schliesslich pflegte der Ausschuss einen Meinungsaustausch über die PRISM-Affäre und die Enthüllungen über die Aktivitäten der NSA und ihre Folgen für die Menschenrechte und Grundfreiheiten. In einem Schreiben an das Ministerkomitee des Europarats fordert der Ausschuss Beratungen hinsichtlich einer Verstärkung der Massnahmen, mit denen der für die Bearbeitung von Personendaten im Rahmen von Überwachungsprogrammen zum Zwecke der nationalen Sicherheit geltende rechtliche Rahmen umgesetzt werden soll, um allen betroffenen Personen die Wahrung ihrer Rechte zu garantieren. Er erinnert daran, dass diese Bearbeitungen einer effektiven, unabhängigen und transparenten Kontrolle unterworfen sein müssen. Der Ausschuss prangert auch den Einsatz von Massenüberwachungstechniken an, welche die Achtung der Menschenrechte und die Demokratie in schwerwiegender Weise beeinträchtigen könnten.

Europäische Konferenz der Datenschutzbeauftragten

Die europäische Konferenz der Datenschutzbeauftragten fand auf Einladung der portugiesischen Datenschutzkommission vom 16. bis 17. Mai 2013 in Lissabon statt. Unter dem Titel «Protecting Privacy: the challenge ahead» bot die Konferenz die Gelegenheit, zu den laufenden Reformen des Datenschutzrechts in der Europäischen Union, im Europarat und in der OECD Bilanz zu ziehen. So haben wir den Fortschritt der Modernisierungsarbeiten zum Übereinkommen 108 und seinen Inhalt erläutert. Die Datenschutzbeauftragten berieten auch über die Frage, wie der Datenschutz in der Praxis, insbesondere im Internet und in den sozialen Netzwerken, wirksamer gestaltet werden kann. Die Zusammenarbeit der Datenschutzbehörden, die Probleme der Datensicherheit und die künftige Rolle der Datenschutzbehörden in der Europäischen Union wurden ebenfalls erörtert.

Die Konferenz verabschiedete drei Resolutionen (vgl. unsere Website www.derbeauftragte.ch, Der EDÖB – Internationale Zusammenarbeit – Europäische Konferenzen der Datenschutzbeauftragten). Die erste Resolution gilt der Zukunft des Datenschutzes in Europa. Die Beauftragten rufen die europäischen Staaten dazu auf, die Persönlichkeitsrechte zu stärken und die Annahme eines rechtlichen Rahmens zur Gewährleistung eines effektiven Datenschutzes in einer hochtechnologisierten und globalisierten Welt zu unterstützen.

Dieser Rahmen muss solide und kohärent sein und das gleiche Schutzniveau im öffentlichen und privaten Sektor sicherstellen. Er muss verstärkte Zusammenarbeitsmechanismen zwischen den Datenschutzbehörden ermöglichen, die über effektive Kompetenzen und Befugnisse sowie über ausreichende personelle und finanzielle Mittel verfügen müssen, um ihre Überwachungsaufgaben unabhängig wahrnehmen zu können.

Die zweite Resolution betrifft den Entwurf eines Freihandelsabkommens zwischen der Europäischen Union und den Vereinigten Staaten. Die Beauftragten verlangen, dass in dieses Abkommen auch Datenschutzbestimmungen aufgenommen werden. Die dritte Resolution betrifft die für Europol vorgesehenen neuen Rechtsgrundlagen und die notwendige Sicherstellung eines angemessenen Datenschutzniveaus.

Internationale Konferenz der Datenschutzbeauftragten

Die 35. Konferenz der Datenschutzbeauftragten fand vom 13. bis 26. September in Warschau statt. Vertreter aus rund vierzig Staaten, sowie Vertreter der Wirtschaft, der Verwaltungen, der Zivilgesellschaft und aus akademischen Kreisen kamen zusammen, um über die aktuellen Themen im Bereich des Datenschutzes zu beraten, darunter namentlich die Interoperabilität der Tools für den internationalen Datentransfer, den Datenzugriff der staatlichen Behörden, die digitale Kompetenz, die Big Data, die Computer- und Netzsicherheit, die Befugnisse und die Rolle der Datenschutzbehörden sowie die Problematik der mobilen Anwendungen. Letztere war Gegenstand einer Erklärung der Beauftragten zur «Applification» der Gesellschaft.

Mit dieser Erklärung verpflichten sich die Beauftragten, darauf zu achten, dass die Nutzer über eine bessere Erfahrung im Datenschutz verfügen, und sie planen, sich mit den verschiedenen Akteuren des öffentlichen und privaten Sektors über ihre Rolle und ihre Verantwortung zu beraten. Dabei erinnern sie daran, dass die Nutzer über die sie betreffenden Daten die Kontrolle behalten müssen, damit sie entscheiden können, welche Informationen zu welchem Zweck bekannt gegeben werden dürfen.

Überdies müssen die Applikationsentwickler den Datenschutzanforderungen schon ab der Planung einer Anwendung Rechnung tragen. Sie müssen eine klare Entscheidung über die Daten treffen, die sie für eine korrekte Funktionsweise der Applikation als notwendig erachten, und sie müssen sich vergewissern, dass keine anderen Daten ohne das aufgeklärte Einverständnis des Nutzers erhoben werden. Schliesslich betonen die Beauftragten, dass die Anbieter von Betriebssystemen ebenfalls für den Datenschutz auf ihren Plattformen verantwortlich sind. Die Beauftragten werden sich während des Jahres 2014 für eine Verbesserung des Datenschutzes im Bereich der Applikationen einsetzen und auch auf ihrer 36. Konferenz wieder auf diese Frage eingehen.

Die Beauftragten verabschiedeten mehrere Resolutionen (siehe unter www.derbeauftragte.ch, Der EDÖB – Internationale Zusammenarbeit – Internationale Konferenz der Datenschutzbeauftragten). In einer Resolution fordern die Beauftragten die Organisationen, die Profilbildung (Profiling bzw. Profilierung) betreiben, insbesondere auf:

- die Notwendigkeit und den praktischen Nutzen jeder Profilierungstätigkeit klar zu bestimmen und sicher zu stellen, dass vor der Profilierung angemessene Sicherheitsmassnahmen eingeführt werden;
- schon in der Planungsphase die Menge der im erforderlichen Rahmen zu rechtmässigen Zwecken erhobenen notwendigen Daten zu begrenzen und für die Aktualisierung und Richtigkeit der Daten zu sorgen;
- über die Profilierungsaktivitäten zu informieren, namentlich darüber, wie die Profile erstellt werden und welche Zwecke damit verfolgt werden;
- sich insbesondere bei Entscheidungen mit erheblichen rechtlichen Auswirkungen für Personen zu vergewissern, dass diese über ihr Recht informiert sind, Einsicht in die Personendaten zu nehmen und sie zu berichtigen und gegebenenfalls ein menschliches Eingreifen zu veranlassen;
- sicherzustellen, dass jede Profilierungstätigkeit angemessen überwacht wird.

In einer zweiten Resolution über Webtracking und Schutz der Privatsphäre anerkennen die Beauftragten, dass Tracking zwar gewisse Vorteile für die Verbraucher mit sich bringt, dass diese Aktivität aber eine beispiellose Gefahr für die Privatsphäre darstellt. Sie fordert daher die beteiligten Parteien auf:

- den Grundsatz der Zweckbindung zu beachten;
- die Nutzer über den Einsatz von Tracking-Elementen zu informieren und ihnen die Kontrolle über diese Elemente zu überlassen;
- auf den Einsatz von unsichtbaren Tracking-Methoden ausser zum Zwecke der Sicherheit oder der Aufdeckung von Betrug oder für die Netzwerkverwaltung zu verzichten;
- bei allen Tracking-Praktiken im Netz mit der angemessenen Transparenz vorzugehen;
- den Nutzern kundenfreundliche Tools anzubieten, mit denen sie die Erhebung und Verwendung ihrer Personendaten angemessen unter Kontrolle haben können;
- auf die Überwachung der Online-Aktivität von Kindern oder auf den für Kinder bestimmten Websites zu verzichten;

- der Privatsphäre schon bei der Planung Rechnung zu tragen und neue Projekte bereits zu Beginn entsprechend zu evaluieren;
- Techniken zur Verminderung der Auswirkungen auf die Privatsphäre, namentlich die Entpersonalisierung und die Verwendung von Pseudonymen, einzusetzen;
- die Festlegung technischer Normen zu fördern, um den Nutzern eine bessere Kontrolle zu ermöglichen.

Eine dritte Resolution verlangt eine verbesserte und verstärkte Transparenz im Bereich der Personendaten, ein wesentlicher Grundsatz, der es den Betroffenen ermöglicht, aufgeklärte Entscheidungen über die Verwendung ihrer Personendaten zu treffen und entsprechend zu handeln, um ihre Privatsphäre zu schützen und ihre Rechte geltend zu machen. Diese Resolution wird durch eine Resolution zur digitalen Kompetenz für alle ergänzt. Die digitale Welt ist integrierender Bestandteil unseres Alltags.

Angesichts der Herausforderung für den Datenschutz kann der rechtliche Rahmen nicht alle notwendigen Antworten und Garantien liefern. Die Beauftragten halten es daher für unerlässlich, eine allgemeine digitale Bildung zu fördern, gemeinsam mit den betroffenen Akteuren darauf hinzuwirken und ein gemeinsames Programm, namentlich im Hinblick auf eine Weiterbildung der digitalen Kompetenz zu beschliessen.

Rückblickend auf die Erklärungen und auf die bei früheren Konferenzen verabschiedeten Resolutionen nahmen die Beauftragten eine Resolution an, in der sie die Aufnahme des Datenschutzes und des Schutzes der Privatsphäre ins internationale Recht fordern (siehe insbesondere die Erklärung von Montreux, 13. Tätigkeitsbericht 2005/2006). Im Anschluss an die Enthüllungen von Edward Snowden erachten sie es für immer dringlicher, ein rechtlich verbindliches Abkommen über den Datenschutz zu schaffen, das die Achtung der Menschenrechte bei der Bearbeitung von Personendaten gewährleistet und gleichzeitig auf ausgewogene Weise der Sicherheit, den wirtschaftlichen Interessen und der Meinungsäusserungsfreiheit Rechnung trägt.

In zwei weiteren Resolutionen schliesslich – die eine über die Koordination des Gesetzesvollzugs auf internationaler Ebene, die andere über die strategische Ausrichtung der internationalen Konferenz – verpflichten sich die Beauftragten zu einer Verbesserung und Verstärkung ihrer Zusammenarbeit, namentlich um eine Koordination der transnationalen Untersuchungen zu gewährleisten. Ein globales und multilaterales Dokument, mit dem ein Rahmen für die Koordination der internationalen Tätigkeiten im Bereich der Kontrolle und des Informationsaustauschs geschaffen werden soll, wird der 36. Konferenz im Oktober 2014 auf Mauritius zur Annahme unterbreitet werden.

Arbeitsgruppe der OECD über die Informationssicherheit und den Schutz der Privatsphäre

Die Arbeitsgruppe beschäftigte sich dieses Jahr hauptsächlich mit der Vollendung der Richtlinien zu Sicherheit und Datenschutz. Nach intensiven Diskussionen wurde entschieden, an den acht bestehenden Grundprinzipien festzuhalten. Hingegen sind neu «privacy management»-Programme vorgesehen, mit welchen Unternehmen den Kunden und Behörden insbesondere alle für den Schutz der Privatsphäre relevanten Informationen systematisch zur Verfügung stellen müssen. Bei Verletzungen der Datensicherheit oder des Datenschutzes wird eine Informationspflicht eingeführt («data breach notification»). Weiter wurden die Kriterien für Datenübermittlungen ins Ausland präziser definiert, die internationale Zusammenarbeit verstärkt und die Sensibilisierung und Ausbildung der Bevölkerung hervorgehoben. Auch die Aufforderung, datenschutzfreundliche Technologien anzuwenden, wurde aufgenommen. Schliesslich wurde das Recht auf Privatsphäre als Grundrecht anerkannt. Nachdem auch das Ministerkomitee die Richtlinien verabschiedet hat, wird sich die Arbeitsgruppe nun mit der Umsetzung der revidierten Richtlinien befassen.

Die Rolle der Personendaten in der Wirtschaft nahm einen zentralen Platz in den Diskussionen ein. Durch die stark zunehmende Digitalisierung der Bearbeitung und Speicherung von Personendaten sind Cloud Computing, Big Data und Open Data permanente Themen der Arbeitsgruppe geworden. Es ist unbestritten, dass das wirtschaftliche Wachstum der Zukunft mit der Verwertung der in Unmengen anfallenden Daten verbunden ist (data driven economy). Dabei wird der Schutz der Privatsphäre von zentraler Bedeutung sein. Immer wichtiger wird abgesehen von Staat und Wirtschaft besonders die Rolle des Internet-Benutzers, der den grössten Teil der online verfügbaren Personendaten generiert und es meistens nicht einmal realisiert. Um insbesondere in diesem Umfeld dem Fehlen von Transparenz und Datenschutz entgegenzuwirken, sind weitere Arbeiten erforderlich. Angesichts des enormen Datenvolumens stellt sich gezwungenermassen die Frage der Sicherheit. Dabei entsteht auch eine Verbindung zu den kürzlich revidierten OECD-Richtlinien über Datenschutz und den noch zu revidierenden OECD-Richtlinien über Sicherheit.

Anzumerken ist, dass sich viele Mitgliedsländer besorgt zeigen, weil ihrer Meinung nach die Rahmenbedingungen zum Schutz der Privatsphäre bei Big Data, Open Data usw. die erhoffte wirtschaftliche Entwicklung hemmen könnten. Einig ist man sich jedoch darin, dass sich neue Datenbearbeitungsmethoden und -prozesse nach den vor Ort geltenden Datenschutzbestimmungen richten müssen und nicht umgekehrt.

Französischsprachige Vereinigung der Datenschutzbehörden

Die französischsprachige Vereinigung der Datenschutzbehörden (AFAPDP) hielt ihre siebte Konferenz und ihre Generalversammlung vom 21. bis 22. November 2013 in Marrakesch ab. Die Konferenz vereinte Vertreter aus 25 französischsprachigen Staaten. Für die Datenschutzbehörden dieser Staaten bot sie die Gelegenheit zu einem Austausch über aktuelle Fragen. So zogen sie eine Bilanz der laufenden gesetzgeberischen Entwicklungen auf nationaler und internationaler Ebene in den verschiedenen Regionen der Welt. Sie befassten sich mit der Frage der Verteidigung der Freiheiten im Internet, der Rolle der mobilen Geräte und Dienste in der Gesellschaft und den Herausforderungen, die sie für die Rechte und Grundfreiheiten darstellen. Sie tauschten sich auch aus über ihren Umgang mit der Kommunikation nach aussen und ihrer Medienpolitik, sowie über die Ausübung ihrer Kompetenzen, insbesondere ihrer Kontrollbefugnis.

Auf der Generalversammlung wählten die Datenschutzbehörden des französischsprachigen Raums Jean Chartier (Quebec) erneut zu ihrem Vorsitzenden. Jean-Philippe Walter, stellvertretender Eidgenössischer Beauftragter, wurde neben Marguerite Ouedraogo (Burkina Faso) als Vizevorsitzender wiedergewählt. Isabelle Falquier-Pierrotin wurde erneut in das Amt der Generalsekretärin gewählt.

Die Versammlung verabschiedete zudem drei Resolutionen (s. auf unserer Website www.derbeauftragte.ch, Der EDÖB – Internationale Zusammenarbeit – AFADPD). Der erste Text zielt darauf ab, eine grössere Transparenz bei den Praktiken der Erhebung von Personendaten durch die staatlichen Behörden zu gewährleisten und empfiehlt den Regierungen der Mitgliedstaaten der Internationalen Organisation der Frankophonie bei den Vereinten Nationen die Annahme eines verbindlichen Rechtsinstruments für den Datenschutz zu unterstützen, und den Ländern, die eine Datenschutzgesetzgebung eingeführt haben, wird nahe gelegt, den Beitritt zu dem Übereinkommen 108 und seinem Zusatzprotokoll zu beantragen.

Eine zweite Resolution bezieht sich auf die Ausbildung zur digitalen Kompetenz. Die französischsprachigen Behörden verpflichten sich, «weiterhin eine respektvolle und verantwortungsbewusste Nutzung der digitalen Technologien bei den Bürgern und den öffentlichen und privaten Organisationen zu fördern.» Daneben wollen sie «eine lebenslange und jedermann zugängliche Bildung in digitaler Kompetenz zu unterstützen», da es in einem Umfeld der sehr schnellen technologischen Entwicklungen notwendig ist, den Menschen Mittel in die Hand zu geben, um verantwortungsvolle und gleichberechtigte Akteure in der digitalen Welt zu werden.

Die dritte Resolution betrifft die Annahme eines Protokolls für die Zusammenarbeit unter den Mitgliedsbehörden der AFAPDP und die Einführung eines Rahmenverfahrens für die Datentransfers im französischsprachigen Raum, namentlich mittels

zwingender Unternehmensvorschriften (règles contraignantes d'entreprises, RCE). Diese Vorschriften bieten mehrere Vorteile. Sie ermöglichen insbesondere die Gewährleistung eines hohen Datenschutzniveaus. Dieses Instrument sieht die Einhaltung von datenschutzrechtlichen Grundprinzipien in Form von unternehmensinternen Verhaltenskodizes und Umsetzungsmechanismen vor (Datenschutzberater, Auditverfahren, Schulung, Beschwerdeverfahren).

Der EDÖB kann zum heutigen Zeitpunkt diese zwingenden Vorschriften nicht gutheissen. Wie für die europäischen Unternehmensvorschriften kann er jedoch die Garantien, die von anderen Datenschutzbehörden genehmigte RCE beim Datentransfer ins Ausland bieten, als ausreichend anerkennen.

Arbeitsgruppe Border, «Travel & Law Enforcement»

Die «Border, Travel & Law Enforcement Subgroup» (BTLE) ist eine Unterarbeitsgruppe, die von der Datenschutz-Arbeitsgruppe «Artikel 29» eingesetzt wurde. Sie hat die Aufgabe, die gesetzgeberischen Entwicklungen in den Bereichen Polizei, Grenzverkehr und Strafjustiz zu verfolgen, insbesondere soweit sie das Schengen-Acquis betreffen. In diesem Kontext bereitet sie Gutachten und Stellungnahmen vor, die anschliessend von der Arbeitsgruppe zu Artikel 29 der Richtlinie 95/46/EG angenommen werden. Wir haben an den verschiedenen Sitzungen im Berichtsjahr teilgenommen.

