22. Tätigkeitsbericht 2014/2015

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Tätigkeitsbericht 2014/2015 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 2014 und 31. März 2015 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. 410.022.d/f

Inhaltsverzeichnis

Vorwort

Regeln für den digitalen Wildwest

Diese Schlagzeile in einer NZZ des letzten Jahres bringt es auf den Punkt: Die Auseinandersetzung um Big Data und das Internet der Dinge ist in vollem Gange und offenbart gleichzeitig gravierende Regelungslücken. Niemanden lässt das Thema kalt: Trendforscher, Wirtschaftsvertreter, Wissenschaftler, Ethiker und andere beleuchten die verschiedenen Aspekte und setzen sich mit Chancen und Gefahren auseinander. Während die einen den digitalen Wildwest kritisieren und Regeln fordern, bejubeln andere das immense Wirtschaftspotenzial von Big Data und verbreiten Goldgräberstimmung. Ich selber habe an zahlreichen Veranstaltungen referiert und die Kontroverse hautnah erlebt. Einig ist man sich immerhin darin, dass die Entwicklung eine grosse. Herausforderung für den Schutz der Privatsphäre darstellt.

In seinem Buch «Die Null-Grenzkosten-Gesellschaft» betont der Soziologe und Big-Data-Experte Jeremy Rifkin das riesige Potenzial der digitalen Revolution mit dem Internet der Dinge (IoT), warnt aber zugleich, dass «das Problem der Privatsphäre eine wesentliche Sorge bleiben (wird), die in hohem Masse sowohl das Tempo des Übergangs als auch die Wege bestimmen wird, auf denen wir in die nächste Periode unserer Geschichte gehen.» Die Lösungsansätze könnten aber nicht unterschiedlicher sein. Während die einen vor den weitreichenden Folgen warnen, postulieren andere die Abschaffung der Privatsphäre. Die habe es im Altertum auch nicht gegeben, was zu Ende gedacht wohl heisst: Wenn wir den technischen Fortschritt voll auskosten wollen, müssen wir aufklärerisches Gedankengut über Bord werfen und uns letztlich autoritären Gesellschaftsformen unterwerfen. Wie die Sklaven im Altertum! Rifkin geht einen andern Weg und stellt die zentrale Frage, wie sich unter diesen Umständen ein transparenter Datenfluss gewährleisten lässt, der allen nützt und dabei garantiert, dass Informationen über das Leben des Einzelnen nicht ohne dessen Genehmigung und nicht in einer Weise benutzt werden, dass er Schaden nimmt.

Die spannende Frage wird sein, wer in diesem Kampf die Oberhand gewinnen wird. In zehn Jahren dürften wir mehr wissen. Solange wird es wohl dauern, bis sich das Potenzial dieser technischen Entwicklung voll entfaltet haben wird. Denn das Internet der Dinge – der grosse künftige Big-Data-Datenlieferant – ist erst am Anfang. Zwar können mit dem Internetprotokoll Version 6 (IPv6) unbeschränkt viele Gegenstände mit IP-Adressen ausgestattet werden, was eine Kommunikation über das Netz ermöglicht. Die wirtschaftliche Umsetzung wird aber noch einige Zeit dauern. Wollen wir den Gang der Dinge noch beeinflussen, müssen die Regeln rasch

angepasst werden. Sonst wird uns die technische Entwicklung vor vollendete Tatsachen stellen.

Die Frage wird auch sein, ob Europa willens ist, die neofeudalistischen Monopole von Google, Facebook, Amazon und Konsorten in die Schranken zu weisen. Erste Stimmen in europäischen Regierungen, die diesen globalen Giganten mit kartellrechtlichen Massnahmen drohen, lassen aufhorchen. Auch die Schweiz muss sich angesichts dieser technologischen Revolution positionieren und Vor- und Nachteile erwägen. Es braucht eine vertiefte gesellschaftliche Debatte und eine Strategie der digitalen Gesellschaft. Ich hoffe sehr, dass die Kommission Rechsteiner, die bis Ende 2017 Resultate liefern soll, wichtige Impulse geben wird, die auch in die Revision des Datenschutzgesetzes (DSG) einfliessen.

Nach den Anschlägen von Paris und Kopenhagen ist es nicht verwunderlich, dass das neue Nachrichtendienstgesetz, das dem Nachrichtendienst eine Reihe neuer Beschaffungsmassnahmen zur Verfügung stellt, die parlamentarische Hürde ohne weiteres nahm. Ob das Gesetz noch eine Volksabstimmung zu bestehen hat, ist derzeit offen. Mit Blick auf die Enthüllungen von Edward Snowden stellt sich die Frage, ob unser Land mit einem schweizerischen Patriot Act den Weg der USA geht und einer flächendeckenden Überwachung den Weg bereitet. Hier ist eine Differenzierung nötig: Bei aller Skepsis ist darauf hinzuweisen, dass eine Überwachung nur in einem konkreten Fall auf richterliche Anordnung und mit Genehmigung durch den Sicherheitsausschuss des Bundesrates erfolgen darf. Bundesrat Ueli Maurer und der Nachrichtendienst betonen, dass es dabei lediglich um rund zwölf Fälle jährlich gehe. Es liegt nun in der Verantwortung der parlamentarischen Aufsicht – wahrgenommen durch die Geschäftsprüfungsdelegation – darüber zu wachen, dass dieser Rahmen eingehalten wird.

Auch wenn die Forderung nach zusätzlichen Kompetenzen für den Staatsschutz nachvollziehbar ist, bereitet der dem Parlament unterbreitete Entwurf einige Sorgen. Vor allem deshalb, weil die Kompetenzen des Staatsschutzes zum Teil weitergehen, als jene der Strafverfolgungsbehörden. Im Unterschied zu letzteren braucht der Nachrichtendienst für den Einsatz von Zwangsmassnahmen keinen konkreten Tatverdacht. Nicht geklärt ist unter anderem, was zu geschehen hat, wenn die Nachrichtendienste auf strafbare Handlungen stossen. Diese Klärung ist auch deshalb wichtig, weil die Strafverfolgungsbehörden mit der derzeit laufenden Revision des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (Büpf) ebenfalls zusätzliche Mittel erhalten (u.a. den Staatstrojaner).

Die AHV-Nummer breitet sich ausserhalb der Sozialversicherung in verschiedenen Verwaltungsbereichen weiter aus. Dieses Jahr ist zum Beispiel das Handelsregister an der Reihe. Wir plädierten dafür, dass die Zentrale Ausgleichsstelle (ZAS) wie beim elektronischen Patientendossier (EPDG) einen von der AHV unabhängigen

Identifikator kreiert. Im Rahmen der Ämterkonsultation konnte der Widerstand des Handelsregisteramtes teilweise überwunden werden. Das Handelsregisteramt wird künftig einen von der AHV-Nummer abgeleiteten sektoriellen Identifikator schaffen und damit deren direkten Verwendung einen Riegel schieben. Wir hätten eine von der AHV-Nummer unabhängige Lösung bevorzugt, wie dies beim EPDG der Fall ist. Wir bedauern auch, dass damit in verschiedenen Verwaltungseinheiten unterschiedliche Konzepte etabliert werden. Der Bundesrat sollte diese Frage mit Blick auf die Schaffung einer einheitlichen Praxis klären. Es braucht einen Grundsatzentscheid darüber, ob eine generalisierte Verwendung der AHV-Nummer als einheitlichen Personenidentifikator angesichts der Risiken für die Grundrechte zulässig ist.

Ein weiteres zentrales Thema, mit dem wir uns im Berichtsjahr befasst haben, betraf die Vielzahl von Daten, die von Wirtschaftsinformationsplattformen wie Moneyhouse weit über den Aspekt der Kreditwürdigkeit hinaus bearbeitet werden. Aufgrund zahlreicher Beschwerden untersuchten wir die Praktiken dieses Unternehmens sehr ausführlich und beendeten die Sachverhaltsabklärung mit zahlreichen Empfehlungen. Die Betreiberin von Moneyhouse hat Anfang 2015 unsere Empfehlungen teilweise angenommen (vgl. unsere Webseite www.derbeauftragte.ch, Datenschutz – Empfehlungen). Die Punkte, bei denen keine Einigung erzielt wurde, werden wir nun dem Bundesverwaltungsgericht zur rechtlichen Klärung unterbreiten.

Positiv vermelden können wir die Entwicklung im Gesundheitswesen. In Zusammenhang mit der Einführung der Fallkostenpauschalen (SwissDRG) und der damit verbundenen Ausweitung der Datenströme konnten wir durchsetzen, dass die datenschutzkonforme Triage der digitalisierten Rechnungen innerhalb der Versicherer durch unabhängige und zertifizierte Datenannahmestellen (DAS) zu erfolgen hat, die der Aufsicht des EDÖB unterstehen. Seit der Einführung haben wir zahlreiche DAS überprüft und dabei massgebende Richtlinien entwickelt. Heute können wir festhalten, dass das neue Konzept nach unseren Vorstellungen umgesetzt wurde und wesentlich dazu beiträgt, dass die Datenflüsse im Gesundheitswesen geordnet und nach einheitlichen Kriterien abgewickelt werden.

Momentan ist die Auslagerung von Diensten in die Cloud oder deren Einbezug im Trend. Wir werden immer wieder von Bundesorganen angefragt, ob sie Datenbearbeitungen an ausländische Anbieter übertragen dürfen. Wir haben entschieden darauf hingewiesen, dass ihnen die Pflicht obliegt, sorgsam mit den Personendaten der Bürger umzugehen und sie insbesondere vor einem unbefugten Zugriff durch ausländische Behörden zu schützen. Auf eine solche Auslagerung ist daher in der Regel zu verzichten. Aber auch als Privatanwender ist es zunehmend schwierig, Geräte ohne die Verwendung von Clouddiensten zu nutzen. Bisher konnten mobile Geräte lokal gesichert oder synchronisiert werden. Die Produkte der neuesten Generation zwingen den Anwender, seine persönlichen Daten an unbekannte Datencenter zu

übertragen. Dies ist eine Entmündigung der Nutzer durch die Hersteller und führt letztlich zum Entzug der Kontrolle über die eigenen Daten.

Am 16. April 2014 verabschiedete der Bundesrat die Open-Government-Data-Strategie Schweiz 2014-2018, welche interessierte Kreise dazu bewog, dem Bundesrat Fragen zu stellen zum wirtschaftlichen Potenzial einer innovativen Datennutzung im Energie-, Verkehrs- und Gesundheitsbereich und wie sich die Schweiz im globalen Datenwettbewerb positionieren wolle. Wichtig aus unserer Sicht ist der Hinweis des Bundesrates, dass er bis Ende Jahr prüfen wolle, ob sich im Bereich Big Data Handlungsbedarf ergebe, namentlich mit Bezug auf Datenschutz und Verfügungsrecht über die eigenen Daten. Wir werden diesen Aspekt – vor allem auch im Hinblick auf die Revision des DSG – aufmerksam verfolgen.

Im Kontext des Öffentlichkeitsgesetzes (BGÖ) gilt es das wegweisende Urteil des Bundesverwaltungsgerichts zu erwähnen, das unsere Empfehlung in Sachen KTI (Kommission für Technologie und Innovation) stützte. Das Gericht kam zum Schluss, dass die Öffentlichkeit ein erhebliches Interesse hat zu erfahren, wie im Zusammenhang mit der Innovationsförderung öffentliche Gelder verwendet werden. Vor einem Jahr habe ich in Zusammenhang mit der Evaluation des BGÖ die Befürchtung geäussert, dass sich der Bericht als Steilvorlage für eine Schwächung des Gesetzes entpuppen könnte. Dies vor allem deshalb, weil der Anstoss zur Evaluation von gewissen Ämtern kam, die sich durch das Gesetz behindert sahen. Inzwischen ist der Bericht da. Eine ausführliche Würdigung findet sich in Kapitel 2.4.1. Erfreulich ist für uns zunächst, dass das Schlichtungsverfahren, so wie wir es bis anhin praktizieren, auf grosse Akzeptanz stösst, und dies obwohl wir in den meisten Fällen wegen fehlender Ressourcen die Fristen nicht einhalten können. Und: Für eine Aufweichung des Gesetzes bietet dieser Bericht keine Grundlage. Im Gegenteil: Wichtig ist die Feststellung, dass der durch das BGÖ geforderte Paradigmenwechsel noch immer nicht in der ganzen Bundesverwaltung vollzogen ist. Gleichwohl möchten wir betonen, dass sich die Akzeptanz laufend verbessert, vor allem dort, wo die Umsetzung des BGÖ auf Führungsstufe angesiedelt ist. Dazu tragen nicht zuletzt auch die zahlreichen Urteile des Bundesverwaltungsgerichts und des Bundesgerichts bei, welche die Empfehlungen des EDÖB bisher in den meisten Fällen stützten.

Abkürzungsverzeichnis

AHVN13	13-stellige AHV-Nummer
BAG	Bundesamt für Gesundheit
BAV	Bundesamt für Verkehr
BAZL	Bundesamt für Zivilluftfahrt
BBl	Bundesblatt
BFM	Bundesamt für Migration (alte Bezeichnung)
BFS	Bundesamt für Statistik
BGÖ	Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung
BGS	Geldspielgesetz
BJ	Bundesamt für Justiz
BK	Bundeskanzlei
BöB	Bundesgesetz über das öffentliche Beschaffungswesen
BPG	Bundespersonalgesetz
BPI	Bundesgesetz über die polizeilichen Informationssysteme des Bundes
BR	Bundesrat
BSV	Bundesamt für Sozialversicherungen
BÜPF	Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs
BWIS	Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit
DAS	Datenannahmestelle
DRG	Diagnosebezogene Fallgruppen
DSG	Bundesgesetz über den Datenschutz
DSMS	Datenschutz-Managementssystem
EDA	Eidgenössisches Departement für auswärtige Angelegenheiten
EFD	Eidgenössisches Finanzdepartement
EFK	Eidgenössische Finanzkontrolle
EPA	Eidgenössisches Personalamt
EPDG	Bundesgesetz über das elektronische Patientendossier
ESTV	Eidgenössische Steuerverwaltung

FDK	Konferenz der kantonalen Finanzdirektorinnen und Finanzdirektoren
fedpol	Bundesamt für Polizei
FINMA	Eidgenössische Finanzmarktaufsicht
FMedG	Bundesgesetz über die medizinisch unterstützte Fortpflanzung
GUMG	Bundesgesetz über genetische Untersuchungen beim Menschen
HFG	Bundesgesetz über die Forschung am Menschen
ICD	International Classification of Diseases
IDAG	Interdepartementale Arbeitsgruppe
IKT	Informatik- und Kommunikationstechnologien
ISAS	Informationssystem Äussere Sicherheit
ISB	Informatiksteuerungsorgan des Bundes
ISDS	Informationssicherheit und Datenschutz
ISIS	Staatsschutz-Informationssystem
ISO/IEC	ISO/International Electrotechnical Commission
ISV-NDB	Verordnung über die Informationssysteme des Nachrichtendienstes des Bundes
JANUS	Informationssystem der Bundeskriminalpolizei
KVG	Bundesgesetz über die Krankenversicherung
KVV	Verordnung über die Krankenversicherung
LFG	Luftfahrtgesetz
LG	Bundesgesetz betreffend Lotterien und gewerbsmässige Wetten
MARS	Statistiken der ambulanten Gesundheitsversorgung
MG	Bundesgesetz über die Armee und die Militärverwaltung
NDB	Nachrichtendienst des Bundes
OKP	Obligatorische Krankenpflegeversicherung
PBG	Personenbeförderungsgesetz
RHG	Bundesgesetz über die Harmonisierung der Einwohnerregister und anderer amtlicher Personenregister
SAS	Schweizerische Akkreditierungsstelle
SBB	Schweizerische Bundesbahnen
SBG	Spielbankengesetz
SEM	Staatssekretariat für Migration

SIF	Staatssekretariat für internationale Finanzfragen
SIK	Schweizerische Informatikkonferenz
SIS	Schengener Information System
SIS II SCG	Koordinierungsgruppe für die Aufsicht über SIS II
SIS II	Schengener Information System II
StFG	Bundesgesetz über die Forschung an embryonalen Stammzellen
StGB	Schweizerisches Strafgesetzbuch
TINs	Steueridentifikationsnummer
UCC	Unified Communication and Collaboration
UPI	Unique Personal Identifier Database
VBS	Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport
VDSG	Verordnung zum Bundesgesetz über den Datenschutz
VDSZ	Verordnung über die Datenschutzzertifizierungen
VöB	Verordnung über das öffentliche Beschaffungswesen
XML	Extensible Markup Language
ZAS	Zentrale Ausgleichsstelle
zefix	Zentraler Firmenindex
ZNDG	Bundesgesetz über die Zuständigkeiten im Bereich des zivilen Nachrichtendienstes

1. Datenschutz

1.1 Grundrechte

1.1.1 Neue Richtlinien in Sachen Datenschutzzertifizierung

Nach dem Inkrafttreten der ISO-Normen 27001 und 27002 im Herbst 2013 haben wir im Frühjahr 2014 unsere Richtlinien über die Datenschutz-Zertifizierung und ihre Anhänge angepasst.

Die grundlegend überarbeiteten Normen ISO/IEC 27001:2013 für die Informationssicherheits-Managementsysteme sind seit 1. Oktober 2013 in Kraft. Da sich unser Zertifizierungsstandard stark an diese beiden internationalen Normen anlehnt, wurde eine entsprechende Anpassung unserer Richtlinien über die Mindestanforderungen an ein Datenschutzmanagementsystem (DSMS) sowie ihres Anhangs notwendig. Die strukturellen Änderungen («Anforderungen») von ISO 27001 betreffen im Wesentlichen eine Angleichung an den Anhang SL des konsolidierten Nachtrags der ISO/IEC-Richtlinien. Unsere neuen Richtlinien, die am 1. Mai 2014 in Kraft getreten sind, aktualisieren namentlich die Definitionen gemäss der Norm ISO/IEC:2014. Zudem gibt es eine Übergangsbestimmung, die bis zum 1. Oktober 2014 den Abschluss der laufenden Zertifizierungsverfahren nach der alten Regelung ermöglicht.

Die Norm ISO 27002 («Code of practice») hat dagegen mit der Einführung neuer Kapitel betreffend Kryptographie und Lieferantenbeziehungen sowie mit der Trennung der Betriebs- von der Kommunikationssicherheit eine tiefer greifende Neugestaltung erfahren. Die Norm besteht nun aus insgesamt 18 Kapiteln, die zusammen 114 Massnahmen umfassen. All diese Änderungen wirken sich auf den Anhang zu unseren Richtlinien unter dem Titel «Leitfaden für das Datenschutzmanagement» aus. Der Anhang enthält eine Anpassung der Umsetzungsmassnahmen für die Datensicherheit, indem bezüglich der Datenvertraulichkeit die neu vorgesehenen Massnahmen für Informationssicherheit im Projektmanagement, für Mobilgeräte und Telearbeit sowie die Massnahmen für Kryptographie hinzugefügt werden. Im Endergebnis sind im Anhang immer noch neun Ziele aufgeführt, die 20 Massnahmen umfassen, von denen die Massnahmen zur Datensicherheit nunmehr auf 71 Massnahmen der neuen Norm ISO 27002 verweisen. Die von der Schweizerischen Akkreditierungsstelle (SAS) bisher zertifizierten Organisationen haben uns im Nachhinein bestätigt, dass insbesondere im Rahmen der Datenannahmestellen (DAS) der Übergang gut verlaufen sei.

1.1.2 Änderungen des ZGB – Infostar und Grundbuch

Für den Betrieb des elektronischen Zivilstandsregisters (Infostar) soll neu der Bund alleine verantwortlich sein. Zudem wird die AHV-Versichertennummer als Personenidentifikator im Grundbuch eingeführt und damit eine landesweite Suche nach Grundstücken ermöglicht. Wir haben zu diesen Änderungen in der Ämterkonsultation Stellung genommen. Der Bundesrat ist unserem Vorschlag der Schaffung eines sektoriellen Personenidentifikators nicht gefolgt.

Angesichts der grossen Bedeutung von Infostar als zentrales Personen-Informationssystem haben wir dem Bundesamt für Justiz im Rahmen der Ämterkonsultation vorgeschlagen, das Register auf gesetzlicher Ebene umfassend zu regeln. Die Erstellung eines Datawarehouses als gespiegelte Datenbank von Infostar, das der Qualitätsüberwachung dienen soll, schien uns zudem in der Vorlage ungenügend geregelt.

Die Einführung der AHV-Nummer im Grundbuch haben wir erneut als unverhältnismässig kritisiert (vgl. unseren 20. Tätigkeitsbericht 2012/2013, Ziffer 1.1.2). Wir haben unsere Positionierung betreffend die Verwendung dieser Nummer als universellen Personenidentifikator pointiert wiederholt. Unserem Vorschlag, einen sektoriellen Identifikator analog dem im Bundesgesetz betreffend das elektronische Patientendossier vorgesehenen Verfahren einzuführen, ist der Bundesrat leider nicht gefolgt (vgl. unseren 21. Tätigkeitsbericht 2013/2014, Ziffer 1.5.1). Wir verfolgen die Entwicklung, die AHV-Nummer als universellen Personenidentifikator in der ganzen Verwaltung und darüber hinaus einzusetzen, aufmerksam.

1.1.3 Revision des Handelsregisterrechts

Auch in diesem Berichtsjahr haben wir zur Revision des Handelsregisterrechts Stellung genommen. Wir meldeten erneut Bedenken hinsichtlich der Verwendung der AHV-Versichertennummer und des Verzichts auf die Einführung des Rechts auf Vergessen an. Die Handelsregisterämter sind neu berechtigt, für die Abfrage von Belegen eine Gebühr zu verlangen. Die Kostenhürde soll unverhältnismässige Abfragen erschweren.

Wir haben in den beiden letzten Tätigkeitsberichten über datenschutzrechtliche Aspekte der Revision des Handelsregisterrechts informiert (2012/2013 und 2013/2014, jeweils Ziffer 1.8.4). Auch im Berichtsjahr hatten wir Gelegenheit, uns dazu zu äussern. Es ist immer noch vorgesehen, Personendaten, die bei einer Anmeldung bei einem Handelsregister gemacht werden, über die UPI-Datenbank bei der Zentralen Ausgleichskasse (ZAS) abzugleichen. Die ZAS verwaltet in dieser Datenbank die zur AHV-Nummer zugehörigen Personendaten. Mit diesem Abgleich

soll die Datenqualität im Handelsregister verbessert werden; u.a. sollen doppelte oder dreifach vorhandene Einträge zur selben Person gefunden und zusammengeführt werden. Der Kreis der Stellen, die Zugriff auf die AHV-Nummer haben, wurde nun in der Vorlage eingeschränkt.

Es ist im Gesetz selber zudem vorgesehen, dass die AHV-Nummer nicht öffentlich einsehbar ist. Zusätzlich soll für natürliche Personen ein sektorieller Identifikator geschaffen werden, der nicht auf die AHV-Nummer rückführbar ist. Für das Zugänglichmachen von Belegen, die zum Teil auch besonders schützenswerte Personendaten enthalten, sollen Handelsregisterämter neu eine Gebühr verlangen können. Von dieser Kostenhürde erhofft man sich, dass Belege zurückhaltender konsultiert werden. Zudem müssen sich die abfragenden Personen beim Bezahlungsprozess identifizieren, was missbräuchliche Abfragen verhindern soll.

Wir hatten das eidgenössische Handelsregisteramt (EHRA) in unserer Stellungnahme auch auf das Urteil des europäischen Gerichtshofs bezüglich des Rechts auf Vergessen aufmerksam gemacht. Der Gerichtshof hatte in seinem Urteil vom 13. Mai 2014 festgehalten, dass Suchmaschinenbetreiber verantwortlich sind für die Bearbeitung von Personendaten, die in den Suchresultaten auf ihren Websites erscheinen. Sie müssen deshalb unter bestimmten Voraussetzungen auf Gesuch der betroffenen Person gewisse Links löschen.

Ein Recht auf Vergessen sollte anfänglich in die Gesetzesrevision aufgenommen werden, wurde dann aber aufgrund des fehlenden Interesses der Vernehmlassungsteilnehmer fallen gelassen. Das EHRA vertrat die Ansicht, dass die Plattform www.zefix.ch nicht von der Stossrichtung des Entscheids des europäischen Gerichtshofs betroffen sei. Dieser richte sich an Suchmaschinenbetreiber und die Plattform www.zefix.ch sei nicht suchmaschinenindexiert. Einige unserer Anliegen wurden vom EHRA berücksichtigt, der Persönlichkeitsschutz ist dadurch verstärkt worden.

1.1.4 Bundesgesetz zum Schuldner- und Zahlstellenprinzip bei der Verrechnungssteuer

Wir haben uns in der Ämterkonsultation zum Entwurf des neuen Bundesgesetzes zum Schuldner- und Zahlstellenprinzip gegen die Einführung der AHV-Versichertennummer als Personenidentifikator für natürliche Personen ausgesprochen. Mit unserer Intervention erzielten wir einen Teilerfolg. Der Bundesrat wird zu einem späteren Zeitpunkt entscheiden, ob die AHV-Nummer oder ein sektorieller Personenidentifikator verwendet werden soll.

Die zurzeit geltende Verrechnungssteuer beruht auf dem Schuldnerprinzip und erfasst ausschliesslich Erträge aus inländischen Quellen. Steuerpflichtig ist der inländische Schuldner, beispielsweise die Unternehmung mit Sitz in der Schweiz, die eine Obligation ausgibt, und den Investoren darauf einen Zins entrichtet. Die Steuer wird unabhängig von der Person des Gläubigers erhoben, d.h. namentlich auch bei institutionellen Anlegern. Mit einem Systemwechsel bei der Verrechnungssteuer will das Eidgenössische Finanzdepartement (EFD) einigen Nachteilen, die sich aus diesem System ergeben, begegnen. Neu soll die Verrechnungssteuer nicht mehr vom Schuldner erhoben werden, sondern von der schweizerischen Zahlstelle (Bank), die die betreffenden Erträge ihrem Kunden gutschreibt.

Im Entwurf des Gesetzes war zu Beginn vorgesehen, dass die Zahlstellen in der Meldung an die Eidgenössische Steuerverwaltung (ESTV) zwingend die AHV-Nummer oder die Unternehmensidentifikationsnummer (UID) angeben müssen. Damit wäre der Kreis derjenigen Stellen, die die AHV-Nummer systematisch verwenden dürfen, ein weiteres Mal ausgedehnt worden. Über die Gefahren für den Persönlichkeitsschutz, wenn in der Verwaltung ein einziger Personenidentifikator verwendet wird, berichten wir im vorliegenden Tätigkeitsbericht in den Artikeln 1.1.3 und 1.1.7.

Wir haben entsprechend zu dieser Gesetzesvorlage Stellung genommen und die Schaffung eines sektoriellen Identifikators für den Steuerbereich verlangt. Die Vorlage wurde daraufhin geändert und dem Bundesrat vorgeschlagen, zu einem späteren Zeitpunkt zu entscheiden, ob im Steuerbereich die AHV-Nummer oder ein sektorieller Identifikator verwendet werden soll. Uns ging dieser Vorschlag zu wenig weit. Der Bundesrat hat unsere im Bericht vorgetragenen Befürchtungen zwar zur Kenntnis genommen, sich aber gegen unseren Antrag entschieden.

1.1.5 Projekt MARS des Bundesamtes für Statistik und des Bundesamtes für Gesundheit

Bezüglich des Statistik-Projekts MARS (Statistiken der ambulanten Gesundheitsversorgung) haben wir die zuständigen Bundesämter daran erinnert, dass es noch der Ausarbeitung detaillierter Vorschriften bedarf. Mit der anstehenden Änderung der Verordnung über die Krankenversicherung bietet sich die Gelegenheit, die Einzelheiten der Datenbearbeitung in diesem Projekt zu regeln. Ein Bearbeitungsreglement ist ebenfalls in Ausarbeitung.