Die Unterarbeitsgruppe hat insbesondere eine Stellungnahme zum Projekt «intelligente Grenzen» im Anschluss an zwei Verordnungsvorschläge der Kommission vorbereitet. Diese betreffen zum Einen die Schaffung eines Einreise-/Ausreisesystems für die Registrierung der Ein- und Ausreisen der Staatsangehörigen von Drittländern, welche die Aussengrenzen der Mitgliedstaaten der Europäischen Union überqueren. Zum Anderen beziehen sie sich auf die Einrichtung eines Programms zur Registrierung von Reisenden.

Die Gruppe verfolgte aufmerksam die Schaffung eines europäischen Rahmens für die Bekanntgabe der PNR-Daten an Drittländer und für die Verwendung der PNR-Daten zu Strafverfolgungszwecken. Sie verfolgt auch die Revision des rechtlichen Rahmens des Lissabon-Vertrags der Europäischen Union. Die Gruppe erstellt zudem ein Gutachten zum Notwendigkeitsprinzip im Bereich des Datenschutzes. Seit der Snowden-Affäre leistet sie schliesslich auch aktiv Beratung in Bezug auf das PRISM-Programm und andere ähnliche Programme.

Koordinationsgruppe für die Kontrolle des SIS II

Am 11. Juni 2013 fand die erste offizielle Sitzung der Koordinationsgruppe des SIS II statt, welche im Anschluss an die am 9. April 2013 erfolgte Inkraftsetzung des SIS II die Gemeinsame Kontrollinstanz von Schengen (GKI) ersetzt hat. Die

Koordinationsgruppe SIS II ist gleich aufgebaut wie die mit der Kontrolle der Eurodac und des VIS betraute Gruppe und besteht ebenfalls aus dem Europäischen Datenschutzbeauftragten und den nationalen Datenschutzbehörden. Eine zweite Sitzung wurde am 17. Oktober 2013 abgehalten.

Die Gruppe verabschiedete bei diesen Tagungen ihre Geschäftsordnung, wählte ihre Vorsitzende und ihren Vize-Vorsitzenden und nahm ihr neues Arbeitsprogramm an, das in grossen Teilen das Programm der von der GKI initiierten Arbeiten übernimmt. Die Kommission setzte sie in Kenntnis über den reibungslosen Verlauf der Migration vom SIS I+ zu dem seit dem 9. April 2013 einsatzfähigen SIS II sowie über die diesbezügliche Informationskampagne. Bei der ersten Gruppensitzung berichtete die dänische Datenschutzbehörde von einem Hackerangriff auf das dänische N-SIS.

Im Anschluss an diese Information wurde ein Schreiben ausgearbeitet, in dem alle Datenschutzbehörden ihr nationales SIRENE-Büro ersuchten, sich zu vergewissern, dass sämtliche notwendigen Sicherheitsmassnahmen getroffen worden sind und kein ähnlicher Vorfall eingetreten ist. Schliesslich bildete die Gruppe eine Untergruppe mit dem Auftrag, ein Dokument zur Inspektion der Alarmsysteme SIS II, VIS und EURODAC auszuarbeiten.

Auf schweizerischer Ebene erfolgt die Koordination der Tätigkeiten im Zusammenhang mit Schengen in einer Koordinationsgruppe, der der EDÖB und die kantonalen Datenschutzbehörden angehören. Diese Gruppe kommt mindestens zwei Mal jährlich zusammen. Sie ermöglicht es den vertretenen Behörden, sich über die laufenden Entwicklungen und über die Tätigkeiten der GKI zu informieren, Kontrollaktivitäten zu planen und Informationen auszutauschen.

Europäische Arbeitsgruppe für die Behandlung datenschutzrelevanter Fälle

Das 25. Treffen der europäischen Arbeitsgruppe für die Behandlung datenschutzrelevanter Fälle («Case Handling Workshop») fand vom 2. bis 3. Oktober 2013 in Sarajevo statt. Die Arbeitsgruppe, die sich aus Vertretern von 29 nationalen Datenschutzbehörden zusammensetzt, befasste sich zunächst mit der Problematik der sozialen Netzwerke und des Internet. Daraus ging hervor, dass die Öffentlichkeit unbedingt für die Gefahren dieser Netzwerke sensibilisiert und ihrer Verantwortung bewusst gemacht werden muss; mehrere Datenschutzbehörden haben einen Leitfaden für jugendliche Nutzer ausgearbeitet. Der EDÖB seinerseits unterstützt die Initiative der Sensibilisierungskampagne «NetLa – Meine Daten gehören mir!», die sich an Kinder und Jugendliche richtet (s. unseren 18. Tätigkeitsbericht 2010/2011, Ziff. 3.3 und www.netla.ch).

In einer zweiten Phase drehte sich die Diskussion um die neuen datenschutzrechtlichen Herausforderungen, die durch den Einsatz der Mobiltelefonie entstehen,

namentlich durch die Verwendung des Mitteilungsdienstes «WhatsApp». Schliesslich wurden das Direktmarketing, die Verwendung biometrischer Daten sowie die Videoüberwachung im öffentlichen und privaten Sektor thematisiert und mittels einiger konkreter Fälle aus der Praxis der verschiedenen Datenschutzbehörden veranschaulicht. Die bosnische Datenschutzbehörde wird demnächst ein Handbuch zu allen auf dieser Tagung behandelten Themen herausgeben.

Besuch der georgischen Datenschutzbeauftragten

Auf Ersuchen des EDA haben wir die georgische Datenschutzbeauftragte sowie die Verantwortliche der Abteilung für internationale Beziehungen und Kommunikation zu einem Tag der Information und des Gedankenaustauschs über unsere Beratungs- und Kontrollpraktiken empfangen.

Das EDA organisierte im Dezember 2013 einen diplomatischen Besuch der georgischen Datenschutzbeauftragten. Das georgische Datenschutzgesetz ist seit dem Frühjahr 2013 in Kraft, und die Beauftragte hat ihr Amt im Laufe des Sommers angetreten. Ihre Dienststelle, die 14 Personen umfasst, ist im Aufbau begriffen. Ihre Tätigkeiten konzentrieren sich auf Beratungsaufgaben, und ab dem Jahr 2016 werden Kontrollverfahren im Privatsektor durchgeführt werden können.

In diesem Rahmen legt die Beauftragte besonderen Wert auf die Begegnung mit verschiedenen Datenschutzbehörden in Europa, um sich über ihre Organisation und ihre Arbeitsweise zu informieren. In Begleitung der Verantwortlichen der Abteilung internationale Beziehungen und Kommunikation wählte sie für ihren ersten Besuch unsere Behörde aus, da zwischen der Schweiz und Georgien sehr gute diplomatische Beziehungen bestehen.

So pflegten wir in unseren Räumlichkeiten einen eintägigen Gedankenaustausch. Wir empfingen die georgische Delegation, die vom Datenschutzberater des EDA begleitet wurde, zu einem offiziellen Besuch und stellten ihr unsere interne Organisation vor. Sodann erläuterten wir unsere Aufgaben im Einzelnen und führten zur Veranschaulichung verschiedene Beispiele aus unseren Beratungs- und Kontrolltätigkeiten an. Wir präsentierten ihr auch unsere Arbeitsmethode, die uns zur Verfügung stehenden Instrumente und Infrastrukturelemente und schliesslich unsere Sensibilisierungsmassnahmen für den Datenschutz.

2. Öffentlichkeitsprinzip

2.1 Zugangsgesuche

2.1.1 Departemente und Bundesämter

Gemäss den uns mitgeteilten Zahlen sind im Jahr 2013 bei den Bundesbehörden insgesamt 469 Zugangsgesuche eingereicht worden. In 218 Fällen gewährten die Behörden einen vollständigen, in 103 einen teilweisen Zugang. Bei 122 Gesuchen wurde die Einsichtnahme vollständig verweigert. 18 Zugangsgesuche wurden zurückgezogen, wobei dies vermutlich in der Hälfte der Fälle aufgrund der durch die Behörde veranschlagten Gebühren erfolgte. Acht Fälle meldeten die Behörden Ende Berichtsjahr noch als hängig.

Was die Gesamtzahl der Zugangsgesuche und die Praxis der Behörden im Umgang mit diesen anbelangt, zeigen die Zahlen mit Blick auf vergangene Jahre insgesamt ein stabiles Bild. Das spricht dafür, dass sich das Öffentlichkeitsgesetz (BGÖ) als nützliches und griffiges Instrument der Informationsbeschaffung für Private und Medienschaffende etabliert hat. Gleichwohl bleibt zu hoffen, dass der Bekanntheitsgrad und die Nutzung des BGÖ weiter zunehmen.

Am meisten Zugangsgesuche für das Jahr 2013 auf Stufe Amt meldete uns das BAG (33 Gesuche). Danach folgen das BLW (30), das ENSI (26) und das BFM (24). Bei den Departementen liegen das UVEK (100 Gesuche), das EDI (92) und das EDA (73) an der Spitze. Besonders transparenzfreundlich fallen die Quoten beim EDA aus, welches von insgesamt 73 Gesuchen 63 vollständig positiv beantwortete, in fünf Fällen den Zugang teilweise gewährte und bei lediglich fünf Gesuchen den Zugang vollständig verweigerte. 19 von 71 Behörden meldeten uns für das Berichtsjahr, dass bei ihnen kein einziges Zugangsgesuch eingegangen sei. Der Beauftragte selbst sah sich im Berichtsjahr mit 14 Zugangsgesuchen konfrontiert, wovon er den Zugang zehnmal vollständig und dreimal teilweise gewährte und in einem Fall vollständig verweigerte.

Wie bereits im letzten Jahr wurden auch im Berichtsjahr nur noch relativ moderate Gebühren im Gesamtumfang von CHF 6502.50 in Rechnung gestellt (Vorjahr 6300 Franken). Interessant ist dabei der Umstand, dass während drei Departemente und die Bundeskanzlei überhaupt keine Gebühren erhoben, vier Departemente ihren Zeitaufwand den jeweiligen Gesuchstellern teilweise verrechneten. Von den insgesamt erhobenen Gebühren über CHF 6502.50 entfiel knapp die Hälfte alleine auf das Eidgenössische Nuklearsicherheitsinspektorat ENSI. Obwohl von den gesamthaft in Rechnung gestellten Gebühren nur gerade 2015 Franken auf die Einheiten der zentralen Bundesverwaltung entfielen, erachtete es die Generalsekretärenkonferenz

GSK als notwendig, eine Arbeitsgruppe einzusetzen, welche Richtlinien zur Gebührenerhebung für Zugangsgesuche nach BGÖ erarbeiten sollte (vgl. Ziffer 2.6.1 des vorliegenden Tätigkeitsberichts).

Was den Zeitaufwand für die Bearbeitung der Zugangsgesuche anbelangt, weisen wir erneut darauf hin, dass die Behörden nicht verpflichtet sind, diesen zu erfassen, und dass es 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 erstmals wieder abgenommen (2010: 815 Stunden; 2011: 1519 Stunden; 2012: 2155 Stunden; 2013: 1707 Stunden). Der Zeitaufwand für die Mitwirkung in Schlichtungsverfahren erhöhte sich von 480 Stunden im 2012 um über 60 Prozent auf 778 Stunden im 2013.

2.1.2 Parlamentsdienste

Die Parlamentsdienste meldeten für das Berichtsjahr kein einziges Zugangsgesuch.

2.1.3 Bundesanwaltschaft

Die Bundesanwaltschaft meldete uns für das Jahr 2013 ein Zugangsgesuch, wobei es den Zugang vollständig verweigerte.

2.2 Schlichtungsanträge

Im 2013 wurden insgesamt 76 Schlichtungsanträge eingereicht (2012: 78). Im Gegensatz zum Vorjahr wurden im Berichtsjahr wieder am meisten Anträge von Privatpersonen eingereicht (27), dicht gefolgt von Medienschaffenden (24). Diese Zahlen lassen folgende Schlüsse und Bemerkungen zu: In 225 Fällen verweigerte die Bundesverwaltung den Zugang vollständig (122) respektive teilweise (103). Dem stehen 76 bei uns eingereichte Schlichtungsanträge gegenüber. Im Berichtsjahr wurde somit in rund 30 Prozent aller Fälle von ganz oder teilweise abgelehnten Zugangsgesuchen ein Schlichtungsantrag eingereicht.

Insgesamt konnten im Berichtsjahr 81 Schlichtungsanträge abgeschlossen werden. Davon stammen 31 Anträge aus dem Berichtsjahr selbst, 30 aus dem Jahr 2012 und 17 noch aus dem Jahr 2011. In 16 Fällen konnte zwischen den Beteiligten eine Schlichtung erzielt werden. Insgesamt erliessen wir 37 Empfehlungen, wo keine einvernehmliche Lösung möglich oder von vornherein ersichtlich war. 13 Schlichtungsanträge wurden zurückgezogen und in sieben Fällen waren die Voraussetzungen für die Anwendung des Öffentlichkeitsgesetzes nicht gegeben. In vier Fällen wurde der Schlichtungsantrag nicht fristgerecht eingereicht.

Antragstellende müssen aufgrund der nach wie vor ungenügenden personellen Ressourcenlage weiterhin länger als die gesetzlich vorgesehenen 30 Tage auf die Durchführung eines Schlichtungsverfahrens warten.

2.3 Abgeschlossene Schlichtungsverfahren

2.3.1 Empfehlungen

Nachfolgend werden die im Jahr 2013 erlassenen Empfehlungen im Bereich des Öffentlichkeitsgesetzes (BGÖ) kurz zusammengefasst. Die vollständigen Versionen sind auf unserer Webseite www.derbeauftragte.ch, Öffentlichkeitprinzip – Empfehlungen – 2013 zu finden.

1. Empfehlung armasuisse / Benützungsvereinbarung Militärflugplatz Buochs (25. Januar 2013)

Der Antragsteller verlangte Zugang zur aktuellen Vereinbarung über die zivile Mitbenützung des Militärflugplatzes Buochs zwischen armasuisse und der Airport Buochs AG, inkl. Anhänge und Beilagen. armasuisse verweigerte den Zugang vollständig unter Verweis auf den Schutz der freien Meinungs- und Willensbildung der Behörde sowie auf Berufs-, Geschäfts- und Fabrikationsgeheimnisse. Trotz mehrmaliger schriftlicher und telefonischer Aufforderung durch den Beauftragten reichte armasuisse eine detaillierte begründete Stellungnahme und die verlangten amtlichen Dokumente nicht ein.

In seiner Empfehlung kam der Beauftragte zum Schluss, dass armasuisse durch dieses Versäumnis ihre Mitwirkungspflicht verletzt hat. Da die Beweislast zur Widerlegung der Vermutung des freien Zugangs zu amtlichen Dokumenten der Behörde obliegt, erachtete der Beauftragte den Beweis über das Vorliegen eines Ausnahmetatbestandes zur Rechtfertigung einer Zugangsverweigerung als nicht erbracht und er empfahl, die verlangten Dokumente unter Vorbehalt allfälliger Ausnahmebestimmungen des BGÖ zugänglich zu machen.

2. Empfehlung armasuisse / Dokumente im Zusammenhang mit einem geplanten Grundstücksverkauf (28. Januar 2013)

Die Antragsteller reichten bei armasuisse ein Kaufangebot für ein Grundstück in der Gemeinde Y ein. Daraufhin teilte ihnen armasuisse mit, dass das betreffende Grundstück entgegen der Ausschreibung nicht zu verkaufen sei. In der Folge verlangten die Antragsteller Kopien aller amtlichen Dokumente im Zusammenhang mit diesem Verkaufsgeschäft. armasuisse teilte den Antragstellern die Gründe mit, welche zu diesem Kurswechsel geführt hatten, und erklärte sich allenfalls bereit, ihnen eine beschränkte Einsicht in die verlangten Unterlagen vor Ort zu gewähren. In einem weiteren Schreiben bestätigten die Antragsteller ihr Zugangsgesuch und wiesen armasuisse darauf hin, dass ihnen als Antragstellende die Wahl zustehe, Kopien oder bloss Einsicht vor Ort zu verlangen.

Trotz mehrmaliger schriftlicher und telefonischer Aufforderung kam armasuisse dem Ersuchen des Beauftragten nicht nach, eine detailliert begründete Stellungnahme und die verlangten amtlichen Dokumente einzureichen.

In seiner Empfehlung kam der Beauftragte zum Schluss, dass armasuisse durch dieses Versäumnis ihre Mitwirkungspflicht verletzt hat. Da die Beweislast zur Widerlegung der Vermutung des freien Zugangs zu amtlichen Dokumenten der Behörde obliegt, erachtete der Beauftragte den Beweis über das Vorliegen eines Ausnahmetatbestandes zur Rechtfertigung einer Zugangsverweigerung/-beschränkung als nicht erbracht. Auch war für ihn nicht nachvollziehbar, weshalb armasuisse bloss eine (beschränkte) Einsichtnahme vor Ort in Betracht gezogen hatte. Er empfahl, den Antragstellern die verlangten Dokumente unter Vorbehalt allfälliger Ausnahmebestimmungen des BGÖ in Kopie zuzustellen.

3. Empfehlung Staatssekretariat für Wirtschaft SECO/ Erfolgsrechnungen und Bilanzen Vollzugskostenbeiträge (20. Februar 2013)

Der Antragsteller verlangte beim SECO Erfolgsrechnungen und Bilanzen der paritätischen Kommissionen, welche diese gestützt auf eine Klausel in der Allgemeinverbindlicherklärung ihrer Gesamtarbeitsverträge dem SECO einreichen müssen.

Das SECO lehnte die Einsicht mit der Begründung ab, ein selbstständiger Anspruch eines Dritten auf Einsicht in diese Dokumente sei gesetzlich nicht vorgesehen. Ausserdem enthielten die verlangten Dokumente Geschäftsgeheimnisse, und es sei auch die Privatsphäre Dritter beeinträchtigt.

In seiner Empfehlung kam der Beauftragte zum Schluss, dass die Erfolgsrechnungen und Bilanzen keine Geschäftsgeheimnisse enthalten, da keine Wettbewerbssituation vorhanden ist. Hinsichtlich der Personendaten empfahl er die Offenlegung derselben dort, wo ein überwiegendes öffentliches Interesse besteht.

4. Empfehlung VBS / Bericht Feststellungen Kassenrevision bei der Gebirgsinfanteriebrigade 12 (4. März 2013)

Der Antragsteller verlangte Zugang zu allen Unterlagen im Zusammenhang mit einer VBS-internen Untersuchung wegen finanzieller Unregelmässigkeiten bei der Verwendung von Sponsorengeldern durch eine militärische Einheit. Das VBS verweigerte den Zugang unter anderem mit der Begründung, die Dokumente enthielten Personendaten des damaligen Brigadekommandanten, welche nicht anonymisierbar seien. Ausserdem sei kein überwiegendes öffentliches Interesse an den nachgesuchten Informationen auszumachen. Im Übrigen machte es geltend, dass der Schutz der Privatsphäre als durch die Verfassung und die EMRK geschütztes Grundrecht höher zu gewichten sei als das Recht auf Zugang zu amtlichen Informationen, welches nur indirekt verfassungsrechtlich geschützt werde.

Der Beauftragte hielt in seiner Empfehlung fest, dass bereits aus Sinn und Zweck des Öffentlichkeitsgesetzes ein gewichtiges öffentliches Interesse an amtlichen Dokumenten resultiere. Für ein besonderes öffentliches Interesse spreche vorliegend zudem der Umstand, dass es sich um eine möglicherweise vorschriftswidrige Verwendung von privaten Sponsorengeldern durch einen Angestellten des Bundes in hoher Stellung und mit besonderer Funktion handle.

Im Ergebnis kam der Beauftragte zum Schluss, die Interessenabwägung zwischen einem Zugang aufgrund eines öffentlichen Interesses und dem Interesse des Betroffenen am Schutz seiner Privatsphäre müsse zugunsten des Zugangs ausfallen. Er wies das VBS an, vor einer allfälligen Zugangsgewährung den Betroffenen anzuhören und die in den Dokumenten vorhandenen besonders schützenswerten Personendaten unkenntlich zu machen.

5. Empfehlung ENSI / Messdaten der Kamininstrumentierung des Kernkraftwerks Mühleberg (KKM) (18. März 2013)

Der Antragsteller verlangte Einsicht in die Daten der laufend erfassten Aktivität der Abluft des Kernkraftwerks Mühleberg für die Zeiträume Juli und August 2012 sowie – zu Vergleichszwecken – Juli bis und mit September 2011. Das ENSI verweigerte den Zugang unter anderem mit der Begründung, dass die verlangten Messdaten nicht in einer Form vorlägen, die es erlaube, aus aufgezeichneten Informationen mittels eines einfachen elektronischen Vorgangs ein amtliches Dokument zu erstellen.

Weiter machte das ENSI darauf aufmerksam, dass die verlangten Messdaten, welche ihm ausschliesslich für eine Intervention im Notfall übermittelt werden, gemäss den Bestimmungen des einschlägigen Betriebsreglements nach spätestens 30 Tagen automatisch und unwiderrufbar gelöscht worden seien.

Wie der Beauftragte in seiner Empfehlung festhielt, ist aufgrund der schriftlichen Bestätigung des ENSI über die erfolgte Löschung der Daten sowie der Einsicht in das referenzierte Betriebsreglement davon auszugehen, dass die verlangten Messdaten spätestens zum Zeitpunkt der Eröffnung des Schlichtungsverfahrens bereits restlos gelöscht waren. Folglich seien sie nicht mehr aufgezeichnet und damit auch nicht mehr im Besitz des ENSI gewesen. Der Beauftragte wies jedoch darauf hin, dass das ENSI seiner Ansicht nach die zum Zeitpunkt des Eingangs des Gesuches noch vorhandenen Daten hätte solange sichern können, bis das Zugangsverfahren abgeschlossen gewesen wäre.

Er befasste sich auch mit der Frage, ob es dem ENSI möglich gewesen wäre, mittels eines einfachen elektronischen Vorgangs aus aufgezeichneten Informationen ein amtliches Dokument zu erstellen. Dabei beschränkte er sich auf die Feststellung, dass diese Erfordernis bereits dann zu bejahen sei, wenn in der angefragten Behörde ein einzelner Mitarbeiter beschäftigt werde, dem es ohne unverhältnismässigen

Aufwand möglich sei, mit der entsprechenden Software vorhandene Daten in ein amtliches Dokument umzuwandeln. Im Ergebnis stützte der Beauftragte die Zugangsverweigerung des ENSI mit der Begründung, dass die tatsächliche Löschung der verlangten Daten die Gewährung des Zugangs verunmögliche.

6. Empfehlung BJ / Akten eines Gerichtsverfahrens (21. März 2013)

Der Antragsteller richtete ein Gesuch um Zugang an das Bundesamt für Justiz (BJ) betreffend die Sache Portmann c. Schweiz beim Europäischen Gerichtshof für Menschenrechte (EGMR). Der Antragsteller ersuchte um Zugang zur Beschwerde und zu den Bemerkungen des Beschwerdeführers sowie zu den von der Schweiz eingereichten Bemerkungen.

Die Behörde teilte dem Antragsteller die Abweisung des Gesuchs um Zugang zu den beantragten Dokumenten mit der Begründung mit, dass das Gesetz im vorliegenden Fall nicht anwendbar sei, da ein Verfahren vor der Grossen Kammer hängig sei.

Der Beauftragte stellte fest, dass das aus fünf Richtern bestehende Kollegium der Grossen Kammer den Antrag auf Rückweisung abgewiesen hat, sodass das am 11. Oktober 2011 gefällte Urteil der zweiten Sektion des EGMR demnach am 8. März 2012 aufgrund von Artikel 44 § 2 lit. C EGMR rechtskräftig geworden ist. Bei den beantragten Dokumenten handelt es sich um Prozessschriften, die von den Parteien in der Sache Portmann c. Schweiz im Rahmen des Gerichtsverfahrens vor dem EGMR verfasst und hinterlegt wurden. Der Beauftragte kam demnach zum Schluss, dass diese Unterlagen aufgrund dessen während und nach Abschluss des Verfahrens vor dem EGMR vom materiellen Geltungsbereich des BGÖ ausgenommen sind.

7. Empfehlung BJ / Verfahren zur Einstellung und Auswahl der Kandidaten für das Amt eines Richters beim EGMR (25. März 2013)

Der Antragsteller richtete ein Zugangsgesuch an das Bundesamt für Justiz (BJ) betreffend die im Jahr 2010 erfolgte Ausschreibung der Stelle eines Richters für die Schweiz beim Europäischen Gerichtshof für Menschenrechte (EGMR) sowie das Verfahren zur Einstellung und Auswahl der drei durch die Schweiz der parlamentarischen Versammlung des Europarats zur Wahl vorgestellten Kandidaten.

Das BJ hiess das Gesuch um Zugang teilweise gut und gab dem Gesuchsteller gewisse Informationen zum Einstellungs- und Auswahlprozess bekannt, und zwar die Zahl der Bewerber sowie die Liste der drei an das beratende Sachverständigengremium für die Wahl der Richter am EGMR weitergeleiteten Namen. Die Behörde weigerte sich hingegen ausdrücklich, die Liste der Kandidaten und die Klassierung der Kandidaten bekannt zu geben.

Der Beauftragte hiess die Beschwerdegründe des Gesuchstellers nur sehr begrenzt gut und befand, dass das BJ einzig verpflichtet sei, dem Gesuchsteller eine Liste der betreffenden amtlichen Dokumente zuzustellen. Auch müsse es ihn auffordern, sein zweites Gesuch genauer auszuführen und auf dieser Grundlage zu beurteilen, ob der Zugang zu den verlangten Dokumenten gewährt werden könne.

8. Empfehlung ESTV / Gesuch um Zugang zu Daten betreffend die direkte Bundessteuer (22. August 2013)

Der Gesuchsteller beantragte bei der Eidgenössischen Steuerverwaltung (ESTV) die Daten betreffend die direkte Bundessteuer ab dem Jahr 1990 in Form einer strukturierten Datenbank. Der Beauftragte stellte fest, dass gemäss den von der ESTV erteilten Informationen die zur Erstellung des verlangten Dokuments notwendigen Vorgänge die Ausführung zusätzlicher komplexer Programmierungsvorgänge, das heisst eine von einem spezialisierten Mitarbeiter vorgenommene manuelle Eingabe neuer Abfragen in die verschiedenen betroffenen Datenbanken erfordert.

Der Beauftragte gelangte zu dem Schluss, dass es sich angesichts der Komplexität, des Umfangs und der Dauer der zur Erstellung des beantragten Dokuments notwendigen Vorgänge im vorliegenden Fall nicht um eine einfache elektronische Bearbeitung im Sinne des BGÖ handelt. Somit folgerte der Beauftragte abschliessend, dass die ESTV nicht verpflichtet sei, den vom Gesuchsteller beantragten Zugang zu den verlangten Dokumenten zu gewähren.

9. Empfehlung ENSI / Berichte zur Erdbebensicherheit des Kraftwerks Mühleberg (10. April 2013)

Der Antragsteller verlangte Zugang zu zwei Berichten über die Erdbebensicherheit des Kraftwerks Mühleberg. Das ENSI verweigerte ihm diesen mit dem Hinweis, dass er zugleich als Partei in einem kantonalen Verwaltungsverfahren Akteneinsicht in dieselben Dokumente verlangt habe. Über seinen Antrag, die bezeichneten Dokumente zu den Verfahrensakten zu nehmen, sei jedoch noch nicht entschieden worden. Weiter hielt das ENSI fest, dass Dokumente eines erstinstanzlichen Verwaltungsverfahrens zwar grundsätzlich dem Recht auf Zugang unterstünden, dies jedoch erst, wenn die entsprechende Verfügung rechtskräftig sei.

Der Beauftragte hielt in seiner Empfehlung fest, dass die verlangten Dokumente zwar zum Zeitpunkt des Erlasses der Empfehlung erwiesenermassen (noch) nicht zu den kantonalen Verfahrensakten gehörten, über deren Beizug in das laufende Verfahren jedoch noch nicht entschieden worden sei. Er empfahl daher, einen Zugang bis zum abschliessenden Entscheid der kantonalen Behörde über den Einbezug der bezeichneten Berichte zu den Verfahrensakten aufzuschieben.

10. Empfehlung BAZL / Dokumente zum Passagier-Profiling an Schweizer Flughäfen (15. April 2013)

Der Antragsteller verlangte Zugang zu bestehenden Plänen oder Richtlinien betreffend das Passagier-Profiling an Schweizer Flughäfen. Das BAZL verweigerte diesen unter anderem mit der Begründung, dass das entsprechende Dokument im Falle einer Zugangsgewährung die innere und äussere Sicherheit der Schweiz ernsthaft gefährde. In Kenntnis der konkreten Profiling-Massnahmen sei es für potentiell Terrorverdächtige ein Leichtes, diese zu umgehen. Das betreffende Dokument sei deshalb auch als vertraulich klassifiziert.

Der Beauftragte hielt in seiner Empfehlung fest, dass er die Auffassung des BAZL, wonach eine Einsicht in Dokumente betreffend konkrete Profiling-Massnahmen eine Gefahr für die Flugsicherheit darstelle, grundsätzlich teile. Unter Bezugnahme auf das zu beurteilende Dokument kam er jedoch zum Schluss, dass dieses sehr offen formuliert sei und daher keinerlei Informationen enthalte, welche im Falle der Bekanntgabe eine Gefährdung der Sicherheit zur Folge hätten.

Im Ergebnis empfahl der Beauftragte den Zugang zum verlangten Dokument nach einer entsprechenden Entklassifizierung zu gewähren.

11. Empfehlung EFD / Anpassung des Schweizerischen Steuerrechts an die OECD-Standards (27. Mai 2013)

Der Antragsteller verlangte beim EFD Zugang zu einem Bericht betreffend die Rolle der Verwaltung bei der Anpassung der Voraussetzungen der Amtshilfe in Steuersachen an den OECD-Standard sowie zu dessen Beilagen. Das EFD lehnte den Zugang zu den verlangten Dokumenten mit der Begründung ab, es handle sich um einen Bericht, welcher gestützt auf einen Bundesratsbeschluss und zu Handen des Bundesrates verfasst worden und daher Bestandteil eines Bundesratsgeschäftes sei, weshalb er nicht dem BGÖ unterstellt sei. Ausserdem habe bis zur Unterschrift der Departementschefin unter das Aussprachepapier lediglich ein Entwurf des Berichtes bestanden, weshalb er nicht als amtliches Dokument gelte.

Sodann unterscheide sich der Bericht in seiner Entstehungsgeschichte und in seiner verfahrensrechtlichen Stellung nicht vom Aussprachepapier, dem er als Beilage angefügt worden sei. Es sei zudem sachlich geboten, den Bericht als Teil des Mitberichtsverfahrens zu behandeln und daher vom BGÖ auszunehmen.

In der vorliegenden Empfehlung kam der Beauftragte zum Schluss, dass der Bericht ein amtliches und fertig gestelltes Dokument darstellt, welches jedoch nicht als Teil des Aussprachepapiers zu qualifizieren ist, sondern als dessen Beilage gilt. Des Weiteren kann der Bericht gemäss Ansicht des Beauftragten nicht einem Dokument aus dem Mitberichtsverfahren gleichgestellt werden. Der Beauftragte empfahl daher dem EFD, dem Antragsteller eine Auflistung der dem Bericht angehängten Dokumente zuzustellen und diesen aufzufordern, sein Zugangsgesuch diesbezüglich zu präzisieren.

12. Empfehlung SECO / Untersuchungsunterlagen über exportierte Handgranaten nach Syrien (28. Mai 2013)

Der Antragsteller verlangte Zugang zu Untersuchungsunterlagen über aus der Schweiz exportierte Handgranaten. Das SECO verweigerte den Zugang, unter anderem mit der Begründung, dass die Unterlagen nicht in den persönlichen Geltungsbereich des BGÖ fielen und Dokumente des Mitberichtsverfahrens darstellten.

Der Beauftragte kam in der Empfehlung zum Schluss, dass die verlangten Unterlagen als Dokumente des Gesamtbundesrates zu qualifizieren bzw. Teil des Mitberichtsverfahrens sind, weshalb der Zugang zu verweigern sei. Sodann sei der Zugang zu den übrigen Dokumenten aufgrund der Sicherheit des Landes und der aussenpolitischen Beziehungen zu verweigern. Schliesslich hielt der Beauftragte fest, dass zu zwei verlangten Dokumenten kein Rechtsanspruch besteht, weil diese von der Geschäftsprüfungskommission des Nationalrates erstellt worden sowie an den Bundesrat gerichtet sind und somit ein Spezialtatbestand zum BGÖ vorliegt.

Das Parlamentsgesetz hält nämlich fest, dass Beratungen und Sitzungsunterlagen der Kommissionen vertraulich sind. In Bezug auf zwei diplomatische Noten kam der Beauftragte hingegen zum Schluss, dass der Zugang zu diesen zu gewähren ist, da seitens des SECO kein rechtsgenüglicher Beweis für einen Ausnahmegrund des BGÖ vorgebracht worden ist.

13. Empfehlung ENSI / Dokumente zu internem Brand bzw. interner Überflutung des Kraftwerks Mühleberg (27. Juni 2013)

Der Antragsteller verlangte Zugang zu Akten-Anschnitten betreffend einen internen Brand bzw. eine Überflutung des Kraftwerks Mühleberg. Das ENSI verweigerte ihm den Zugang unter Verweis auf eine mögliche Gefährdung der inneren Sicherheit der Schweiz und verwies ausserdem auf die Klassifizierung der betreffenden Dokumente als vertraulich. Weiter wies das ENSI darauf hin, dass der Antragsteller bereits in einem Verwaltungsverfahren als Kollektiveinsprecher über sein Akteneinsichtsrecht versucht hatte, Zugang zu denselben Unterlagen zu erhalten. Das Bundesverwaltungsgericht (BVGer) habe dieses Akteneinsichtsgesuch jedoch mit einer Zwischenverfügung vom 8. Dezember 2010 abgelehnt.

In seiner Empfehlung hielt der Beauftragte fest, dass die Frage der Sicherheitsrelevanz der vorliegend zu beurteilenden Dokumente im Rahmen des erwähnten Verwaltungsverfahrens bereits vom BVGer geprüft und schliesslich bejaht worden war. Er sah folglich weder Raum noch Anlass für eine erneute Beurteilung im Hinblick auf einen allfälligen Zugang und schloss sich der Sicherheitsbeurteilung des BVGer an. Im Ergebnis empfahl er dem ENSI, an seiner ablehnenden Stellungnahme festzuhalten.

14. Empfehlung SUVA / Personalverleihbetriebe mit GAV (4. Juli 2013)

Der Antragsteller verlangte von der SUVA eine Auflistung aller Personalverleihbetriebe, welche in der Klasse 70C SUVA-versichert sind, bezüglich der verliehenen Arbeitnehmenden pro Kalenderjahr eine Lohnsumme von mindestens 1 200 000 Franken aufweisen und damit unter den allgemeinverbindlich erklärten GAV Personalverleih fallen. Die SUVA verweigerte eine entsprechende Auskunft unter Bezugnahme auf eine Datenschutzvorschrift im Unfallversicherungsgesetz (UVG), welche eine Bekanntgabe von Personendaten an Unberechtigte untersage und als Spezialbestimmung dem BGÖ vorgehe.

In seiner Empfehlung hielt der Beauftragte fest, dass weder die Schweigepflichtnorm im allgemeinen Sozialversicherungsrecht noch die darauf aufbauenden konkretisierenden Ausnahmeregelungen als Spezialbestimmungen dem BGÖ vorgehen. In der anschliessenden Prüfung der Zugänglichkeit der verlangten Informationen nach den Bestimmungen des BGÖ kam der Beauftragte zum Schluss, dass eine solche Auflistung zwar nicht anonymisierbar sei, an der Bekanntgabe der Firmennamen jener Betriebe, welche unter den GAV Personalverleih fallen, aber ein überwiegendes öffentliches Interesse bestehe. Folglich empfahl er der SUVA, die verlangte Auflistung herauszugeben.