Das Bundesamt für Statistik (BFS) hat laut dem Bundesstatistikgesetz die Aufgabe, Statistiken im öffentlichen Interesse zu erstellen. Im Gesundheitsbereich hat das BFS den spezifischen Auftrag, die notwendigen statistischen Grundlagen zur Beurteilung von Funktions- und Wirkungsweise des Krankenversicherungsgesetzes (KVG) zu erarbeiten. Zu diesem Zweck müssen die eidgenössischen Erhebungen

auf die ambulante Medizin ausgeweitet werden, um Daten über den Umfang der ambulanten Versorgung, über die Gründe für die Inanspruchnahme dieser Versorgung (Diagnostik) sowie über die Leistungen und Kosten des ambulanten Sektors zu erlangen. Aufgrund des KVG erhebt das BFS auch Daten bei den Leistungserbringern, um den mit gesetzlichen Überwachungsaufgaben betrauten Behörden die entsprechenden Angaben bereitstellen zu können.

Gemäss KVG muss der Bundesrat noch nähere Vorschriften zur Erhebung, Bearbeitung, Weitergabe und Veröffentlichung der Daten unter Wahrung des Verhältnismässigkeitsprinzips erlassen (Art. 22a Abs. 4). An diesen Punkt haben wir in einem Schreiben an das Bundesamt für Gesundheit und das BFS erinnert. Wir haben sie auch auf die Notwendigkeit hingewiesen, so rasch wie möglich ein Bearbeitungsreglement zu erstellen, in dem die Verwendung der AHV-Nummer, die Datenverknüpfungen, die Pseudonymisierung und Anonymisierung sowie das kryptologische Verfahren und das Key Management eingehend behandelt werden.

An der Versammlung der Ärztekammer der FMH im Mai 2014 haben wir in unseren öffentlichen Ausführungen ebenfalls die Notwendigkeit einer raschen Konkretisierung der erwähnten Bestimmung hervorgehoben. In Anbetracht der besonders schützenswerten Natur der erhobenen Personendaten beobachten wir die Entwicklung des Projekts weiterhin aufmerksam und achten darauf, dass die Datenschutzanforderungen vollumfänglich eingehalten werden.

1.1.6 Adressdatenaustausch zwischen Einwohnerregistern, Post und anderen Dateninhabern

Wir haben an den beratenden Arbeiten zum Austausch von Personendaten zwischen Einwohnerregistern, der Post und anderen Dateninhabern mitgewirkt. Der Bundesrat hat die Idee eines automatischen Austausches von Adressdaten zwischen der Post und den Einwohnerregistern aufgegeben. Er hat hingegen das Eidgenössische Justiz- und Polizeidepartement beauftragt, Lösungen für den Adressdatenaustausch zwischen den verschiedenen öffentlichen Organen zu prüfen.

Am 12. November 2014 erstellte der Bundesrat einen Bericht in Erfüllung des Postulats 12.3661 der Staatspolitischen Kommission des Nationalrats («Adressdatenaustausch zwischen Einwohnerregistern, Post und anderen Dateninhabern»), eingereicht als Reaktion auf die parlamentarische Initiative 11.488 vom 29. September 2011. Der Bundesrat sollte untersuchen, ob gesetzliche Grundlagen für die Einführung eines automatischen und regelmässigen Austauschs von Adressdaten zwischen verschiedenen öffentlichen Dateninhabern, namentlich zwischen der Schweizerischen Post und den Einwohnermeldeämtern, zu schaffen sind.

Aufgrund der Ergebnisse der Arbeitsgruppe, an der wir mitwirkten, kam der Bundesrat zu dem Schluss, dass die Einrichtung eines solchen Austausches zwischen der Post und den Einwohnerkontrollen nicht sinnvoll wäre. Die Adresslisten der Einwohnerregister seien bereits von sehr guter Qualität, und die Einführung eines automatischen und regelmässigen Datenaustausches zwischen der Schweizerischen Post und den Einwohnermeldeämtern wäre aus Gründen des Datenschutzes problematisch. Die Weitergabe dieser Daten setzt nämlich die Verwendung einer eindeutigen Kennung, der AHV-Nummer, voraus. Es bestünde die Gefahr, dass die Post diese Nummer an andere Vertriebsunternehmen weitergäbe, was ein erhöhtes Missbrauchsrisiko nach sich zöge. Das System läge im Interesse der Post, die als einzige Institution des Landes in den Besitz einer aktualisierten Adressdatenbank aller Einwohner gelangen würde.

Äusserst nützlich wäre indes eine Adressdatei für die öffentlichen Verwaltungen auf allen Stufen des Staates, die bei praktisch allen ihren Aktivitäten auf eine eindeutige Identifikation der Bürger und die Kenntnis ihres Wohnsitzes angewiesen sind. In den Gemeinden sind diese Angaben im Einwohnerregister verfügbar, das ständig nachgeführt wird. Sie sind in der Regel auch auf Kantonsebene zugänglich. Nur auf interkantonaler und eidgenössischer Ebene fehlen sie. Die Verwaltungen sind gezwungen, auf eine Nachführung der bei ihnen vorhandenen Daten zu verzichten oder sie fallweise bei den Gemeinden und den Kantonen zu beschaffen, was manche Verwaltungsabläufe bedeutend erschwert. Als Beispiele lassen sich die Erhebung des Militärpflichtersatzes, die Zahlung der Krankenkassenprämien oder die Durchführung von Betreibungsverfahren nennen, wenn der Schuldner in einen anderen Kanton zieht. Diese Schwierigkeiten könnten vermieden und die Verwaltungsabläufe erheblich vereinfacht werden, wenn auf nationaler Ebene eine zuverlässige Adressdatenbank verfügbar wäre.

Verschiedene Lösungen sind denkbar. Zunächst könnte die Qualität der Adressdaten in den Einwohnerregistern verbessert werden, wenn alle Kantone dafür sorgen, dass die Vermieter und Beherberger auf Personen hinweisen, die ihrer Meldepflicht bei der Einwohnerkontrolle nicht nachgekommen sind. Überdies könnte man eine Adressdatenbank schaffen, auf die öffentliche Verwaltungen zur Erfüllung ihrer Aufgaben Zugriff hätten. Diese Datenbank könnte aus den bestehenden kantonalen Plattformen gebildet werden oder aber auf Plattformen des Bundes beruhen: die Datenbank des Bundesamtes für Statistik; ein noch zu schaffendes nationales Personenverzeichnis; eine Erweiterung der Datenbank UPI (Unique Personal Identifier Database), die von der zentralen Ausgleichsstelle benutzt wird.

Der Bundesrat hat das Eidgenössische Justiz- und Polizeidepartement beauftragt, die Vor- und Nachteile dieser Varianten und namentlich ihre Machbarkeit, ihre Kompatibilität mit dem Datenschutz, ihre Kosten und ihre Auswirkungen vertieft

zu untersuchen. Als Mitglied der Arbeitsgruppe verfolgen wir die Entwicklung sehr genau, um eine datenschutzrechtlich einwandfreie Bearbeitung zu gewährleisten.

1.1.7 Verwendung eines universellen Personenidentifikators im Bereich E-Government

Wir haben in einer Arbeitsgruppe mitgewirkt, die für den Bundesrat die Frage der Ausarbeitung von Gesetzesgrundlagen für die Verwendung eines administrativen Personenidentifikators im Bereich E-Government prüfte. In diesem Zusammenhang haben wir unsere Befürchtungen betreffend die generelle Verwendung eines einheitlichen und universellen Identifikators, wie ihn die AHV-Versichertennummer darstellt, erläutert.

Im Januar 2014 ersuchte die Konferenz der kantonalen Finanzdirektorinnen und -direktoren (FDK) auf Antrag des Vorstands der Schweizerischen Informatikkonferenz (SIK) Bundesrätin Eveline Widmer-Schlumpf, die Frage der Schaffung von Gesetzesgrundlagen für die Einführung einer klaren und universellen administrativen Personenkennung, im Idealfall auf Basis der AHV-Nummer, zu prüfen. Nach Ansicht der SIK müssen für den elektronischen Austausch von Personendaten zwischen den Informationssystemen und damit für sämtliche E-Government-Anwendungen die Daten mit Hilfe eines klaren Identifikators jeder betroffenen Person zugewiesen werden können. Die AHV-Nummer wäre eine Kennung, die den Vorteil hat, dass sie einerseits jeder in der Schweiz wohnhaften Person zugewiesen wird und andererseits wegen ihrer zufälligen Zusammensetzung keine Rückschlüsse auf die fragliche Person ermöglicht. Die FDK befürwortet im Übrigen eine gewisse gesetzgeberische Flexibilität für eine vereinfachte Verwendung der AHV-Nummer im ganzen E-Government-Bereich.

Die Bundesrätin räumte ein, dass diese Thematik dem Bundesrat unterbreitet werden sollte und beauftragte das Informatiksteuerungsorgan des Bundes (ISB) mit der Bildung einer Arbeitsgruppe zur Erstellung eines Papiers, auf dessen Grundlage der Bundesrat über das weitere Vorgehen entscheiden könnte. Im Rahmen der Arbeitsgruppe hatten wir die Gelegenheit, unseren Befürchtungen bezüglich der generellen Verwendung eines einheitlichen und universellen Identifikators, wie ihn die AHV-Nummer darstellt, im Rahmen von E-Government Ausdruck zu verleihen und auf die erheblichen Risiken für die Privatsphäre der betroffenen Personen hinzuweisen. Eine kostengünstige, zuverlässige und leicht umzusetzende Alternative wäre die Einführung einer sektorspezifischen Nummer, wie sie für das elektronische Patientendossier geplant ist.

Abgesehen von der auszuarbeitenden Rechtsgrundlage stellt sich auch die Frage nach der Notwendigkeit und der Verhältnismässigkeit einer Verwendung der

AHV-Nummer ausserhalb des Sektors der Sozialversicherungen. Zudem muss sich der Bürger im Klaren darüber sein, welche Dienste und Institutionen sich systematisch der AHV-Nummer ausserhalb des Sozialversicherungsbereichs bedienen. In dieser Hinsicht ist eine Gesetzesgrundlage im formellen Sinn auszuarbeiten, die den Verwendungszweck und die berechtigten Nutzer bestimmt. Wir befürchten, dass sich die Verwendung der AHV-Nummer ausserhalb eines klar abgegrenzten gesetzlichen Rahmens auf den Privatsektor ausdehnen könnte. Es wäre dann nicht mehr möglich, die Kontrolle über die Bearbeitung zu behalten und deren Berechtigung zu überprüfen.

1.2 Datenschutzfragen allgemein

1.2.1 Totalrevision des Gesetzes 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 zum Gesetz und zur Botschaft Stellung genommen. Insbesondere haben wir uns zur Bekanntgabe von Daten aus dem Nationalen Informationssystem für Sport und dem Informationssystem für leistungsdiagnostische Daten geäussert.

Das im Oktober 2012 in Kraft getretene Bundesgesetz über die Informationssysteme des Bundes im Bereich Sport wurde totalrevidiert. Dabei sollte insbesondere das Verwaltungsinformationssystem der Eidgenössischen Hochschule für Sport formalgesetzlich verankert werden, weil dieses System u.a. Daten zu Disziplinarverfahren enthält. Bei der Revision wurden auch die mit der Anwendung des 2012 neu eingeführten Gesetzes gemachten Erfahrungen berücksichtigt und neben dem erwähnten auch für drei weitere Informationssysteme, die bereits betrieben werden oder im Aufbau begriffen sind, formalgesetzliche Grundlagen geschaffen. Es handelt sich dabei um ein Informationssystem für die Bearbeitung leistungsdiagnostischer Daten, ein System für die Evaluation von Kursen und Lehrgängen sowie ein Informationssystem der nationalen Agentur gegen Doping.

Mit den Änderungen bei der Datenbekanntgabe beim Nationalen Informationssystem für Sport wurde die regelmässige, aber beschränkte Weitergabe von Daten an Stellen und Personen, mit denen im Bereich des fairen und sicheren Sports zusammengearbeitet wird (z.B. beim Präventionsprogramm «cool and clean» oder an die Luftrettungsorganisation REGA), der Praxis angepasst. Neu sieht das Gesetz explizit vor, dass die Daten nicht für kommerzielle Zwecke verwendet werden dürfen. Wir haben dem Bundesamt für Sport (BASPO) vorgeschlagen, dass zusätzlich die Weitergabe der Daten durch die Empfänger eingeschränkt werden soll, um die im Nationalen Informationssystem für Sport erfassten Personen vor Persönlichkeitsverletzungen zu schützen. Es erschien uns zudem wichtig, dass das Bundesamt die Kontrolle über die Empfänger von elektronischen Datensätzen und Listen behält. Das BASPO verpflichtet die Datenempfänger bereits jetzt dazu, dass die Daten nicht weitergegeben werden dürfen. Es hat daher unseren Vorschlag angenommen und in den gesetzlichen Bestimmungen die Weitergabe der Daten durch die Datenempfänger explizit untersagt.

Das Gesetz sieht beim Informationssystem für die Bearbeitung leistungsdiagnostischer Daten weiter vor, dass die Daten und Ergebnisse unter anderem an Personen, Behörden und Organisationen, welche die Tests und Untersuchungen in Auftrag

gegeben haben, bekanntgegeben werden dürfen. Für diese Bekanntgabe ist keine explizite Zustimmung der Betroffenen vorgesehen. Da die betroffenen Sportler für die leistungsdiagnostischen Tests durch Organisationen oder Behörden aufgeboten werden, werden sie im Rahmen des Aufgebotes von den Verantwortlichen (Trainer, Verbandsärzte etc.) über die Datenbearbeitung informiert, insbesondere über den Zweck der Tests, die anschliessende Analyse durch die verantwortlichen Spezialisten und die Empfänger der Resultate. Die weitere Datenbearbeitung durch die Empfänger richtet sich in der Folge nach dem DSG, insbesondere bezüglich Zweckbindung und Verhältnismässigkeit.

Da der Ablauf der leistungsdiagnostischen Tests im Entwurf der Botschaft nicht ausgeführt wurde, bestand aus unserer Sicht die Gefahr, dass es ohne weitere Kenntnisse der Abläufe nicht nachvollziehbar ist, warum im Gesetz kein Einverständnis für die Datenbekanntgabe in diesem Fall verlangt wird. Wir regten daher an, die Botschaft mit Ausführungen zur Datenbekanntgabe an die Empfänger zu ergänzen. Das BASPO kam diesem Begehren nach und ergänzte die Botschaft entsprechend.

1.2.2 Informationssystem betreffend Reisende ohne gültigen Fahrausweis

Die neue gesetzliche Grundlage für ein Informationssystem über Reisende ohne gültigen Fahrausweis wurde vom Parlament verabschiedet. Entsprechende Verordnungsbestimmungen befinden sich in Ausarbeitung.

Zur Schaffung einer gesetzlichen Grundlage für Informationssysteme über Reisende ohne gültigen Fahrausweis hat das Bundesamt für Verkehr (BAV) eine neue Bestimmung im Personenbeförderungsgesetz (PBG) ausgearbeitet (vgl. unseren Tätigkeitsbericht 2013/2014, Ziff. 1.2.6). Diese neue Bestimmung (Art. 20a PBG) wurde als Teil des Gesetzgebungspakets «Strassentransportunternehmens- und Verkehrsstrafrecht Änderung» vom Parlament beraten und in leicht geänderter Form verabschiedet. Das Parlament hat der Bestimmung einen neuen Absatz hinzugefügt, wonach auch der Dachverband der Branche die Informationssysteme betreiben könne.

Die gesetzliche Bestimmung sieht vor, dass konzessionierte Transportunternehmen Informationssysteme über Reisende ohne gültigen Fahrausweis betreiben können und regelt bestimmte Punkte wie etwa die Löschung der Daten. Das BAV arbeitet nun die Ausführungsbestimmungen aus. Die konzessionierten Unternehmen, gegebenenfalls der Dachverband, werden die konkrete Ausgestaltung der Informationssysteme noch detailliert regeln müssen, sei es in Weisungen, Bearbeitungsreglementen oder in anderer Form.

1.2.3 Zentrale Speicherung von Kundenfotos bei Skistationen – Allgemeine Erläuterungen

Wir haben Erläuterungen dazu veröffentlicht, wie die von den meisten Schweizer Skistationen verwendeten Zutrittskontrollsysteme datenschutzkonform konfiguriert und betrieben werden können.

Nachdem im vergangenen Jahr die bei einer Skistation durchgeführte Sachverhaltsabklärung abgeschlossen werden konnte (vgl. 21. Tätigkeitsbericht 2013/2014, Ziff. 1.2.1), haben wir allgemeine Erläuterungen dazu verfasst, wie die von den meisten Schweizer Skistationen verwendeten Zutrittskontrollsysteme datenschutzkonform konfiguriert und betrieben werden können. Wir führen darin insbesondere aus, welche Daten wie lange gespeichert werden dürfen, zu welchen Zwecken sie verwendet werden können, wem Zugriff darauf zu gewähren ist und wie die Kunden korrekt informiert werden. Die Erläuterungen sind auf unserer Webseite www.derbeauftragte.ch, unter Datenschutz – Freizeit und Sport – Zutrittskontrollsysteme in Freizeitanlagen, einsehbar.

1.2.4 Videoüberwachung in Fahrzeugen (Dashcams)

Der Einsatz sogenannter Dashcams verstösst in der Regel gegen Datenschutzrecht, weshalb darauf verzichtet werden sollte. Wir haben zu diesem Thema Erläuterungen veröffentlicht.

Ein Autounfall ist schnell passiert, und oft ist im Nachhinein nicht einfach festzustellen, wer den Unfall verursacht hat. Daher werden in Fahrzeugen immer häufiger Videokameras installiert, welche die Strasse vor (und teilweise auch hinter) dem Fahrzeug filmen, um so Beweismittel zu generieren. In einigen Ländern sind diese sogenannten Dashcams obligatorisch, aber auch hierzulande erfreuen sie sich steigender Beliebtheit. Nebst der Verwendung als Beweismittel werden Dashcam-Aufnahmen auch zur Unterhaltung auf Online-Portale und Soziale Netzwerke hochgeladen oder, wie beim landesweit bekannt gewordenen Baggertransporter-Unfall auf der Autobahn A1, durch die Medien zu Informationszwecken veröffentlicht.

Wenngleich solche Aufnahmen auf die eine oder andere Art von Nutzen sein können, so sind sie aus datenschutzrechtlicher Sicht doch problematisch. Da in der Regel mit einer Dashcam permanent gefilmt wird, beschränkt sich die Datenbearbeitung nicht auf diejenigen Personen, die in ein Ereignis verwickelt sind (z.B. in einen Unfall) oder sich regelwidrig verhalten. Vielmehr zeichnen die Kameras wahllos Daten sämtlicher Personen auf, die sich in ihrem Aufnahmebereich aufhalten. Zudem wissen die Betroffenen in der Regel nicht, dass sie gefilmt werden. Damit werden durch die Verwendung von Dashcams die Grundsätze der Verhältnismässigkeit und der Transparenz empfindlich verletzt. Dies kann einerseits zu

widerrechtlichen Persönlichkeitsverletzungen führen, andererseits aber auch dazu, dass die Aufnahmen nicht als Beweismittel zugelassen werden.

Anders ist die Situation zu beurteilen, wenn die Kamera nur im Ereignisfall eingeschaltet wird. Hier werden nicht sämtliche Verkehrsteilnehmer unter Generalverdacht gestellt, und es findet keine Datenbearbeitung auf Vorrat statt. Beschränkt sich die Aufnahme auf ein konkretes Ereignis, kann die Datenbearbeitung durch ein überwiegendes Interesse gerechtfertigt sein.

Genaueres hierzu kann auf unserer Webseite in unseren Erläuterungen zum Thema nachgelesen werden (www.derbeauftragte.ch, Datenschutz – Videoüberwachung – Dashcam).

1.2.5 Neues Geldspielgesetz

Laut dem Entwurf zum neuen Geldspielgesetz sollen in der Schweiz auch Onlinespiele legal angeboten werden. In diesem Zusammenhang haben wir uns zu Sperrlisten und Authentifikationsproblemen geäussert.

Das neue Geldspielgesetz soll sowohl das Spielbankengesetz wie auch das Bundesgesetz betreffend Lotterien und gewerbsmässige Wetten ersetzen. Neben verschiedenen Neuerungen zur Organisation der zuständigen Behörden ist vorgesehen, dass Geldspiele künftig auch online angeboten werden dürfen. In unserer Stellungnahme zum Vorentwurf wiesen wir auf die verschiedenen Probleme hin, die sich mit der Überprüfung der Angaben ergeben, welche die Spielenden bei der Eröffnung ihrer Benutzerkonten machen.

Problematisch waren aus datenschutzrechtlicher Sicht zudem die Einblendung einer Stoppseite, falls Spielende auf gesperrte ausländische Angebote zugreifen wollen, die Auswertung dieser Zugriffe und die Erstellung der Sperrlisten an und für sich. Im Anschluss an unsere Stellungnahme haben wir unsere Bedenken mit den zuständigen Fachleuten des Bundesamtes für Justiz besprochen. Die Vernehmlassung zum Geldspielgesetz ist im August 2014 abgeschlossen worden; wir werden die Gesetzgebungsarbeiten weiterhin aufmerksam verfolgen.

1.3 Internet und Telekommunikation

1.3.1 Auslagerung von Datenbearbeitungen durch Bundesorgane in die Cloud

Bundeorgane beabsichtigen vermehrt, Datenbearbeitungen in die Cloud auszulagern. So haben uns auch in diesem Berichtsjahr die verantwortlichen Stellen kontaktiert und uns um eine datenschutzrechtliche Einschätzung der geplanten Auslagerungen gebeten.

Möchten Bundesbehörden Datenbearbeitungen auslagern, müssen sie aus datenschutzrechtlicher Sicht neben den allgemeinen Grundsätzen auch folgende Punkte beachten:

- Sie dürfen gemäss dem Datenschutzgesetz (DSG) Personendaten nur dann an Dritte weitergeben, wenn dafür eine Rechtsgrundlage im Sinne von Art. 17 DSG besteht oder eine Ausnahmebestimmung von Art. 19 Abs. 1 DSG zur Anwendung kommt.
- Besteht eine gesetzliche oder vertragliche Geheimhaltungspflicht, so dürfen die Daten nicht an den Cloud-Anbieter übertragen werden. Diese Abklärung kann auch zum Ergebnis führen, dass nur ein Teil der Datenbearbeitung ausgelagert werden darf.
- Der Dateninhaber muss sicherstellen, dass der Auftragsdatenbearbeiter die Daten nur so bearbeitet, wie er es selbst tun dürfte. Es liegt am Bundesorgan, die Einhaltung der Datenbearbeitungsverträge regelmässig zu überprüfen.
- Befinden sich die Server des Dienstleistungsanbieters im Ausland, sind darüber hinaus die datenschutzrechtlichen Regelungen zum grenzüberschreitenden Datentransfer zu beachten. Die Übermittlung von Personendaten der Webseitenbesucher ins Ausland unterliegt u.a. der Gefahr, dass ausländische Behörden aufgrund ihrer nationalen Gesetzgebungen auf die sich in ihrem Land befindlichen Daten zugreifen können. Angesichts der Pflicht der Bundesorgane, sorgsam mit den Personendaten der Bürger umzugehen und sie insbesondere vor unbefugten Zugriffen zu sichern, dürfte sich dieser Punkt als heikel erweisen.

Kritisch beurteilten wir das teilweise fehlende Weisungsrecht gegenüber dem Auftragsdatenbearbeiter. Zum Beispiel ist eine lange Aufbewahrungsdauer nicht verhältnismässig und entspricht nicht den Anforderungen des DSG. Da die Dienstleistungsanbieter in der Regel keine Anpassungen ihrer Standardvertragsklausel erlauben, hat das verantwortliche Bundesorgan zu beurteilen, ob unter den gemachten Bedingungen ein Bezug der Dienstleistungen in Frage kommt oder nicht.

Gerade bei der Wahl von amerikanischen Unternehmen als Dienstleistungsanbieter müssen die Risiken der Auslagerung genau abgeschätzt werden. So hat am 25. April 2014 das Gericht des Southern District of New York betreffend des Zugriffs der US-Behörden auf Kundendaten, die in der EU gespeichert sind, ein brisantes Urteil gefällt. Gemäss dem Urteil können US-Behörden auf Daten zugreifen, welche von Unternehmen mit Sitz in den USA im Auftragsverhältnis bearbeitet werden. Wir gehen davon aus, dass die Cloud-Anwendungen von US-Unternehmen somit auch mit einer Zusatzvereinbarung das Risiko bergen, dass US-Behörden ohne den Weg über die internationale Rechtshilfe auf Kundendaten, welche auf Servern in der EU oder der Schweiz gespeichert sind, Zugriff erhalten.

Aus diesen Gründen raten wir Bundesorganen davon ab, Datenbearbeitungen an Firmen auszulagern, welche einer Gesetzgebung ohne angemessenem Datenschutzniveau unterstellt sind. Weiter ist anzumerken, dass es sich bei den auszulagernden Datenbearbeitungen um kritische Infrastrukturen handeln kann, die entsprechend den Vorgaben des Bundesrats nur an Firmen ausgelagert werden dürfen, welche «ausschliesslich unter Schweizer Recht handeln, sich zur Mehrheit in Schweizer Eigentum befinden und ihre Leistung gesamtheitlich innerhalb der Schweizer Landesgrenzen erzeugen».

1.3.2 Teilrevision des Bundesgesetzes über Radio und Fernsehen – Verwendung der AHV-Nummer durch die Billag

Die eidgenössischen Räte haben die Teilrevision des Bundesgesetzes über Radio und Fernsehen verabschiedet, welches ein schweizweites Register aller in der Schweiz erfassten Personen vorsieht, das auch deren AHV-Nummer enthält. Aus unserer Sicht ist diese Datenbearbeitung nicht notwendig und daher nicht verhältnismässig.

Im September 2014 hat das Parlament die Teilrevision des Radio- und Fernsehgesetzes verabschiedet. Leider haben die Räte, wie zuvor schon das Bundesamt für Kommunikation, unserem Anliegen, auf die Verwendung der AHV-Nummer zur Gebührenerhebung zu verzichten, nicht Rechnung getragen. Wir sind nach wie vor der Ansicht, dass die Verwendung der AHV-Nummer ausserhalb der Sozialversicherung des Bundes zur Gebührenerhebung nicht notwendig und daher aus Datenschutzsicht unverhältnismässig ist. Wir haben vorgeschlagen, eine bereichsspezifische bzw. sektorielle Nummer zu verwenden, welche die Problematik der Verknüpfung der verschiedenen Datenbanken erheblich reduzieren würde. Weitere Ausführungen zum Thema sind in unserem 21. Tätigkeitsbericht 2013/2014, in Ziffer 1.2.8, zu finden.

1.3.3 Neuer Büroautomationsdienst in der Bundesverwaltung (UCC)

Mit dem Programm «Unified Communication and Collaboration» (UCC) ist in der Bundesverwaltung das Festtelefonnetz durch einen neuen Büroautomationsstandard ersetzt worden. Wir haben den Projektverantwortlichen unsere Bemerkungen zu den zu berücksichtigenden Datenschutz- und Datensicherheitsaspekten zukommen lassen.

Mit Beschluss vom 9. November 2011 zur IKT-Strategie des Bundes hat der Bundesrat das Informatiksteuerungsorgan des Bundes (ISB) beauftragt, den neuen Standarddienst für Büroautomation der Bundesverwaltung auszuarbeiten; dazu gehören die Sprachkommunikation (Festnetz- und Mobiltelefonie), Videotelefonie, Videokonferenztechnik, Screen Sharing, Instant Messaging, und die E-Mail-Kommunikation. Die Integration dieses Dienstes erfolgt im Rahmen des UCC-Programms, das Ende 2015 abgeschlossen sein sollte.

Die Bundeskanzlei (BK) hatte beschlossen, diese Migration rasch einzuführen, damit sie ihre Rolle bei der interdepartementalen Koordinierung bestmöglich wahrnehmen kann. Da der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte administrativ der BK angeschlossen ist, sind wir sowohl als Anwender als auch als Beratungs- und Aufsichtsorgan der Bundesorgane im Bereich Datenschutz betroffen. In dieser Eigenschaft wurden wir zu einer Vorstellung des Projekts im Rahmen einer Sitzung der Interdepartementalen Arbeitsgruppe «Datenschutz» (IDAG) eingeladen. Die Präsentation gab Anlass zu verschiedenen Fragen, insbesondere betreffend die gesetzlichen Grundlagen und die Existenz eines Informationssicherheits- und Datenschutzkonzepts (ISDS) gemäss den Anforderungen des Hermes-Verfahrens. Die Teilnehmer zeigten sich erstaunt darüber, dass sie erst so spät zu diesem Thema informiert und konsultiert wurden.