15. Empfehlung BLW / Auszüge aus dem Dokumentenverwaltungssystem (8. Juli 2013)

Die Antragstellerin verlangte drei Auszüge aus dem Dokumentenverwaltungssystem des Bundesamts für Landwirtschaft (BLW) betreffend die Zulassungsverfahren dreier Pflanzenschutzmittel von zwei verschiedenen Bewilligungsinhaberinnen. Das BLW verweigerte einen Zugang in anonymisierter Form ohne Anhörung der betroffenen Unternehmen, da die Dokumentenlisten Personendaten der Herstellerfirmen enthielten und aufgrund der Veröffentlichung des Pflanzenschutzmittelverzeichnisses durch das BLW nicht mehr anonymisierbar seien. Weiter würde eine Anhörung der Bewilligungsinhaberinnen die Möglichkeit bieten, das BLW auf allenfalls in den Dokumentenlisten enthaltene Geschäfts- und Fabrikationsgeheimnisse aufmerksam zu machen.

Der Beauftragte verneinte in seiner Empfehlung sowohl eine Anonymisierungs- als auch eine Anhörungspflicht des BLW. Ebenso verneinte er das Vorhandensein von Geschäfts- und Fabrikationsgeheimnissen in den zu beurteilenden Dokumentenlisten. Hingegen bejahte er einerseits aufgrund der besonderen Stellung zwischen den Bewilligungsinhaberinnen und dem Bund und andererseits aufgrund der jüngsten, intensiven Medienberichterstattung im Zusammenhang mit dem Einsatz von Pflanzenschutzmitteln ein überwiegendes öffentliches Interesse an einem Zugang. Er empfahl eine uneingeschränkte Zugangsgewährung zu den verlangten Dokumentenlisten unter Verzicht auf die Erhebung von Gebühren.

16. Empfehlung BLW / Empfängerlisten Verkäsungs- und Siloverzichtszulage (7. August 2013)

Der Antragsteller verlangte die Listen der Empfänger der Verkäsungs- und Siloverzichtszulage der Jahre 2006 bis 2011. Das Bundesamts für Landwirtschaft (BLW) verweigerte den Zugang zu der elf Seiten langen Liste mit der Begründung, sowohl die Namen der Empfänger der Zulagen als auch der Betrag der Zulage seien geschützte Personendaten, und ein überwiegendes öffentliches Interesse am Zugang könne nicht bejaht werden.

Erst im Schlichtungsverfahren teilte das BLW mit, dass bei einer Anhörung 2500 Personen zu kontaktieren wären und für diesen Aufwand sowie für die Versandkosten mit insgesamt 275 000 Franken zu rechnen sei. In der Schlichtungsverhandlung konnten sich der Antragsteller und das BLW dahingehend einigen, dass das Zugangsgesuch nur die 40 grössten Empfänger der Listen für die Jahre 2006 bis 2012 betrifft. Nach erfolgter Schlichtungsverhandlung verlangte das BLW zusätzlich für die Erstellung der Liste eine Gebühr in der Höhe von 1800 Franken.

Der Beauftragte stufte in seiner Empfehlung sowohl die Namen der Zulagenempfänger als auch die Höhe der Zulagen als Personendaten ein, deren Bekanntgabe jedoch, wenn überhaupt, die Privatsphäre der Empfänger lediglich geringfügig beeinträchtigt. Er kam zum Schluss, dass im vorliegenden Fall der uneingeschränkte Zugang zu den Listen auch ohne Anhörung der Zulagenbezüger gewährt werden kann, zumal keine Ausnahmegründe nach BGÖ vorliegen. In Bezug auf die Gebühren verneinte der Beauftragte sowohl die Gebührenerhebung für die Anhörung (Verwaltungsaufwand und Versandkosten) als auch für die Erstellung der Listen (Verwaltungsaufwand). In der Folge veröffentlichte das BLW auf seiner Website die Liste unter dem Titel «Zulagenbezüger mit > CHF 1 Mio. pro Jahr von 2006 – 2012».

17. Empfehlung ESTV / Daten betreffend die direkte Bundessteuer (22. August 2013)

Der Gesuchsteller beantragte bei der Eidgenössischen Steuerverwaltung (ESTV) die Daten betreffend die direkte Bundessteuer ab dem Jahr 1990 in Form einer strukturierten Datenbank. Der Beauftragte stellte fest, dass gemäss den von der ESTV erteilten Informationen die zur Erstellung des verlangten Dokuments notwendigen Vorgänge die Ausführung zusätzlicher komplexer Programmierungsvorgänge, das heisst eine von einem spezialisierten Mitarbeiter vorgenommene manuelle Eingabe neuer Abfragen in die verschiedenen betroffenen Datenbanken erfordert.

Der Beauftragte gelangte zu dem Schluss, dass es sich angesichts der Komplexität, des Umfangs und der Dauer der zur Erstellung des beantragten Dokuments notwendigen Vorgänge im vorliegenden Fall nicht um eine einfache elektronische

Bearbeitung im Sinne des BGÖ handelt. Somit folgerte der Beauftragte abschliessend, dass die ESTV nicht verpflichtet sei, den vom Gesuchsteller beantragten Zugang zu den verlangten Dokumenten zu gewähren.

18. Empfehlung EPA / Sprachenvertretung bei Personen in leitender Stellung in der Bundesverwaltung (22. August 2013)

Der Antragsteller reichte ein Zugangsgesuch beim Eidgenössischen Personalamt (EPA) ein und beantragte den Zugang zur Sprachenverteilung nach Muttersprache bei den Personen, die in der Bundesverwaltung als Direktoren, Direktionsmitglieder oder Abteilungschefs tätig sind. Der Antrag bezog sich auf jedes Amt und jede Verwaltungseinheit.

Wie der Beauftragte angesichts der vom EPA erteilten Informationen feststellte, kann mit den bestehenden automatischen Suchfunktionen das beantragte Dokument nicht automatisch erstellt werden. In Anbetracht der Komplexität, des Umfangs und der Dauer der für die Erstellung der vom Gesuchsteller beantragten Statistik erforderlichen Vorgänge kam der Beauftragte zu dem Schluss, dass es sich vorliegend nicht um eine einfache elektronische Bearbeitung im Sinne des BGÖ handeln kann.

19. Empfehlung WEKO / Mitarbeiterlisten (3. September 2013)

Der Antragsteller verlangte unter anderem Zugang zur Liste der Mitarbeitenden der WEKO, welche an den beiden Übernahmen Migros/Denner und Emmi/Fromalp gearbeitet haben. Die WEKO verweigerte den Zugang mit der Begründung, die arbeitsrechtlichen Bestimmungen des OR verböten eine Bearbeitung und Zugänglichmachung der verlangten Daten.

Der Beauftragte kam in der Empfehlung zum Schluss, dass für die Herausgabe der Listen nicht das OR, sondern das Bundespersonalgesetz massgeblich ist, welches aber seinerseits nicht als Spezialbestimmung im Sinne des BGÖ gilt. Ausserdem sind nach Ansicht des Beauftragten im Falle einer Zugänglichmachung der Personendaten keine nachteiligen Folgen für die Mitarbeitenden zu erwarten, und es besteht, wenn überhaupt, nur eine sehr geringfügige Verletzung der Privatsphäre der Betroffenen und somit auch keine Anonymisierungspflicht. Sodann überwiegt das öffentliche Interesse an der Transparenz das Interesse am Schutz der Privatsphäre der betroffenen Mitarbeitenden, weshalb die verlangte Liste mit den Mitarbeiternamen gemäss unserer Empfehlung zugänglich zu machen ist.

20. Empfehlung BAZL / Sicherheitsabklärungen Südabflüge 16 straight (4. September 2013)

Der Antragsteller verlangte Zugang zu Unterlagen über die Sicherheitsabklärungen des BAZL zu den Anflugpisten 10 und 34 am Flughafen Zürich. Das BAZL verweigerte den Zugang zu den verlangten Unterlagen unter anderem mit der Begründung,

dass die Dokumente das laufende «Sachplan Infrastruktur der Luftfahrt»-Verfahren beträfen; aufgrund dieses erstinstanzlichen Verwaltungsverfahrens seien sie vom sachlichen Geltungsbereich des BGÖ ausgenommen. Ausserdem werde durch eine vorzeitige Herausgabe der verlangten Unterlagen die Meinungs- und Willensbildungsfreiheit des Bundesrates wesentlich beeinträchtigt.

In der Empfehlung hielt der Beauftragte fest, dass der Zugang zu einem Teil der verlangten Dokumente nicht zu gewähren ist, weil diese vor Inkrafttreten des BGÖ erstellt worden sind. Ausserdem kommt er zum Schluss, dass die verlangten Unterlagen mit einem bevorstehenden Bundesratsbeschluss in Zusammenhang stehen und daher ein laufendes Verfahren betreffen. Aus diesem Grund müssen auch die anderen, nach Inkrafttreten des BGÖ erstellen Dokumente nicht zugänglich gemacht werden.

21. Empfehlung GS-UVEK / Angaben zu Konzerngesellschaften der Schweizerischen Post (11. September 2013)

Der Antragsteller verlangte Angaben zu Kauf und Verkauf von ausländischen Konzerngesellschaften der Schweizerischen Post sowie deren Erfolgsrechnungen. Das Generalsekretariat des UVEK machte ihn auf die öffentlich zugänglichen Informationen im Geschäftsbericht der Post aufmerksam. Im Übrigen verweigerte es den Zugang – soweit ihm die verlangten Dokumente überhaupt vorlagen – unter Hinweis auf das Vorhandensein von Geschäftsgeheimnissen.

Da sich im Laufe des Schlichtungsverfahrens herausstellte, dass die verlangten Informationen dem UVEK tatsächlich nicht vorliegen, konnte der Beauftragte die Frage offen lassen, ob sie Geschäftsgeheimnisse enthalten. Im Ergebnis stützte er folglich die teilweise Zugangsverweigerung des UVEK.

22. Empfehlung BAZL / Monitoring Nachtflugverkehr am Flughafen Zürich (17. September 2013)

Der Antragsteller verlangte Zugang zu den Resultaten, die sich bisher aus dem Monitoring zum Nachtflugverkehr am Flughafen Zürich durch eine Arbeitsgruppe ergeben haben. Das BAZL stellte ihm daraufhin eine siebenseitige Dokumentation mit Grafiken und Statistiken zu und teilte ihm zugleich mit, es beständen keine weiteren amtlichen Dokumente in diesem Zusammenhang. Im Verlaufe des Schlichtungsverfahrens stellte sich heraus, dass der Antragsteller in erster Linie an den Sitzungsprotokollen der sogenannten Monitoring-Gruppe interessiert war.

Das BAZL verweigerte den Zugang zu diesen Protokollen, da der Informationsaustausch innerhalb der Arbeitsgruppe vertraulich sei und eine Bekanntgabe der Sitzungsinhalte die zielkonforme Durchführung der künftigen Bewilligungspraxis in diesem Bereich durch den Flughafen Zürich gefährden oder gar verunmöglichen würde.

Der Beauftragte verneinte jedoch das Vorliegen einer Vertraulichkeitszusicherung im Zusammenhang mit den Sitzungsinhalten der Monitoring-Gruppe. Zudem erachtete er es als vom BAZL nicht rechtsgenügend dargelegt, wieso bzw. inwiefern eine Zugangsgewährung die künftige Bewilligungspraxis im Bereich Nachtflugverkehr am Flughafen Zürich negativ beeinflussen könnte. Im Ergebnis empfahl er dem BAZL die Herausgabe der verlangten Sitzungsprotokolle sowie aller weiterer allenfalls vorhandener amtlichen Dokumente betreffend das Monitoring.

23. Empfehlung SECO / Direktionssitzungsprotokolle und Unterlagen (18. September 2013)

Der Antragsteller verlangte beim SECO den Zugang zu den Protokollen der Direktionssitzungen und Handouts/Foliensets oder anderen Beilagen für den Zeitraum zwischen August und Dezember 2011. Das SECO verweigerte den Zugang und erklärte, die Sitzungsprotokolle seien keine amtlichen Dokumente. Selbst wenn sie es wären, würde es den Zugang trotzdem verweigern. Es berief sich auf verschiedene im BGÖ vorgesehene Ausnahmen. In der Stellungnahme an den Beauftragten wiederholte das SECO seine Begründung und teilte ausserdem mit, vom Zugangsgesuch seien insgesamt 74 Dokumente betroffen.

In seiner Empfehlung kam der Beauftragte zum Schluss, dass die Stellungnahme des SECO an den Antragsteller den Anforderungen einer summarischen Begründung nicht entspricht und es ihn nicht genügend unterstützt hat. In Bezug auf die Sitzungsprotokolle rief der Beauftragte in Erinnerung, dass es sich hierbei um amtliche Dokumente handelt. Da das SECO für alle 74 Dokumente auf einer knappen Seite pauschal mehrere Ausnahmen vom Öffentlichkeitsgesetz geltend gemacht hatte, versäumte es nach Ansicht des Beauftragten, für jedes einzelne Dokument die Vermutung des freien Zugangs umzustossen. Demzufolge empfahl der Beauftragte den Zugang zu allen Dokumenten, unter Beachtung des Schutzes der Personendaten.

24. Empfehlung BFM / Objektverträge Verfahrenszentren Asylwesen (8. Oktober 2013)

Der Antragsteller verlangte Zugang zu der aktuellen Leistungsvereinbarung des Bundesamts für Migration (BFM) mit der ORS Service AG sowie zu den letzten vier Tätigkeitsberichten, welche letztere an das BFM übermittelt hatte. Das BFM vertrat entgegen der ORS Service AG die Auffassung, dass die verlangten Objektverträge zugänglich gemacht werden müssten. An der darauf folgenden Schlichtungsverhandlung hielten die Parteien in einer Teileinigung fest, dass die Rahmenvereinbarungen die Erstellung von Tätigkeitsberichten nicht vorsehen und keine solchen bestehen, und dass die Rahmenvereinbarungen nicht Gegenstand des Schlichtungsverfahrens sind.

Nach der Schlichtungsverhandlung verweigerte die ORS Service AG den Zugang zu den verlangten Objektverträgen weiterhin mit der Begründung, dass der darin enthaltene Betreuungsschlüssel und die vereinbarte Abgeltung Geschäftsgeheimnisse darstellten, welche geschwärzt und verweigert werden müssen. Der Beauftragte erliess daraufhin am 8. Oktober 2013 eine Empfehlung in der er zum Schluss kam, dass die geschwärzten Angaben keine Geschäftsgeheimnisse darstellen und dass der Zugang zu den Objektverträgen gewährt werden muss.

25. Empfehlung BAZL / Radardaten Überflüge (9. Oktober 2013)

Der Antragsteller verlangte beim BAZL Zugang zu den Daten aller (militärischen) Überflüge ohne Transpondersignal vom 15. Juni 2012. Das BAZL verwies den Antragsteller an die Flugsicherungsgesellschaft Skyguide, weil es selber nicht im Besitz der verlangten Unterlagen war. Skyguide verweigerte jedoch den Zugang mit der Begründung, dass sie nicht unter den persönlichen Geltungsbereich des BGÖ falle.

In der Empfehlung kam der Beauftragte zum Schluss, dass das BAZL den Zugang zu den verlangten Unterlagen aufgrund fehlenden Besitzes zu Recht nicht gewährt hat. Ausserdem hielt er fest, dass Skyguide unzweifelhaft Verwaltungsaufgaben für den Bund erfüllt, welche normalerweise von der Zentralverwaltung wahrzunehmen wären. Aus diesem Grund subsumierte er Sykguide unter die Bundesverwaltung und somit unter den persönlichen Geltungsbereich des BGÖ.

26. Empfehlung BJ / Verfahrensakten EGMR (10. Oktober 2013)

Der Antragsteller verlangte beim Bundesamt für Justiz (BJ) den Zugang zu einem Dokument, welches letzteres beim Europäischen Gerichtshof für Menschenrechte (EGMR) eingereicht hatte, um damit die Neubeurteilung eines Urteils des EGMR zum Fall «Gross gegen die Schweiz» bei der Grossen Kammer zu beantragen. Das BJ verweigerte den Zugang zum Dokument mit der Begründung, das Öffentlichkeitsgesetz sei auf Verfahren vor dem EGMR nicht anwendbar und der Zugang sei durch die Verordnung des EGMR separat geregelt.

Aufgrund des Sachverhaltes stellte der Beauftragte fest, dass das vom BJ erstellte Dokument Teil der Akten eines hängigen Verfahrens vor dem EGMR ist, für welches ein eigenes Prozessrecht gilt. Er kam zum Schluss, dass für den Zugang zur Rechtsschrift des BJ die spezialrechtliche Bestimmung von Artikel 33 der Verfahrensordnung des EGMR massgebend ist.

Weiter wies der Beauftragte darauf hin, dass gerichtliche und aussergerichtliche Streitverfahren mit internationalem Bezug nicht in den Geltungsbereich des BGÖ fallen. Daher stützte er im Ergebnis die Zugangsverweigerung des BJ, wonach das verlangte Dokument Teil des hängigen gerichtlichen Verfahrens sei und damit das Öffentlichkeitsgesetz nicht zur Anwendung komme.

27. Empfehlung BFE / Erdbebensicherheit WKW Mühleberg (15. Oktober 2013)

Der Antragsteller verlangte Zugang zu Berichten und zu einem Protokoll über die Überprüfung der Erdbebensicherheit des Wasserkraftwerks Mühleberg. Das BFE verweigerte dem Antragsteller den Zugang zu den verlangten Unterlagen mit der Begründung, dass durch die Herausgabe der Dokumente die zielkonforme Durchführung der Sicherheitsaufsicht über die Talsperren beeinträchtigt wäre. Sodann sei allen Betreibern von Talsperren Vertraulichkeit zugesichert worden.

Der Beauftragte hielt in der Empfehlung fest, dass die Aufsichtstätigkeit des BFE auch nach Bekanntmachung der Dokumente weiterhin problemlos erfüllt werden kann und die zielkonforme Durchführung konkreter behördlicher Massnahmen durch die Kenntnis des verlangten Protokolls nicht beeinträchtigt wird. Schliesslich konnte das BFE auch keine schriftliche Vertraulichkeitszusicherung erbringen. Bezüglich der in den verlangten Unterlagen enthaltenen Personendaten hielt der Beauftragte fest, dass die aufgeführten Mitarbeitenden der öffentlichen Verwaltung offenzulegen sind, während die Namen der übrigen im Protokoll genannten Personen anonymisiert werden können.

28. Empfehlung BFM/ Asylunterkunft Jaunpass (29. Oktober 2013)

Der Antragsteller verlangte beim BFM den Zugang zu drei Dokumenten, welche die Asylunterkunft auf dem Jaunpass betrafen.