Die erste Version des ISDS-Konzepts wurde auf unser Ersuchen durch ein Dokument ergänzt, das unter anderem eine detaillierte Beschreibung der Restrisiken und eine Analyse der Rechtsgrundlagen unter dem Blickwinkel des Datenschutzes und der Informationssicherheit enthält. Die Projektverantwortlichen haben auch eine Datenschutz-Folgenabschätzung mit Hilfe des auf unserer Website verfügbaren Tools vorgenommen (www.derbeauftragte.ch, Datenschutz – Handel und Wirtschaft – Unternehmen – Evaluationsraster). Wir haben zu diesen neuen Dokumenten Stellung genommen und dabei die unter dem Gesichtspunkt des Datenschutzes und der Datensicherheit zu berücksichtigenden Elemente hervorgehoben.

In technischer Hinsicht haben wir mit Verwunderung erfahren, dass die Nutzung dieses Dienstes nur für die als «intern» klassifizierten Telefongespräche erlaubt ist,

obwohl doch die eingesetzten kryptographischen Protokolle theoretisch einen ausreichenden Schutz für Gespräche der Stufe «vertraulich» oder «besonders schützenswert» ermöglichten. Ausserdem haben wir uns für die Beibehaltung einer ebenso hohen Vertraulichkeit wie bisher ausgesprochen und dazu eine unabhängige Risikobeurteilung vorgeschlagen. Auch haben wir darauf hingewiesen, wie wichtig die Gewährleistung einer der alten Lösung gleichwertigen Verfügbarkeit ist (separates physisches Netzwerk). Letztlich stellt sich für uns die Frage, ob der Entscheid für den Lync Client 2013 von Microsoft richtig war.

Rechtlich betrachtet, war uns eine endgültige Beurteilung nicht möglich, da gewisse Einzelheiten besonders im Zusammenhang mit den Randdaten und ihrer Erfassung nicht klar waren. Wir haben indes bestätigt, dass trotz der noch bestehenden Ungewissheiten zusätzliche gesetzliche Grundlagen nicht notwendig erscheinen. Wir wiesen darauf hin, dass dies nicht als formelle Zustimmung zur Einführung des Systems ausgelegt werden dürfe. Die Verantwortung für eine solche Bearbeitung liegt nämlich beim Betreiber des Dienstes (also der jeweiligen Behörde), während für die Umsetzung das ISB zuständig ist. Wir hoffen, dass dieses unseren Bemerkungen und Ratschlägen Rechnung trägt und werden die Entwicklung des Projekts weiterhin aufmerksam verfolgen.

1.3.4 Kostenloses WiFi der SBB

Seit Herbst 2014 bieten die SBB an verschiedenen Bahnhöfen kostenlosen Internetzugang via WiFi (SBB Free WiFi) an. Wir wollten von ihnen wissen, welche Daten sie in diesem Zusammenhang bearbeiten. Auch wiesen wir sie darauf hin, dass aufgrund der geltenden Allgemeinen Geschäftsbedingungen (AGB) die Verwendung der Userdaten weder zu Marketingzwecken noch zur Analyse von Personenströmen erlaubt ist.

Im September 2013 begannen die SBB an verschiedenen Bahnhöfen mit der Freischaltung eines kostenlosen Internetzugangs via WiFi (SBB Free WiFi). Kunden, die von diesem Angebot profitieren wollen, müssen sich registrieren und bestätigen, dass sie die Nutzungsbestimmungen gelesen haben und damit einverstanden sind. In den entsprechenden AGB behalten sich die SBB vor, die Daten zu verschiedenen Zwecken zu bearbeiten, unter anderem um das Bewegungsverhalten der Kunden zu analysieren. Wir haben die SBB auf die damit verbundene datenschutzrechtliche Problematik hingewiesen und stellten ihnen zur Klärung der Sachlage verschiedene Fragen. Die Thematik wurde auch anlässlich einer Sitzung zwischen dem CEO der SBB und dem EDÖB besprochen.

Unsere Abklärungen ergaben einerseits, dass die SBB die anfallenden Userdaten zu jenem Zeitpunkt einzig gestützt auf das Bundesgesetz betreffend die Überwachung

des Post- und Fernmeldeverkehrs (BÜPF) bearbeiteten; insbesondere wurden noch keine Daten zu Marketingzwecken bearbeitet. Andererseits mussten wir feststellen, dass die Nutzungsbestimmungen zu wenig präzis formuliert waren und daraus nicht hervorging, welche Daten für welche Zwecke bearbeitet werden sollten. Daher wäre die Einwilligung der User, wie sie für eine Datenbearbeitung zu Marketingzwecken und zur Analyse von Personenströmen nötig ist, nicht rechtsgültig. Vielmehr müssten die AGB entsprechend angepasst werden. Dagegen besteht für die Datenbearbeitung nach BÜPF eine gesetzliche Grundlage und somit ein Rechtfertigungsgrund. Jedoch heisst es in den AGB, dass die Daten zwölf statt der zurzeit im BÜPF vorgesehenen sechs Monate aufbewahrt würden. Auch hier ist eine Anpassung der AGB erforderlich.

Wir teilten den SBB die Ergebnisse unserer Abklärungen schriftlich mit. Allerdings haben sie die AGB bis zum Redaktionsschluss des vorliegenden Tätigkeitsberichts (31. März 2015) noch nicht angepasst.

1.3.5 Open-Government-Data-Strategie des Bundes

Im Rahmen der Ämterkonsultation haben wir zur Open-Government-Data-Strategie Schweiz 2014-2018 Stellung genommen und dabei die datenschutzrechtlichen Anforderungen erläutert.

Als Open-Government-Data bezeichnet man offene Verwaltungsdaten, also jene Datenbestände des öffentlichen Sektors, die im Interesse der Allgemeinheit ohne jede Einschränkung im Sinne eines Open Government frei zugänglich gemacht werden. Typischerweise handelt es sich dabei nicht um Personendaten. Trotzdem besteht ein Risiko, dass in Verbindung mit anderen Daten ein Personenbezug hergestellt werden kann.

Bei der Ämterkonsultation zur Open Government Data Strategie Schweiz 2014-2018 wiesen wir in unserer Stellungnahme deshalb darauf hin, dass datenschutzrechtliche Aspekte bereits in der Planungs- und Entwicklungsphase von Open-Government-Data-Projekten berücksichtigt werden müssen. Wir haben angeregt, dass im Strategiepapier Verfahren eingeplant werden, welche technische und organisatorische Massnahmen vorsehen, um eine versehentliche Offenlegung personenbezogener Daten zu verhindern. Stützt sich die Behörde darauf, dass bloss aggregierte und anonymisierte Datensätze publiziert werden, muss sie eine gründliche Analyse der Datenschutzfolgen vornehmen, damit die Rückidentifizierung natürlicher oder juristischer Personen verunmöglicht wird.

1.3.6 Urheberrechtsschutz im Internet

Die von der Arbeitsgruppe AGUR 12 vorgeschlagenen Anpassungen des Urheberrechts sollen nun gesetzgeberisch umgesetzt werden. Wir werden den Gesetzgebungsprozess begleiten und auf die Aufrechterhaltung des Persönlichkeitsschutzes hinwirken.

Nachdem die von Bundesrätin Simonetta Sommaruga eingesetzte Arbeitsgruppe AGUR 12 im Dezember 2013 ihren Schlussbericht vorgelegt hat (vgl. 21. Tätigkeitsbericht 2013/2014, Ziff. 1.3.1), sollen nun die dort vorgeschlagenen Anpassungen des Urheberrechts geprüft und umgesetzt werden. Wir begrüssen es, dass damit die zurzeit herrschende Rechtsunsicherheit betreffend korrekte Beschaffung und Bearbeitung von Personendaten von Urheberrechtsdelikten im Internet beseitigt wird. Gleichzeitig möchten wir darauf hinwirken, dass die eingeführten Massnahmen den Persönlichkeitsschutz berücksichtigen. Wir verfolgen daher die laufenden Entwicklungen und werden den Gesetzgebungsprozess begleiten.

1.3.7 Berichterstattung über Lehrpersonen im Internet

Internetplattformen, auf denen Berichte über politische Einflussnahmen durch Lehrpersonen veröffentlicht werden, können die Persönlichkeitsrechte der betroffenen Personen verletzen. Daher ist darauf zu achten, dass die Texte nur in anonymisierter Form veröffentlicht werden.

Politische Indoktrination im Schulunterricht ist ein heikles Thema. Nicht immer gelingt es den Lehrkräften, ihren Unterricht politisch neutral zu gestalten. Gerade wenn politische oder gesellschaftliche Themen behandelt werden, dringt die politische Gesinnung der Lehrkraft gerne bis zu den Schülern durch, ob absichtlich oder nicht. Diesen Umstand nahm eine politische Partei zum Anlass, eine Internetplattform zu errichten, auf der öffentlich über solche Erlebnisse berichtet werden kann. Damit sollen Lehrkräfte davon abgeschreckt werden, ihre politische Meinung allzu freimütig an ihre Schüler weiter zu geben, um diese in ihrem Sinne zu beeinflussen.

Eine derartige Plattform birgt die Gefahr, die Persönlichkeitsrechte der betroffenen Lehrkräfte zu verletzen. Ähnlich wie bei einem Internetpranger (vgl. 20. Tätigkeitsbericht 2012/2013, Ziff. 1.3.1) können die aufgeführten Lehrkräfte stigmatisiert und unnötig herabgesetzt werden, ohne sich dagegen wehren zu können. Ein Rechtfertigungsgrund ist hier nicht ersichtlich. Wenngleich die Gewährung eines politisch neutralen Schulunterrichts zweifellos als öffentliches Interesse gewertet werden kann, so ist es nicht Aufgabe Privater, dieses Interesse durchzusetzen. Vielmehr bestehen in allen Kantonen Aufsichtsorgane, denen Fälle politischer Einflussnahme durch Lehrpersonen gemeldet werden können. Diese Organe haben dann die

Möglichkeit, passende Massnahmen zu treffen. Dieser Weg ist nicht zuletzt aus rechtsstaatlicher Sicht einzuhalten.

Da die Plattform der Veröffentlichung von Berichten über politische Einflussnahmen durch Lehrkräfte dient und damit politische Ansichten oder Tätigkeiten der fraglichen Personen thematisiert, werden Daten bearbeitet, die nach Datenschutzgesetz als besonders schützenswert gelten. Dementsprechend sind bei uns sehr viele Anfragen zu dieser Plattform eingegangen. Wir haben daraufhin ein Verfahren zur Abklärung des Sachverhalts eröffnet. Es hat sich gezeigt, dass sämtliche eingehenden Berichte vor deren Veröffentlichung durch die Plattformbetreiber geprüft und anonymisiert werden, so dass der Leser in der Regel nicht erkennt, um welche Lehrkraft es sich handelt. Damit kann die Plattform in der aktuellen Form nicht als Internetpranger bezeichnet werden.

Dennoch gilt es zu beachten, dass für eine Anonymisierung die einfache Streichung von Namen nicht immer ausreichend ist. Vielmehr könnten die in einem Bericht erwähnten Lehrpersonen z.B. aus den geschilderten Situationen oder Umständen heraus erkennbar sein. Daher muss die Anonymisierung solcher Berichte mit grösster Sorgfalt durchgeführt werden und, wo eine solche nicht möglich ist, auf die Veröffentlichung des fraglichen Berichts verzichtet werden.

1.4 Justiz/Polizei/Sicherheit

1.4.1 Datenschutz im Rahmen der zweiten Schengen-Evaluation

Anlässlich der zweiten Schengen-Evaluation in der Schweiz wurden die Kompetenzen des eidgenössischen Beauftragten, weiterer Instanzen auf Bundesebene und mehrerer kantonaler Datenschutzbehörden geprüft. Diese zweite Evaluation schloss mit einer positiven Bilanz.

Der Schengen-Besitzstand entwickelt sich kontinuierlich weiter. Die richtige Umsetzung und Anwendung der Bestimmungen von Schengen werden in sämtlichen Mitgliedsstaaten etwa alle vier Jahre geprüft. Im Jahr 2008 durchlief die Schweiz das erste Evaluierungsverfahren, das die Inbetriebnahme des Schengener Informationssystems (SIS) möglich machte. Die nächste Evaluation erfolgte im Frühjahr 2014: zwischen März und Juli führten fünf Teams, bestehend aus Sachverständigen des Europäischen Rates, der Europäischen Kommission und der übrigen Schengen-Staaten die zweite Evaluation durch. Diese betraf die korrekte Anwendung der Vorschriften für die polizeiliche Zusammenarbeit, den Datenschutz, die Visumserteilung, den Aussengrenzschutz und das Schengener Informationssystem der zweiten Generation (SIS II).

Die Datenschutzevaluierung bezog sich auf die Umsetzung des Abkommens zwischen der Schweizerischen Eidgenossenschaft, der Europäischen Union und der Europäischen Gemeinschaft, auf die Assoziierung der Schweizerischen Eidgenossenschaft bei der Umsetzung, der Anwendung und der Entwicklung des Schengen-Besitzstands (SAA), insbesondere auf die Kompetenzen der eidgenössischen Kontrollbehörde (EDÖB) und der kantonalen Datenschutzbehörden. Diese wurden auf Grund eines Fragebogens und von örtlichen Inspektionen beurteilt. Im Besonderen wurden die Befugnisse der Kontrollbehörden in den Bereichen Aufsicht, Abklärungen und Sanktionen sowie ihre Unabhängigkeit überprüft. Dabei ging es um die Analyse der Rechtsgrundlagen und im Speziellen um die Kontrollbefugnisse bezüglich des SIS II und der an seinem Betrieb beteiligten Dienststellen. Die Rechte der betroffenen Personen, die Datensicherheit, die Zusammenarbeit mit den ausländischen Behörden und die Information der Öffentlichkeit wurden ebenfalls einer Prüfung unterzogen.

Wir haben uns aktiv in die Vorbereitung dieser Evaluation eingebracht, in enger Zusammenarbeit namentlich mit dem Bundesamt für Justiz (BJ), dem Bundesamt für Polizei (fedpol), dem Staatssekretariat für Migration (SEM), dem Eidgenössischen Departement für auswärtige Angelegenheiten (EDA) und den kantonalen Datenschutzbehörden. Es ging um die Beantwortung des von der Europäischen Union

an die Schweiz gerichteten Fragebogens (Juni 2013) und die Vorbereitungen für die örtlichen Inspektionen. Der Evaluationsbesuch bei den schweizerischen Behörden zum Thema Datenschutz fand vom 12. bis 16. Mai 2014 statt. Die Sachverständigengruppe untersuchte die Kompetenzen des EDÖB und der Datenschutzbehörden der im Besuchsprogramm vorgesehenen Kantone Neuenburg/Jura und Bern.

Die Ergebnisse der Evaluation wurden in einen Datenschutzbericht aufgenommen. Am 18. November 2014 hat der Rat der EU auf Ministerebene die zweite Schengen-Evaluation offiziell abgeschlossen und dabei festgehalten, dass die Datenschutzanforderungen aufgrund des Assoziierungsabkommens von Schengen in der Schweiz erfüllt sind. - Die nächste Evaluierung der Schweiz ist für 2018 vorgesehen.

1.4.2 Entwurf des Nachrichtendienstgesetzes

Das Nachrichtendienstgesetz ist dem Parlament im Entwurf unterbreitet worden. Wir haben unseren Standpunkt bei einer Anhörung vor der Sicherheitspolitischen Kommission des Nationalrats dargelegt.

Wir wurden von der Sicherheitspolitischen Kommission des Nationalrats zu einer Anhörung eingeladen, um zum Gesetzesentwurf über den Nachrichtendienst Stellung zu nehmen: Wir begrüssten in diesem Rahmen die verschiedenen Kontrollen, die für genehmigungspflichtige Massnahmen zur Informationsbeschaffung und für die Massnahmen zur Datensicherheit vorgesehen sind (Bearbeitung der Daten in einer spezifischen, für einen begrenzten Mitarbeiterkreis zugänglichen Datensammlung). Um in diesem Bereich eine wirksame Überwachung zu gewährleisten, haben wir vorgeschlagen, dass das interne Aufsichtsorgan des Departements und die Delegation der Geschäftsprüfungskommissionen verpflichtet werden, sämtliche genehmigungspflichtigen Beschaffungsmassnahmen systematisch zu kontrollieren. Zudem wiesen wir darauf hin, dass auch auf die Gewährleistung einer unabhängigen externen Kontrolle der Datenbearbeitungen zu achten ist, damit überprüft und sichergestellt werden kann, dass der rechtliche Rahmen eingehalten wurde und die angeordneten Massnahmen angemessen und tatsächlich notwendig waren.

Wir haben erneut aufgezeigt, dass der Entwurf noch einige datenschutzrechtlich problematischen Elemente enthält: der Einsatz von Luftfahrzeugen und Satelliten, die Möglichkeit zum Eindringen in Computersysteme und -netzwerke sowie die Ausnahme der Informationsbeschaffung gemäss NDG vom Geltungsbereich des Öffentlichkeitsgesetzes. Bei dieser Anhörung haben wir auch daran erinnert, dass die Kabelaufklärung trotz der vorgeschlagenen Bestimmungen die Gefahr erheblicher Persönlichkeitsverletzungen mit sich bringt (vgl. unseren 21. Tätigkeitsbericht 2013/2014, Ziff. 1.4.6 und Ziff. 2.5.1).

1.4.3 Revision der Verordnung über die Informationssysteme des Nachrichtendienstes des Bundes

Wir haben im Rahmen der Revision der Verordnung über die Informationssysteme des Nachrichtendienstes des Bundes Stellung genommen. Unseren Bemerkungen zur vorgesehenen Regelung der periodischen Kontrollen im Informationssystem äussere Sicherheit (ISAS) und in den übrigen Informationssystemen des Nachrichtendienstes des Bundes wurde Rechnung getragen.

Die Änderung des Bundesgesetzes über die Zuständigkeiten im Bereich des zivilen Nachrichtendienstes (ZNDG) vom 21. März 2014 und die Verordnung über die Informationssysteme des Nachrichtendienstes des Bundes (ISV-NDB) sind am 1. November 2014 in Kraft getreten. Seit diesem Zeitpunkt ist das Informationssystem äussere Sicherheit (ISAS) kein Pilotprojekt mehr, sondern eine Datensammlung mit einer definitiven Gesetzesgrundlage. Neben den durch die Revision des ZNDG notwendig gewordenen Anpassungen wurde die ISV-NDB im Interesse einer grösseren Klarheit neu strukturiert. Im Rahmen der Ämterkonsultation vertraten wir die Ansicht, dass die vorgeschlagenen Lösungen für die verschiedenen periodischen Kontrollen in ISAS und in den übrigen Informationssystemen des Nachrichtendienstes des Bundes (NDB) nicht befriedigend seien (die Kontrollen betreffend das Informationssystem innere Sicherheit (ISIS) gaben hingegen keinen Anlass zu Bemerkungen). Nach mehreren Gesprächen mit dem NDB konnten folgende Lösungen gefunden werden:

Die für die Datenerfassung zuständigen Mitarbeiterinnen und Mitarbeiter des NDB überprüfen periodisch die Datensätze in ISAS, die Objekte zu Personen oder Organisationen enthalten. Sie beurteilen unter Berücksichtigung der aktuellen Lage, ob die Datensätze für die Erfüllung der Aufgaben des NDB noch notwendig sind. Sie löschen nicht mehr benötigte Dateien. Sie berichtigen, kennzeichnen oder löschen als unrichtig erkannte Daten. Schliesslich halten sie die Durchführung und das Ergebnis der Überprüfung fest. Die periodische Überprüfung erfolgt bei jeder Ergänzung eines Datensatzes. In jedem Fall erfolgt eine periodische Überprüfung je nach Bereich zehn bis zwanzig Jahre nach der Erfassung des Objekts oder der letzten periodischen Überprüfung. Überdies führt die Qualitätssicherungsstelle mindestens einmal jährlich planmässige Kontrollen durch.

Die Qualitätssicherungsstelle überprüft mittels Stichproben die in den übrigen Informationssystemen des NDB erfassten Daten. Namentlich prüft sie, ob die Daten richtig sind und ob sie rechtmässig, angemessen und zweckmässig bearbeitet werden. Diese tut dies für jedes Informationssystem mindestens einmal jährlich nach einem Kontrollplan.

1.4.4 Totalrevision Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs

Im Berichtsjahr haben wir an den Sitzungen der Kommission für Rechtsfragen des Nationalrats bezüglich der Totalrevision des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs teilgenommen. Thema war dabei auch die Herausgabe von Randdaten bei rückwirkender Überwachung.

Im vergangenen Jahr lud uns die Kommission für Rechtsfragen des Nationalrats 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).

Wird das revidierte BÜPF von den Räten verabschiedet, werden wir bei den nachfolgenden Totalrevisionen der Verordnungen unser Hauptaugenmerk auf die Einhaltung des vom Gesetz vorgegebenen Rahmens richten.

1.4.5 Revision der Verordnung über das Informationssystem der Bundeskriminalpolizei (JANUS)

Der Einsatz von Informatikinstrumenten für die Bearbeitung von besonders schützenswerten Daten oder Persönlichkeitsprofilen im Rahmen der Informationssysteme der Bundeskriminalpolizei erfordert eine Gesetzesgrundlage im formellen Sinn. Auf diesen Umstand haben wir bei der Ämterkonsultation zur Revision der Verordnung über das Informationssystem der Bundeskriminalpolizei (JANUS) hingewiesen.

Das Bundesamt für Polizei (fedpol) hat Informatikinstrumente für eine effektivere Bearbeitung von Informationen entwickelt, die für das System zur Unterstützung gerichtspolizeilicher Abklärungen des Bundes, das System zur Bearbeitung von Daten betreffend Bundesdelikte und das Datenbearbeitungssystem der internationalen und interkantonalen Polizeikooperation bestimmt sind. Um eine rechtskonforme Nutzung dieser Instrumente zu ermöglichen, hat fedpol eine Revision der Verordnung über das Informationssystem der Bundeskriminalpolizei (JANUS-Verordnung) vorgeschlagen.

Im Rahmen der Ämterkonsultation wiesen wir darauf hin, dass das Bundesgesetz über die polizeilichen Informationssysteme des Bundes (BPI) den Einsatz dieser Informatikinstrumente nicht ausdrücklich vorsehe. Die Änderung der JANUS-Verordnung sei somit problematisch, da sich die vorgesehenen Bestimmungen nicht auf eine ausreichende Gesetzesgrundlage stützten (insbesondere die Bestimmungen über die Funktionen dieser Informatikinstrumente, die der Aufbewahrung besonders schützenswerter Daten dienen). Da es sich ausschliesslich um Informatikinstrumente zur erleichterten Bearbeitung von Daten handelt, die für die oben erwähnten Informationssysteme bestimmt sind, wurde eine befristete Regelung auf Ebene der Verordnung vorgesehen. Bei der nächsten Revision des BPI würden diese Informatikinstrumente ausdrücklich in einer Gesetzesgrundlage im formellen Sinn aufgeführt.

1.4.6 Änderung der Rechtsgrundlagen für die Weiterentwicklung der Armee

Im Rahmen der Ämterkonsultationen zur Änderung der Rechtsgrundlagen für die Weiterentwicklung der Armee äusserten wir uns zur präventiven Anordnung von Blutuntersuchungen oder Impfungen sowie zum Erfordernis medizinischer Routineuntersuchungen. Der Bundesrat hat unsere diesbezüglichen Anliegen in seine Botschaft aufgenommen und auch unserem Ersuchen, die Routineuntersuchungen auf eine beschränkte Anzahl Personen zu begrenzen, Folge geleistet. Eine Divergenz gab es hingegen in Bezug auf Sicherheitsprüfungen bei Militärpersonen ohne deren Einwilligung.

Der Änderungsentwurf zum Bundesgesetz über die Armee und die Militärverwaltung (MG) sieht vor, dass der Bundesrat für die Ausübung von Armeefunktionen, die mit einem hohen Infektionsrisiko verbunden sind, präventiv Blutuntersuchungen oder Impfungen anordnen kann. Wir forderten in der Botschaft zum Gesetzesentwurf sehr viel genauere Ausführungen zu den verschiedenen vorgesehenen Blutanalysen und Impfungen sowie zu den Funktionen, die solche Massnahmen erfordern. Dass Sanitätspersonal oder Einsätze im Ausland als Beispiele genannt werden, erschien uns zu vage. Unseres Erachtens müssen in der Botschaft die Grenzen festgelegt werden, innerhalb derer der Bundesrat die im Gesetz erwähnten Massnahmen in der Ausführungsverordnung konkretisieren kann. Das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) hat unseren Bemerkungen Rechnung getragen und die Botschaft entsprechend abgeändert.

Andererseits wurde im Änderungsentwurf zum MG zunächst festgelegt, dass das VBS für das militärische Personal und das oberste Kader der Militärverwaltung des Bundes regelmässige medizinische Routineuntersuchungen vorsehen kann,

die von einem Vertrauensarzt oder vom ärztlichen Dienst durchgeführt werden. Diese medizinischen Untersuchungen sind bisher freiwillig und betreffen nur eine begrenzte Anzahl Personen (höhere Stabsoffiziere und das oberste Kader der Militärverwaltung des Bundes). Gemäss dem Entwurf sollte der Kreis der betroffenen Personen erheblich ausgeweitet werden (militärisches Personal und das oberste Kader der Militärverwaltung des Bundes), und zudem sollten diese medizinischen Routineuntersuchungen für obligatorisch erklärt werden.

Aufgrund der knappen Angaben in der Botschaft konnte nicht überprüft werden, ob eine solche Massnahme dem Grundsatz der Verhältnismässigkeit entspricht. Es erschien auch erstaunlich, dass sich das gesamte Militärpersonal medizinischen Routineuntersuchungen unterziehen sollte. Wir haben deshalb darum ersucht, dass der Kreis der davon betroffenen Personen eingegrenzt werde. Das VBS hat unseren Bemerkungen insofern Rechnung getragen, als dass die medizinischen Routineuntersuchungen nun einzig bei Stabsoffizieren, dem militärischen Personal der Militärpolizei und dem obersten Kader der Militärverwaltung des Bundes durchgeführt werden sollen.

Der Änderungsentwurf zum Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (BWIS) wiederum sieht vor, dass Militärpersonen auch ohne ihre Einwilligung Sicherheitsprüfungen unterzogen werden können, wenn dies für die Ausübung der aktuellen oder geplanten Funktion erforderlich ist. Da Militärpersonen Aufgaben gegen ihren Willen zugewiesen werden können, sind wir der Ansicht, dass die Möglichkeit solcher Sicherheitsprüfungen ohne die Einwilligung der betroffenen Personen dem Grundsatz der Verhältnismässigkeit widerspricht. Überdies ist es unseres Erachtens für die Sicherheit problematisch, wenn einer Person eine Funktion gegen ihren Willen übertragen wird. Wir können indessen nachvollziehen, dass in Ausnahmefällen eine Sicherheitsprüfung ohne die Einwilligung der betroffenen Person gerechtfertigt sein kann. Das VBS hat unsere Bemerkungen nicht berücksichtigt. Diese Divergenz wurde im Bundesratsantrag ausgewiesen.

1.4.7 Kontrolle der Logfiles beim Staatssekretariat für Migration als Endnutzer des SIS

Im Rahmen der Schengen-Assoziierungsabkommen haben wir im Berichtsjahr beim Staatssekretariat für Migration (SEM) eine Kontrolle durchgeführt. Dabei wurden die Logfiles, die bei der Nutzung des Schengener Informationssystems (SIS) durch das SEM anfallen, überprüft. Die Analyse der Logfiles hat ergeben, dass der Zugang der regionalen Sektionen zum SIS regelkonform ist.

Im Rahmen der Schengen-Assoziierungsabkommen führen wir jährliche Kontrollen bei den Endnutzern des SIS durch. In diesem Jahr konzentrierten wir uns auf die

regionalen Sektionen des Staatssekretariats für Migration (SEM, ehemals Bundesamt für Migration/BFM), deren Hauptaufgaben die Bearbeitung von Einzelfällen im Bereich Visa, die Genehmigung von Aufenthaltsbewilligungen sowie die Bearbeitung von Fernhaltemassnahmen sind. Über die gesamte Dauer der Kontrolle war der Datenschutzberater des SEM unser Hauptgesprächspartner.

Für diese Überprüfung wählten wir nach dem Zufallsprinzip drei regionale Sektionen des SEM aus. Nachdem wir diesem unsere Kontrolle angemeldet hatten, erhielten wir die Liste der Mitarbeiter der drei betroffenen Sektionen, worauf wir unverzüglich das Bundesamt für Polizei (fedpol) kontaktierten, um uns die Logfiles zu beschaffen, in denen die Zugriffe der Mitarbeiter auf das SIS in der ausgewählten Woche aufgeführt sind. Die Kontrolle wurde zwar beim SEM angekündigt, aber den betroffenen Mitarbeitern wurde nicht mitgeteilt, dass ihre Zugriffe auf das System im Nachhinein analysiert würden.

Wir haben die Analyse in unseren Räumlichkeiten auf der Grundlage der von fedpol bereitgestellten Dokumente durchgeführt. Unsere Prüfung betraf hauptsächlich die Zahl der Zugriffe je Sektion und Mitarbeiter sowie den Inhalt der von den Mitarbeitern getätigten Recherchen.

Auf diese Weise konnten wir feststellen, dass die drei Sektionen unterschiedliche Praktiken anwenden, insbesondere dass die Mitarbeiter, die in erster Linie für die Recherchen im System verantwortlich sind, nicht alle dieselbe Funktion innehaben. Missbräuche wurden indes keine festgestellt. Überdies erschien keine Recherche verdächtig oder unangemessen. Wir konnten daher die Überprüfung ohne einen Besuch an Ort und Stelle abschliessen.

1.5 Gesundheit und Forschung

1.5.1 Herausgabe der Krankengeschichte im Original

Gestützt auf das Datenschutzgesetz (DSG) haben Patienten das Recht, vom Arzt Ihre vollständige Krankengeschichte in Form einer Kopie oder eines Ausdrucks herauszuverlangen. Ein Anspruch auf die Herausgabe der Krankengeschichte im Original lässt sich aus dem DSG hingegen nicht ableiten.

Im Berichtsjahr haben wir uns erneut mit der juristisch umstrittenen Frage betreffend die Herausgabe der Krankengeschichte im Original durch einen Arzt befasst. Anlass war die Anfrage eines im Kanton Zürich tätigen Psychiaters. Ein Patient verlangte von diesem die Herausgabe der Krankengeschichte im Original mittels eines Auskunftsgesuchs gemäss Artikel 8 des DSG. Der Psychiater kontaktierte daraufhin den kantonsärztlichen Dienst des Kantons Zürich und erkundigte sich dort, ob er die Originalunterlagen an den Patienten herausgeben darf. Der Psychiater erhielt die Auskunft, dass es sich bei der betreffenden Bestimmung des Gesundheitsgesetzes des Kantons Zürich um zwingendes öffentliches Recht handelt und diese die Gesundheitsfachpersonen zur Aufbewahrung der Originalunterlagen für den Zeitraum von zehn Jahren verpflichtet.

Der Psychiater hat uns diese Stellungnahme zugestellt und uns um eine Einschätzung gebeten. Nach einem Informationsaustausch mit dem kantonsärztlichen Dienst stellten wir fest, dass die massgeblichen Bestimmungen des Kantons Zürich die Gesundheitsfachpersonen tatsächlich zur Aufbewahrung der behandlungsrelevanten Dokumente im Original für einen Zeitraum von zehn Jahren verpflichten. Aufgrund der zwingenden öffentlich-rechtlichen Natur der Bestimmung kamen wir zudem zum Schluss, dass die Gesundheitsfachperson durch eine individuelle Vereinbarung mit dem Patienten nicht von dieser Aufbewahrungspflicht befreit werden kann. Eine Herausgabe der Krankengeschichte im Original ist somit während der Dauer der gesetzlichen Aufbewahrungspflicht ausgeschlossen.

Die Diskussionen haben uns dazu bewogen, unsere Position in dieser Frage zu konkretisieren. Konkret halten wir fest, dass sich aus dem Auskunftsrecht gemäss Artikel 8 DSG alleine kein Anspruch auf Herausgabe der Krankengeschichte im Original ergibt. Die Auskunft ist in der Regel schriftlich in Form von Kopien oder eines Ausdrucks zu erteilen. Ob ein auftragsrechtlicher Anspruch auf die Herausgabe der Krankengeschichte im Original besteht und ob er im betreffenden Kanton durchgesetzt werden könnte, ist nicht durch uns zu beurteilen. Möglich ist eine Einsichtnahme vor Ort, aber nur wenn der Patient damit einverstanden ist.

Wenn der Arzt einen sogenannten Aufklärungsschaden befürchtet, hat er das Recht den Ausdruck oder die Kopie der Krankengeschichte an einen vom Patienten bezeichneten Arzt zu übermitteln. Dieser kann dem Patienten bei der Einsicht in die Krankengeschichte beistehen und ihn vor eventuellem Schaden bewahren. Dieses Vorgehen stellt gemäss unserer Auffassung einen Ausnahmefall dar, da Patienten aufgrund der Informationspflichten des Arztes im Verlauf einer Behandlung üblicherweise gut über ihren Zustand informiert sein sollten und sich mittlerweile relativ schnell und einfach über die Bedeutung von Fachbegriffen erkundigen können. Die Kopie der Krankengeschichte ist dem Patienten grundsätzlich kostenlos zuzustellen. Nur wenn das Erstellen der Kopie mit einem besonders hohen Aufwand verbunden ist oder wenn der Patient innerhalb von zwölf Monaten schon eine Kopie verlangt hat, kann der Arzt eine Kostenbeteiligung in der Höhe von maximal 300 Franken verlangen.

1.5.2 Notverkauf von Patientendaten im Rahmen eines Konkursverfahrens

Ein Konkursamt kann Patientendaten nicht ohne vorgängige Nachfrage bei den Patienten an einen zur Praxisübernahme bereiten Nachfolger verkaufen. Die Einwilligung der Patienten ist eine notwendige Voraussetzung für die Übergabe der Daten.

Dass Patientendaten einen Geldwert haben, sahen wir im Berichtsjahr durch ein kantonales Konkursamt bestätigt. Das Amt erwog den Notverkauf der Patientenkartei eines Zahnarztes mitsamt den zugehörigen Dossiers an einen potentiellen Praxisnachfolger, und zwar ohne die betroffenen Patientinnen und Patienten vorgängig zu informieren. Das Amt meldete sich bei uns und bat um eine Einschätzung der Durchführbarkeit des Vorhabens, im Wissen, dass der EDÖB für den vorliegenden Fall eigentlich nicht zuständig ist, weil es sich bei einem Konkursamt um eine kantonale Stelle handelt, die der Aufsicht des kantonalen Datenschutzbeauftragten unterstellt ist. Wir teilten dem Amt mit, dass der in Betracht gezogene Notverkauf der Patientenkartei und der zugehörigen Dossiers nicht ohne vorgängige Konsultation der betroffenen Personen durchgeführt werden darf.

Patientendaten, soweit es sich um Gesundheitsdaten handelt, sind gemäss des Bundesgesetzes über den Datenschutz (DSG) besonders schützenswert. Für ihr Bearbeiten braucht es, falls eine Einwilligung als Rechtfertigungsgrund für das Bearbeiten notwendig ist, eine ausdrückliche Einwilligung der betroffenen Person, welche sie freiwillig nach einer angemessenen Aufklärung abgegeben hat (Artikel 4 Absatz 5 DSG). Weiter ist zu berücksichtigen, dass der Zahnarzt hier einer kantonalen Aufbewahrungspflicht unterliegt, welche über den Betrieb der Praxis hinaus bestehen bleibt.

1.5.3 Diebstahl von Patientendaten aus einer Arztpraxis

Wird ein Computer mit Patientendaten aus einer Arztpraxis gestohlen, so trifft den bestohlenen Arzt gegenüber dem EDÖB keine gesetzliche Informationspflicht. Eine Information der Patientinnen und Patienten kann aber sinnvoll sein.

Der Diebstahl eines persönlichen Computers ist eine mühsame Angelegenheit. Erinnerungsfotos oder wichtige Korrespondenz sind für immer verloren, wenn nicht eine Sicherungskopie erstellt wurde. Besonders heikel ist es, wenn aus einer Arztpraxis ein Computer mit Patientendaten gestohlen wird. Die Vorstellung, dass der Computer mitsamt Patientendaten verkauft werden könnte, lässt wahrscheinlich Ärzte und Patienten erschaudern. Eine von einem solchen Diebstahl betroffene Ärztin hat uns telefonisch kontaktiert und sich erkundigt, ob sie ihre Patienten oder eine Aufsichtsbehörde über den Diebstahl informieren muss.

Im Gegensatz zu anderen europäischen Ländern sieht das Schweizer Recht eine solche Information beim Verlust bzw. der unrechtmässigen Datenbekanntgabe an Dritte von besonders schützenswerten Personendaten nicht vor. Allenfalls könnte aus dem datenschutzrechtlichen Transparenzgrundsatz eine Pflicht zur Information der betroffenen Personen abgeleitet werden, da in einem solchen Fall eine zwar ungewollte aber nicht mit dem ursprünglichen Zweck zu vereinbarende Datenbekanntgabe stattgefunden hat. Allerdings kann die Information der Patientinnen und Patienten aus einem anderen Grund als sinnvoll betrachtet werden. Sollten diese nämlich auf einem anderen Weg von dem Diebstahl Kenntnis erhalten, so dürfte das Vertrauensverhältnis zwischen ihnen und dem Arzt Schaden nehmen.

Aus datenschutzrechtlicher Sicht bleibt noch darauf hinzuweisen, dass die Ärztin oder der Arzt die Patientendaten auf dem eigenen Computer durch geeignete technische Massnahmen vor unberechtigten Zugriffen schützen muss. Die ergriffenen Massnahmen müssen dabei dem gegenwärtigen Stand der Technik entsprechen und der Sensibilität der Daten angepasst sein. Der blosse Schutz durch Benutzerkennwort und Passwort reicht bei Gesundheitsdaten nicht aus. Vielmehr müssen entsprechende Verschlüsselungstechnologien eingesetzt werden. Sicher ist, dass die betroffene Ärztin den Diebstahl entspannter hätte hinnehmen können, wenn die Daten auf ihrem Computer verschlüsselt gewesen wären.

1.5.4 Sachverhaltsabklärung beim ärztlichen Dienst des Bundes (MedicalService AeD)

Im Berichtsjahr haben wir beim ärztlichen Dienst der Bundesverwaltung und der bundesnahen Betriebe (MedicalService AeD) eine Sachverhaltsabklärung eröffnet. Im Fokus der Untersuchung steht namentlich die Bearbeitung der Gesundheitsdaten von Stellenbewerberinnen und -bewerbern.

Nachdem wir im Berichtsjahr mehrere Bürgeranfragen zu MedicalService AeD, dem ärztlichen Dienst der Bundesverwaltung und der bundesnahen Betriebe, erhalten hatten, eröffneten wir im Herbst 2014 im Rahmen unserer Aufsichtstätigkeit eine Sachverhaltsabklärung betreffend Gesundheitsdaten im Arbeitsbereich bei dieser Organisation, die den SBB angegliedert ist. Wir prüfen aktuell, ob die Bearbeitung der Gesundheitsdaten von Stellenbewerberinnen und -bewerbern den Datenschutzanforderungen genügen. Dabei steht vor allem die Bearbeitung und Bekanntgabe der Daten durch MedicalService sowie der Datenfluss zwischen MedicalService und dem Arbeitgeber im Fokus.

Wir beziehen uns dabei auf die Kompetenzübertragung des Eidgenössischen Personalamtes an den ärztlichen Dienst (in diesem Fall MedicalService), welcher gemäss Bundespersonalgesetz (BPG) in gewissen Fällen besonders schützenswerte Personendaten über die Gesundheit bearbeiten darf. Gemäss BPG darf der ärztliche Dienst die interessierten Stellen jedoch nur über die «Schlussfolgerungen aus ärztlichen Feststellungen» orientieren. Er darf also z.B. mitteilen, ob der Bewerber aus gesundheitlichen Gründen für eine Stelle geeignet ist oder nicht. Keinesfalls aber darf er Dritten – ohne schriftliche Zustimmung der betroffenen Person – eine eigentliche Diagnose mitteilen. Wir erachten es als notwendig, die in diesem Zusammenhang stehenden Datenbearbeitungen vertiefter anzusehen und auf die Konformität mit dem Bundesgesetz über den Datenschutz im Rahmen einer Sachverhaltsabklärung zu überprüfen.

Der erste Teil des Verfahrens ist inzwischen abgeschlossen. Bei diesem wurden die erhaltenen Unterlagen ausgewertet. Als nächstes werden wir vor Ort bei MedicalService einen Augenschein nehmen, um zu prüfen, ob die Prozesse und Datenbearbeitungen den Anforderungen des DSG genügen.

1.5.5 Aufbewahrung von Patientenakten in einer Cloud

Vermehrt wollen Ärzte ihre Patientenakten in einer Cloud aufbewahren. Dies bietet einerseits viele Vorteile, andererseits ist es für Ärzte aufgrund ihres im Strafrecht verankerten Berufsgeheimnisses nicht unproblematisch. Insbesondere gilt es bei der Auslagerung der Aufbewahrung von Patientenakten dafür zu sorgen, dass keine ungerechtfertigte Bearbeitung der Patientendaten durch Dritte erfolgt.

Gemäss Datenschutzgesetz kann das Bearbeiten von Personendaten und somit die Verwaltung von Patientendossiers an einen Dritten übertragen werden. Dies allerdings nur unter den Voraussetzungen, dass die Daten nur so bearbeitet werden, wie der Auftraggeber selbst (also der Arzt) es tun dürfte und wenn keine gesetzliche oder vertragliche Geheimhaltungspflicht es verbietet. Ärzte sind in Bezug auf die Krankengeschichte bzw. auf den Inhalt des Patientendossiers an das strafrechtlich verankerte Berufsgeheimnis gebunden. Dies ist eine gesetzliche Geheimhaltungspflicht, deren Übertragung auf einen Dritten nicht oder allenfalls nur bedingt mittels Vertrag erfolgen kann. Folglich bleibt die Verantwortung für die Bearbeitung der Patientendaten beim Arzt.

Wir haben bei sämtlichen Anfragen die Ärzte und Cloud-Anbieter auf unsere Erläuterungen bezüglich Cloud Computing hingewiesen, um sie für diese Problematik zu sensibilisieren. Insbesondere haben wir die Anfragenden auf Folgendes aufmerksam gemacht: Sollte der Arzt die Bearbeitung seiner Patientendossiers an einen Dritten übertragen, wäre er nach wie vor für die Geheimhaltung verantwortlich. Er müsste deshalb dafür sorgen, dass die Datensicherheit beim Dritten – also in der Cloud – im Sinne des Datenschutzgesetzes gewährleistet ist. Das bedeutet, dass die Patientendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden müssen. Es muss für Vertraulichkeit, Verfügbarkeit und Integrität der Daten gesorgt sein und der Arzt muss dies kontrollieren und überwachen können.

Aus diesem Grund gibt es aus unserer Sicht für einen in der Schweiz tätigen Arzt nur die folgende Lösung: Der Cloud-Anbieter bzw. die Cloud müssen in der Schweiz sein und dem Arzt vertraglich garantieren, dass keine Patientendaten die Schweiz verlassen. Die Patientendaten müssen konsequent clientbasiert verschlüsselt sein, was heisst, dass der Arzt als Dateninhaber als einzige Person den Schlüssel zu den sich in der Cloud befindlichen Daten hat. Der Cloud-Anbieter darf nicht in Besitz des Schlüssels kommen. Der Dateninhaber bzw. der Arzt kann Daten, die durch ihn vorgängig vollständig anonymisiert wurden, für Statistikzwecke zur Verfügung stellen. Nur durch diese Massnahmen kann aus unserer Sicht vollumfänglich gewährleistet werden, dass der Arzt seine strafrechtlich verankerte Geheimhaltungspflicht

wahren kann und dass zu keinem Zeitpunkt eine ungerechtfertigte Bearbeitung der Patientendaten stattfindet.

1.5.6 eHealth – Identifikation der Patienten und Zugriffe auf das ePatientendossier

Das Projekt eHealth kommt in eine entscheidende Phase. Nachdem die Empfehlungen V verabschiedet wurden, werden Detailspezifikationen für die Identifikation der Patienten und Zugriffsrechte auf das ePatientendossier definiert. Sie bilden die Grundlage für die eigentliche Implementierung aber auch für die Verordnung zum Elektronischen Patientendossiergesetz (EPDG).

Damit die bisher von uns durchgesetzten Datenschutzmassnahmen nicht in der Implementierungsphase geopfert werden, haben wir uns entschieden, auch weiterhin einen Teil unserer knappen Ressourcen im Bereich eHealth einzusetzen. Das Projekt befindet sich in einer Phase, in der detaillierte Verfahren für den Umgang mit dem elektronischen Patientendossier definiert werden. Erfahrungsgemäss wird in vielen Grossprojekten zu diesem Zeitpunkt die ursprünglich grosse Bereitschaft für datenschutzkonforme Lösungen über Bord geworfen. Kosten und Komplexität werden als Argumente bemüht, um die Systeme zu optimieren und die Persönlichkeitsrechte einzuschränken. Diese Gefahr besteht auch im eHealth-Projekt.

Durch permanente Feinkorrekturen sorgen wir in den Teilprojekten dafür, dass das Datenschutzrecht nicht nur ein politisches Ziel bleibt, sondern auch in der Umsetzung berücksichtigt wird. Ganz besonders gilt das für das Mandat des Koordinationsorgans eHealth für die «Detailspezifikationen Zugriffsrechte», die Verordnung zum EPDG und die Zertifizierung der Gemeinschaften. Vor der Kommission für soziale Sicherheit und Gesundheit des Ständerates hatten wir die Gelegenheit genutzt, unseren Standpunkt darzulegen und die Einführung eines eigenen, von der AHV-Nummer unabhängigen Patientenidentifikators zu fordern. Sowohl die Kommission als auch der Ständerat sind unserer Argumentation gefolgt und haben den entsprechenden Gesetzesentwurf des Bundesrats angenommen.

1.5.7 Entwurf für ein Bundesgesetz über die Registrierung von Krebserkrankungen

Der Bundesrat hat dem Parlament den Gesetzesentwurf zur Erfassung der Krebserkrankungen in der Schweiz vorgelegt. Anlässlich der zweiten Ämterkonsultation haben wir auf unsere Divergenzen betreffend die Erhebung zusätzlicher Daten und auf unsere Vorbehalte bezüglich der Nutzung der AHV-Nummer verwiesen.

Die Schweiz soll künftig über ein nationales Register der Krebserkrankungen verfügen. Der Bundesrat hat dem Parlament eine Gesetzesvorlage unterbreitet. Damit die Datenbank vollständig ist, werden Ärzte, Spitäler und andere Einrichtungen zur Meldung der Fälle verpflichtet. Die Patienten können sich jedoch jederzeit einer Registrierung ihrer Daten widersetzen. Das neue Gesetz regelt die Erhebung, die Registrierung und die Übertragung der Daten, damit die in den kantonalen Tumorregistern enthaltenen Informationen ausgewertet und auf nationaler Ebene veröffentlicht werden können. So soll es möglich werden, die Prävention und die Früherkennung zu verbessern und die Qualität der Versorgung, der Diagnostik und der Behandlungen zu beurteilen.

Die Regierung hat ihren Entwurf nach Massgabe der im Vernehmlassungsverfahren geäusserten Kritiken überarbeitet. Dabei ging es insbesondere um Bemerkungen zu den erhobenen Daten, ihren Schutz und die Rechte der Patienten. Die neue Fassung enthält gewisse Anpassungen, die bedeutende Folgen für die Patientenrechte haben und Risiken einer Verletzung der Persönlichkeitsrechte der betroffenen Personen mit sich bringen (siehe unsere früheren Bemerkungen zu dem Thema in unserem 21. Tätigkeitsbericht 2013/2014, Ziffer 1.5.3).

So haben wir zur Kenntnis genommen, dass der Bundesrat trotz unserer Bedenken beschlossen hat, die AHV-Nummer zwecks Personenkennung in den Registern beizubehalten. In unseren früheren Stellungnahmen hatten wir darauf hingewiesen, dass die systematische Verwendung der AHV-Nummer als einziges Identifikationsmerkmal grosse Risiken für die Privatsphäre der betroffenen Personen birgt, da sich durch diese Erweiterung unerwünschte Verknüpfungen zwischen verschiedenen Datenbanken herstellen lassen. Wir befürworteten daher die Einführung einer alternativen Identifikationsnummer (zum Beispiel einer sektorspezifischen Kennung für Krebsregister), wobei die sektorspezifische Patientenidentifikationsnummer im Rahmen des Entwurfs für das Bundesgesetz über das elektronische Patientendossier (EPDG) als Vorbild dienen könnte. Dieser Ansatz hat den Vorteil, dass er das Risiko einer Verknüpfung der Informationen verringert, was umso wichtiger ist, als die Daten der Tumorregister besonders schützenswert sind und die Erstellung von Persönlichkeitsprofilen ermöglichen.

Bezüglich der Erhebung zusätzlicher Daten haben wir uns für die Beibehaltung der ausdrücklichen Einwilligung anstelle des schliesslich in der Neufassung gewählten Widerspruchsrechts ausgesprochen. Es handelt sich hierbei nämlich um besonders schützenswerte Daten, anhand derer die Krankheitsentwicklung und der Behandlungsverlauf bewertet sowie das Lebensumfeld der betroffenen Personen ermittelt werden können. In Verbindung mit den Grunddaten erschliessen sich so sehr ausführliche Informationen über den Gesundheitszustand einer Person. Das Erfordernis einer ausdrücklichen Einwilligung ist nicht nur in Artikel 4 Absatz 5 DSG,

sondern auch in verschiedenen neueren Gesetzen vorgesehen. Etwa im Bundesgesetz über genetische Untersuchungen beim Menschen (GUMG), im Bundesgesetz über die medizinisch unterstützte Fortpflanzung (FMedG), im Bundesgesetz über die Forschung am Menschen (HFG) sowie im Bundesgesetz über die Forschung an embryonalen Stammzellen (StFG).

Schliesslich haben wir uns dafür ausgesprochen, zwecks Aktualisierung und Vervollständigung das Todesdatum in den Tumorregistern nicht wie im Entwurf vorgesehen mit dem in der zentralen Ausgleichsstelle vermerkten Datum abzugleichen, sondern mit dem Datum der kantonalen Einwohnerregister oder des Zivilstandsregisters. Die zentrale Ausgleichsstelle ist nämlich kein nationales Einwohnerregister und nicht dazu bestimmt, Personendaten, die sie zu Sozialversicherungszwecken bearbeitet, an Behörden oder Dritte zu übermitteln.

1.6 Versicherungen

1.6.1 Kontrolle der Datenannahmestellen der Krankenversicherer

Seit dem 1. Januar 2014 muss jeder Krankenversicherer über eine zertifizierte Datenannahmestelle für den Empfang der Rechnungen des Typus ‹Diagnosis Related Groups› (DRG) verfügen. Unsere Kontrollen von zwölf Datenannahmestellen haben gezeigt, dass diese grundsätzlich gut funktionieren. In einigen Fällen haben wir aber auch Mängel festgestellt, die wir der jeweiligen Zertifizierungsstelle gemeldet haben.

Im Berichtsjahr haben wir bei zwölf Krankenversicherern im Rahmen von Sachverhaltsabklärungen die Datenannahmestelle kontrolliert. Dabei haben wir auch die Schnittstellen zwischen den Spitälern, allfälligen dazwischengeschalteten Intermediären und den Datenannahmestellen sowie zwischen den Annahmestellen und den Versicherern geprüft.

Bei diesen Kontrollen stellten wir unter anderem Folgendes fest:

Der Aufbau bzw. die Form der Datenannahmestelle fällt je nach Krankenversicherer sehr unterschiedlich aus. Grössere Versicherer haben tendenziell eine eigene Annahmestelle im Haus. Diese betreiben sie zum Teil mit eigenentwickelten oder mit gekauften bzw. lizenzierten Systemen. Mittlere und kleine Krankenversicherer hingegen haben die Annahmestelle eher an einen Dritten ausgelagert, der sie in ihrem Auftrag betreibt. Die Datenübermittlung von den Spitälern an die Annahmestelle erfolgt immer über einen Intermediär. Einige Annahmestellen sind sehr komplex und bestehen aus mehreren miteinander kombinierten Überprüfungssystemen, andere wiederum bestehen nur aus einem System.

Der grösste Teil der Rechnungen des Typus DRG werden in elektronischer Form übermittelt. Dies zeigt, dass die meisten Leistungserbringer heute so ausgerüstet sind, dass sie elektronische Rechnungen liefern können. Trotzdem konnten wir teilweise erstaunliche und nicht nachvollziehbare Unterschiede zwischen den einzelnen kontrollierten Krankenversicherern bezüglich Anteil der Rechnungen in elektronischer Form und in Papierform feststellen. Obwohl es sich oftmals um den gleichen Leistungserbringer handelt, werden die Krankenversicherer unterschiedlich beliefert. So erhält beispielsweise ein Versicherer hauptsächlich Rechnungen in Papierform, während ein anderer nur elektronische Rechnungen erhält. Grundsätzlich stellten wir jedoch eine starke Tendenz zu einer rein elektronischen Rechnungsstellung fest.

Des Weiteren haben wir festgestellt, dass Artikel 59a der Verordnung über die Krankenversicherung (KVV) teilweise so verstanden wurde, dass nur der medizinische

Datensatz an die Annahmestelle geleitet werden müsse, da sich nur darauf medizinische Angaben befänden. Wir haben in der Folge sämtliche an der Umsetzung des Artikels Beteiligten darauf aufmerksam gemacht, dass die Formulierung klar besagt, dass sämtliche Datensätze an die Annahmestelle zu liefern sind. Nur so ist gewährleistet, dass diese ihre Funktion gesetzeskonform wahrnehmen kann, nämlich zu bestimmen, welche Rechnung eine weitere Überprüfung benötigt und dafür zu sorgen, dass nur die Daten zum Krankenversicherer gelangen, die dieser wirklich benötigt (Grundsatz der Verhältnismässigkeit). Wir haben ausserdem darauf hingewiesen, dass sich auf dem administrativen Datensatz auch medizinische Angaben befinden, insbesondere der DRG-Code, der in den meisten Fällen schon eine klare Aussage über die Gesundheit des Patienten macht und daher ein Gesundheitsdatum darstellt.

Im Rahmen der Kontrollen haben wir zudem festgestellt, dass es nicht immer klar ist, welche Bearbeitungsverfahren Teil der Annahmestelle sind und somit einer Zertifizierung unterliegen. Wir haben den Krankenversicherern, ihren Dienstleistern und dem jeweiligen Zertifizierer mitgeteilt, welche Prozesse bzw. Datenbearbeitungen zwingend durch die Annahmestelle vorzunehmen sind und in welcher Reihenfolge diese Prozesse stattzufinden haben. Sämtliche Prüfprozesse, seien es elektronische oder von Menschen durchgeführte, die darüber entscheiden, ob eine Rechnung vertieft zu prüfen ist oder nicht, müssen Teil der Annahmestelle sein; unabhängig davon, ob es sich um Prozesse für Rechnungen in Papierform oder in elektronischer Form handelt. Ausserhalb der Annahmestelle darf keine systematische Prüfung sämtlicher Rechnungen stattfinden. Die Gesamtheit dieser Prozesse bzw. Datenbearbeitungsverfahren sind Teil der Datenannahmestelle und sind zu zertifizieren.

Insbesondere bei kleineren Krankenversicherern stellte sich diesbezüglich teilweise das Problem, dass Kontrollen, die dazu dienen, zu entscheiden, ob eine vertiefte Prüfung der betreffenden Rechnung stattfinden muss, durch Mitarbeiter des Krankenversicherers durchgeführt werden. Diese Mitarbeiter bzw. deren Funktion sind ebenfalls Teil der Annahmestelle und sind zu zertifizieren. Das kann zu organisatorischen Problemen innerhalb von kleinen Krankenversicherern führen. Deren Mitarbeiter nehmen oftmals eine Doppelfunktion wahr. Einerseits sind sie Teil der Datenannahmestelle, weil sie die oben erwähnten Kontrollen durchführen, und andererseits Mitarbeiter der Leistungsabteilung und nehmen in dieser Funktion die vertiefte Prüfung der von ihnen selbst ausgelenkten Rechnungen wahr. Dies widerspricht dem Grundgedanken der Unabhängigkeit der Annahmestelle vom Krankenversicherer. Um diese zu gewährleisten, müssen technische und/oder organisatorische Anpassungen vorgenommen werden. So werden beispielsweise zwei Arbeitsplätze geschaffen, an denen nur die jeweilige Aufgabe ausgeführt wird und/oder mittels unterschiedlichen Zugriffsberechtigungen dafür gesorgt wird, dass

man nur auf die Daten Zugriff hat, die es für die jeweilige Aufgabe effektiv braucht. So wird sowohl organisatorisch wie auch technisch verhindert, dass jemand auf alle Daten zugreifen kann.