Das BFM verweigerte den Zugang mit der Begründung, die Offenlegung der fraglichen Dokumente würde die Beziehungen zwischen dem Bund und den Kantonen/ Gemeinden einerseits sowie zwischen den Kantonen und Gemeinden andererseits beeinträchtigen. Auch sähe das BFM eine Beeinträchtigung der behördlichen Massnahmen im Rahmen der Verhandlungen betreffend die Unterkünfte für Asylsuchende mit Kantonen und Gemeinden gegeben.

Im Schlichtungsverfahren stellte sich heraus, dass die vom BFM eingereichten Unterlagen nicht jene waren, in welche der Antragsteller Einsicht begehrt hatte. Es zeigte sich, dass das BFM nicht über die verlangten Dokumente verfügte und sich die eingereichte Stellungnahme nicht auf die im Schlichtungsverfahren strittigen Dokumente bezogen hat. Da der Beauftragte auf die Mitteilungen des BFM letztlich vertrauen muss und er überdies auch keinen Grund hatte, an der Glaubwürdigkeit des Amts zu zweifeln, stützte er dessen Bescheid, dem Gesuch des Antragstellers auf Zugang zu den verlangten Dokumenten nicht zu entsprechen.

Der Beauftragte hat in der Empfehlung überdies festgehalten, dass er keine Aufsichtspflicht betreffend die rechtskonforme Führung von Akten in der Bundesverwaltung hat.

29. Empfehlung ENSI / Sitzungsprotokolle zur Überprüfung der Erdbebensicherheit WKW Mühleberg (30. Oktober 2013)

Zwei Antragsteller verlangten Zugang zu Sitzungsprotokollen über die Überprüfung der Erdbebensicherheit des Wasserkraftwerks Mühleberg. Das ENSI verweigerte den Zugang zu den verlangten Sitzungsprotokollen mit der Begründung, dass diese eng mit einem kantonalen Baubewilligungsverfahren verknüpft seien, welches seinerseits noch nicht abgeschlossen sei.

Nachdem der Beauftragte jedoch festgestellt hatte, dass das Verfahren vor Bundesverwaltungsgericht abgeschlossen war, forderte er das ENSI zu einer neuen Stellungnahme auf. Dieses machte erneut die Verweigerung aufgrund eines laufenden Verfahrens geltend. Weitere Abklärungen seitens des Beauftragten ergaben schliesslich, dass die verlangten Sitzungsprotokolle nicht Teil der kantonalen Verfahrensakten bilden. Aus diesem Grund führte der Beauftragte in seiner Empfehlung aus, dass der Zugang zu den verlangten Unterlagen zu gewähren ist, da sie nicht Teil eines laufenden Verfahrens bilden. Ausserdem fehlten gegenüber dem Beauftragten sowohl eine rechtsgenügliche Begründung als auch Hinweise des ENSI, die eine Verweigerung gerechtfertigt hätten.

30. Empfehlung BAZL / Rechtssetzungsakte EU-Kommission (19. November 2013)

Der Antragsteller schreibt eine wissenschaftliche Arbeit und ersuchte in diesem Zusammenhang Zugang zu nicht veröffentlichten Beschlüssen der Europäischen Kommission betreffend die Massnahmen für die Durchführung der gemeinsamen Grundstandards der Luftsicherheit.

Das BAZL verweigerte den Zugang zu den fraglichen Rechtssetzungsakten der Europäischen Kommission mit der Begründung, es handle sich um eine EU-Verschlusssache, zu welcher nur Personen Zugang hätten, die diese Informationen für die Ausübung ihrer Tätigkeit benötigten. Der Antragsteller gehöre nicht zu diesem Personenkreis, da er keine Aufgaben oder Aufträge im Dienst der Schweizer Luftfahrt ausübe. Zudem sei durch die Zugänglichmachung der fraglichen Beschlüsse die innere und äussere Sicherheit der Schweiz gefährdet und es würden die internationalen Beziehungen beeinträchtigt.

Der Beauftragte kam zum Schluss, dass die EU-Transparenzverordnung nur dann anwendbar ist, wenn das Zugangsgesuch direkt bei der Europäischen Kommission gestellt wird. Vorliegend ist das Zugangsgesuch an das BAZL gerichtet worden, so dass das BGÖ anwendbar ist, da für die Schweiz, wie für die Mitgliedstaaten der EU, das nationale Recht auf Zugang zu amtlichen Dokumenten gilt. Die Ausnahmegründe zum Schutz der öffentlichen Interessen nach EU-Recht finden sich auch im BGÖ.

Der Beauftragte stützte das BAZL in seinem Entscheid, den Zugang zu den Beschlüssen zu verweigern, da er es als erwiesen erachtete, dass mit der Zugänglichmachung die innere und äussere Sicherheit der Schweiz gefährdet und die internationale Sicherheit beeinträchtigt würde. Der Beauftragte hielt jedoch fest, dass das BAZL prüfen könne, ob es im konkreten Fall dem Antragsteller aufgrund des nachgewiesenen Forschungsinteresses einen Zugang unter Auflagen gewähren wolle.

31. Empfehlung BFE / Überwachungsreglement Wohlensee-Staumauer (28. November 2013)

Der Antragsteller verlangte Zugang zum Überwachungsreglement der Wohlensee-Staumauer. Das BFE verweigerte den Zugang mit der Begründung, dass es sich um Verfahrensakten handle und das BGÖ nicht anwendbar sei.

Der Beauftragte kam in der Empfehlung zum Schluss, dass das verlangte Überwachungsreglement nicht Teil der Akten eines laufenden Verfahrens bildet, weshalb der Zugang zu diesem nicht aufgeschoben werden kann. Aus diesem Grund führte er in der Empfehlung aus, dass der Zugang zum verlangten Dokument samt den dazugehörigen Beilagen zu gewähren ist.

32. Empfehlung SNF / Dokumente im Zusammenhang mit dem Nationalen Forschungsprogramm «Lebensende» (5. Dezember 2013)

Der Antragsteller verlangte beim SNF Zugang zu verschiedenen Dokumentengruppen im Zusammenhang mit dem vom SNF durchgeführten Nationalen Forschungsprogramm «Lebensende» (NFP 67). Im Einzelnen ersuchte er einerseits um Zustellung von Unterlagen zur Vorbereitung und Antragstellung zuhanden des Bundesrates (Begehren A) und zu Vorschlägen der Zusammenstellung und Wahl der Leitungsgruppe des NFP 67 (Begehren B), sowie andererseits betreffend neun namentlich genannter Forschungsprojekte zu den entsprechenden Gesuchen um Beiträge (Begehren C), zu den Namen der dazu zur Stellungnahme eingeladenen Gutachter (Begehren D) und den entsprechenden Gutachten selbst (Begehren E).

Der SNF gewährte daraufhin Zugang zu den unter Begehren A verlangten Dokumenten, wobei die darin enthaltenen Personendaten zum Teil anonymisiert wurden. Die übrigen Teilbegehren (B-E) lehnte der SNF mit verschiedenen Begründungen ab.

Der Beauftragte kam in seiner Empfehlung zu folgenden Ergebnissen:

Die Namen der am NFP 67 mitwirkenden Personen, welche anonymisiert wurden, müssen vom SNF offengelegt werden (Begehren A).

Ebenso muss der SNF die Wahlanträge, die Wahlentscheide sowie die entsprechenden Protokollauszüge betreffend die Mitglieder der Leitungsgruppe des NFP 67 zugänglich machen (Begehren B), wobei die ausführlichen Lebensläufe der Wahlkandidaten nicht offen zu legen sind.

Die Gesuche um Beiträge zu neun namentlich genannten Forschungsprojekten können nicht zugänglich gemacht werden. Sie enthalten schützenswerte Informationen über geplante Forschungsarbeiten. Die blossen Anmeldeformulare sind dem Antragsteller hingegen herauszugeben (Begehren C).

Weiter darf der SNF die Namen der Gutachtenspersonen im Rahmen des sogenannten «Peer-Review-Verfahrens» mit Blick auf eine Spezialbestimmung im Gesetz über die Förderung der Forschung und der Innovation (FIFG), welche die Geheimhaltung der Expertennamen explizit vorsieht, nicht zugänglich machen (Begehren D).

Auch die Gutachten selbst können dem Antragsteller aufgrund der direkten und inhaltlich engen Verknüpfung mit den Inhalten der Forschungsgesuche aufgrund des Schutzbedarfs der enthaltenen Informationen im Zusammenhang mit geplanten Forschungsprojekten nicht zugänglich gemacht werden (Begehren E).

Schliesslich erachtet der Beauftragte auch die Erhebung einer Gebühr über 800 Franken für die Bearbeitung dieses Zugangsgesuches als angemessen und damit rechtmässig.

33. Empfehlung BJ und SIF / Zuständigkeit für die Bearbeitung eines Zugangsgesuches (18. Dezember 2013)

Der Antragsteller begehrte im Hinblick auf einen geplanten Dokumentarfilm zum Steuerkonflikt zwischen den USA und der Schweiz den Zugang zur Korrespondenz des Direktors und Vizedirektors des Bundesamtes für Justiz sowie der Korrespondenz zwischen diesen und der Departementsvorsteherin für den Zeitraum vom 16. Dezember 2011 bis 18. Januar 2012. Nachdem sich das BJ zunächst für die Bearbeitung des Zugangsgesuches für zuständig erklärt und auch materiell geäussert hatte, vereinbarte es im Rahmen der Anhörung der involvierten Ämter mit dem SIF dessen Zuständigkeit. Das SIF und das BJ begründeten dies damit, dass die mögliche Lieferung der Mitarbeiterdaten an die USA lediglich ein Teilaspekt des Dossiers Steuerstreit mit den USA sei, für welches das SIF die Federführung habe. Ausserdem argumentierten beide Behörden, dass Dokumente der FINMA nicht nach Öffentlichkeitsgesetz zugänglich seien, da siediesem nicht unterstehe.

Der Beauftragte kam zum Schluss, dass die Dokumente der FINMA, welche sie einer dem Öffentlichkeitsgesetz unterstellten Behörde zusendet, unter Vorbehalt der gesetzlichen Ausnahmegründe zugänglich seien. Zentral prüfte der Beauftragte die Frage, ob die von BJ und SIF vereinbarte behördliche Zuständigkeit gesetzeskonform ist. Er hielt vorweg fest, dass die Koordinationsbestimmungen in der Verordnung ausschliesslich dazu dienen, der gesuchstellenden Person den Zugang zu erleichtern. Konkret verneinte er die Zuständigkeit des SIF, da er das Kriterium des «gleichen Geschäftes» im Sinne von Artikel 11 Abs. 2 VBGÖ nicht als erfüllt betrachtet hat. Auch erachtete er eine behördliche Konzentration der Zugangsbearbeitung als nicht mit dem Konzept des Öffentlichkeitsgesetzes vereinbar.

Der Beauftragte erklärte schliesslich das BJ als zuständig für die Bearbeitung des Zugangsgesuches zu den von ihm selber erstellten Dokumenten sowie für diejenigen Dokumente, welche es von Dritten, einschliesslich der FINMA, erhalten hatte. Da keine abschliessende Stellungnahme des BJ zum Zugangsgesuch vorlag, äusserte sich der Beauftragte nicht zu den vom BJ und SIF vorgetragenen materiellen Ausnahmegründen.

34. Empfehlung BBL / Auswertung bzw. Statistik des Beschaffungscontrollings 2011 für alle Departemente und die BK (23. Dezember 2013)

Die Antragsteller ersuchten beim Bundesamt für Bauten und Logistik (BBL) um Zugang zu den Controlling-Berichten sowie zur Auswertung der Statistik der Beschaffungszahlen 2011 der Departemente und der Bundeskanzlei (BK). Neben einigen Dokumenten, welche das BBL ohne Einschränkungen zugänglich machte, wurden den Antragstellern acht Tabellen mit einer Auflistung der jeweils 40 umsatzstärksten Kreditoren (Lieferfirmen) der Departemente und der BK zugänglich gemacht. Die Namen dieser 40 Firmen wurden unter Hinweis auf den Schutz von Geschäftsgeheimnissen anonymisiert.

Das BBL argumentierte, ein Zugang zu diesen Listen komme ohne Anonymisierung nicht in Betracht, da eine Kombination der darin enthaltenen Informationen inklusive der dazugehörigen Firmennamen ein schützenswertes Geschäftsgeheimnis darstelle, welches im Falle einer Bekanntgabe zu einer Wettbewerbsverzerrung führen würde.

Gegenüber dem Beauftragten berief sich das BBL im Rahmen seiner Zugangsbeschränkung zudem auf ein im Zusammenhang mit dem zu beurteilenden Zugangsgesuch verfassten Aussprachepapier des Bundesrates vom 23. April 2013 und einen entsprechenden Bundesratsbeschluss vom 1. Mai desselben Jahres, wonach eine entsprechende Anonymisierung der in den Listen enthaltenen Firmennamen zwingend vorgesehen sei (vgl. Ziffer 2.5.2 des vorliegenden Tätigkeitsberichts).

In seiner Empfehlung kam der Beauftragte zum Schluss, dass die bis anhin anonymisierten Firmennamen der jeweils 40 umsatzstärksten Lieferfirmen der Departemente und der BK vollständig offenzulegen seien. Hinsichtlich jener Beschaffungen, welche die beschaffungsrechtlichen Schwellenwerte erreichten, sei die Bekanntgabe der berücksichtigten Firmen sogar gesetzlich vorgeschrieben und demnach eine beschaffungsrechtliche Spezialbestimmung anwendbar. In Bezug auf die Beschaffungen unterhalb der Schwellenwerte verneinte der Beauftragte das Vorliegen einer Ausnahmebestimmung nach Öffentlichkeitsgesetz. Insbesondere erachtete er den Hinweis auf den Schutz von Geschäftsgeheimnissen als nicht statthaft.

Weiter beurteilte der Beauftragte die drei Lösungsvorschläge des erwähnten Aussprachepapiers und des entsprechenden Bundesratsbeschlusses vom 1. Mai 2013 als im vorliegenden Fall nicht mit den Bestimmungen des Öffentlichkeitsgesetzes vereinbar und lehnte diese folglich ab. Abschliessend hielt er fest, dass auch alle weiteren in diesem Zusammenhang allenfalls bestehenden amtlichen Dokumente nach den Vorgaben des Öffentlichkeitsgesetzes zugänglich zu machen sind.

35. Empfehlung Swissmedic / Erlass einer Gebührenverfügung (23. Dezember 2013)

Der Antragsteller verlangte bei Swissmedic Zugang zu einer Liste aller Dokumente im Zusammenhang mit der Zulassung von Tamiflu. Nachdem er sein Zugangsgesuch präzisiert hatte und diesem vollumfänglich entsprochen worden war, bestritt er in seinem Schlichtungsantrag lediglich die Gebührenerhebung.

Der Beauftragte führte daher in der Empfehlung aus, dass dem Antragsteller seine Präzisierung während des Zugangsverfahrens anzurechnen ist, und verwies ihn in der noch offenen Gebührenfrage an Swissmedic für den Erlass einer Gebührenverfügung.

2.3.2 Schlichtungen

Nachfolgend eine Auswahl von Fällen, in denen im Berichtsjahr Schlichtungen erzielt werden konnten:

1. Schlichtung VBS / Beirat Weiterentwicklung der Armee

Der Antragsteller verlangte beim VBS Zugang zu Unterlagen über eine allfällige Bezahlung und Entschädigung des Beirates der Weiterentwicklung der Armee sowie weitere Dokumente ab dessen Gründung. Nachdem der Beauftragte anlässlich einer Sitzung zusammen mit dem VBS die Unterlagen geprüft hatte, erklärte sich das Departement bereit, sämtliche vom Antragsteller verlangten Unterlagen herauszugeben. Dadurch konnte schliesslich eine Einigung erzielt werden.

2. Schlichtung UVEK / Weihnachts- und Neujahrsgrüsse

Der Antragsteller verlangte beim UVEK Zugang zur «Liste der Staatspräsidenten, Organisationen und Ämter sowie weiterer Personen, die im Jahr 2010 Weihnachts- oder Neujahrsgrüsse von der damaligen Bundespräsidentin Doris Leuthard erhalten haben.» Er verzichtete auf unsere Anfrage hin ausdrücklich auf Angaben von Privatpersonen.

Im Schlichtungsverfahren gelangte der Beauftragte zum Schluss, dass keine Ausnahmebestimmungen nach Öffentlichkeitsgesetz vorliegen, welche eine Verweigerung resp. einen Aufschub der Herausgabe der erwähnten Liste rechtfertigen würden. Das UVEK nahm die Ansicht des Beauftragten zur Kenntnis und erklärte sich bereit, dem Antragsteller eine Liste von Personen mit politischer Funktion zuzustellen. Der Antragsteller erklärte sich mit dieser Liste einverstanden.

3. Schlichtung ENSI / Quellpfad in Verfügungen

Der Antragsteller verlangte beim ENSI Einsicht in die Originale von Verfügungen, welche das ENSI im Internet aufgeschaltet hatte. Mit Hilfe der Vermittlung des Beauftragten konnten die Beteiligten sich in der Folge einigen: Da das ENSI dem Antragsteller die Vorgänge, die zu den unterschiedlichen Quellenpfaden der veröffentlichten Verfügungen geführt hatten, nachvollziehbar darlegen konnte, war das Zugangsgesuch für den Antragsteller erledigt.

4. Schlichtung BLW / Präzision Zugangsgesuch

Der Antragsteller verlangte beim BLW Einsicht in die Empfängerlisten der auf die Milchpreisstützung basierenden Verkäsungszulage der Jahre 2006 bis 2011. Für denselben Zeitraum verlangte er die Empfängerlisten der Zulagen für die Fütterung ohne Silage.

Der Antragsteller und das BLW konnten sich dahingehend einigen, das Zugangsgesuch auf die 40 grössten Empfänger der Verkäsungs- und Siloverzichtszulage der Jahre 2006 bis 2011 zu reduzieren und noch im gleichen Umfang auf das Jahr 2012 auszudehnen. Soweit keine Einigung erzielt werden konnte, erliess der Beauftrage am 7. August 2013 eine Empfehlung (siehe Ziffer 2.3.1 des vorliegenden Tätigkeitsberichts, Empfehlung 16).