Eine weitere organisatorische Schwierigkeit im Hinblick auf die Aufgabenteilung ist die Herausforderung, vertrauliche, d.h. für den Vertrauensarzt bestimmte Daten, gesetzeskonform zu handhaben. Müssen bei der vertieften Überprüfung der von der Annahmestelle ausgelenkten Rechnungen zusätzliche Auskünfte medizinischer Natur (Austritts- und Operationsberichte) eingefordert werden, so sind diese im Normalfall für den Vertrauensarzt des Krankenversicherers bestimmt. Der Vertrauensarzt nimmt sodann die medizinische Beurteilung vor. Müssen jedoch auch Fragen betreffend Codierung geprüft werden, muss er oftmals sogenannte Codierer oder DRG-Mitarbeiter der Leistungsabteilung hinzuziehen, die organisatorisch nicht dem vertrauensärztlichen Dienst angehören. In der Praxis wird auch dieses Problem mit den oben erwähnten technischen und organisatorischen Massnahmen gelöst.

So konnten wir anlässlich unserer Kontrollen feststellen, dass es teilweise separate Arbeitsplätze mit einer spezifischen Zugriffsregelung im vertrauensärztlichen Dienst gibt, die für die Mitarbeiter mit Doppelfunktion vorgesehen sind, so dass auch hier eine Trennung der beiden Aufgaben und des Datenzugriffs gewährleistet werden kann. Zusätzlich werden diese Mitarbeiter mit Doppelfunktion als sogenannte Hilfspersonen des Vertrauensarztes qualifiziert, so dass sie, wenn sie die Aufgabe für den Vertrauensarzt wahrnehmen, derselben Schweigepflicht unterliegen wie der Vertrauensarzt selbst (Artikel 321 StGB).

Flankierend zu unserer Kontrolltätigkeit fanden im Laufe des Berichtsjahres mehrere Koordinationssitzungen mit dem Bundesamt für Gesundheit (BAG) statt. Dies mit dem Ziel, die sich teilweise überschneidende Aufsichtstätigkeit zu koordinieren und offene Fragen bezüglich Datenannahmestellen zu klären.

Zudem fand auch in diesem Berichtsjahr wieder die jährliche Sitzung mit den Zertifizierern sowie der Akkreditierungsstelle (SAS) statt. Diese Sitzung diente dem konstruktiven Meinungsaustausch und der Beseitigung von allfälligen Unklarheiten, sei es in Bezug auf die Zertifizierung und die Funktion einer Annahmestelle sowie die Schnittstellen zwischen Leistungserbringern, Annahmestelle und Krankenversicherern.

Rückblickend können wir feststellen, dass der Betrieb der Datenannahmestellen gut funktioniert und somit die Umsetzung des Artikels 59a KVV – obwohl es keine konkreten Vorgaben oder einen Prototypen einer Annahmestelle gab – zu einem grossen Teil erfolgreich und gesetzeskonform verläuft. Die Implementation der Annahmestelle und deren Betrieb ist ein Prozess, der wie jede andere Umsetzung eines neuen Gesetzes Zeit braucht, um Vor- und Nachteile sowie Verbesserungspotentiale

erkennen zu können. Wir werden auch im nächsten Berichtsjahr Kontrollen durchführen und hoffen, dass, falls datenschutzrechtliche Mängel behoben werden müssen, weiterhin eine gute Zusammenarbeit mit den Zertifizierern, den Krankenversicherern sowie deren Dienstleistern stattfinden wird.

1.6.2 Das Datenaustauschformat XML 4.4 für DRG-Rechnungen

Die elektronischen Daten für die Abrechnung von stationären Leistungen werden in einer definierten Struktur und mit vorgegebenem Inhalt vom Spital an den Versicherer geschickt. Eine Analyse der DRG-Rechnungen unsererseits zeigte, dass der verwendete Standard von den gesetzlichen Vorgaben abweicht.

Die Verordnung über die Krankenversicherung (KVV) regelt u.a., welche Daten die Spitäler den Versicherern für die Leistungsabrechnung nach DRG bereitstellen müssen. Das Forum Datenaustausch stellt für den elektronischen Datentransfer ein standardisiertes Format zur Verfügung, das sowohl die Struktur als auch den Inhalt (Metadaten) umfasst. Der entsprechende Standard wird XML 4.4 genannt. Eine detaillierte Analyse des Standards zeigte uns, dass er von den gesetzlichen Anforderungen abweicht. Gemäss Verordnung muss der Versicherer gleichzeitig mit der Rechnung Datensätze mit den administrativen Daten und den minimalen medizinische Daten (das sogenannte MCD) erhalten, damit er die Rechnung gesetzeskonform überprüfen kann.

XML 4.4 verpackt eine Rechnungsdatei (invoice) und eine MCD-Datei in einen XML-Container. Das MCD enthält die medizinischen und die administrativen Daten. Der Container wird vom Leistungserbringer an den Versicherer elektronisch transferiert. Der Nachteil dieser Struktur ist, dass der Zugriff auf die administrativen Daten automatisch zu einer Offenlegung der medizinischen Daten führt und umgekehrt. Die gesetzlich vorgeschriebene Trennung von administrativen und medizinischen Daten muss deshalb am Schluss der Verarbeitungskette, in den Systemen der Versicherer, vorgenommen werden.

Ein weiteres Problem ist, dass im XML 4.4 Invoice, also der eigentlichen elektronischen Rechnung, der DRG-Code und die Diagnose (kodiert nach ICD) aufgeführt werden. Beides sind medizinische Informationen, die nicht in der Rechnung sondern nur im MCD aufgeführt werden sollten. Auch das hat zur Folge, dass der Versicherer in seinen Systemen die Rechnung so aufbereiten muss, dass weder DRG- noch ICD-Code in das Inkasso der Versicherung gelangen.

Wir haben sowohl das Forum Datenaustausch als auch das Bundesamt für Gesundheit auf den Missstand hingewiesen und eine Lösung verlangt. In Zukunft sollte in der Verordnung klar beschrieben sein, was in der Rechnung stehen darf; die klare Trennung von medizinischen und administrativen Daten sollte bereits in den XML-Dateien vollzogen werden, weder der DRG- noch der ICD-Code dürfen im Invoice enthalten sein.

1.6.3 Krankenzusatzversicherungen: Löschung der Antragsdaten

Uns wurde wiederholt gemeldet, dass einige Krankenzusatzversicherungen die Gesundheitsdaten von Antragsstellern, bei denen kein Vertrag zustande gekommen war, nicht gelöscht haben. Diese Daten hat die Versicherung jedoch unaufgefordert zu löschen.

Die Krankenzusatzversicherung muss nicht jede Person aufnehmen. Sie hat das Recht, den Gesundheitszustand des Antragstellers zu prüfen und Gesundheitsvorbehalte zu machen oder den Antrag ganz abzulehnen. Indem der Antragsteller das Antragsformular ausfüllt und einschickt, willigt er ein, dass die Versicherung diese Daten zur Prüfung seines Antrags bearbeiten darf. Auf dem Fragebogen hat er neben den Personalien in der Regel auch Angaben zur Gesundheit zu machen. Um diese Angaben überprüfen zu können, fordern die Versicherer auf dem Formular oftmals dazu auf, die behandelnden Ärzte von ihrer Geheimhaltungspflicht zu entbinden.

Lehnt die Versicherung nach Prüfung der Daten den Antrag ab oder bringt sie einen Vorbehalt an, kommt der gewünschte Vertrag nicht zustande. In diesen Fällen liegen die Daten trotzdem bei der Zusatzversicherung. Der Antragssteller hat jedoch nur in die Datenbearbeitung im Rahmen der Antragsprüfung eingewilligt. Daher muss die Krankenzusatzversicherung die Daten löschen, auch ohne explizite Aufforderung des Antragsstellers. Den Gesundheitsangaben ist bei der Bearbeitung besondere Beachtung zu schenken, da es sich um besonders schützenswerte Daten handelt.

Wir haben die Versicherer, welche die Daten der betroffenen Personen auch nach deren Aufforderung nicht gelöscht haben, zur Löschung angehalten. Die Löschungspflicht steht jedoch in einem gewissen Spannungsverhältnis zu den Interessen der Versicherung. Die Krankenzusatzversicherung möchte festhalten, wer einen Antrag bei ihr gestellt hat und aus welchem Grund sie diesen abgelehnt hat, damit sie bei einem erneuten Antrag der Person nicht nochmals dieselben Abklärungen treffen muss. Wir erachten das Interesse der Versicherung, die Personalien des Antragstellers sowie eine Kurzbegründung der Ablehnung in ihrem System für eine gewisse Zeit zu speichern, als berechtigt. Unverhältnismässig wäre es jedoch, würden

sämtliche Antragsformulare mit den medizinischen Angaben sowie weiteren eingeholten medizinischen Informationen aufbewahrt.

1.6.4 Vollmachten im Versicherungsbereich

Wie wir im Berichtsjahr festgestellt haben, herrscht im Versicherungsbereich Unklarheit bezüglich Vollmachten, insbesondere wenn diese Gesundheitsdaten betreffen. Wir werden regelmässig von versicherten Personen oder Antragsstellern gefragt, ob die ihnen vorgelegte Vollmacht nicht zu weit gehe. Wünschenswert wäre es, wenn die Versicherungen eine einheitliche, datenschutzkonforme Praxis in diesem Bereich einführten.

Eine Vollmacht ist dort notwendig, wo die von der Versicherung gewünschte Datenbeschaffung nicht gesetzlich geregelt ist. Als Konsequenz bedeutet dies, dass der von der Versicherung angefragte Arzt oder Arbeitgeber nur bei Vorliegen einer Vollmacht Auskunft über die Gesundheit der betroffenen Person erteilen darf. Viele Personen sind verunsichert, wenn sie beim Wechsel von einem Versicherer zum andern eine Vollmacht auszufüllen haben, und sie dies beim vorherigen nicht mussten. Die Versicherungen haben sehr unterschiedliche Praxen, wann sie eine Vollmacht einholen und wann nicht.

Die Versicherungen müssen für jedes neu eingetretene versicherte Ereignis eine neue Ermächtigung einholen. Denn eine Vollmacht kann sich nicht auch auf sämtliche künftige Ereignisse beziehen. Sie muss den Zweck nennen – z.B. den Schadensfall vom xx.xx.2015 – und die Datenbearbeitung auf die dafür notwendigen Daten beschränken.

Versicherungen verwenden in der Regel eigene Standardvollmachten, die sie allen Versicherten bei Vertragsschluss oder bei Eintritt des versicherten Ereignisses aushändigen. Da ein und dieselbe Vollmacht regelmässig für verschiedene Ereignisse eingesetzt wird, nennt sie oftmals sehr viele Stellen (behandelnder Arzt, Spital, Arbeitgeber, andere Versicherungen etc.), bei denen Informationen eingeholt werden können. Dies heisst aber nicht, dass die Versicherung bei allen genannten Stellen auch tatsächlich Informationen einholen darf. Denn von der Einwilligung der betroffenen Person sind nur die für den konkreten Fall notwendigen Datenbearbeitungen gedeckt. Umgekehrt hat auch die angefragte Stelle trotz vorliegender Vollmacht zu prüfen, ob die gewünschten Daten überhaupt notwendig sind für den angestrebten Zweck und ob keine überwiegenden privaten Interessen der betroffenen Person einer Datenbekanntgabe entgegenstehen.

Die Praxis hat gezeigt, dass die Versicherungen in der Regel eine Modifikation der Vollmacht durch den Versicherten nicht akzeptieren, sondern vielmehr umgehend

eine Leistungskürzung für den Fall der Verletzung der Mitwirkungspflicht androhen. Es besteht faktisch ein Zwang zur Unterzeichnung der Vollmacht.

Trotz den sehr weit gehenden Entscheidungskompetenzen der Versicherungen über die benötigten Daten haben sie die Prinzipien des Datenschutzes zu beachten. Um der Unsicherheit der betroffenen Personen entgegenzuwirken, wäre es wünschenswert, wenn sich die Versicherer des jeweiligen Versicherungszweiges auf eine einheitliche Praxis zu den Vollmachten einigen könnten. Den Personen, die wissen wollen, welche Gesundheitsdaten schliesslich über sie beschafft worden sind, empfehlen wir, bei der betreffenden Stelle ein Auskunftsbegehren zu stellen. Die Vollmacht kann zudem grundsätzlich jederzeit widerrufen werden.

1.6.5 Datenbekanntgabe durch die Krankenversicherer im Rahmen der Prämienverbilligung

Die Bekanntgabe des vollständigen Versichertenbestands durch die Krankenversicherer an die Kantone für die Durchführung der Prämienverbilligung ist heikel. Die Verhältnismässigkeit der Datenbekanntgabe muss ernsthaft in Zweifel gezogen werden.

Im Rahmen der Prämienverbilligung sollen die obligatorischen Krankenversicherer den zuständigen kantonalen Durchführungsorganen den vollständigen Versichertenbestand übermitteln können, wenn eine kantonale rechtliche Grundlage für die Datenbekanntgabe besteht. Entsprechend wurden die massgeblichen gesetzlichen Bestimmungen auf Bundesebene angepasst.

Wir haben uns von Anfang an gegen dieses Vorhaben gestellt, da wir in Zweifel ziehen, dass den Kantonen eine Regelungskompetenz für Datenbearbeitungen von Bundesorganen zukommen soll. Auch sind wir überzeugt, dass es mit der Bekanntgabe des vollständigen Versichertenbestands zu einer Verletzung des Grundsatzes der Verhältnismässigkeit kommt. Eine sehr grosse Zahl der von einer solchen Datenbekanntgabe betroffenen Personen hat keinen Anspruch auf eine Prämienverbilligung oder will diesen, auch wenn er gegeben ist, nicht geltend machen. Zudem sehen auch heute noch die meisten Kantone ein explizites Antragsverfahren für Prämienverbilligungen vor. Die kantonalen Durchführungsstellen kommen über dieses Verfahren ohne weiteres zu den notwendigen Angaben der versicherten Person.

Das Argument, dass die Übermittlung des vollständigen Versichertenbestandes den kantonalen Durchführungsstellen das Verfahren vereinfacht, vermag die Verletzung des Grundsatzes der Verhältnismässigkeit nicht zu rechtfertigen. Dies ist auch dann der Fall, wenn die betroffene Versicherung sich von der kantonalen Durchführungsstelle schriftlich bestätigen lässt, dass die Versichertendaten nur für den Zweck der Prämienverbilligung verwendet werden.

1.7 Arbeitsbereich

1.7.1 Videoüberwachung in Restaurants und Take-aways

Wir haben in diesem Jahr Sachverhaltsabklärungen zum Einsatz von Videoüberwachungsanlagen in Restaurants und Take-away-Betrieben vorgenommen. Es ist uns ein Anliegen, in diesem Bereich weiterhin auf die datenschutzrechtliche Problematik aufmerksam zu machen.

Wir wurden wiederholt von betroffenen Personen oder deren Vertretern darauf aufmerksam gemacht, dass in Gastgewerbebetrieben Videoüberwachungssysteme installiert seien, die die Mitarbeitende konstant überwachten. Es wurde uns weiter mitgeteilt, dass teilweise auch Gespräche mitgehört und aufgezeichnet würden. Aufgrund dieser Angaben haben wir uns entschlossen, bei den entsprechenden Betrieben eine Sachverhaltsabklärung durchzuführen. Auf unsere Ankündigung mit Fragekatalog hin, wurde uns mitgeteilt, dass die Kameras inzwischen abmontiert worden seien. Unsere Kontrolle bestätigte dies. Da deshalb keine Datenbearbeitung mehr durchgeführt wurde, haben wir die Kontrolle abgeschlossen.

Auf eine weitere Meldung hin haben wir eine Sachverhaltskontrolle bei einem Unternehmen im Take-away-Bereich durchgeführt. Dabei haben wir sowohl bei der Firma als auch bei den einzelnen Agenturpartnern Abklärungen betreffend Art und Umfang von allfälligen Videoüberwachungen vorgenommen. Auch hier wurden im Verlauf der Untersuchung die Kameras abmontiert.

Diese Fälle haben uns gezeigt, dass bei der Videoüberwachung im Arbeitsbereich grosser Bedarf an Sensibilisierung und Information besteht. Wir werden deshalb einerseits unsere einschlägigen Erläuterungen präzisieren, und andererseits haben wir Kontakt mit dem Eidgenössischen Arbeitsinspektorat aufgenommen, um allfällige Sensibilisierungsprojekte in diesem Bereich zu koordinieren. Dies vor dem Hintergrund, dass es sich bei Videoaufnahmen, die zu einer systematischen Verhaltensüberwachung führen können, um eine unrechtmässige Überwachung gemäss Arbeitsverordnung handelt. Die Ahndung von Verstössen gegen diese Verordnung liegt in der Zuständigkeit der kantonalen Arbeitsinspektorate, weshalb wir die betroffenen Personen jeweils auch an diese Behörden verweisen.

1.7.2 Gesundheitsfragebogen bei Bewerbungsverfahren

Unter welchen Voraussetzungen dürfen Arbeitgeber Stellenbewerber zum Ausfüllen eines Gesundheitsfragebogens auffordern? Mit dieser Frage haben wir uns im Berichtsjahr näher beschäftigt und entsprechende Antworten erarbeitet.

Personendaten über Mitarbeitende dürfen nur beschafft, aufbewahrt oder anderweitig bearbeitet werden, sofern sie die Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrages erforderlich sind. Für die Abklärung, ob eine Person für eine bestimmte Arbeitsstelle geeignet ist, darf der Arbeitgeber auch Gesundheitsdaten bearbeiten. Jedoch muss die Bearbeitung verhältnismässig sein, das heisst es dürfen nur so viele Daten erhoben werden, wie für die Zweckerreichung notwendig sind. Die erhobenen Daten müssen zudem unter objektiven Gesichtspunkten zur Eignungsabklärung beitragen, das heisst es muss immer ein Arbeitsplatzbezug bestehen. Demnach muss der Arbeitgeber abklären, ob ein Gesundheitsfragebogen für die zu besetzende Stelle notwendig ist.

Unserer Ansicht nach dürfen solche Fragebogen nicht flächendeckend für sämtliche Funktionen obligatorisch sein. Vielmehr erachten wir eine Abklärung nur für Positionen notwendig, die an den Bewerbenden spezielle Anforderungen stellen, wie zum Beispiel einen erhöhten Sicherheitsbedarf oder besondere körperliche Belastungen. Sofern eine Abklärung notwendig sein sollte, darf sich ein Arbeitgeber jedoch nicht selbst über den Gesundheitszustand des Bewerbers erkundigen. Er kann diese Aufgabe aber an den zuständigen ärztlichen Dienst oder einen Vertrauensarzt delegieren. Diese dürfen nur diejenigen Gesundheitsdaten bearbeiten, die notwendig sind für die Eignungsbeurteilung der Bewerberinnen und Bewerber bei der Anstellung. Sie teilen dem Arbeitgeber dann mit, ob der Bewerbende für die zu besetzende Stelle geeignet ist oder nicht, dürfen jedoch keine Diagnosen bekannt geben.

Zusammenfassend kann gesagt werden, dass es bezüglich der Zulässigkeit eines solchen Fragebogens auf die Stelle bzw. Funktion ankommt. Für den Fall dass ein Bewerber einen Fragebogen ausfüllen muss, hat er seine Krankheiten (z.B. Diabetes) wohl anzugeben, jedoch darf der Arzt dem Arbeitgeber keine Diagnose mitteilen. Er darf nur über eine ungenügende Eignung für die Stelle informieren, zum Beispiel wenn die Krankheit direkt und aktuell die Arbeitsfähigkeit beeinträchtigt oder die Arbeitserfüllung verunmöglicht.

1.7.3 Entscheid des Bundesverwaltungsgerichts in Sachen Whistleblowing-Stelle der Eidgenössischen Finanzkontrolle

Das Bundesverwaltungsgericht ist in seinem Entscheid bezüglich der Whistleblowing-Meldestelle der Eidgenössischen Finanzkontrolle (EFK) unseren Anträgen gefolgt und hat unsere Beschwerde im Zusammenhang mit der Sachverhaltsabklärung bei der EFK gutgeheissen.

Wie im letzten Tätigkeitsbericht erläutert, haben wir bei der EFK eine Sachverhaltsabklärung durchgeführt und gestützt auf diese eine Empfehlung erlassen, wonach

die EFK ihre Datensammlung bei uns anzumelden und ein Bearbeitungsreglement zu erstellen hat (vgl. unseren 21. Tätigkeitsbericht 2013/2014, Ziff. 1.7.2). Die EFK wollte dieser Empfehlung nicht folgen, weshalb wir den Fall vor das Bundesverwaltungsgericht (BVGer) weiterzogen. Dieses ist unseren Anträgen in seinem Entscheid vom 16. Dezember 2014 vollumfänglich gefolgt (A-788/2014). Das BVGer geht darin zuerst auf die Definition von Personendaten ein und kommt zum Schluss, dass die EFK in diesem Bereich solche bearbeitet. Danach geht das Gericht auf die Ausführungen zur Datensammlung gemäss der Botschaft zum Datenschutzgesetz (DSG) ein und vertritt die Ansicht, dass das weite Verständnis der Legaldefinition, wonach jeder Bestand von elektronisch gespeicherten Textdokumenten regelmässig eine Datensammlung darstellt, zu Recht von der Literatur kritisiert werde.

Das Bundesverwaltungsgericht ist jedoch der Auffassung, dass die Kategorisierung der Daten durchaus möglich sei, da es letztlich darum gehe, Meldungen die gestützt auf Artikel 22a Bundespersonalgesetz (BPG) ergehen, zu erfassen. Daran ändere nichts, dass es der EFK nicht darum gehe, eine Datenbearbeitung als solche zu erstellen, sondern lediglich eine interne Ablage. Betreffend Erschliessbarkeit führt es aus, dass Personennamen und weitere Angaben durch die EFK erfasst würden (solange die Hinweise nicht anonym erfolgt sind). Somit würden sich mit Hilfe der Suchfunktion innerhalb der Dokumente Personendaten auffinden lassen, ohne dass ein besonderes Fachwissen erforderlich wäre. Aus diesen Gründen stützt das Gericht unsere Feststellung, dass die Verzeichnisse der Whistleblowing-Meldestelle Datensammlungen darstellen.

Gemäss BVGer ist es nicht ausgeschlossen, dass in den beschriebenen, hier betroffenen Datensammlungen auch besonders schützenswerte Personendaten enthalten seien, namentlich über die Gesundheit, administrative oder strafrechtliche Massnahmen oder aber auch betreffend Ansichten und Tätigkeiten. Die EFK müsse demnach ein die Anforderungen von Artikel 21, Absatz 2 der Verordnung zum Datenschutzgesetz erfüllendes Bearbeitungsreglement erstellen. Mit Blick auf das Verhältnismässigkeitsprinzip sei die Erstellung des Reglements auch angemessen, da keine Ausführungsverordnung verlangt würde. Die Pflicht zur Erstellung sei deshalb auch vom Aufwand her vertretbar und stelle keine einschneidende Massnahme dar.

Das BVGer hat zusammenfassend unsere Anträge als begründet angesehen und die Beschwerde gutgeheissen. Die EFK muss uns demnach ihre beiden Datensammlungen innerhalb von zwei Monaten nach Rechtskraft dieses Urteils anmelden und wird angewiesen, ein Bearbeitungsreglement für die Datenbearbeitung in diesen beiden Beständen zu erstellen. Die EFK will das Urteil allerdings nicht akzeptieren und hat es daher an das Bundesgericht weitergezogen.

1.7.4 Referenzauskünfte im Bewerbungsprozess

Viele Anrufe an unseren telefonischen Beratungsdienst zum Thema Referenzauskünfte im Bewerbungsprozess haben gezeigt, dass teilweise Unwissen darüber herrscht, welche Rechte der Bewerber diesbezüglich hat und wie er sich gegen unerlaubt erteilte oder nicht wahrheitsgemässe Referenzen wehren kann.

Vermehrt haben wir im Berichtsjahr Anfragen zum Einholen von Referenzauskünften bei ehemaligen Arbeitgebern erhalten. Wir haben den betroffenen Bewerbern mitgeteilt, dass in solchen Fällen die Grundprinzipien des Datenschutzgesetzes (DSG) einzuhalten sind. Sowohl das Einholen wie auch das Erteilen einer Referenz haben rechtmässig sowie nach Treu und Glauben zu erfolgen und müssen verhältnismässig sein, d.h. es dürfen nur diejenigen Informationen über den Bewerber weitergegeben bzw. eingeholt werden, die für das zukünftige Arbeitsverhältnis relevant oder zur Durchführung des Arbeitsvertrages erforderlich sind.

Beim Einholen oder Erteilen einer Referenz werden wesentliche Züge der Persönlichkeit des Bewerbers beurteilt. Gemäss DSG handelt es sich hierbei um Persönlichkeitsprofile. Damit solche Daten überhaupt bearbeitet werden dürfen, ist die vorgängige und ausdrückliche Einwilligung erforderlich. Diese Einwilligung kann somit nicht einfach angenommen werden, wenn der Arbeitnehmer beispielsweise die früheren Arbeitgeber in seinem Lebenslauf auflistet. Befinden sich in den Bewerbungsunterlagen jedoch unter dem Titel «Referenzen» Angaben zu einem ehemaligen Arbeitgeber oder einem ehemaligen Vorgesetzen, darf dies als Einwilligung bzw. Zustimmung zum Einholen von Referenzen gewertet werden.

Der ehemalige Arbeitgeber der um Referenz gebeten wird, muss sich – bevor er Auskunft gibt – vergewissern, dass der Bewerber die Zustimmung dazu erteilt hat. Dies muss nicht zwingend durch eine direkte Nachfrage beim Bewerber selbst erfolgen, sondern kann auch dadurch bestätigt werden, dass der ehemalige Arbeitgeber Einsicht in die vom Bewerber eingereichte Referenzliste erhält. Der Bewerber hat ein Recht darauf, vom ehemaligen Arbeitgeber, den er als Referenzperson angegeben hat, zu erfahren, ob und an wen Auskunft erteilt wurde und was ihr Inhalt war.

Erteilt ein ehemaliger Arbeitgeber Referenz, ohne dass der Bewerber eingewilligt hat verletzt er damit die Persönlichkeit des Bewerbers widerrechtlich. Der betroffene Bewerber kann diese Verletzung bzw. die ungerechtfertigte Bearbeitung seiner Personendaten gemäss Artikel 15 DSG einklagen. Der betroffene Bewerber hat zudem die Möglichkeit gemäss Artikel 35 DSG strafrechtlich gegen den ehemaligen Arbeitgeber vorzugehen, wenn dieser ohne Einwilligung des Bewerbers geheime, besonders schützenswerte Personendaten oder Persönlichkeitsprofile bekannt gegeben hat.

Grundsätzlich dient die Referenz dazu, den durch das Arbeitszeugnis vermittelten Eindruck zu vertiefen. Es gilt deshalb auch hier wie beim Zeugnis der Grundsatz, dass eine Referenz sachlich, wahrheitsgetreu und zugleich wohlwollend sein muss. Eine Referenz darf genauso wie ein Zeugnis das wirtschaftliche Fortkommen des ehemaligen Arbeitnehmers nicht behindern und auch nicht gegen die Fürsorgepflicht des Arbeitgebers, die Persönlichkeit des Arbeitnehmers zu schützen, verstossen. Diese Fürsorgepflicht gilt nicht nur während des Arbeitsverhältnisses sondern begrenzt auch über die Anstellungszeit hinaus. Erteilt der ehemalige Arbeitgeber eine Referenz, die zwar bewilligt, deren Inhalt aber unwahr ist und dazu geführt hat, dass der Bewerber die Stelle aufgrund genau dieser Referenz nicht erhalten hat, hat der ehemalige Arbeitgeber seine arbeitsrechtliche Fürsorgepflicht verletzt. In diesem Fall kann der betroffene Bewerber nicht nur die Verletzung seiner Persönlichkeit, sondern auch allfälligen Schaden und immaterielle Unbill geltend machen.