5. Schlichtung BFE / KNS-Sitzungsprotokolle

Der Antragsteller verlangte beim BFE Zugang zu sämtlichen Protokollen der Sitzungen der Eidgenössischen Kommission für nukleare Sicherheit (KSN) im Jahr 2011. Nachdem das BFE auf die Empfehlung des Beauftragten vom 16. Dezember 2011 hingewiesen worden war, überprüfte es die vom Antragsteller verlangten Dokumente erneut und kam zum Schluss, dass weitgehend Einsicht gewährt werden könne. Nach einem schriftlichen und telefonischen Austausch zwischen dem Antragsteller, dem Beauftragten und dem BFE unterbreitete das Amt dem Antragsteller einen Einigungsvorschlag. Dieser erklärte in der Folge gegenüber dem BFE und dem Beauftragten, seinem Gesuch sei mit diesem Vorschlag weitgehend entsprochen worden.

6. Schlichtung BFM / Objektverträge Verfahrenszentren Asylwesen

Der Antragsteller verlangte Zugang zur aktuellen Leistungsvereinbarung des BFM mit der ORS Service AG sowie zu den letzten vier Tätigkeitsberichten, welche die ORS Service AG an das BFM übermittelt habe. In der Schlichtungsverhandlung hielten die Parteien in einer Teileinigung fest, dass die Rahmenvereinbarungen die Erstellung von Tätigkeitsberichten nicht vorsehen und keine solchen bestehen, sowie dass die Rahmenvereinbarungen nicht Gegenstand des Schlichtungsverfahrens sind. Für die offenen Punkte erliess der Beauftragte am 8. Oktober 2013 eine Empfehlung, in der er zum Schluss kam, dass die geschwärzten Angaben keine Geschäftsgeheimnisse darstellen, weshalb die Objektverträge zugänglich zu machen sind (siehe Ziffer 2.3.1 des vorliegenden Tätigkeitsberichts, Empfehlung 24).

7. Schlichtung EDA / Entwicklungszusammenarbeit

Der Antragsteller verlangte Zugang zu den Fortschritts- bzw. Jahres- und Evaluationsberichten der Jahre 2007 bis 2010 in Zusammenhang mit drei genannten Entwicklungsprojekten von Swisscontact und der DEZA (Nepal, Kenia und Bolivien). Weiter ersuchte er um Zugang zu einer Liste sämtlicher Aufträge, welche im Jahr 2011 an die Organisationen Helvetas, Intercooperation, Helvetas Swiss Intercooperation und Swisscontact vergeben wurden.

Anlässlich des Schlichtungsverfahrens zog der Gesuchsteller sein Begehren in Bezug auf die Berichte zu einem Projekt zurück (Kenia), da er sich mit dem EDA diesbezüglich einigen konnte. Da er sich aber mit den übrigen gelieferten Unterlagen und insbesondere mit zwei ergangenen Gebührenrechnungen über insgesamt 1300 Franken nicht einverstanden erklärte, kam es am 25. Oktober zu einer Schlichtungsverhandlung. Im Rahmen dieser Verhandlung einigten sich die Parteien über eine vollständige Zugangsgewährung in Bezug auf die beiden verbleibenden Projektberichte (Nepal und Bolivien), soweit der Zugang durch das EDA nicht ohnehin bereits gewährt worden war. Die geschuldete Gebühr für diese beiden Teilgesuche wurde neu verhandelt und festgesetzt. Im Nachgang zu dieser Verhandlung gewährte das EDA dem Antragsteller schliesslich auch Einsicht in eine vollständige Liste der an die vier genannten Organisationen vergebenen Aufträge des Jahres 2011.

8. Schlichtung BFS / Tourismusstatistik

Der Antragsteller verlangte Zugang zu mehreren Dokumenten über die Tourismusstatistik. Der Beauftragte lud nach einer Besprechung mit dem BFS die Parteien zur Schlichtungsverhandlung ein. Sie einigten sich darauf, dass das Amt dem Antragsteller ein bestimmtes Dokument mit den vom BFS vorgenommenen Einschwärzungen innert Frist zustellt. Ausserdem erklärte sich das BFS in der Schlichtungsvereinbarung bereit, mit dem Antragsteller ein persönliches Gespräch betreffend sein Forschungsprojekt zu führen.

9. Schlichtung BSV / Auditberichte IV-Stelle und RAD Zürich

Der Antragsteller verlangte Zugang zu den letzten beiden Auditberichten betreffend IV-Stelle/RAD Zürich des BSV. Im Rahmen des Schlichtungsverfahrens kam es zu diversen Gesprächen zwischen dem Beauftragten und dem Gesuchsteller einerseits und dem Beauftragten und dem BSV andererseits. In der Folge wurden dem Antragsteller die verlangten Dokumente mit wenigen Anonymisierungen zur Einsicht vorgelegt. In einer Vereinbarung erklärten sich die Parteien zudem als auseinandergesetzt und beantragten gemeinsam die Einstellung des Schlichtungsverfahrens.

2.4 Gerichtsentscheide zum Öffentlichkeitsgesetz

2.4.1 Bundesverwaltungsgericht

Nachfolgend eine Auswahl von Urteilen, die das Bundesverwaltungsgericht (BVGer) in Zusammenhang mit dem Zugang zu amtlichen Dokumenten im Jahr 2013 gefällt hat:

1. BSV / Sitzungsprotokolle der AHV/IV-Kommission

Gegen die Empfehlung des Beauftragten vom 16. August 2012 (vgl. unseren Tätigkeitsbericht 2012/2013, Ziff. 2.3.1) hat das Bundesamt für Sozialversicherung BSV eine Verfügung erlassen, die an das BVGer weitergezogen wurde. Der Beschwerdeführer verlangte die Aufhebung der Verfügung und die Gewährung des Zugangs zu den Sitzungsprotokollen der AHV/IV-Kommission. Er machte geltend, die Kommission werde seit Inkrafttreten der Änderungen des Regierungs- und Verwaltungsorganisationsgesetzes (RVOG) per 1. Januar 2009 zur dezentralen Bundesverwaltung gerechnet und sei somit dem BGÖ unterstellt. Demgegenüber hat das BSV die Auffassung vertreten, die AHV/IV-Kommission falle als Verwaltungskommission nicht in den Geltungsbereich des BGÖ. Dabei berief sich das BSV auf den historischen Gesetzgeber.

Betreffend die Frage, ob Verwaltungskommissionen vom Öffentlichkeitsgesetz erfasst sind, hat sich das Gericht eingehend mit der Auslegung des BGÖ und des RVOG auseinandergesetzt. Es kam zum Schluss, dass sämtliche Auslegungsmethoden zum Ergebnis führen, dass die ausserparlamentarischen Kommissionen, also sowohl Behörden- als auch Verwaltungskommissionen, der dezentralen Bundesverwaltung zuzurechnen sind und damit in den Anwendungsbereich des BGÖ fallen. Die AHV/IV-Kommissionen wären nur dann ausgenommen, wenn eine explizite vom Bundesrat vorgesehene Ausnahmeregelung vorhanden wäre.

Das Gericht hiess die Beschwerde gut und hob die Verfügung auf. Es gewährte den Zugang zu den verlangten Sitzungsprotokollen im konkreten Fall, da das BSV sich weder in seiner Verfügung noch in seiner Stellungnahme zu möglichen Ausnahmegründen geäussert und es versäumt hatte, die Vermutung des freien Zugangs zu widerlegen. Im Bezug auf den Schutz der Personendaten erklärte das Gericht, auch dazu habe sich das BSV nicht geäussert. Es wies das Bundesamt an, die Personennamen der natürlichen Personen durch Einschwärzen zu anonymisieren. Davon auszunehmen seien die Mitarbeiter von Behörden und der Kommissionsmitglieder sowie die Personenamen der Vertreter der Institutionen und Organisationen, soweit sie nicht in behördlicher Funktion tätig sind (Urteil vom 22. April 2013, Ref. A-4962/2012).

2. ESTI / Liste der im Jahr 2011 kontrollierten Elektrogeräte

Der Redaktionsleiter der Konsumentenzeitschrift saldo verlangte beim Eidgenössischen Starkstrominspektorat (ESTI) Zugang zu einer Liste der im Jahr 2011 kontrollierten Elektrogeräte mit den entsprechenden Resultaten, einschliesslich der ausgesprochenen Verkaufsverbote. Das ESTI stellte dem Gesuchsteller die Unterlagen schliesslich zu und auferlegte ihm mit einer entsprechenden Verfügung eine Gebühr von 700 Franken. Dagegen erhob der Gesuchsteller Beschwerde vor Bundesverwaltungsgericht und beantragte die Aufhebung der Gebührenverfügung sowie die Gewährung des Zugangs unter Verzicht auf eine Kostenauferlegung.

In seinem Urteil bestätigte das Bundesverwaltungsgericht, dass Medienschaffende keinen verfassungsrechtlich geschützten Anspruch auf unentgeltlichen Zugang zu amtlichen Dokumenten hätten (vgl. Urteil des BVGer 1200/2012; s.a. unseren Tätigkeitsbericht 2012/2013, Ziff. 2.4.1). Ein entsprechendes Privileg habe auch der Bundesrat in der Öffentlichkeitsverordnung nicht vorgesehen, obwohl er sich dieser Möglichkeit bewusst gewesen war. Im Ergebnis erachtete es eine Gebührenerhebung auch gegenüber Medienschaffenden als zulässig. Ein Gebührenverzicht gegenüber Medienschaffenden sei Gericht nur dann angezeigt, wenn es um Leistungen gehe, die für den Staat oder den Einzelnen von existenzieller Bedeutung seien, was nach Ansicht der Richter im zu beurteilenden Fall nicht gegeben war.

Im Ergebnis beurteilte das Bundesverwaltungsgericht die Gebührenauferlegung gegenüber dem Journalisten grundsätzlich als rechtmässig, wobei es den geschuldeten Betrag um 100 Franken reduzierte, da nach den Bestimmungen des BGÖ für das Erlassen einer Verfügung keine Gebühren verlangt werden dürfen (Urteil vom 22. April 2013, Ref. A-3363/2012).

3. SECO / Gewerkschaftsdokumente betreffend einen Gesamtarbeitsvertrag im westschweizerischen Ausbaugewerbe

In einem weiteren Fall erliess das SECO, gestützt auf unsere Empfehlung vom 18. September 2012, eine Verfügung, welche an das BVGer weitergezogen wurde. Dabei ersuchte der Beschwerdeführer ursprünglich beim SECO Zugang zu den eingereichten Unterlagen des Gesuches von Gewerkschaften um die Allgemeinverbindlicherklärung einiger Bestimmungen des Gesamtarbeitsvertrages für die vorzeitige Pensionierung im westschweizerischen Ausbaugewerbe (KVP), namentlich betreffend den Nachweis der vorhandenen Quoren.

Das SECO verweigerte den Zugang, weil ein direkter und unmittelbarer Zusammenhang zwischen den verlangten Dokumenten und dem bevorstehenden Beschluss des Bundesrats bestehe. Da der Bundesrat im Laufe des Rechtsmittelverfahrens vor dem BVGer zu einem Beschluss über das Gesuch zur Änderung einiger Bestimmungen der Allgemeinverbindlicherklärung des KVP gekommen war, und weil

keine Ausnahmebestimmungen des BGÖ vorlagen, hiess das BVGer im Urteil vom 8. Oktober 2013 die Beschwerde gut und wies das SECO an, dem Beschwerdeführer Zugang zu den eingereichten Unterlagen zu gewähren (Urteil vom 8. Oktober 2013, Ref. A-5489/2012).

4. SECO / Abrechnungen der paritätischen Kommissionen I

In einem weiteren Urteil befasste sich das BVGer mit der Beschwerde mehrerer paritätischer Kommissionen gegen eine Verfügung, welche das Staatssekretariat für Wirtschaft SECO entsprechend der Empfehlung des Beauftragten vom 20. Februar 2013 erlassen hatte (vgl. Ziffer 2.3.1 des vorliegenden Tätigkeitsberichts, Empfehlung 3). Streitgegenstand war der Zugang zu Abrechnungen des Jahres 2010, welche die paritätischen Kommissionen dem SECO als Aufsichtsbehörde zustellen mussten. Die Beschwerdeführerinnen rügten u.a. die Verletzung des rechtlichen Gehörs, da das SECO in den Verfügungen lediglich auf die Erwägungen in der Empfehlung des Beauftragten verwiesen habe.

Das Gericht hielt fest, dass das SECO ausnahmsweise auf eine ausführliche Begründung verzichten konnte, da es sich mit der Empfehlung des Beauftragten in allen Punkten als einverstanden erklärt hat und die beschwerdeführenden Parteien im vorinstanzlichen Verfahren ihre Gesuche um Erlass einer Verfügung nicht begründet hatten. Entgegen der Meinung der Beschwerdeführerinnen erklärte das Gericht, dass das BGÖ auf die Abrechnungen der privatrechtlich organisierten paritätischen Kommissionen anwendbar ist. Es hielt explizit fest, dass der Anwendungsbereich des BGÖ gerade in Bezug auf Informationen aus privaten Quellen weit zu fassen ist, diese also grundsätzlich zugänglich sind, sofern sie als amtliche Dokumente zu qualifizieren sind.

Weiter erklärte das Gericht, dass die gesuchstellende Person für ein Zugangsgesuch zu solchen privaten Dokumenten, die der aufsichtsrechtlichen Tätigkeit dienen, weder ein besonderes Interesse nachweisen muss, noch das BGÖ einen besonderen Verwendungszweck vorgebe. Sofern die Beschwerdegegnerin im Falle des Zugangs Unregelmässigkeiten in den Abrechnungen feststelle und darüber berichte, würde damit gleichzeitig die aufsichtsrechtliche Tätigkeit der Vorinstanz beleuchtet. Rechtsmissbräuchliches Verhalten dürfe daher nicht leichthin angenommen werden, da ein Zugangsgesuch die Transparenz der Verwaltung bezwecke und die Beschwerdegegnerin von Rechten Gebrauch mache, die ihr zustünden.

Materiell befand das Gericht, dass als Ausnahmegrund einzig der Schutz von Personendaten in Frage komme. Es gab zu bedenken, dass die Einschwärzung von Bank- und Postkontonummern im Sinne der Klarheit auch in das Dispositiv der Verfügung hätte aufgenommen werden sollen. Auch seien Personendaten von Drittpersonen, welche am Verfahren nicht beteiligt sind, einzuschwärzen. Eine von

den Beschwerdeführerinnen darüber hinaus begehrte Anonymisierung wies das Gericht zurück und erklärte, dass ein hohes Interesse der Öffentlichkeit bestehe, ihrerseits die Aufsichtstätigkeit einer Behörde nachzuvollziehen. Das setze voraus, dass der Zugang zu den Abrechnungen gewährt werde.

Abschliessend äusserte sich das Gericht zur Praxisänderung des SECO. Zunächst fragte sich das Gericht, ob sich für Zugangsgesuche zu Abrechnungen der paritätischen Kommissionen bereits eine ständige Praxis entwickelt habe. Es kam zum Schluss, dass das Interesse an der richtigen Rechtsanwendung vorliegend höher zu werten sei als das Einzelinteresse der Beschwerdeführenden. Das SECO hätte auf eine vorherige Ankündigung einer allfälligen Praxisänderung verzichten können.

Das Schlichtungsverfahren vor dem Beauftragten würde überdies seines Sinnes beraubt, wenn es den Behörden anschliessend verwehrt wäre, in besserer Erkenntnis der «ratio legis» und gestützt auf die Empfehlungen des Beauftragten von ihrer ursprünglich vertretenen Auffassung abzuweichen (Urteil vom 9. Dezember 2013, Ref. A-2434/2013). In Bezug auf die Kosten der nicht am Beschwerdeverfahren beteiligten gesuchstellenden Partei wird auf das nachfolgende Urteil verwiesen.

5. SECO / Abrechnungen mehrerer paritätischer Kommissionen II

Das BVGer befasste sich mit einer weiteren Verfügung, welche das Staatssekretariat für Wirtschaft SECO entsprechend der Empfehlung des Beauftragten vom 20. Februar 2013 erlassen hatte (vgl. den vorliegenden Tätigkeitsbericht, Ziff. 2.3.1, Empfehlung 3). Diese Verfügung steht in Zusammenhang mit dem erwähnten Urteil, in welchem der Zugang zu sämtlichen Abrechnungen mehrerer paritätischer Kommissionen für das Jahr 2010 Streitgegenstand war.

Die Beschwerdeführerin (eine paritätische Kommission) rügte, das SECO habe als Vorinstanz offensichtlich übersehen, dass der Beauftragte in ihrem Fall die Ablehnung des Zugangsgesuches empfohlen habe. Das Dispositiv der Verfügung stehe im klaren Widerspruch zu den Erwägungen des Beauftragten. Zudem machte die Beschwerdeführerin geltend, dass das BGÖ nicht auf privatrechtlich organisierte paritätische Kommissionen anwendbar sei.

Das SECO war der Meinung, dass die Beschwerdeführerin kein schützenswertes Interesse am Zugang habe. Entsprechend der Empfehlung des Beauftragten sei kein Zugang zu den Abrechnungen gewährt worden, da die Beschwerdeführerin für das Jahr 2010 nicht zur Einreichung von Abrechnungen verpflichtet gewesen sei.

Das Gericht hat die Beschwerde gutgeheissen. Es hob die Verfügung aufgrund eines Formmangels der Vorinstanz auf und stellte auch fest, dass kein amtliches Dokument vorhanden sei. Auf die übrigen Rügen der Beschwerdeführerin ist das Gericht nicht eingegangen.

In Bezug auf die Kosten für den Gesuchsteller hat das Gericht festgehalten, dass eine Partei, die im erstinstanzlichen Verfahren Anträge gestellt oder das Verfahren veranlasst habe, sich ihrer Kostenpflicht in einem von einer anderen Partei angestrengten Beschwerdeverfahren nicht dadurch entziehen könne, indem sie dort keine Anträge stelle. Sie bleibe notwendige Gegenpartei und damit kostenpflichtig, soweit sie mit ihren im erstinstanzlichen Verfahren gestellten Anträgen unterliege.

Ausnahmen von diesen Grundsätzen würden sich nur rechtfertigen, wenn ein nicht von ihr verschuldeter Verfahrensfehler zur Gutheissung der Beschwerde führe und die Beschwerdegegnerin entweder die Gutheissung des Rechtsmittels beantrage oder sich eines Antrages enthalten habe. Im konkreten Fall wurden die Verfahrenskosten ausnahmsweise erlassen, weil die Gründe, die zur Gutheissung der Beschwerde geführt haben, bei Verfahrensfehlern des SECO zu suchen waren (Urteil vom 9. Dezember 2013, Ref. A-2064/2013).