Konkret kann der betroffene Bewerber die unwahre und nachteilige Referenzauskunft, die seine Persönlichkeit verletzt hat, mittels Zivilklage gerichtlich verbieten lassen. Ist ihm ein konkreter Schaden durch die Falschaussage seines ehemaligen Arbeitgebers entstanden, hat er namentlich eine Stelle aufgrund der unwahren und nachteiligen Referenz nicht erhalten, kann er zudem Schadenersatz und Genugtuung einfordern. Dies bedingt aber einen direkten Zusammenhang zwischen der unwahren Referenz und der Entscheidung des potentiellen neuen Arbeitgebers. Dieser Nachweis dürfte jedoch in der Realität nicht einfach zu erbringen sein. Betroffenen Bewerbern wird deshalb empfohlen, sich rechtlich beraten zu lassen, bevor sie den Rechtsweg gegen einen ehemaligen Arbeitgeber beschreiten.

1.7.5 Datenübermittlung im Bereich der flankierenden Massnahmen

Im Bereich der flankierenden Massnahmen und des Entsendegesetzes haben wir die datenschutzrechtlichen Problemfelder analysiert. Im Fokus unserer Abklärungen stand dabei die Übermittlung von Mitarbeiterdaten durch Subunternehmen.

Wir wurden in diesem Jahr wiederholt von Firmen, die als Subunternehmen auf grossen Baustellen arbeiten, angefragt, wie und ob eine Bekanntgabe von Daten über ihre Mitarbeitenden an die Generalunternehmen rechtmässig sei. Aufgrund dieser Anfragen haben wir uns vertiefter mit den Datenübermittlungen, die im Rahmen von Kontrollen gemäss des Entsendegesetzes vorgesehen sind, auseinandergesetzt. Dabei haben wir uns auch mit dem Staatssekretariat für Wirtschaft getroffen, um die einzelnen Kontrollprozesse in diesem Bereich besser zu verstehen.

Aufgrund unserer Prüfungen sind wir zum Schluss gekommen, dass Personendaten der Mitarbeitenden der Subunternehmen dann übermittelt werden dürfen, wenn es sich um einen Fall der Solidarhaftung oder um eine Kontrolle im Rahmen des Entsendegesetzes handelt. Das Prinzip der Verhältnismässigkeit muss dabei jedoch immer beachtet werden, das heisst es dürfen nur diejenigen Daten übermittelt werden, die für den geplanten Zweck notwendig sind.

1.8 Handel und Wirtschaft

1.8.1 Datenschutz im Smart Grid

Im Rahmen der Vorbereitung zur flächendeckenden Einführung von Smart Metering haben wir das Bundesamt für Energie beratend unterstützt.

Nachdem wir im letzten Berichtsjahr die Arbeitsgruppe des Bundesamtes für Energie (BFE) in Sachen Smart Metering (Digitale Stromzähler) und Datenschutz beratend begleitet haben, ist die Studie der Arbeitsgruppe auf der Webseite des BFE veröffentlicht worden (www.bfe.admin.ch/smartgrids). Gemäss der Studie wird im Bereich des Betriebs des Smart Grids (intelligentes Stromnetz) eine einheitliche Regelung auf Bundesebene bzw. die Unterstellung unter das eidgenössische Datenschutzgesetz als sinnvoll erachtet. Daher wurden wir vom BFE gebeten, die Abklärung einer möglichen schweizweiten Regelung der Datenbearbeitungen beim Smart Metering zu unterstützen.

1.8.2 Kundenkarten im Detailhandel

Die umfassenden Nachkontrollen im Bereich der Kundenkarten von Migros und Coop wurden dieses Jahr fortgesetzt. Unsere entsprechenden datenschutzrechtlichen Beurteilungen haben wir in Berichten festgehalten.

Letztes Jahr haben wir Nachkontrollen zum Thema Kundenkarten bei den Grossverteilern Migros und Coop durchgeführt (vgl. 21. Tätigkeitsbericht 2013/2014, Ziff. 1.8.2). Die Nachkontrolle bei Migros hat gezeigt, dass sich das Unternehmen der datenschutzrechtlichen Risiken bewusst ist und sich bemüht, die Gefahren durch geeignete Massnahmen zu minimieren. Im Bericht zeigt sich deshalb ein überwiegend positives Gesamtbild bei der Beurteilung der Datenbearbeitungen. Wir haben jedoch auch festgestellt, dass noch verschiedene Verbesserungen im Bereich der Information und Transparenz erforderlich sind und haben entsprechende Vorschläge formuliert.

Zudem haben wir in einer formellen Empfehlung festgehalten, dass Migros den Kunden bei Auskunftsgesuchen mitteilen muss, welchen Segmenten sie aufgrund der Warenkorb-Analysen zugeordnet werden. Diese Zuordnung stellt eine wesentliche Komponente der Datenbearbeitung dar. Und nur wenn einer betroffenen Person mitgeteilt wird, wie sie aufgrund der gesammelten Daten vom Unternehmen beurteilt wird, kann sie sich ein Bild über die Analysekriterien machen, deren Richtigkeit beurteilen und sich entsprechend verhalten. Migros hat alle unsere

Verbesserungsvorschläge und die Empfehlung akzeptiert und setzt sie entsprechend um bzw. hat sie bereits umgesetzt.

Der Bericht zur Nachkontrolle in Sachen Supercard, der Kundenkarte von Coop, wurde dem Unternehmen zur Stellungnahme geschickt. Die Abklärung konnte jedoch noch nicht abgeschlossen werden, da es noch einzelne Differenzen zu unseren Einschätzungen gibt.

1.8.3 Abklärungen im Bereich von Kredit- und Wirtschaftsauskunfteien

Im laufenden Berichtsjahr haben wir unsere zweite Sachverhaltsabklärung betreffend Datenschutzkonformität der auf der Internetplattform www.moneyhouse.ch angebotenen Dienstleistung mit dem Erlass einer Empfehlung abgeschlossen.

Im Berichtsjahr konnten wir den zweiten Teil unserer Abklärungen betreffend die von der itonex AG betriebene Plattform www.moneyhouse.ch abschliessen. Wir haben die umfangreiche Untersuchung mit einigen Empfehlungen in unserem Schlussbericht beendet. Seit Beginn unserer letzten Sachverhaltsabklärung, über die wir zuletzt im 21. Tätigkeitsbericht 2013/2014, Ziffer 18.5 berichtet haben, hat itonex AG das Dienstleistungsangebot von Moneyhouse stetig erweitert. Neben der Einsichtnahme in Informationen, die aus dem Handelsregister stammen, können bspw. auch Bonitäts-, Zahlweise- und Inkassoabonnemente abgeschlossen und zudem Informationen zu Baugesuchen und -bewilligungen oder Jobangebote abgerufen werden.

In unserem Schlussbericht sind wir deshalb zur Auffassung gelangt, dass die itonex AG Persönlichkeitsprofile bearbeitet. Die Bearbeitung von Persönlichkeitsprofilen birgt grosse Risiken für die betroffenen Personen, weshalb das Datenschutzgesetz (DSG) dafür besondere Bearbeitungsvorschriften enthält. Das von itonex AG angebotene Erteilen von Bonitätsauskünften ist in diesem Zusammenhang problematisch. Wer Bonitätsauskünfte erteilt, darf nach DSG nämlich nicht zugleich Persönlichkeitsprofile bearbeiten.

Andere Probleme aus datenschutzrechtlicher Sicht sahen wir speziell beim Bearbeiten von Daten von Kindern, beim Zugänglichmachen von Handelsregisterdaten über das Resultat von Suchmaschinen (vgl. Ziffer 1.1.3 des vorliegenden Berichts), bei der Sicherstellung der richtigen Verknüpfung von Personendaten und des Nicht-Wiederzugänglichmachens von gelöschten Inhalten. Die Itonex AG hat Anfangs 2015 unsere Empfehlungen teilweise angenommen (vgl. unsere Webseite www.derbeauftragte.ch, Datenschutz – Empfehlungen). Die Punkte, bei denen keine

Einigung erzielt wurde, werden wir nun dem Bundesverwaltungsgericht zur rechtlichen Klärung unterbreiten.

1.8.4 Umsetzung des Auskunfts- und Widerspruchsrechts durch Inhaber von Datensammlungen

Infolge zahlreicher Beschwerden von Privatpersonen, denen die Auskunft über ihre Daten verweigert worden war, haben wir die Inhaber der fraglichen Datensammlungen auf die Rechtslage aufmerksam gemacht und sie an ihre diesbezüglichen Pflichten erinnert. In einem Fall haben wir eine Empfehlung ausgesprochen.

Gemäss Bundesgesetz über den Datenschutz (DSG) kann jede Person vom Inhaber einer Datensammlung Auskunft darüber verlangen, ob Daten über sie bearbeitet werden. Der Inhaber muss dem Gesuchsteller alle ihn betreffenden Daten, einschliesslich der verfügbaren Angaben über deren Herkunft, mitteilen. Die Auskunft ist kostenlos und schriftlich innert dreissig Tagen zu erteilen. Das Auskunftsrecht kann nur aufgeschoben, eingeschränkt oder verweigert werden, wenn überwiegende Interessen es erfordern. In diesem Fall muss der Inhaber der Datensammlung seine Weigerung begründen. Überdies kann jedermann die Löschung seiner Daten verlangen, wenn keine Rechtfertigungsgründe für die Bearbeitung vorliegen.

Bei uns gehen regelmässig Klagen gegen Firmen ein, die Auskunfts- und Sperrgesuche nicht beantworten, obwohl sie gesetzlich dazu verpflichtet sind. Wir haben insbesondere mehrere Beschwerden gegen zwei Firmen, einen Verlag und einen Adressenhändler erhalten. Aufgrund unserer Aufsichtsbefugnisse und in Anbetracht der Anzahl Fälle haben wir diese Firmen angeschrieben, um sie an ihre datenschutzrechtlichen Verpflichtungen zu erinnern. In einem Fall haben wir eine formelle Empfehlung erlassen (vgl. www.derbeauftragte.ch, Datenschutz – Dokumentation – Empfehlungen).

1.8.5 Bekanntgabe von Mitgliederdaten an Versicherungen

Im Berichtsjahr haben wir erneut Anfragen von Privatpersonen erhalten, die sich erkundigten, inwiefern Verbände und Vereine die Daten ihrer Mitglieder zu Werbezwecken an Sponsoren weitergeben dürfen. Wir werden die Verbände sowie die beiden hauptsächlich betroffenen Sponsoren anschreiben, um sie auf die Rechtslage in Sachen Datenschutz aufmerksam zu machen.

Wir bekommen regelmässig Anfragen von Privatpersonen oder Sportvereinen betreffend die Bekanntgabe von Mitgliederdaten an Versicherungen zu Werbezwecken (vgl. unsere früheren Tätigkeitsberichte 2008/2009, Ziff. 1.8.5 und 17.

Tätigkeitsbericht 2009/2010, Ziff. 1.8.4). Es ist daran zu erinnern, dass ein Sportverband Dritten die Adressen seiner Mitglieder nur dann zu Marketingzwecken bekannt geben darf, wenn die Mitglieder eingewilligt haben. Es braucht dafür eine freie Einwilligung nach vorgängiger Information, die allerdings im Falle einfacher Adressdaten implizit erfolgen kann, beispielsweise wenn eine solche Nutzung der Daten in den Statuten vorgesehen ist und die Mitglieder sie nicht untersagt haben.

Wir stellen fest, dass es immer häufiger die Verbände sind, die den Sponsoren die Daten einzelner Mitglieder bekannt geben. Die Daten werden von den Vereinen meistens im Rahmen der Erteilung einer Lizenz oder anderer administrativer Verwendungszwecke weitergegeben. Der Verband kann zwar durchaus, beispielsweise in seiner Satzung, vorsehen, dass die Sponsoren die Daten seiner Mitglieder erhalten. Diese müssen aber die Möglichkeit haben, die Bekanntgabe zu untersagen. Die Daten anderer Athleten kann der Verband auf dieser Basis jedoch nicht bekannt geben. Wer Sponsoren Daten zugänglich macht, die dem Verband zu administrativen Zwecken mitgeteilt wurden (beispielsweise für die Erlangung einer Lizenz), verletzt den Grundsatz der Zweckbindung und handelt, soweit kein Rechtfertigungsgrund vorliegt, widerrechtlich.

Damit die Bekanntgabe der Daten an Sponsoren rechtmässig ist, muss sich der Verband im konkreten Fall vergewissern, dass er über die Einwilligung der betroffenen Personen, also der Vereinsmitglieder, verfügt. Ohne gültige Einwilligung ist jede Bekanntgabe an Sponsoren rechtswidrig. Auf jeden Fall müssen die Athleten die Möglichkeit haben, eine solche Verwendung ihrer Daten zu untersagen. Wir werden die Verbände kontaktieren, um sie auf ihre diesbezüglichen Pflichten hinzuweisen.

Die Sponsoren ihrerseits müssen (mindestens vertraglich) sicherstellen, dass die weitergegebenen Adressdaten zu Werbezwecken verwendet werden dürfen. Wie wir feststellten, betrafen die meisten im Berichtsjahr gemeldeten Fälle zwei Versicherungen. Wir werden diese anschreiben, um sie auf die Rechtslage aufmerksam zu machen und dafür zu sorgen, dass sie den datenschutzrechtlichen Anforderungen in den Sponsorenverträgen Rechnung tragen.

1.9 Finanzen

1.9.1 Abklärungen zur Bearbeitung von Kundendaten bei Postfinance

Postfinance hat Ende 2014 eine neue Version ihrer E-Banking-Plattform eingeführt. Die Kunden wurden aufgefordert, die neuen Teilnahmebestimmungen zu akzeptieren, da sie sonst ihren elektronischen Zugang verlören. Wir sind daran, die Datenbearbeitungen im Rahmen einer Sachverhaltsabklärung zu beurteilen.

Anfang 2014 hat uns Postfinance erstmals mitgeteilt, dass sie ihre E-Banking-Plattform überarbeiten will. In zwei Sitzungen und verschiedenen Dokumentationen wurden wir über das Projekt informiert. Postfinance bat uns um eine datenschutzrechtliche Beurteilung, da mit der revidierten Plattform verschiedene neue Datenbearbeitungen verbunden sind. Wir haben daraufhin dem Unternehmen eine ausführliche Stellungnahme geschickt, jedoch ohne einen Gegenbericht zu erhalten.

Ab August 2014 hat Postfinance ihre Kunden auf einer Zwischenseite der E-Banking-Plattform über die Einführung der neuen Version und die damit verbundenen Überarbeitungen informiert. Unter anderem wird eine Analysesoftware für die Budgetplanung und Darstellung der Geldflüsse für alle Kunden verpflichtend. Zudem soll eine Transaktionsanalyse dazu dienen, dass der Postfinance-Kunde auf seiner E-Banking-Seite spezielle Angebote von Drittfirmen angezeigt bekommt. Die Kunden wurden aufgefordert, die neuen Teilnahmebedingungen zu akzeptieren, damit sie zukünftig den elektronischen Kontenzugang weiterhin nutzen können. Aufgrund dieser Sachlage und zahlreicher Bürgermeldungen haben wir eine Sachverhaltsabklärung eröffnet, um die Datenbearbeitungen zu prüfen.

Die in diesem Zusammenhang unterbreiteten Änderungsvorschläge hat Postfinance angenommen und zugesichert, die Plattform entsprechend anzupassen. Dies hat insbesondere zur Folge, dass die Kunden besser informiert werden, Wahlmöglichkeiten erhalten und ohne ihre Einwilligung keine Auswertungen vorgenommen werden.

1.9.2 Konsultation im Hinblick auf den automatischen Austausch von Steuerinformationen

Im Zuge der Einführung des neuen internationalen OECD-Standards für den automatischen Informationsaustausch in Steuersachen wurden wir aufgefordert, in den vom Staatssekretariat für internationale Finanzfragen (SIF) eingesetzten Arbeitsgruppen mitzuwirken. Im Rahmen dieser Konsultationen ergriffen wir die Gelegenheit, das SIF auf zentrale Fragen in Bezug auf die Persönlichkeitsrechte aufmerksam zu machen.

Im Berichtsjahr fanden verschiedene Rundtischgespräche statt, um namentlich das Ausführungsgesetz zur Regelung des automatischen Austausches von Steuerinformationen vorzubereiten. Der Plan beinhaltet anspruchsvolle Zielvorgaben, da der Bund schon im Jahr 2017 Daten erheben und ab 2018 mit den Partnerstaaten austauschen möchte. Bis dahin sollten die Abkommen und das Ausführungsgesetz in Kraft sein, da andernfalls der Austausch mangels gesetzlicher Grundlage nicht aufgenommen werden kann.

Im Rahmen dieser Arbeiten steht die Frage des Datenschutzes im Zentrum der Debatte. Wir konnten uns vor und während der Ämterkonsultation zu mehreren wichtigen Punkten äussern. Dem Vorhaben wird namentlich angelastet, dass die AHV-Nummer als Steuer-Identifikationsnummer (SIN) verwendet werden soll, die auch im Ausland bearbeitet würde. Eine solche Verwendung der Sozialversicherungsnummer widerspricht ihrer ursprünglichen Zweckbindung und wäre darüber hinaus auch riskant. Wir haben das SIF daher auf die erheblichen Gefahren hingewiesen, die eine solche Massnahme für den Persönlichkeitsschutz mit sich brächte. Die Nutzung der AHV-Nummer ausserhalb der Sozialversicherungen würde eine unerlaubte Datenverknüpfung durch technische Mittel ermöglichen. Vorliegend denkt man spezifisch an die Verknüpfung von Datenbanken durch immer leistungsfähigere Algorithmen. Eine universelle Identifikationsnummer wie die AHV-Nummer macht die Verknüpfung noch einfacher. Sie ermöglicht namentlich die Erstellung von Persönlichkeitsprofilen, Identitätsdiebstahl usw. Wir haben uns daher für die Ausarbeitung einer sektorspezifischen Nummer, d. h. einer von der AHV-Nummer unabhängigen SIN ausgesprochen, gleich wie in mehreren europäischen Staaten, die bereits über eine spezifische Nummer für den Steuersektor verfügen.

Im Anschluss an unsere Bemerkungen sowie an die Kommentare des Bundesamtes für Sozialversicherungen (BSV) beschloss das Eidgenössische Finanzdepartement (EFD), auf die Verwendung der AHV-Nummer im Rahmen des automatischen Informationsaustausches im Steuerbereich zu verzichten. Ausserdem haben wir bezüglich der Einhaltung des Öffentlichkeitsprinzips und des Grundsatzes von Treu und Glauben im Rahmen des Verfahrens für den automatischen Informationsaustausch

eine kompromisslose Haltung eingenommen. Zudem verlangten wir die Berücksichtigung der grundlegenden Datenschutzprinzipien. Thematisiert wurden diese Grundsätze in der Stellungnahme des Beratenden Ausschusses zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten des Europarats vom 4. Juni 2014. Das Dokument wird auch von der Arbeitsgruppe «Artikel 29» in ihrem Schreiben vom 18. September 2014 an die OECD angeführt, in dem im Wesentlichen gefordert wird, dass bei der Anwendung des automatischen Austauschverfahrens die Datenschutzgrundsätze beachtet und im Lichte des innerstaatlichen Rechts jedes Landes umgesetzt werden.

Die Achtung der Grundrechte des Einzelnen bildet das Fundament unseres Engagements in diesem Vorhaben. Wir setzen daher alles daran, dass die von einer Meldung betroffenen Personen in jedem Fall rechtzeitig angehört werden und ihre namentlich auf dem Eidgenössischen Datenschutzgesetz beruhenden Rechte geltend machen können, d.h. bevor ihnen ein Schaden entsteht, weil beispielsweise fehlerhafte Angaben ins Ausland übermittelt wurden.

1.9.3 Abschluss der Sachverhaltsabklärung zum Risikomanagement-System bei einem Finanzdienstleister

Das Verfahren zur Abklärung des Sachverhalts betreffend den Betrieb des Risikomanagement-Systems eines Finanzinstituts wurde im Berichtsjahr abgeschlossen. Sämtliche von uns ausgesprochenen Empfehlungen wurden angenommen.

Im Jahr 2012 hatten wir ein Verfahren eröffnet zur Feststellung des Sachverhalts im Zusammenhang mit dem Betrieb des Risikomanagement-Systems eines im internationalen Bereich tätigen Finanzinstituts. Am Ende der Sachverhaltsabklärung (vgl. unseren 20. Tätigkeitsbericht 2012/2013, Ziff. 1.8.7 und unseren 21. Tätigkeitsbericht 2013/2014, Ziff. 1.9.1) sind wir zu dem Schluss gelangt, dass die operative Umsetzung des genannten Systems den auf dem Bankenrecht beruhenden Verpflichtungen entspricht. Die Datenbearbeitung ist im vorliegenden Fall somit gerechtfertigt. Datenschutzrechtlich waren allerdings gewisse Unregelmässigkeiten festzustellen.

Diese betreffen insbesondere die fehlende Transparenz bei der Datenbearbeitung. Wir haben daher dem Finanzinstitut empfohlen, die Öffentlichkeit generell auf den Zweck und die Nutzung des Systems aufmerksam zu machen und die von einer Bearbeitung betroffenen Personen spezifisch zu informieren. Es muss zudem gewisse Änderungen am System vornehmen, um bei der Datenbearbeitung den Grundsatz der Verhältnismässigkeit in zeitlicher Hinsicht einzuhalten, d.h. für die Löschung der Daten nach einer gewissen Zeitspanne zu sorgen.

Unsere Empfehlungen wurden am 28. August 2014 angenommen. Der Schlussbericht befindet sich auf unserer Website (www.derbeauftragte.ch, Datenschutz – Handel und Wirtschaft – Finanzwesen).

1.9.4 Auslagerung von pseudonymisierten Bankkundendaten ins Ausland

Im Rahmen der Konsultation der eidgenössischen Finanzmarktaufsicht (FINMA) im Jahr 2013 zur Teilrevision des Rundschreibens «operationelle Risiken Banken» (2008/21) haben wir unsere Position bezüglich der Pseudonymisierung von Personendaten und die damit verbundenen Folgen im Bankwesen erläutert.

Im Verlauf des Berichtsjahrs hat die FINMA uns darauf hingewiesen, dass Diskrepanzen zwischen der Umsetzung ihres Rundschreibens 2008/7 «Outsourcing Banken» in der Praxis und der Position des EDÖB bestehen. Ein Grossteil der beaufsichtigten Finanzinstitute in der Schweiz sei der Meinung, dass keine Verpflichtung bestehe, ihre Kunden über vorgenommene Auslagerungen ihrer Personendaten in pseudonymisierter Form speziell zu informieren. Die Branche vertrete nämlich die Auffassung, dass diese Daten nicht dem Geltungsbereich des Datenschutzgesetzes (DSG) unterstehen.

Diese Position beruht auf einer divergierenden Auslegung des Begriffs der Bestimmbarkeit von Personen, deren Daten pseudonymisiert wurden. Das Datenschutzgesetz sieht nämlich vor, dass alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen, Personendaten sind. Die Vertreter der Finanzindustrie kommen zum Schluss, dass pseudonymisierte Daten keine Personendaten im Sinne des DSG seien, weil sie keine Rückschlüsse auf bestimmte bzw. bestimmbare Personen zuliessen. Beliebige Drittpersonen, die in den Besitz der Daten gelangen, verfügten nämlich nicht über die nötigen Informationen, um eine Reidentifikation durchzuführen. Bei dieser Argumentation werden die Daten aus Sicht des Empfängers der Pseudonyme qualifiziert, wobei davon ausgegangen wird, dass dieser nicht in der Lage ist, die erhaltenen Daten den betreffenden Personen zuzuordnen. Würde man dieser Auslegung folgen, könnte man das DSG schlicht und einfach durch technische Massnahmen aushebeln, was nicht mit dem Willen des Gesetzgebers vereinbar ist.

Um die technische Sachlage zu verstehen, ist eine klare Begriffsbestimmung vorzunehmen. Pseudonymisierte Personendaten sind Daten, bei denen mittels eines spezifischen Vorganges sämtliche Elemente, die eine Identifizierung ermöglichen, durch einen neutralen Identifikator (nämlich ein Pseudonym) ersetzt werden. Dieses Pseudonym wird parallel in einer separaten Korrespondenztabelle zusammen mit den Identifizierungselementen gespeichert und ermöglicht es den Berechtigten,

eine Verknüpfung mit der betroffenen Person herzustellen, die dadurch bestimmbar im Sinne des DSG wird. Diese Methode hat zur Folge, dass derart pseudonymisierte Daten gegenüber allen Personen, die keinen Zugang zur Korrespondenztabelle haben, als nicht identifizierbar gelten. Obschon durch den Pseudonymisierungsvorgang der direkte Bezug zu einer Person für jemanden, der keine Identifizierungsmöglichkeiten besitzt, beseitigt wird, bleibt die Bestimmbarkeit seitens des Inhabers der Korrespondenztabelle bestehen.

In diesem Fall kann eine Bank zum Beispiel ihre Korrespondenztabelle geschützt in der Schweiz aufbewahren und die pseudonymisierten Bankkundendaten ins Ausland auslagern. Es stellt sich demnach die Frage, aus wessen Gesichtspunkt die massgebende Qualifikation betreffend die Bestimmbarkeit der betroffenen Personen (der sogenannte Beurteilungshorizont) zu prüfen ist: exklusiv aus Sicht des Datenempfängers (A), exklusiv aus Sicht des Datenlieferanten (B) oder braucht es eine alternative Würdigung (C)? Das DSG ist je nach gewähltem Anknüpfungspunkt anwendbar oder nicht. Bei Variante A ist eine Reidentifikation kaum mehr möglich, weshalb die ausgelagerten Informationen aus Sicht des Datenempfängers nicht mehr als Personendaten qualifiziert werden können und das DSG somit nicht anwendbar ist. Bei Variante B kommt man zur gegenteiligen Schlussfolgerung. Bei Variante C geht man von einer alternativen Sichtweise aus. Das heisst, dass die Beurteilung entweder aus Sicht der auslagernden Bank oder des Datenempfängers erfolgen kann. Bei dieser Variante ist das DSG immer anwendbar.

Das DSG enthält selbst keinen ausdrücklichen Hinweis betreffend den zum Tragen kommenden Beurteilungshorizont. Der Gesetzgeber hat aber die rasante technologische Entwicklung im digitalen Bereich erkannt und bewusst ein technisch neutrales Gesetz geschaffen, das mit den Entwicklungen des modernen Zeitalters mithalten und auf alle Sachverhalte Anwendung finden kann, die Persönlichkeitsrechte gefährden. Darüber hinaus hat das Bundesgericht unsere Position im Logistep-Entscheid (BGE 136 II 508) bestätigt (vgl. unseren 18. Tätigkeitsbericht 2010/2011, Ziff. 1.3.5). Darin hat das Bundesgericht die Voraussetzungen festgesetzt, aus welchem Blickwinkel die Qualifikation der Bestimmbarkeit zu erfolgen hat, und wendet diesbezüglich die sogenannte alternative Betrachtungsweise an.

Aus dem zuvor Gesagten geht hervor, dass das Datenschutzgesetz bei Auslagerungen von Bankkundendaten ins Ausland zur Anwendung kommt, was gewisse Verpflichtungen für die auslagernden Banken begründet. Gemäss FINMA-RS 2008/7 «Outsourcing Banken» (Rz. 35) müssen die Kunden mit einem besonderen Schreiben detailliert über die Auslagerung informiert werden. Zudem muss den Kunden bei solch einer Konstellation die Möglichkeit gewährt werden, die strittige Klausel ohne Nachteile abzulehnen (Opt-out) oder das Vertragsverhältnis abzubrechen. Dies erachten wir heutzutage im Bereich des elektronischen Finanzdatenverkehrs,

wo ein latentes Risiko der Datenmanipulation und des unerlaubten Zugriffs besteht, als zwingend. Aus diesem risikobasierten Ansatz leitet sich weiterhin die Verantwortung der Finanzinstitute ab, die Erkennbarkeit dieser Art von Bearbeitungen gegenüber den betroffenen Personen zu garantieren, damit sie ihre informationellen Selbstbestimmungsrechte unvermindert geltend machen können.

Bezüglich des zu wählenden Informationsgefässes sieht das DSG keine Vorgaben vor. Eine ausführliche und präzise Information in den allgemeinen Geschäftsbedingungen (AGB) der Bank, auch betreffend die Risiken der Auslagerung, ist denkbar unter der Voraussetzung, dass der Kunde auch anderweitig informiert wird und keine Globalübernahme der AGB im Vertragswerk stattfindet. Wie oben erwähnt, muss für den Kunden diesbezüglich die Möglichkeit bestehen, ein Opt-out zu tätigen. Das heisst, dass die Bank dem Kunden eine angemessene Frist gewähren muss, innert welcher der Kunde die strittige AGB-Klausel verwerfen oder seinen Vertrag ohne Nachteile kündigen kann. Andernfalls scheitert die Einwilligung des Kunden am Tatbestandsmerkmal der Freiwilligkeit. Wird innert der angesetzten Frist kein Opt-out getätigt, kann eine stillschweigende Einwilligung des Kunden angenommen werden. Sind besonders schützenswerte Personendaten oder Persönlichkeitsprofile von der Auslagerung ins Ausland betroffen, muss zwingend eine ausdrückliche Einwilligung (Opt-in) eingeholt werden. Solange dies nicht erfolgt ist, bleibt die Auslagerungsklausel ungültig.

1.10 International

1.10.1 Internationale Zusammenarbeit

In einer globalisierten und vernetzten Welt gehört die internationale Zusammenarbeit weiterhin zu den unabdingbaren Aktivitäten der Datenschutzbehörden. Die vergangenen zwölf Monate waren geprägt durch die laufenden Reformen des Datenschutzrechts innerhalb der Europäischen Union und des Europarates. Die Verstärkung der internationalen Zusammenarbeit ist nicht nur ein Anliegen der europäischen Datenschutzbehörden, sondern auch der internationalen Konferenz der Datenschutzbeauftragten und der französischsprachigen Vereinigung der Datenschutzbehörden (AFAPDP).

Europarat

Die Modernisierung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen 108) hat in den Aktivitäten des Europarates weiterhin eine vorrangige und zentrale Bedeutung. Eine wichtige Etappe war die Annahme eines Entwurfs zur Abänderung des Übereinkommens durch das Ad-hoc-Komitee für Datenschutz (CAHDATA); darin werden die Vorschläge des Beratenden Ausschusses des Übereinkommens 108 (T-PD) in ihrer Gesamtheit aufgegriffen (s. unseren 20. Tätigkeitsbericht 2012/2013, Ziff. 1.9.1). Der Text soll an das Ministerkomitee zur endgültigen Verabschiedung weitergeleitet und dann den Parteien des Übereinkommens zur Annahme vorgelegt werden. Die Arbeiten könnten sich allerdings erheblich verzögern, da die Europäische Kommission zahlreiche Vorbehalte angemeldet hat. Russland hat, was allerdings erwartet wurde, seinerseits zwei Vorbehalte angebracht; der eine betraf die Bestimmungen über den grenzüberschreitenden Datenverkehr mit der Beibehaltung der EU-Regelung (Angemessenheitsentscheidung), der andere die Stimmrechte, die der Kommission anstelle der EU-Mitgliedstaaten übertragen werden sollen.

Die Haltung der Europäischen Kommission, die eine grosse Zahl von Vorbehalten mit der Begründung einbrachte, dass es noch keinen gemeinsamen Standpunkt innerhalb der EU gebe und dass diese die Prüfung ihres rechtlichen Rahmens für den Datenschutz noch nicht abgeschlossen habe, hat mehrere Delegationen vor den Kopf gestossen. Die Schweiz hat übrigens offiziell ihre Enttäuschung kundgetan. Als Folge dieser Vorbehalte wird das Ministerkomitee den Text wahrscheinlich nicht wie ursprünglich geplant im ersten Halbjahr 2015 verabschieden können. Dieser Aufschub hat auch interne Auswirkungen, denn er könnte die Revisionsarbeiten an der Schweizerischen Datenschutzgesetzgebung verzögern. Er setzt auch ein schlechtes Zeichen gegenüber Drittstaaten, die dem Übereinkommen 108 beitreten möchten. Mehrere dieser Staaten waren an den Arbeiten des CAHDATA beteiligt.

Das modernisierte Übereinkommen 108 stellt heute und künftig die Konvergenz mit den Texten der EU sicher, so dass die beiden Rechtssysteme komplementär bleiben. Eine Verzögerung der Annahme der revidierten Fassung birgt die Gefahr, dass die Politik zur Förderung des Übereinkommens in Frage gestellt und Drittstaaten von einem Beitritt abgehalten werden. Das würde das Datenschutzrecht nicht nur in Europa sondern weltweit schwächen. Der T-PD hat seinerseits die Überarbeitung der Empfehlung R(89)2 über den Schutz persönlicher Daten, die für Beschäftigungszwecke verwendet werden, abgeschlossen (s. 21. Tätigkeitsbericht 2013/2014, Ziff. 1.10.1); dieser Text sollte 2015 vom Ministerkomitee verabschiedet werden.

Der T-PD nahm Kenntnis von einem Sachverständigenbericht über die datenschutzrechtlichen Auswirkungen des zunehmenden zwischenstaatlichen und automatischen Austauschs von personenbezogenen Daten zu Verwaltungs- und Steuerzwecken sowie im Rahmen der Bekämpfung der Geldwäscherei, der Finanzierung des Terrorismus und der Korruption. Der Bericht wurde auf der Website des Europarats publiziert. Ausserdem verabschiedete er mit einstimmigem Beschluss ein Gutachten zu den Auswirkungen des automatischen zwischenstaatlichen Datenaustauschs zu Verwaltungs- und Steuerzwecken auf den Schutz personenbezogener Daten. Diese Stellungnahme ging an die OECD und an die für diese Problematik zuständigen nationalen Behörden. Das Gutachten, das veröffentlicht werden soll, fordert mit Nachdruck die Einhaltung der im Übereinkommen 108 begründeten Datenschutzvorschriften und des Rechts auf Achtung des Privatlebens gemäss Artikel 8 der Europäischen Menschenrechtskonvention.

Um die Achtung der Grundrechte im Rahmen der Einführung dieser Mechanismen zu gewährleisten, braucht es spezifische Garantien. Dabei geht es insbesondere darum, die Gefahr einer Verletzung der Privatsphäre und diskriminierender Massnahmen, die gegen die betroffenen Personen ergriffen werden könnten, möglichst gering zu halten. In diesem Zusammenhang sollten die zur Organisation dieses Austausches erstellten Übereinkommen und Verträge klar und eindeutig formuliert werden. Dies betrifft namentlich ihr Geltungsbereich, die verwendeten Begriffe, die konkreten Kategorien der betroffenen Personen, die Zweckbindung der Erhebung und Bearbeitung, die bearbeiteten und ausgetauschten Daten, oder die Bezeichnung der zur Beschaffung und Bearbeitung dieser Daten berechtigten nationalen Behörde. Ebenso betrifft es die Vorschriften für die Aufbewahrung der Daten durch die Empfängerbehörde, die Periodizität der Informationsübermittlungen und die praktischen Modalitäten des automatischen Austausches, die Vorschriften für die Weitergabe der Daten an andere nationale Behörden im Empfängerland oder in Drittländern sowie die Rechtsmittel der betroffenen Personen.

Der T-PD verabschiedete auch eine Stellungnahme zu einer Empfehlung der Parlamentarischen Versammlung des Europarates für eine Verbesserung des Schutzes

und der Sicherheit der Nutzer im Internet. Diese Stellungnahme unterstützt die Initiative der parlamentarischen Versammlung des Europarates. Sie weist darauf hin, dass die effektive Gewährleistung der Menschenrechte im Netz namentlich darin besteht, dass die universellen Prinzipien des Schutzes personenbezogener Daten gefördert und die Mitgliedstaaten auf ihre positive Verpflichtung hingewiesen werden, einen angemessenen Rechtsschutz in Bezug auf das Abfangen, die Überwachung, das Erstellen von Persönlichkeitsprofilen und die Archivierung der Nutzerdaten sicherzustellen.

Die Ausarbeitung eines Zusatzprotokolls zum Übereinkommen über die Cyberkriminalität für schwerwiegende Verletzungen der Grundrechte der Nutzer von Online-Diensten setzt nach Auffassung des T-PD die Einhaltung des durch Artikel 8 der Europäischen Menschenrechtskonvention (EMRK) geschützten Rechts auf Achtung des Privatlebens und des Übereinkommens 108 und seines Zusatzprotokolls voraus. In diesem Sinne erachtet es der T-PD als wünschenswert, dass sich Staaten, die das Übereinkommen über die Cyberkriminalität ratifizieren oder ihm beitreten, auch dem Übereinkommen 108 und seinem Zusatzprotokoll anschliessen.

Des Weiteren hat der T-PD erste Beratungen zum Datenschutz im Zeitalter von Big Data aufgenommen. Schliesslich wählte er den stellvertretenden eidgenössischen Beauftragten für eine dritte aufeinander folgende Amtszeit zu seinem Vorsitzenden.

Europäische Konferenz der Datenschutzbeauftragten

Die europäische Konferenz der Datenschutzbeauftragten wurde von der französischen Commission de l'informatique et des libertés (CNIL) und dem Europarat organisiert. Sie fand am 5. Juni 2014 in Strassburg statt. Im Vordergrund dieser Konferenz stand die Zusammenarbeit zwischen den Datenschutzbehörden, die in einer immer enger verflochtenen Welt eine hohe Priorität hat. Dieses Thema hat mit den tagtäglichen Aufgaben der Datenschutzbehörden und der Effektivität ihrer Tätigkeit zu tun. Dank der Zusammenarbeit zwischen den Behörden können Synergien genutzt und gemeinsame angemessene Antworten gefunden werden. So beurteilte die Konferenz verschiedene Zusammenarbeitsmodelle auf der Welt, in der Europäischen Union oder im Europarat. Dabei hatten wir die Gelegenheit, den gesetzlichen Rahmen der Zusammenarbeit aufgrund des Übereinkommens 108 zu erläutern.

Die Konferenz beschloss die Einsetzung einer Arbeitsgruppe, die Vorschläge zur Verbesserung und Verstärkung der Zusammenarbeit zwischen den Datenschutzbehörden der Unterzeichnerparteien des Übereinkommens 108 vorlegen soll. Sie verabschiedete auch eine Resolution zur Überarbeitung des Übereinkommens, in der sie dazu aufruft, den bisherigen Schutzumfang entsprechend dem Vorschlag des T-PD in dem am 29. November 2012 angenommenen Text zu bewahren und gegebenenfalls zu erweitern.

Internationale Konferenz der Datenschutzbeauftragten

Die 36. Internationale Konferenz der Datenschutzbeauftragten fand vom 13. bis 17. Oktober 2014 erstmals in Afrika, auf der Insel Mauritius statt. Vertreter von rund 80 nationalen und regionalen Datenschutzbehörden, und Vertreter von Unternehmen, Regierungen, internationalen Organisationen und der Zivilgesellschaft sowie Sachverständige aus akademischen Kreisen nahmen daran teil. Wie üblich bestand die Konferenz aus zwei Teilen, von denen der eine den bei der Konferenz akkreditierten Datenschutzbehörden vorbehalten war und der andere allen interessierten Parteien offen stand. Ziel war ein Meinungs- und Erfahrungsaustausch zwischen verschiedenen Datenschutzakteuren und die Verstärkung der Zusammenarbeit zwischen den Behörden und zwischen Behörden und Zivilgesellschaft.

An der geschlossenen Tagung führte die Konferenz eine Aussprache über das Internet der Dinge, das in Verbindung mit Big Data eine der grossen Herausforderungen bildet, der sich unsere Gesellschaften in den nächsten Jahren stellen müssen und die dringend eine öffentliche Debatte erfordert. Die Konferenz veröffentlichte daher eine Erklärung, in der sie an die Herausforderungen erinnert, die das Internet der Dinge für den Datenschutz und die Sicherheit stellt. Der Datenschutz beginnt mit der Datenerhebung. Es ist daher wesentlich, dass bei der Planung der Technologien, Systeme und Bearbeitungen von Anfang an den Datenschutzanforderungen Rechnung getragen wird (privacy by design, privacy by default).

Der frei zugängliche Teil der Konferenz bot die Gelegenheit zu Gesprächen und einem Austausch über die internationalen Initiativen in den Bereichen Zusammenarbeit, Überwachung, Gesundheit und elektronische Patientendossiers, über den rechtlichen Rahmen des Datenschutzes, namentlich innerhalb der EU mit der umstrittenen Frage der einzigen Anlaufstelle. Thematisiert wurden auch die Risikobewertungen in Sachen Datenschutz, die zwingenden Unternehmensvorschriften im Rahmen des grenzüberschreitenden Datenverkehrs und die Herausforderungen von Big Data für die Grundrechte und -freiheiten.

Die Beauftragten verabschiedeten ausserdem folgende Texte:

- Eine Resolution über die internationale Zusammenarbeit im Bereich Kontrolle und Ermittlungen. In dieser Resolution geht es darum, einen weltweiten nicht zwingenden Rahmen für die grenzüberschreitende Zusammenarbeit einzurichten und eine sichere und neutrale Plattform für den Informationsaustausch für die bei der Konferenz akkreditierten Behörden zu schaffen. Seit der Annahme der Erklärung von Montreux anlässlich der 27. Internationalen Konferenz erarbeiten die Datenschutzbeauftragten Lösungen zur Verstärkung ihrer Zusammenarbeit, um den grenzüberschreitenden Gesetzesvollzug zu verbessern.

- Eine Resolution über Big Data, mit der alle Akteure aufgefordert werden, die Datenschutzprinzipien zu beachten, insbesondere die Eingrenzung der Zweckbindung, den Grundsatz der Verhältnismässigkeit, das Prinzip der Öffentlichkeit der Bearbeitung und die Gewährleistung der Rechte der betroffenen Personen (Auskunftsrecht, Information, Recht auf Berichtigung oder Löschung der Daten).
- Eine Resolution über den Schutz der Privatsphäre im digitalen Zeitalter, in der der Exekutivausschuss der internationalen Konferenz beauftragt wird, an den multipartiten Gesprächen über den digitalen Schutz unter der Führung der Vereinten Nationen teilzunehmen. Diese Resolution fordert auch dazu auf, die grundlegenden Datenschutzprinzipien, wie sie namentlich im Übereinkommen 108 aufgeführt sind, auch bei Aktivitäten der elektronischen Überwachung einzuhalten.

Die 37. Internationale Konferenz der Datenschutzbeauftragten findet im Herbst 2015 in Amsterdam statt.

Französischsprachige Vereinigung der Datenschutzbehörden

Wegen der Ebola-Epidemie in Westafrika sah sich die französischsprachige Vereinigung der Datenschutzbehörden (AFAPDP) gezwungen, ihre 8. Konferenz, die in Ouagadougou (Burkina Faso) hätte stattfinden sollen, abzusagen. Sie hat ihre Generalversammlung deshalb in elektronischer Form abgehalten. Diese Versammlung bot die Gelegenheit, Bilanz über die Tätigkeiten der Vereinigung im vergangenen Jahr zu ziehen. Die französischsprachigen Datenschutzbehörden haben 2014 zwei praktische Hilfsmittel herausgegeben: das eine ist ein Leitfaden für die Konsolidierung von Zivilstandsregistern, der Wählerlisten und des Datenschutzes und wurde in Zusammenarbeit mit der Internationalen Organisation der Frankophonie verfasst. Das zweite Hilfsmittel besteht aus zwingenden Unternehmensvorschriften für die in französischsprachigen Ländern tätigen multinationalen Unternehmen; diese Regeln wurden 2013 angenommen (siehe 21. Tätigkeitsbericht 2013/2014, 1.10.1) und haben Anlass zu mehreren Massnahmen und namentlich einer Schulungsveranstaltung für Mitglieder der AFAPDP im Juli 2014 gegeben. Diese Hilfsmittel stehen öffentlichen Akteuren und Unternehmen zur Verfügung.

Bei dieser Generalversammlung verabschiedete die AFAPDP auch eine Resolution über die Betreuung der Unternehmen und ihrer technologischen Innovationsbemühungen. Angesichts der zunehmend verbreiteten Erhebung von immer grösseren Datenmengen erinnert die AFAPDP an die Rolle der Datenschutzbehörden, die beraten, sensibilisieren und die Einhaltung der Gesetzesbestimmungen kontrollieren müssen. Sie betont die Bereitschaft dieser Behörden, sich mit den Unternehmen auszutauschen und sie darüber zu beraten, wie sie sich datenschutzrechtskonform

verhalten können. Schliesslich verabschiedete die AFAPDP eine an den 15. Gipfel der Frankophonie in Dakar gerichtete Erklärung, in der sie die französischsprachigen Staaten und Regierungen auffordert, die Einsetzung unabhängiger Behörden und nationaler und internationaler Zusammenarbeitsnetzwerke im Bereich des Datenschutzes zu unterstützen und den internationalen Datenschutz-Vertragswerken wie dem Übereinkommen 108 beizutreten.

Die französischsprachigen Behörden werden ihre nächste Konferenz im Juni 2015 in Brüssel abhalten.

Arbeitsgruppe der OECD über die Informationssicherheit und den Schutz der Privatsphäre

Die Arbeitsgruppe über die Informationssicherheit und den Schutz der Privatsphäre der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) widmete sich auch in diesem Jahr der Revision der OECD-Richtlinien zur Informationssicherheit. Die Struktur der Richtlinie wird noch verbessert und auch verschiedene Themendefinitionen werden geklärt. Sensibilisierung, Transparenz und Definition der möglichen Risiken bleiben im Zentrum der Revisionsarbeiten. Bemerkenswert ist, dass nun Datenschutzkonzepte wie Privacy by Design oder Privacy by Default in diese Arbeiten einfliessen. Gleichzeitig wurde ein Bericht erarbeitet, der die Revision detailliert beleuchtet und erklärt.

Die Bedeutung der Risiken im Zusammenhang mit dem Internet der Dinge (Internet of Things, IoT) und die damit verbundenen Datenschutz- und Sicherheitsrisiken wurden erkannt. Bis Ende 2015 wird ein Bericht dazu erarbeitet, dessen Ziel es ist, nebst der Beschreibung der potenziellen Risiken auch Schutzmöglichkeiten aufzuzeigen und diese dem Benutzer transparent darzustellen. Die Bekämpfung solcher Risiken wird für die Entwicklung der sogenannten datengesteuerten Wirtschaft (data driven economy) ausschlaggebend sein.

Die Vertrauensbildung in der datengesteuerten Wirtschaft und die Rolle der Bearbeitung von Personendaten sind vom künftigen wirtschaftlichen Wachstum abhängig. Dabei wird der Schutz der Privatsphäre von zentraler Bedeutung sein und insbesondere die Rolle des Benutzers (Konsumenten), der den grössten Teil der online verfügbaren Personendaten übermittelt, zur Verfügung stellt bzw. generiert, ohne es zu realisieren. Es wird Bestrebungen geben, um insbesondere der fehlenden Transparenz entgegenzuwirken und den Datenschutz zu verstärken. In einem Dokument zeigt die OECD auf, mit welchen Problemen die Privatsphäre in diesem Umfeld konfrontiert ist und wie den Risiken konkret begegnet werden kann. Es werden Ansätze diskutiert, um die Rechte der Benutzer zu gewährleisten. Dazu müssen die Transparenz der Datenbearbeitungen verstärkt, die informationelle Asymmetrie

zugunsten der Konsumenten ausbalanciert und die aktuellen Datenschutzprinzipien bewahrt werden.

Die Revision der Richtlinie zum Schutz von kritischen Informationsstrukturen wurde auch an die Hand genommen. In diesem Zusammenhang wurde eine Studie zum Internet der Dinge (IoT) im industriellen Kontext präsentiert. Diese beschreibt die Risiken durch IoT in staatlichen Infrastrukturen (Wasser-, Energie-, Grundversorgung etc.). Diese Risiken sind nicht neu, erhalten aber durch die Verknüpfungsmöglichkeiten im Internet eine neue Dimension. Die Studie befasst sich nicht mit IoT-Anwendungen, sondern behandelt einzig die Risiken bei der Vernetzung der industriellen Infrastruktur über das Internet.

Die Bedeutung des richtigen Umgangs mit Datenschutzrisiken (Risk Management in Data Protection) wurde von der Arbeitsgruppe erkannt, und sie diskutierte, inwiefern sie bei Unternehmen und auch beim Gesetzgeber diesbezüglich Einfluss nehmen kann. Nebst der möglichen Integration von Risiko Management in der Gesetzgebung ist es notwendig, dass Unternehmen mit analogen oder gleichen Modellen Risiko Management in die sonstigen Kontrollprozesse der Unternehmung eingliedern. Auch die Datenschutzgruppe der EU-Kommission «Artikel 29» hat einige Dokumente zum Risiko Management im Datenschutz erarbeitet, insbesondere über die Rahmenbedingungen und Regulierung. Es besteht ein breiter Konsens darüber, dass nebst einheitlichen Prüfkriterien auch ein klarer Rechtsrahmen erforderlich ist. Allerdings wird die Umsetzung und Durchführung von Risikobewertungen (Risk Assessment) nicht ohne zusätzliche Arbeiten insbesondere im Bereich der Interoperabilität erfolgen können.

Arbeitsgruppe «Border, Travel & Law Enforcement»

Die «Border, Travel & Law Enforcement subgroup» (BTLE) ist eine Unterarbeitsgruppe, die von der Datenschutz-Arbeitsgruppe «Artikel 29» eingesetzt wurde. Die Untergruppe ist beauftragt, die gesetzgeberischen Entwicklungen in den Sektoren Polizei, Grenzverkehr und Strafjustiz zu begleiten, insbesondere soweit sie den Schengen-Besitzstand betreffen. In diesem Zusammenhang bereitet sie Expertisen und Stellungnahmen vor, die anschliessend «Artikel 29» vorgelegt werden. Wir haben an den verschiedenen Sitzungen im Berichtsjahr teilgenommen.

Die Unterarbeitsgruppe befasste sich insbesondere mit dem Gerichtsurteil der Europäischen Union zur Aufbewahrung von Personendaten, die für die Bekämpfung des organisierten Verbrechens und des Terrorismus verwendet werden. Sie beobachtet mit besonderer Aufmerksamkeit die Fortschritte des Projekts «intelligente Grenzen», nachdem die Kommission einen Verordnungsvorschlag angenommen hat, betreffend die Schaffung eines Einreise- und Ausreisesystems für die Registrierung der Ein- und Ausreisen der Staatsangehörigen von Drittländern beim Übertritt über

die Aussengrenzen der Mitgliedstaaten der Europäischen Union und eine Verordnung über die Einrichtung eines Programms für die Registrierung von Reisenden.

Die Unterarbeitsgruppe richtet ihr Augenmerk auf die Schaffung eines europäischen Rahmens für die Bekanntgabe von Fluggastdatensätzen (PNR-Daten) an Drittländer und für die Verwendung dieser Daten zu Strafverfolgungszwecken. Sie beobachtet auch die Überarbeitung des im Vertrag von Lissabon begründeten rechtlichen Datenschutzrahmens der Europäischen Union. Schliesslich hat die Unterarbeitsgruppe ein Gutachten zum Notwendigkeitsprinzip erstellt. Es soll die Begriffe der Notwendigkeit und der Verhältnismässigkeit bestimmen, die der Gesetzgeber und die verschiedenen zuständigen Behörden im Bereich der Grenzkontrolle berücksichtigen müssen.

Koordinationsgruppe für die Kontrolle des SIS II

Die Koordinationsgruppe für die Kontrolle des SIS II (SIS II SCG) hat im Jahr 2014 zwei Mal getagt. Im Anschluss an eine Erhebung betreffend die Ausübung des Auskunftsrechts in den verschiedenen Schengen-Staaten hat die Gruppe einen Bericht verabschiedet, der demnächst veröffentlicht werden soll. Aus diesem Bericht geht hervor, dass die Zusammenarbeit zwischen den Datenschutzbehörden verbessert werden muss und dass sich eine aktivere Zusammenarbeit mit den Nichtregierungsorganisationen und den übrigen Akteuren in diesem Bereich empfiehlt, um die betroffenen Personen noch besser für ihre Rechte zu sensibilisieren. In diesem Zusammenhang plant die Gruppe auch die Ausarbeitung eines Dokuments, das eine gemeinsame Vorgehensweise bei der Erstellung von Statistiken ermöglichen soll. Die Gruppe hat eine Anleitung zu den Rechten der betroffenen Personen aktualisiert, die in englischer Sprache veröffentlicht worden ist und demnächst in verschiedene europäische Sprachen übersetzt werden soll.

Die SIS II SCG führte auf unseren Wunsch Gespräche über die Praxis einzelner kantonaler Polizeibehörden, welche die Hotelmeldezettel systematisch mit den Ausschreibungen des SIS II vergleichen. Auch gab sie ein Gutachten zur Auslegung von Artikel 45 des Durchführungsübereinkommens heraus, der die Meldepflicht in den Beherbergungsstätten und die Bereitstellung der Meldezettel für die zuständigen Behörden regelt. Sie gelangte zum Schluss, dass eine automatische und systematische Überprüfung aller Ausschreibungen des SIS II anhand der Meldevordrucke nicht im Einklang mit dem Durchführungsübereinkommen steht. Die Gruppe hat auch einen Fragebogen betreffend den Zugang zum SIS II ausgearbeitet, der den zuständigen Behörden zugestellt wurde. Des Weiteren beschloss die Gruppe die Einrichtung eines neuen Internetauftritts.

Auf schweizerischer Ebene verläuft die Koordination der Tätigkeiten im Zusammenhang mit Schengen über eine Koordinationsgruppe, welcher der EDÖB und die

kantonalen Datenschutzbehörden angehören. Diese Gruppe kommt mindestens zwei Mal jährlich zusammen. Die vertretenen Behörden können sich so über die laufenden Entwicklungen und die Aktivitäten der SIS II SCG informieren, Kontrolltätigkeiten planen und Informationen austauschen.

Europäische Arbeitsgruppe für die Behandlung datenschutzrelevanter Fälle

Die 26. Tagung der Europäischen Arbeitsgruppe für die Behandlung datenschutzrelevanter Fälle («Case Handling Workshop») fand vom 6. bis 7. Oktober 2014 in Skopje statt. Die Arbeitsgruppe, die aus Vertretern von 29 nationalen Datenschutzbehörden besteht, ging zunächst auf die Problematik der übermässigen Erhebung von Personendaten und der Interessenabwägung zwischen dem Datenschutz und dem Recht auf Zugang zu Dokumenten der öffentlichen Verwaltung ein.

In einem zweiten Teil drehte sich die Diskussion um die Videoüberwachung und die Verwendung von biometrischen Daten, zwei Themen, die zunehmend an Bedeutung gewinnen. Das Urteil des Gerichtshofs der Europäischen Union vom 13. Mai 2014 zum Recht auf Vergessen wurde ausführlich erörtert. Schliesslich befasste sich die Gruppe mit den datenschutzrechtlichen Herausforderungen, die sich durch die zunehmende Nutzung von WLAN und auf Bluetooth basierenden Monitoringsystemen ergeben. Dabei wurde deutlich, dass die Öffentlichkeit unbedingt für die Gefahren dieser neuen Praktiken sensibilisiert und ihrer Eigenverantwortung bewusst gemacht werden muss.

Sämtliche behandelten Themen wurden anhand konkreter Fälle aus der Praxis der verschiedenen Datenschutzbehörden veranschaulicht. Die Datenschutzbehörde Mazedoniens wird demnächst ein Handbuch zu allen auf dieser Tagung erörterten Themen herausgeben.

Internationale Zusammenarbeit – Aufsichtskoordinationsgruppe Eurodac und VIS

Im Berichtsjahr nahmen wir an den Sitzungen der Koordinierungsgruppe für die Aufsicht über Eurodac teil. Die Koordinierungsgruppe Eurodac arbeitete einen Fragebogen zur revidierten und ab Juli 2015 anwendbaren Eurodac-Verordnung auf nationaler Ebene aus. Ziel ist es, zu erfahren, welche Umsetzungsmassnahmen auf nationaler Ebene getroffen wurden. Mit der neuen Verordnung werden auch Strafverfolgungsbehörden Zugriff erhalten. Damit auch die Schweizer Strafverfolgungsbehörden Zugriff auf Eurodac-Daten erhalten, muss die Schweiz zuerst Verhandlungen mit der EU führen.