2.4.2 Bundesgericht

Gegen das oben besprochene Urteil des Bundesverwaltungsgerichts zur Gebührenerhebung gegenüber Medienschaffenden erhob der Redaktionsleiter der Konsumentenzeitschrift «saldo» Beschwerde vor Bundesgericht mit dem Begehren, dieses Urteil aufzuheben und ihn als Medienschaffenden von der Auferlegung von Gebühren für den Zugang zur verlangten Liste zu befreien.

In seinem Urteil befand das Bundesgericht, entgegen den Erwägungen der Vorinstanz, dass am Zugang der Medien zu amtlichen Dokumenten ein öffentliches Interesse besteht, das einen Gebührenverzicht rechtfertigen kann, ohne dass die Informationsbeschaffung von geradezu existenzieller Bedeutung sein müsse. Die Behörde verfüge aber über einen gewisser Ermessensspielraum, in dessen Rahmen sie neben dem durch das Zugangsgesuch verursachten Kostenaufwand das öffentliche Interesse am Zugang der Medien zu den amtlichen Dokumenten berücksichtigen könne.

Unter Würdigung der konkreten Umstände des zu beurteilenden Falles kam das Bundesgericht zum Schluss, dass das ESTI dem Beschwerdeführer zumindest nicht den vollen Arbeitsaufwand von sechs Stunden und damit eine Gebühr über 600 Franken hätte auferlegen dürfen. Es sprach sich für eine Reduktion der Gebühr um mindestens 50 Prozent aus, wobei es die Frage nach einer bloss entsprechenden Reduktion der Gebühr oder einen gänzlichen Verzicht auf eine Gebührenauferlegung dem pflichtgemäss auszuübenden Ermessen des ESTI überliess, an welches es den Entscheid zurückwies (Urteil vom 19. November 2013, Ref. 1C_550/2013).

Mit diesem Entscheid bestätigt das Bundesgericht seine mit BGE 139 I 114 eingeleitete Praxis hinsichtlich der Gebührenerhebung gegenüber Medienschaffenden für den Zugang zu amtlichen Dokumenten: Im besagten Urteil hatte es einen Entscheid des Bundesverwaltungsgerichts umgestossen (vgl. unseren Tätigkeitsbericht 2012/2013, Ziff. 2.4.1).

2.5 Ämterkonsultationen und weitere Stellungnahmen

2.5.1 Entwurf zu einem Bundesratsantrag betreffend Botschaft zum Nachrichtendienstgesetz

Der Beauftragte hat im Rahmen des Ämterkonsultationsverfahrens über den Entwurf zu einem Antrag an den Bundesrat betreffend Botschaft zum Nachrichtendienstgesetz (NDG) erneut Stellung genommen (vgl. Tätigkeitsbericht 2012/2013, Ziff. 2.5.4).

Dabei wies er erneut darauf hin, dass der Ausschluss der gesamten «Informationsbeschaffung nach dem Nachrichtendienstgesetz» aus dem sachlichen Geltungsbereich sowohl dem Zweck als auch der Systematik des Öffentlichkeitsgesetzes (BGÖ) widerspricht. Weiter sehe der Entwurf keine Unterscheidung von nachrichtendienstlichen Informationen hinsichtlich ihres Sensibilisierungsgrades vor.

Der Beauftragte unterstrich, dass das Instrumentarium des Gesetzes mit all seinen Ausnahmebestimmungen völlig ausreiche, um dem erhöhten Schutzbedarf der nachrichtendienstlichen Tätigkeit gerecht zu werden. Schliesslich gab er erneut zu bedenken, dass es mit Blick auf Sinn und Zweck des BGÖ von eminenter Wichtigkeit sei, der Bevölkerung gerade in sensiblen behördlichen Bereichen ein Mindestmass an Verwaltungstransparenz zuzugestehen. Dies haben nicht zuletzt die jüngsten Geschehnisse im Zusammenhang mit dem US-Nachrichtendienst NSA gezeigt.

Schliesslich weist der Beauftragte mit Blick auf die Jahresstatistik über alle im Berichtsjahr bei der Bundesverwaltung eingegangenen Zugangsgesuche nach dem BGÖ darauf hin, dass bereits die geringe Anzahl von zwölf Gesuchen beim Nachrichtendienst (NDB) die Frage aufwirft, ob sich ein Ausschluss der Kernaufgabe des Dienstes aus dem Geltungsbereich des BGÖ überhaupt rechtfertigen lässt. Wird dabei ebenso berücksichtigt, dass von diesen insgesamt zwölf Gesuchen in immerhin drei Fällen ein teilweiser Zugang bzw. ein Zugang unter zeitlichem Aufschub und in einem Fall sogar ein vollständiger Zugang gewährt wurde, so ist die Notwendigkeit eines Sonderstatus des Nachrichtendienstes erst recht nicht ersichtlich.

Die Haltung des Beauftragten deckt sich mit der Forderung der Internationalen Konferenz der Informationsbeauftragten, welche in ihrer Berliner Erklärung verlangt, dass das Öffentlichkeitsprinzip auch für die Geheimdienste gilt (s. Ziffer 2.7.1 des vorliegenden Tätigkeitsberichts).

2.5.2 Entwurf eines Aussprachepapiers des Bundesrates betreffend das Beschaffungscontrolling der Bundesverwaltung

Der Beauftragte hat im Rahmen der Ämterkonsultation zum Entwurf eines Aussprachepapiers des Bundesrates über den Zugang zu amtlichen Dokumenten nach dem Öffentlichkeitsgesetz (BGÖ) betreffend das Beschaffungscontrolling der Bundesverwaltung Stellung genommen («Loi sur la transparence: accès à des documents officiels concernant le controlling des achats de l'administration fédérale; résultats de la Conférence des Secrétaires généraux du 17 décembre 2012»).

Der Entwurf sah unter anderem vor, dass Behörden amtliche Dokumente vor der Zugänglichmachung anonymisieren sollten, wenn in diesen die Kreditoren (Lieferfirmen) eines Bundesorgans gemäss ihrer Umsatzstärke aufgelistet und Daten enthalten sind, anhand welcher die betreffenden Unternehmen identifiziert werden können. Weiter sah der Entwurf bei der Zuständigkeit für die Bearbeitung von Zugangsgesuchen vom BGÖ abweichende Regeln vor.

Der Beauftragte widersprach der Haltung des Aussprachepapiers, wonach eine Auflistung der jeweils 40 umsatzstärksten Lieferfirmen pro Bundesbehörde inklusive des groben Leistungsinhaltes und des Entgeltes eine Information darstelle, welche mit Blick auf den Ausnahmekatalog des BGÖ als Geschäftsgeheimnis anzusehen sei. Vielmehr sehe das öffentliche Beschaffungsrecht die Publikation dieser Informationen gerade vor. Weiter wies der Beauftragte darauf hin, dass an der Bekanntgabe der betroffenen Firmennamen ein überwiegendes öffentliches Interesse bestehen könne, was der Entwurf des Aussprachepapiers völlig ausser Acht lasse.

So sehe das BGÖ etwa explizit vor, dass der Zugang zu amtlichen Dokumenten mit Personendaten trotz einer möglichen Beeinträchtigung der Privatsphäre der betroffenen Personen gewährt werden könne, sofern das öffentliche Interesse am Zugang überwiege. Zudem gehe die Öffentlichkeitsverordnung gerade in Fällen von besonderen Beziehungen zwischen Behörden und Privaten von einem überwiegenden öffentlichen Interesse aus, sofern dem Privaten aus dieser Beziehung bedeutende Vorteile erwachsen. Im Ergebnis gehe es hier darum, dem Steuerzahler Rechenschaft über die Verwendung von Steuergeldern in Millionenhöhe abzulegen.

Zur Frage der Zuständigkeit für die Bearbeitung von Zugangsgesuchen wies der Beauftragte darauf hin, dass das BGÖ diese Frage abschliessend regle und dazu

einzig auf den Umstand abstelle, welche Behörde das verlangte Dokument erstellt oder als Hauptadressatin empfangen hat.

Zu den Lösungsvorschlägen des Aussprachepapiers und des entsprechenden Bundesratsbeschlusses vom 1. Mai 2013 nahm der Beauftragte ausserdem anlässlich seiner Empfehlung vom 23. Dezember 2013 an das Bundesamt für Bauten und Logistik BBL ausführlich Stellung (vgl. Ziffer 2.3.1 des vorliegenden Tätigkeitsberichts 2013/2014, Empfehlung 34).

2.6 Varia

2.6.1 Mitarbeit in der Arbeitsgruppe «Richtlinien Gebührenerhebung BGÖ»

Im Rahmen der Diskussion über den Umgang mit BGÖ-Gesuchen von Medienschaffenden hat die Generalsekretärenkonferenz (GSK) der Gruppe Datenschutz den Auftrag erteilt, in Zusammenarbeit mit dem Beauftragten und dem BJ, Richtlinien für die Gebührenerhebung bei Zugangsgesuchen zu erarbeiten. Der Beauftragte hat in einer von der Gruppe Datenschutz eingesetzten und unter der Federführung der Bundeskanzlei stehenden Arbeitsgruppe als beigezogener Experte teilgenommen. Dabei brachte er seine Sichtweise ein und unterbreitete mehrere Vorschläge zur Gebührenfrage.

Die Arbeitsgruppe berücksichtigte diese in ihrem Entwurf zuhanden der Gruppe Datenschutz jedoch nur teilweise. Gegenüber dem Entwurf bestehen mehrere Differenzen: So ist der Beauftragte der Ansicht, dass die Richtlinien Artikel 17 Absatz 1 des BGÖ respektieren müssen. Hätte der Gesetzgeber tatsächlich eine absolute Gebührenpflicht gewollt, hätte er in diesem Artikel die Formulierung «in der Regel» weggelassen. Deshalb handelt es sich nach Ansicht des Beauftragten lediglich um ein Gebührenerhebungsrecht. Wenn die Vollzugsbestimmungen den gesetzlichen Ermessensspielraum der Behörden einschränken, wird folglich das Legalitätsprinzip verletzt.

Weiter hat der Gesetzgeber nach Auffassung des Beauftragten bewusst auf die Regelung von Versandkosten verzichtet. Dafür sprechen auch die Ausführungen des BJ über die organisatorischen und technischen Aspekte der Umsetzung des BGÖ aus dem Jahr 2005. Auch ist der Beauftragte der Meinung, dass die Verknüpfung von zwei Interessen (öffentliches Interesse am Zugang zu amtlichen Dokumenten und öffentliches Interesse am unentgeltlichen Zugang) verwirrend und praxisuntauglich ist. Schliesslich ist der Beauftragte gegen die vorgeschlagene Regelung der Gebührenerhebung bei Medienschaffenden. Einerseits schränkt eine auf 20 Prozent limitierte Gebührenreduktion das Ermessen der Behörde ein, sodass eine darüber hinausgehende Reduktion oder sogar ein Verzicht nicht mehr möglich ist. Anderseits entspricht die vorgesehene Regelung weder dem Konzept des BGÖ noch dem Urteil des Bundesgerichts (vgl. BGE 139 I 114).

Der Entwurf der Arbeitsgruppe mitsamt ihren Empfehlungen wurde von der Gruppe Datenschutz zur Kenntnis genommen und an die GSK weitergeleitet. Diese hat die Empfehlungen beraten und diese an der Sitzung vom 22. November 2013 formell erlassen. Entgegen dem Entwurf der Arbeitsgruppe nahm die GSK eine Spezialregelung für Medienschaffende auf, wonach bei deren Zugangsgesuchen die Gebühr um 20 Prozent reduziert werden kann.

Zwar ist der Beauftragte der Ansicht, dass kein Rechtsanspruch auf kostenlosen Zugang zu amtlichen Dokumenten besteht. Er vertritt jedoch weiterhin die Meinung, dass im Rahmen des Ermessens nach Artikel 17 Abs. 1 BGÖ – auch bei Medienschaffenden – auf eine Gebühr verzichtet werden kann. Diese Position entspricht auch der neuesten bundesgerichtlichen Rechtsprechung. Konkret beurteilt wurde die Gebührenerhebung bei Medienschaffenden. Ein Anspruch auf einen Gebührenverzicht verneinte das Gericht. Allerdings entschied es, dass die Gebühren um mindestens die Hälfte zu reduzieren seien. Es befand mit anderen Worten, dass im Einzelfall eine Reduktion um mehr als 50 Prozent möglich ist (vgl. Ziffer 2.4.2 des vorliegenden Tätigkeitsberichts).

2.6.2 Tagung zum Öffentlichkeitsprinzip

In Zusammenarbeit mit dem Bundesamt für Justiz (BJ) organisierte der Beauftragte am 24. Februar 2013 den zweiten «Tag des Öffentlichkeitsprinzips» für die Öffentlichkeitsberaterinnen und -berater der Bundesverwaltung. Diese Veranstaltung ermöglichte einerseits den Erfahrungsaustausch der rechtsanwendenden Behörden, andererseits konnten Fragen, die sich im Zusammenhang mit dem Öffentlichkeitsgesetz (BGÖ) wiederholt stellen, diskutiert und vom Beauftragten, dem BJ und der BK beantwortet werden.

Im Anschluss an diese Tagung überarbeiteten der EDÖB und das BJ das Dokument «Umsetzung des Öffentlichkeitsprinzips in der Bundesverwaltung: Häufig gestellte Fragen» aus dem Jahr 2010. Zusätzlich zu den bisherigen Fragen und Antworten fasst es die an der Veranstaltung beantworteten Fragen zusammen. Das Dokument «FAQ zur Umsetzung des Öffentlichkeitsprinzips» ist auf unserer Website abrufbar (www.derbeauftragte.ch, Öffentlichkeitsprinzip – Dokumentation).

2.6.3 Beziehungen zu kantonalen Schlichtungsstellen – Arbeitsgruppe Schlichtungswesen

Der Beauftragte und die kantonalen Öffentlichkeitsbeauftragten, welche auch Schlichtungsverfahren durchführen, trafen sich auch im Jahr 2013 zum Erfahrungsaustausch. Im Rahmen einer im Herbst 2011 gebildeten Arbeitsgruppe konnten so Fragen der Schlichtungstätigkeit und des Öffentlichkeitsprinzips diskutiert werden. Diese Zusammenarbeit ist für die Beteiligten besonders wichtig und wertvoll, da es sich bei der Öffentlichkeitsgesetzgebung um ein neues Rechtsgebiet handelt und Praxis, Rechtsprechung und Lehre erst spärlich vorhanden sind.

2.7 International

2.7.1 Internationale Konferenz der Informationsfreiheitsbeauftragten

Informationsfreiheitsbeauftragte aus aller Welt fordern in einer Resolution, das Recht auf Zugang zu Informationen zu stärken und die Transparenz staatlichen Handelns zu erhöhen.

Die achte Internationale Konferenz der Informationsfreiheitsbeauftragten fand vom 18. bis 20. September 2013 in Berlin statt. An der Konferenz nahmen Delegierte aus 35 Staaten teil. Im öffentlichen Teil der Konferenz wurden aktuelle Fragen zu Transparenz und Offenheit staatlichen Handelns diskutiert. Die Hauptthemen waren «Transparenz im Spannungsfeld» und «Medien und Netzpolitik».

Im internen Teil, an ihrer Abschlusskonferenz, verabschiedeten die Informationsfreiheitsbeauftragten die «Berliner Erklärung zur Stärkung der Transparenz auf nationaler und internationaler Ebene». In der Resolution fordern sie unter dem Titel «Transparenz – Treibstoff der Demokratie», das Recht auf Informationszugang müsse gestärkt und die staatlichen Akteure zu Transparenz verpflichtet werden. In der «Berliner Erklärung» heisst es u.a. weiter, dass sich die Geheimdienste dem Anspruch auf Transparenz nicht prinzipiell verweigern können. Gerade weil deren Tätigkeit tief in die Grundrechte der Bürgerinnen und Bürger eingreift, ist nach Ansicht der Informationsfreiheitsbeauftragten eine öffentlich nachvollziehbare rechtsstaatliche Kontrolle erforderlich und notwendig.

Die Beauftragten sprechen sich sowohl auf nationaler als auch auf internationaler Ebene für die Schaffung von umfassenden und wirksamen rechtlichen Verpflichtungen für den Informationszugang auf Antrag und für eine aktive Bereitstellung von Informationen aus. Sie unterstützen die Anerkennung der Informationsfreiheit als internationales Grundrecht. Zudem empfehlen sie, dass alle Staaten der Konvention des Europarats über den Zugang zu amtlichen Dokumenten vom 18. Juni 2009 (Tromsø-Konvention) beitreten. Die Schweiz gehört zu den Staaten, die der Konvention bisher nicht beigetreten sind.

Die «Berliner Erklärung» befindet sich auf unserer Webseite www.derbeauftragte.ch, Der EDÖB – Internationale Zusammenarbeit.

3. Der EDÖB

3.1 Achter Datenschutztag

Anlässlich des achten internationalen Datenschutztags organisierten wir ein Podiumsgespräch zu den Enthüllungen Edward Snowdens und ihrer Bedeutung für den Datenschutz in der Schweiz. Bürgerinnen und Bürger konnten auf unserem Blog mitdiskutieren.

An der Diskussion, die am 28. Januar 2014 im Politforum Käfigturm in Bern stattfand, debattierte der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte Hanspeter Thür gemeinsam mit SP-Ständerätin Anita Fetz, FDP-Nationalrat Rudi Noser und Alexis Roussel, dem Präsidenten der Piratenpartei. Geleitet wurde das Podium von René Zeller, dem stellvertretenden Chefredaktor der NZZ. Einig waren sich die Teilnehmer, dass die Affäre rund um den Nachrichtendienst NSA dem Thema «Schutz der Privatsphäre» eine neue Dimension verliehen und die Öffentlichkeit, die Politik inbegriffen, wachgerüttelt hat.

Wie die Runde betonte, zählen nicht nur Geheimdienste und andere Behörden zu den eifrigen Datensammlern sondern insbesondere auch Unternehmen. Stichworte sind Kundenkarten, Soziale Netzwerke, Onlinebörsen, E-Banking oder das Internet der Dinge. Bei der Nutzung solcher Dienste und Technologien fallen Unmengen an Personendaten an, die sich mit ausgeklügelten Methoden auswerten lassen (Big Data). Mit diesen können präzise Aussagen über das gegenwärtige und künftige Verhalten der Menschen generiert werden. Während Ruedi Noser den Nutzen von Big Data hervorhob, wiesen die übrigen Podiumsteilnehmer auf die Risiken für die Privatsphäre der Userinnen und User hin. Besonders bezüglich Transparenz und informationeller Selbstbestimmung bestehe Handlungsbedarf. Thür schlug in diesem Zusammenhang vor, die Sanktionsmöglichkeiten des EDÖB bei Datenschutzverletzungen auszudehnen.

Am selben Tag diskutierten zudem interessierte Bürgerinnen und Bürger auf unserem Blog über die Bedeutung der Affäre Snowden für die Zukunft des Datenschutzes.

3.2 Publikationen des EDÖB im laufenden Geschäftsjahr

Unser wichtigster Publikationskanal ist die Webseite www.derbeauftragte.ch, auf der Bürgerinnen und Bürger nützliche Informationen zu den Bereichen Datenschutz und Öffentlichkeitsprinzip finden. Neu hinzugekommen sind im Berichtsjahr u.a. Erläuterungen im Bereich der Videoüberwachung und zu den Themen Webtracking, Social Media Monitoring sowie Sport und Doping.

Der neuste Trend auf dem Markt der Videoüberwachung heisst «Dashcam». Diese Kameras werden in Fahrzeuge eingebaut, um das Geschehen auf der Strasse zu filmen. Die Gründe dafür reichen von reiner Unterhaltung bis zur Beschaffung von Beweismitteln bei Unfällen. In einigen Ländern sind solche Kameras gesetzlich oder durch die Haftpflichtversicherer vorgeschrieben, in der Schweiz jedoch verstösst ihr Einsatz gegen Grundsätze des Datenschutzgesetzes (www.derbeauftragte.ch, Datenschutz – Technologien – Videoüberwachung).

Heikel ist auch die Videoüberwachung in Garderoben und Toiletten, da sie einen starken Eingriff in die Intimsphäre der betroffenen Personen darstellt. Wie in unseren auf www.derbeauftragte.ch publizierten Erläuterungen erklärt wird, dürfen Kameras in diesem Bereich nur unter Einhaltung strenger Regeln datenschutzkonform betrieben werden (Datenschutz – Technologien – Videoüberwachung). In der selben Rubrik haben wir im Berichtsjahr Erläuterungen zu den Bedingungen für die Herausgabe von Videobildern an Strafverfolgungsbehörden sowie zur Videoüberwachung mittels Drohnen publiziert.

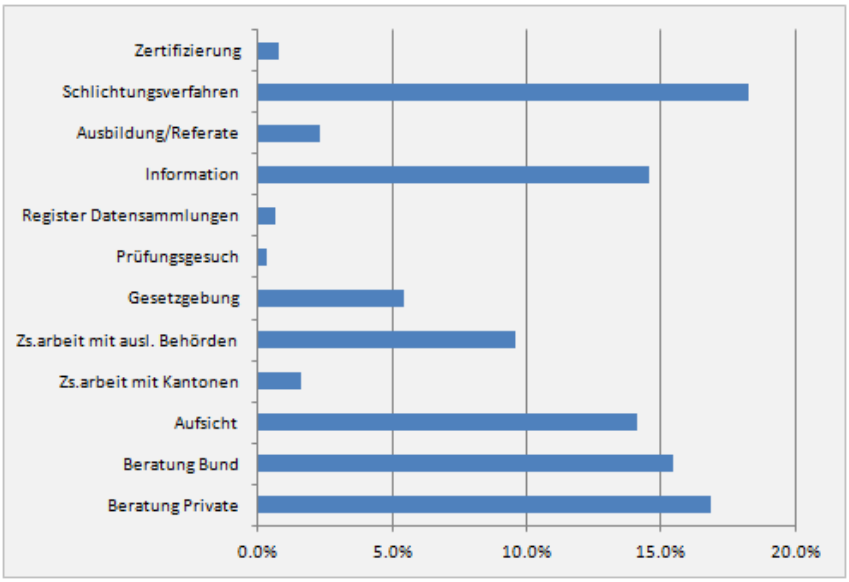
Des Weiteren finden sich auf unserer Website neu Informationen zum Datenschutz bei Social Media Monitoring (Datenschutz – Internet und Computer – soziale Medien). Unter diesem Begriff versteht man das systematische und kontinuierliche Beobachten der für das auftraggebende Unternehmen relevanten Informationen, die online in den sozialen Medien auftauchen. Beim Einsatz von Social Media Monitoring sind die Anforderungen des Datenschutzes zu beachten.

Webtracking-Dienste werden von Webseitenbetreibern und Werbenetzwerken eingesetzt, um die Besucherbewegungen auf einer Website oder das Surfverhalten von Internetnutzern zu erfassen. Die damit erhobenen Daten ermöglichen es, Rückschlüsse auf die Interessen, Vorlieben oder Gewohnheiten der Userinnen und User zu ziehen. Wie unseren Erläuterungen zu entnehmen ist, sind aus datenschutzrechtlicher Sicht viele der bekannten Webtracking-Dienste problematisch (Datenschutz – Internet und Computer – Webtracking).

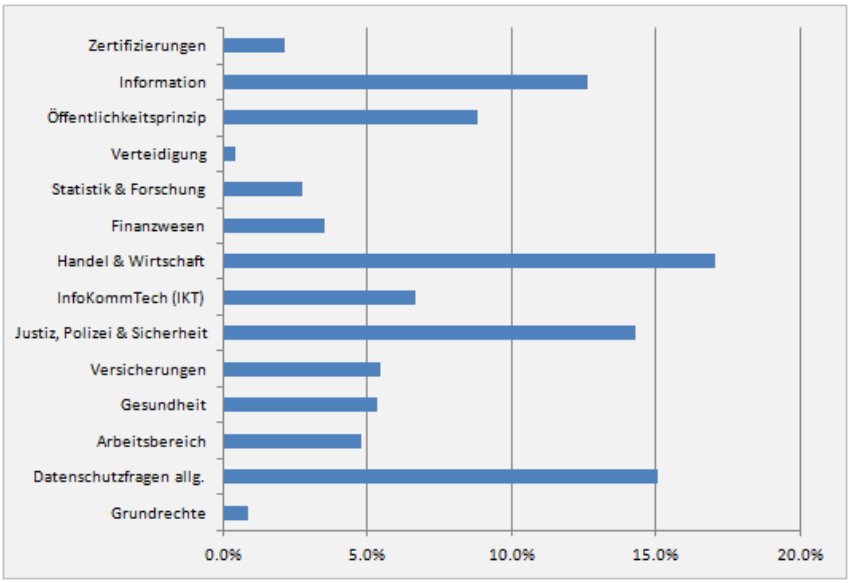
In den ebenfalls neu aufgeschalteten Ausführungen zum Thema Sport und Doping werden die datenschutzrechtlichen Auswirkungen des 2012 in Kraft getretenen Bundesgesetzes über die Förderung von Sport und Bewegung erläutert (Datenschutz – Freizeit und Sport). Das Gesetz regelt insbesondere die Dopingkontrollen und den Datenaustausch zwischen den nationalen und internationalen Anti-Doping-Stellen sowie den Strafverfolgungs- und Gerichtsbehörden.

3.3 Statistik über die Tätigkeit des EDÖB vom 1. April 2013 bis 31. März 2014

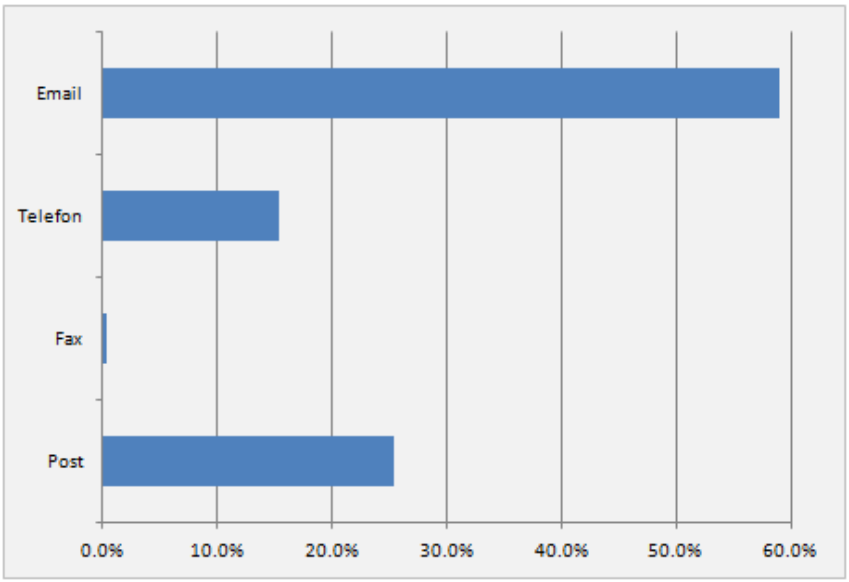
Aufwand nach Aufgabengebiet



Aufwand nach Sachgebiet



Herkunft der Anfragen



3.4 Statistik über die bei den Departementen eingereichten Zugangsgesuche nach Art. 6 des Öffentlichkeitsgesetzes (Zeitraum: 1. Januar 2013 bis 31. Dezember 2013)

Departement	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt / aufgeschoben	Zugangsgesuch hängig	Zugangsgesuch zurückgezogen
BK	27	15	8	4	0	0
EDA	73	63	5	5	0	0
EDI	92	39	18	29	4	2
EJPD	48	17	20	7	2	2
VBS	29	6	17	5	0	1
EFD	32	11	13	8	0	0
WBF	68	19	18	28	0	3
UVEK	100	48	23	17	2	10
Total 2013 (in %)	469 (100 %)	218 (46 %)	122 (26 %)	103 (22 %)	8 (2 %)	18 (4 %)
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 %)	-	-

Bundeskanzlei BK

Betroffener Fachbereich	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt / aufgeschoben	Zugangsgesuch hängig	Zugangsgesuch zurückgezogen
BK	13	5	7	1	0	0
EDÖB	14	10	1	3	0	0
Total	**27**	**15**	**8**	**4**	**0**	**0**

Eidgenössisches Departement für auswärtige Angelegenheiten EDA

Betroffener Fachbereich	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt / aufgeschoben	Zugangsgesuch hängig	Zugangsgesuch zurückgezogen
EDA	73	63	5	5	0	0
Total	**73**	**63**	**5**	**5**	**0**	**0**

Eidgenössisches Departement des Innern EDI

Betroffener Fachbereich	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt / aufgeschoben	Zugangsgesuch hängig	Zugangsgesuch zurückgezogen
GS	12	3	1	8	0	0
EBG	0	0	0	0	0	0
BAK	7	4	0	3	0	0
BAR	4	4	0	0	0	0
METEO CH	0	0	0	0	0	0
NB	0	0	0	0	0	0
BAG	33	15	5	10	3	0
BFS	1	0	0	1	0	0
BSV	13	7	5	1	0	0
BVET*	4	4	0	0	0	0
SNM	0	0	0	0	0	0
SWISS-MEDIC	18	2	7	6	1	2
SUVA	0	0	0	0	0	0
Total	**92**	**39**	**18**	**29**	**4**	**2**

* ab 1. Januar 2014 Bundesamt für Lebensmittelsicherheit und Veterinärwesen BLV

Eidgenössisches Justiz- und Polizeidepartement EJPD

Betroffener Fachbereich	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt / aufgeschoben	Zugangsgesuch hängig	Zugangsgesuch zurückgezogen
GS	5	2	2	1	0	0
BJ	3	2	0	1	0	0
FEDPOL	4	2	1	1	0	0
METAS	2	1	1	0	0	0
BFM	24	9	12	0	2	1
SIR	0	0	0	0	0	0
IGE	1	0	1	0	0	0
ESBK	5	1	0	3	0	1
ESchK	0	0	0	0	0	0
RAB	0	0	0	0	0	0
ISC	4	0	3	1	0	0
NKVF	0	0	0	0	0	0
Total	**48**	**17**	**20**	**7**	**2**	**2**

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS

Betroffener Fachbereich	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt / aufgeschoben	Zugangsgesuch hängig	Zugangsgesuch zurückgezogen
GS	6	3	2	1	0	0
Verteidig. / Armee	3	0	3	0	0	0
NDB	12	1	8	3	0	0
armasuisse	7	1	4	1	0	1
BASPO	0	0	0	0	0	0
BABS	1	1	0	0	0	0
Total	**29**	**6**	**17**	**5**	**0**	**1**

Eidgenössisches Finanzdepartement EFD

Betroffener Fachbereich	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt / aufgeschoben	Zugangsgesuch hängig	Zugangsgesuch zurückgezogen
GS	7	2	3	2	0	0
EFV	2	1	1	0	0	0
EPA	2	0	2	0	0	0
ESTV	5	0	4	1	0	0
EZV	4	3	1	0	0	0
EAV	2	0	1	1	0	0
BBL	2	1	0	1	0	0
BIT	1	0	0	1	0	0
EFK	6	4	0	2	0	0
SIF	1	0	1	0	0	0
PUBLICA	0	0	0	0	0	0
ZAS	0	0	0	0	0	0
Total	**32**	**11**	**13**	**8**	**0**	**0**

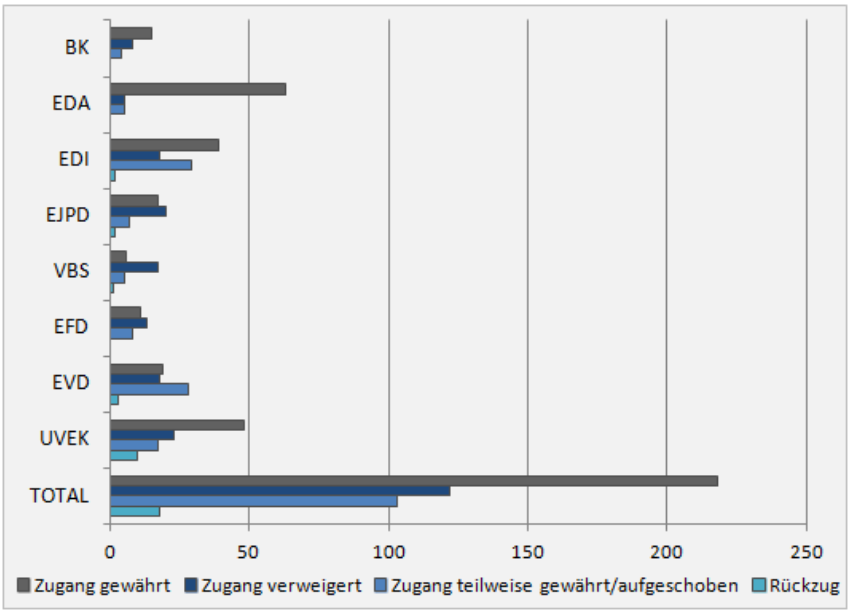
Eidgenössisches Departement für Wirtschaft, Bildung und Forschung WBF

Betroffener Fachbereich	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt / aufgeschoben	Zugangsgesuch hängig	Zugangsgesuch zurückgezogen
GS	2	0	0	2	0	0
SECO	9	3	3	3	0	0
SBFI	4	0	4	0	0	0
BLW	30	4	7	19	0	0
BWL	1	0	1	0	0	0
BWO	0	0	0	0	0	0
PUE	2	1	1	0	0	0
WEKO	16	8	2	3	0	3
ZIVI	0	0	0	0	0	0
BFK	0	0	0	0	0	0
SNF	1	0	0	1	0	0
EHB	0	0	0	0	0	0
ETH Rat	3	3	0	0	0	0
Total	**68**	**19**	**18**	**28**	**0**	**3**

Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK

Betroffener Fachbereich	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt / aufgeschoben	Zugangsgesuch hängig	Zugangsgesuch zurückgezogen
GS	0	0	0	0	0	0
BAV	7	2	1	4	0	0
BAZL	17	10	6	1	0	0
BFE	11	5	3	3	0	0
ASTRA	4	4	0	0	0	0
BAKOM	5	1	0	1	0	3
BAFU	14	6	3	5	0	0
ARE	1	1	0	0	0	0
ComCom	1	1	0	0	0	0
ENSI	26	6	10	3	0	7
PostCom	0	0	0	0	0	0
UBI	14	12	0	0	2	0
Total	**100**	**48**	**23**	**17**	**2**	**10**

Behandlung der Zugangsgesuche



3.5 Statistik über die bei der Bundesanwaltschaft eingereichten Zugangsgesuche nach Art. 6 des Öffentlichkeitsgesetzes (Zeitraum: 1. Januar 2013 bis 31. Dezember 2013)

Bundesanwaltschaft BA

Betroffener Fachbereich	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt / aufgeschoben	Zugangsgesuch hängig	Zugangsgesuch zurückgezogen
BA	1	0	1	0	0	0
Total	**1**	**0**	**1**	**0**	**0**	**0**

3.6 Statistik über die bei den Parlamentsdiensten eingereichten Zugangsgesuche nach Art. 6 des Öffentlichkeitsgesetzes (Zeitraum: 1. Januar 2013 bis 31. Dezember 2013)

Parlamentsdienste PD

Betroffener Fachbereich	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt / aufgeschoben	Zugangsgesuch hängig	Zugangsgesuch zurückgezogen
PD	0	0	0	0	0	0
Total	**0**	**0**	**0**	**0**	**0**	**0**

3.7 Anzahl Schlichtungsgesuche nach Kategorien der Antragsteller (Zeitraum: 1. Januar 2013 bis 31. Dezember 2013)

Kategorie Antragsteller	2013
Medien	24
Privatpersonen (bzw. keine genaue Zuordnung möglich)	27
Interessenvertreter (Verbände, Organisationen, Vereine usw.)	8
Rechtsanwälte	11
Unternehmen	6
Universitäten	0
Total	**76**

3.8 Das Sekretariat des EDÖB

Eidgenössischer Datenschutz-und Öffentlichkeitsbeauftragter:

	Thür Hanspeter, Fürsprecher
Stellvertreter:	Walter Jean-Philippe, Dr. iur.

Sekretariat:

Leiter:	Walter Jean-Philippe, Dr. iur.
Stellvertreter:	Buntschu Marc, lic. iur.
Einheit 1:	11 Personen
Einheit 2:	14 Personen
Einheit 3:	5 Personen
Kanzlei:	2 Personen