Im Anschluss an die oben erwähnten Sitzungen der Koordinierungsgruppe Eurodac fanden die Sitzungen der Koordinierungsgruppe VIS statt, die für die Aufsicht

über das Visa-Informationssystem zuständig ist. Sie verabschiedete drei Fragebögen betreffend Zugriffe der Behörden allgemein, betreffend Zugriffe der Strafverfolgungsbehörden und in Bezug auf die Ausübung der Rechte der betroffenen Personen auf nationaler Ebene. Wir haben die drei Fragebögen dem Staatssekretariat für Migration (SEM; ehemals Bundesamt für Migration [BFM]) geschickt und dessen Antworten nach Brüssel weitergeleitet. Gleichzeitig nahmen wir an der Unterarbeitsgruppe teil, welche die rechtlichen Fragen analysiert, die sich in Zusammenhang mit externen Dienstleistungsanbietern ergeben, die vermehrt von Konsulaten beigezogen werden.

2. Öffentlichkeitsprinzip

2.1 Zugangsgesuche

Gemäss den uns mitgeteilten Zahlen sind im Jahr 2014 bei den Bundesbehörden insgesamt 575 Zugangsgesuche eingereicht worden (inkl. Bundesanwaltschaft und Parlamentarische Dienste 582, siehe dazu Ziffer 2.1.2 f.). Demnach wurden seit Inkrafttreten des Öffentlichkeitsgesetzes im Jahr 2006 noch nie so viele Zugangsgesuche bei der Bundesverwaltung eingereicht. In 297 Fällen gewährten die Behörden einen vollständigen, in 124 einen teilweisen Zugang. Bei 122 Gesuchen wurde die Einsichtnahme vollständig verweigert. 15 Zugangsgesuche wurden zurückgezogen, 17 Fälle meldeten die Behörden Ende Jahr als noch hängig.

2.1.1 Departemente und Bundesämter

Was die Gesamtzahl der Zugangsgesuche (575) und die Praxis der Behörden im Umgang mit Gesuchen 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 2014 auf Stufe Amt meldete uns das Bundesamt für Migration (BFM, seit 1.1.2015 Staatssekretariat für Migration SEM; 33 Gesuche). Danach folgen das BAG (32), das BAFU (31), die EFK (28) und das BLW (25 Gesuche). Bei den Departementen liegen das UVEK (106 Gesuche), das EDA (101) und das EDI (95) an der Spitze. Besonders transparenzfreundlich fallen erneut die Quoten beim EDA aus, welches von insgesamt 101 Gesuchen 87 vollständig positiv beantwortete, in sechs Fällen den Zugang teilweise gewährte und bei lediglich acht Gesuchen den Zugang vollständig verweigerte. 16 von 71 Behörden meldeten uns für 2014, dass bei ihnen kein einziges Zugangsgesuch eigegangen sei. Der Beauftragte selbst sah sich im Berichtsjahr mit neun Zugangsgesuchen konfrontiert, wovon er den Zugang achtmal vollständig und einmal teilweise gewährte.

Was die Erhebung von Gebühren für den Zugang zu amtlichen Dokumenten anbelangt, ist der Gesamtbetrag des in Rechnung gestellten Aufwands im Berichtsjahr mit 2600 Schweizer Franken ausserordentlich bescheiden ausgefallen. Wird zudem berücksichtigt, dass dieser Gesamtbetrag auf lediglich neun von insgesamt 575 gemeldeten Zugangsgesuchen entfällt, wobei 1000 Franken einem einzigen Zugangsgesuch zuzuordnen sind, erscheinen die insgesamt in Rechnung gestellten Gebühren als vernachlässigbar. Ein Überblick über die Erhebung von Gebühren für den Zugang zu amtlichen Dokumenten seit Inkrafttreten des BGÖ im Jahr 2006

zeigt zudem, dass bei weniger als drei Prozent aller dem Beauftragten gemeldeten Zugangsgesuche überhaupt Gebühren erhoben wurden.

Angesichts dieser Zahlen ist für den Beauftragten unverständlich, dass die Verwaltung an den geltenden Bestimmungen und Weisungen der Generalsekretärenkonferenz festhalten will, obwohl in 97 Prozent aller Gesuche keine Gebühren erhoben werden und zahlreiche Verwaltungseinheiten im Rahmen der Evaluation des BGÖ offen erklären, auch in Zukunft keine Gebühren zu verlangen (siehe Ziffer 2.4.1 des vorliegenden Berichts). Aus diesen Gründen erachtet der Beauftragte eine Revision der Gebührenregelung, die sich an der Verwaltungsrealität orientiert, als ebenso sinnvoll wie notwendig. Dabei sollte nach Ansicht des Beauftragten entweder der Gebührenfreibetrag namhaft erhöht (z.B. von 100 auf 750 Franken) oder aber direkt eine Gebührenfreiheit für den Zugang zu amtlichen Dokumenten vorgesehen werden.

Was den Zeitaufwand für die Bearbeitung von Zugangsgesuchen anbelangt, weist der Beauftragte 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 ihm auf freiwilliger Basis übermittelten Angaben sind daher nur bedingt aussagekräftig. Gemäss diesen hat der gemeldete Zeitaufwand trotz einer Zunahme der eingegangenen Zugangsgesuche um rund 20 Prozent weiter abgenommen (2010: 815 Stunden; 2011: 1519 Stunden; 2012: 2155 Stunden; 2013: 1707 Stunden; 2014: 1642 Stunden). Der Zeitaufwand für die Mitwirkung in Schlichtungsverfahren erhöhte sich hingegen von 778 Stunden im 2013 um ca. 85 Prozent auf 1436 Stunden im 2014.

2.1.2 Parlamentsdienste

Die Parlamentsdienste meldeten für das Jahr 2014 ein einziges Zugangsgesuch. Der Zugang zu den verlangten Dokumenten wurde dabei vollständig verweigert.

2.1.3 Bundesanwaltschaft

Die Bundesanwaltschaft meldete uns für das Jahr 2014 sechs Zugangsgesuche, wobei der Zugang fünfmal vollständig gewährt und einmal vollständig verweigert wurde.

2.1.4 Schlichtungsanträge

Im 2014 wurden insgesamt 90 Schlichtungsanträge eingereicht, was einer deutlichen Zunahme um gut 18 Prozent entspricht (2013: 76). Im Gegensatz zum Vorjahr

wurden im Berichtsjahr am meisten Anträge von Medienschaffenden eingereicht (44), gefolgt von Privatpersonen (19).

Diese Zahlen lassen folgende Schlüsse und Bemerkungen zu:

In 246 Fällen verweigerte die Bundesverwaltung den Zugang vollständig (122) respektive teilweise (124). Dem stehen 90 bei uns eingereichte Schlichtungsanträge gegenüber. Im Berichtsjahr wurde somit in gut 36 Prozent aller Fälle von ganz oder teilweise abgelehnten Zugangsgesuchen ein Schlichtungsantrag eingereicht.

Insgesamt konnten im Berichtsjahr 85 Schlichtungsanträge abgeschlossen werden. Davon stammen 35 Anträge aus dem Berichtsjahr selbst, 25 aus dem Jahr 2013 und 25 noch aus dem Jahr 2012. In 15 Fällen konnte zwischen den Beteiligten eine Schlichtung erzielt werden, wovon es in neun Fällen zu einer Schlichtung im eigentlichen Sinne kam und in den übrigen sechs Fällen zu einer Erledigung des Verfahrens aufgrund einer Intervention des Beauftragten. In zwei Fällen wurde der Zugang nach Eröffnung des Schlichtungsverfahrens gewährt. Insgesamt erliess der Beauftragte 49 Empfehlungen, wo keine einvernehmliche Lösung möglich oder von vornherein ersichtlich war. Mit diesen 49 Empfehlungen konnten 55 Schlichtungsanträge erledigt werden. Ein Schlichtungsantrag wurde zurückgezogen und ein weiterer aufgrund des Fernbleibens des Antragstellers an der Schlichtungsverhandlung abgeschrieben. In sieben Fällen waren die Voraussetzungen für die Anwendung des BGÖ nicht gegeben. In vier Fällen wurde der Schlichtungsantrag nicht fristgerecht eingereicht.

Im Berichtsjahr konnten so viele Schlichtungsverfahren wie noch nie abgeschlossen werden, was unter anderem auch darauf zurückzuführen ist, dass der Beauftragte zum ersten Mal zwei Praktikantenstellen besetzen konnte. Antragstellende müssen indes aufgrund der nach wie vor grossen Rückstände in der Bearbeitung der hängigen Schlichtungsverfahren weiterhin länger als die gesetzlich vorgesehenen 30 Tage auf die Durchführung eines Schlichtungsverfahrens warten.

Alle im Berichtsjahr erlassenen Empfehlungen finden Sie auf der Website des Beauftragten (www.derbeauftragte.ch, Öffentlichkeitsprinzip – Empfehlungen).

2.2 Ämterkonsultationen und weitere Stellungnahmen

2.2.1 Einführung des neuen OECD-Standards zum internationalen Austausch in Steuersachen

Der Beauftragte hat sich im Rahmen von Ämterkonsultationen zum internationalen Informationsaustausch in Steuersachen geäussert. Dabei nahm er Stellung zu neuen Bestimmungen des Steueramtshilfegesetzes (StAhiG) und zum Entwurf des Bundesgesetzes über den internationalen automatischen Informationsaustausch in Steuersachen (AIA-Gesetz).

Beide Gesetzesentwürfe enthielten jeweils eine inhaltsgleiche Bestimmung mit dem Titel «Geheimhaltungspflicht». Hierzu wies der Beauftragte darauf hin, dass diese Bestimmung lediglich die im Bundespersonalgesetz festgehaltene Geheimhaltungspflicht (Berufs-, Geschäfts- und Amtsgeheimnis) für Bundesangestellte wiedergibt, und erinnerte daran, dass mit Inkrafttreten des Öffentlichkeitsgesetzes (BGÖ) das Amtsgeheimnis in seiner Tragweite indirekt neu definiert worden ist. Dem Amtsgeheimnis unterliegen nur noch Informationen, die nicht in den Geltungsbereich des BGÖ fallen, die durch spezialgesetzliche Bestimmungen als geheim erklärt werden oder die unter eine der im BGÖ selbst vorgesehenen Ausnahmebestimmungen fallen. Daher können aus der konkret vorgeschlagenen Bestimmung keine weitergehenden Geheimhaltungspflichten abgeleitet werden.

Ob im Rahmen eines Gesuchs um Zugang zu amtlichen Dokumenten Einsicht gewährt werden kann, bestimmt sich demnach alleine aus den Vorgaben des BGÖ (insb. Art. 3ff.). So bieten in Bezug auf amtliche Dokumente mit berechtigtem Schutzbedürfnis etwa die vorgesehenen Ausnahmeklauseln (z.B. Geschäftsgeheimnis oder wirtschafts-, geld- und währungspolitische Interessen der Schweiz) sowie die Bestimmungen zum Schutz von Personendaten ausreichende Möglichkeiten, um den Zugang zu Dokumenten zu verweigern, einzuschränken oder aufzuschieben. Auch im Bereich des internationalen Informationsaustauschs in Steuersachen und in seiner innerstaatlichen Umsetzung ist es somit im Falle von sensiblen Informationen mit den bestehenden Ausnahmebestimmungen des BGÖ ohne weiteres möglich, den konkreten Umständen gebührend Rechnung zu tragen. Der Beauftragte forderte daher, dass zumindest der letzte Teilsatz, wonach der Einblick in amtliche Akten zu verweigern sei, ersatzlos zu streichen ist.

Ebenfalls inhaltsgleiche Bestimmungen sahen die beiden Erlassentwürfe für die Publikation von Statistiken für das Peer Review des Global Forum über Transparenz und Informationsaustausch vor. Demnach sollte zu weitergehenden als den in den Statistiken veröffentlichten Informationen kein Recht auf Zugang bestehen. Auch hier fordert der Beauftragte, den Ausschluss des Zugangsrechts ersatzlos zu

streichen. Er verwies dabei auf den Geltungsbereich des BGÖ, welches bei Verfahren der internationalen Rechts- und Amtshilfe keine Anwendung findet, seine Ausnahmeklauseln, die Bestimmungen zum Schutz von Personendaten sowie auf das Statistikgeheimnis.

2.2.2 Entwurf zur Teilrevision des Luftfahrtgesetzes

Der Beauftragte hat den Entwurf für eine neue Bestimmung im Luftfahrtgesetz, wonach Dokumente betreffend die Aufsichtstätigkeit des Bundesamts für Zivilluftfahrt BAZL vom Öffentlichkeitsgesetz ausgenommen werden sollten, abgelehnt.

Der Beauftragte hat im Rahmen der Ämterkonsultation betreffend die Eröffnung des Vernehmlassungsverfahrens zum Entwurf zur Teilrevision 1+ des Luftfahrtgesetzes (LFG) Stellung genommen. Der Entwurf sah im ersten Absatz eine Pflicht zur aktiven Information vor, wonach das BAZL die Öffentlichkeit periodisch über seine Aufsichtstätigkeit informiert. Dieser Absatz erschien dem Beauftragten nicht hinreichend konkret ausgestaltet, da er weder festlege, über welche Inhalte seiner Aufsichtstätigkeit das BAZL genau informiere, noch den Begriff «periodisch» genauer umschreibe. Im Übrigen besteht unabhängig von einer allfälligen aktiven Informationspflicht stets die Möglichkeit ein Zugangsgesuch gestützt auf das Öffentlichkeitsgesetz (BGÖ) zu stellen.

Der zweite Absatz sah vor, Inspektions- und Auditberichte des BAZL sowie sämtliche Dokumente, die Schlussforderungen über die bei diesen Kontrollen gewonnenen Erkenntnisse und Informationen enthalten, dem Geltungsbereich des BGÖ zu entziehen.

Die vorgeschlagene Regelung lehnte der Beauftragte ab. Er unterstrich, dass das Instrumentarium des BGÖ mit all seinen Ausnahmebestimmungen ausreiche, um dem Schutzbedarf von sensiblen Informationen gerecht zu werden. Zudem knüpft das Gesetz an den Begriff des amtlichen Dokuments an und sieht nicht vor, einzelne Kategorien von Dokumenten, wie Inspektions- oder Auditberichte, davon auszunehmen.

Weiter widersprach der Beauftragte der Argumentation des BAZL, wonach Berichte nicht mehr präzise und aussagekräftig formuliert würden, falls sie nicht vertraulich behandelt würden. Die gesetzliche Aufsichtspflicht des BAZL sowie die entsprechenden Mitwirkungspflichten der beaufsichtigten Unternehmen würden durch das BGÖ nicht durchbrochen. Um seine Meinung zu stützen, verwies der Beauftragte auf die ebenfalls in sensiblen Kontrollbereichen tätige Eidgenössische Finanzkontrolle (EFK), die nach sieben Jahren Erfahrung mit dem BGÖ zum Schluss gekommen ist, dass die Qualität ihrer Arbeit durch dieses Gesetz nicht beeinträchtigt wird.

Der Beauftragte erachtete die ebenfalls vorgebrachte Begründung, dass die Berichte oft technische Einzelheiten enthielten, die von der Öffentlichkeit nur schwer richtig einzuordnen seien, als unhaltbar und anmassend. Spätestens mit Inkrafttreten des BGÖ ist es nicht mehr an der Verwaltung darüber zu befinden, ob bestimmte Informationen für das breite Publikum verständlich sind oder ob eine bestimmte Person die «richtigen» Schlüsse aus einem Dokument ziehen kann. Dies würde letztlich einer Bevormundung des Bürgers gleichkommen. Er gab zu bedenken, dass die Verständlichkeit einer Information kein vom BGÖ vorgesehenes Ausnahmekriterium ist.

Der Beauftragte wies zudem darauf hin, dass die Formulierung der vorgeschlagenen Bestimmung es erlauben würde, die gesamte Aufsichtstätigkeit des BAZL dem BGÖ zu entziehen, was sich angesichts des berechtigten öffentlichen Interesses an einer korrekten Erfüllung dieser Aufsichtstätigkeit im Bereich der Luftfahrt nicht rechtfertigen lässt.

Abschliessend gab der Beauftragte zu bedenken, dass der Gesetzgeber mit dem Erlass des BGÖ ein klares Zeichen gegen Geheimbereiche und -dokumente in der Bundesverwaltung gesetzt hat, was letztlich auch für Aufsichtsbehörden gelten muss, da diese von Gesetzes wegen andere Verwaltungseinheiten oder Private überprüfen. Es ist deshalb nicht nachvollziehbar, weshalb sich Behörden mit Audit- und Inspektionsaufgaben selber jeglicher Überprüfung mittels BGÖ entziehen wollen, obwohl ein, vom Bundesverwaltungsgericht anerkanntes, öffentliches Interesse an der Nachvollziehbarkeit der Aufsichtstätigkeit einer Behörde besteht (A-2434/2013 vom 9. Dezember 2013, E. 10.2).

2.2.3 Revision des Bundesgesetzes und der Verordnung über das öffentliche Beschaffungswesen

Der Beauftragte hat im Rahmen des Vernehmlassungsverfahrens zu den Entwürfen des revidierten Bundesgesetzes über das öffentliche Beschaffungswesen (BöB) und der revidierten Verordnung (VöB) Stellung genommen.

Der Beauftragte begrüsste die grundsätzliche Stossrichtung der Revision des BöB und der VöB, wonach unter anderem die Transparenz im Beschaffungswesen gestärkt sowie ein wirtschaftlicher Einsatz öffentlicher Mittel, die Stärkung des Wettbewerbs und schliesslich die Bekämpfung von Korruption ins Zentrum gerückt werden sollen. Wichtig erschien dem Beauftragten der Umstand, dass ein Ausbau der Transparenz im Bereich des öffentlichen Beschaffungsrechts nicht bloss eine Zielsetzung unter vielen ist, sondern als griffiges Instrument gewissermassen den Motor zur Erreichung der übrigen mit der vorliegenden Revision verfolgten Zielsetzungen darstellt.

Hingegen bedauerte der Beauftragte, dass die Revision nicht zugleich zum Anlass genommen wurde, sich im Rahmen der Transparenzzielsetzung auch mit der behördlichen Informationstätigkeit auf Gesuch hin (Passivinformation) auseinanderzusetzen und damit die Koordination zwischen dem BöB und dem Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung (BGÖ) festzuhalten. Insbesondere vermisste er den Hinweis, dass neben den verschiedenen Bestimmungen der behördlichen Information von Amtes wegen (Aktivinformation) parallel dazu das Recht auf Zugang zu amtlichen Dokumenten des Beschaffungswesens gestützt auf das BGÖ gilt.

In diesem Zusammenhang wies der Beauftragte speziell darauf hin, dass die in Art. 47 Abs. 4 des Vorentwurfs vorgesehene «nicht öffentliche Liste» von sanktionierten Anbietern nach den Bestimmungen des BGÖ zumindest auf Gesuch hin zugänglich zu machen ist. Die «nicht-Öffentlichkeit» dieser Liste könne im Lichte des mit dem BGÖ eingeführten Paradigmenwechsels hin zur Verwaltungsöffentlichkeit nämlich lediglich dahingehend verstanden werden, dass diese nicht aktiv zu publizieren sei. Hingegen sei die «nicht-Öffentlichkeit» dieser Liste nicht als Spezialbestimmung im Sinne von Art. 4 BGÖ zu verstehen, welche eine Zugangsgewährung gestützt auf das BGÖ von vornherein auszuschliessen vermöge. Vielmehr gelte es im Einzelfall zu prüfen, ob der Zugang unter Anwendung einer Ausnahmebestimmung des Öffentlichkeitsgesetzes zu beschränken oder zu verweigern ist.

Weiter beurteilte der Beauftragte die im erläuternden Bericht enthaltene Aussage, wonach zu grosse Transparenz abgestimmte Verhaltensweisen begünstige und sich antikompetitiv auswirken könne, als zu einseitig und polarisierend. Vielmehr führt nach seiner Ansicht mangelnde Transparenz im Beschaffungswesen zu Korruption und Misswirtschaft, was sich in der Praxis bereits eindrücklich gezeigt hat.

2.2.4 Revision von Artikel 15 der Verordnung zum BGÖ

Im Anschluss an den Bundesgerichtsentscheid 1C_550/2013 betreffend die Reduktion der Gebühren von Medienschaffenden beauftragte die Generalsekretärenkonferenz (CSG) die interdepartementale Arbeitsgruppe Datenschutz unter der Federführung der Bundeskanzlei (BK) mit der Prüfung der Rechtsprechung des Bundesgerichts und der Vorbereitung einer Revision der Öffentlichkeitsverordnung (VBGÖ). Nach Diskussionen in einer Untergruppe dieser Arbeitsgruppe hat das Bundesamt für Justiz (BJ) als für die Gesetzgebung im Bereich des Öffentlichkeitsgesetzes (BGÖ) zuständige Behörde einen Entwurf zur Revision des Artikels 15 VBGÖ (Gebühren) unterbreitet.

Im Rahmen der Mitwirkung in dieser Untergruppe sowie im Verfahren der Ämterkonsultation zur geplanten Gebührenrevision nahm der Beauftragte verschiedentlich Stellung: Er war der Ansicht, dass für eine Änderung des Gebührenrechts eine formalgesetzliche Grundlage erforderlich sei. Weiter führte er aus, dass das BGÖ ein Gebührenerhebungsrecht und keine Gebührenerhebungspflicht vorsehe. Schliesslich äusserte er, dass die geplante Norm der Rechtsprechung des Bundesgerichts nicht gerecht werde, da bei Medienschaffenden die Gebühr nach Ermessen auch um mehr als 50 Prozent reduziert werden könne. Das BJ übernahm die Änderungsvorschläge des Beauftragten teilweise.

Der neue Artikel 15 Absatz 4 VBGÖ ist nun seit dem 1. September 2014 in Kraft. Er sieht bei der Gebührenerhebung eine Reduktion für Medienschaffende um mindestens 50 Prozent vor, wobei bei besonders aufwändigen Zugangsgesuchen auf diese Reduktion verzichtet werden kann (vgl. zu den Gebühren auch den Tätigkeitsbericht 2013/2014, Ziffer 2.6.1).

2.3 Varia

2.3.1 Evaluation des Öffentlichkeitsgesetzes und Mitwirkung in der Begleitgruppe

Im 2014 wurde das Öffentlichkeitsgesetz zum zweiten Mal seit seinem Inkrafttreten evaluiert. In der Begleitgruppe zu dieser Evaluation wirkte auch der Beauftragte mit. Der Schlussbericht zeigt keine wesentlichen anderen Ergebnisse als jene der ersten Evaluation im Jahr 2009, enthält dennoch interessante Aussagen und Informationen, von denen einige nachfolgend herausgegriffen werden.

Das Öffentlichkeitsgesetz (BGÖ) wurde zum ersten Mal im Jahr 2009 evaluiert (siehe auf www.derbeauftragte.ch, unter Öffentlichkeitsprinzip – Evaluationen). Nachdem in letzter Zeit Behörden vermehrt Kritik in Bezug auf die Umsetzung des BGÖ geübt hatten, forderte die Generalsekretärenkonferenz eine erneute Überprüfung seines Vollzugs und seiner Wirksamkeit. Mit der Evaluation des BGÖ wurde das Bundesamt für Justiz (BJ) beauftragt. Dieses setzte eine Begleitgruppe ein, die sich aus den Öffentlichkeitsberatenden der Departemente und der Bundeskanzlei, einer Vertretung des Bundesarchivs sowie dem Beauftragten zusammensetzte. Die mit der Evaluation betraute Büro Vatter AG lieferte dem BJ ihren Schlussbericht Ende 2014 ab. Der Bundesrat nahm ihn im Frühling 2015 zur Kenntnis und gab gestützt auf die Resultate der Evaluation die Teilrevision des Gesetzes in Auftrag.

Im Rahmen der Evaluation wurden die Öffentlichkeitsberatenden der Departemente und der Bundeskanzlei, zwölf Öffentlichkeitsberatende ausgewählter Behörden (sogenannte «Fallstudien»), Gesuchstellende, Medienexperten und auch der Beauftragte befragt.

Die Erkenntnisse, zu denen die Evaluatoren gelangt sind, haben den Beauftragten nicht überrascht, denn sie stimmen in wesentlichen Punkten mit jenen der Evaluation aus dem Jahr 2009 überein:

- Paradigmenwechsel: Der seit Inkrafttreten des BGÖ immer wieder geforderte Paradigmenwechsel ist noch immer nicht in der gesamten Bundesverwaltung vollzogen worden. Die Gesuchstellenden nehmen einzelne Behörden oft noch immer so wahr, als wehrten sich diese gegen den Vollzug des BGÖ.
- Vorhandene Dokumente: Wie bereits vor sechs Jahren, kommt auch die neue Evaluation zum Schluss, dass es für Interessierte schwierig ist, überhaupt in Erfahrung bringen zu können, welche Dokumente in der Bundesverwaltung vorhanden sind.
- Koordination innerhalb und zwischen den Departementen: Beide Evaluationen stellen die uneinheitliche Praxis in der Bearbeitung der Zugangsgesuche

über die Behörden und Departemente hinweg fest und schlagen daher vor, über die Grenzen der Verwaltungseinheiten hinaus Synergien zu nutzen und eine Arbeitsgruppe zum Erfahrungsaustausch zu schaffen.

- Gebührenpraxis: Auch die Experten der Evaluation von 2014 stellen fest, dass verwaltungsintern eine Uneinheitlichkeit in der Anwendung der Erhebung von Gebühren besteht, und schlagen ebenfalls vor, den Gebührenfreibetrag zu erhöhen.
- Ausbau der Personalressourcen des Beauftragten: Alle durch die Evaluatoren im Rahmen der zweiten Evaluation befragten Gruppen (Bundesbehörden, Öffentlichkeitsberatende der Departemente, Medienexperten, Gesuchstellende) befürworten, dass der Bundesrat die notwendigen Ressourcen zur Verfügung stellt, um damit nicht zuletzt die Dauer des Schlichtungsverfahren zu verringern. Zu diesem Ergebnis kam bereits die Evaluation im 2009. Der Bundesrat hat bis anhin aber jeden Ressourcenantrag des Beauftragten abgelehnt.

Über diese grundsätzlichen Ergebnisse beinhaltet der Schlussbericht für den Beauftragten einige bemerkenswerte Informationen. Dass sich einige Verwaltungseinheiten auch neun Jahre nach Inkrafttreten des BGÖ mit dem Paradigmenwechsel noch schwer tun. Dies zeigt sich auch daran, dass beispielsweise noch immer über darüber diskutiert wird, ob E-Mails oder klassifizierte Dokumente unter das BGÖ fallen. In den Interviews mit den Experten wurde auch eingebracht, dass die Protokolle von ausserparlamentarischen Kommissionen vom Gesetz ausgenommen werden sollten. Dies ist insofern nicht erstaunlich, als dass auch in der Vergangenheit Versuche unternommen wurden, diese Kommissionen (dazu gehört etwa die Wettbewerbskommission) als Ganzes auszunehmen.

Die Experten haben die Frage betreffend die Protokolle aufgenommen und regen eine Überprüfung an. Sie ziehen dabei einen Vergleich zu parlamentarischen Kommissionen, deren Beratungen gemäss Parlamentsgesetz vertraulich sind. Diese Schlussfolgerung ist für den Beauftragten nicht nachvollziehbar: Zum einen hinkt der Vergleich, da ausserparlamentarische Kommissionen u.a. Aufgaben ausüben, die normalerweise von der Verwaltung erbracht werden müssten. Zum andern hat das Bundesverwaltungsgericht bereits rechtskräftig entschieden, dass sowohl die ausserparlamentarischen Kommissionen als auch ihre Protokolle als amtliche Dokumente unter das BGÖ fallen.

Der Schlussbericht nimmt auch die Forderung einiger Aufsichtsbehörden auf, ihre Tätigkeiten vom BGÖ auszunehmen. Nach Ansicht des Beauftragten ist es nicht haltbar, dass gerade Aufsichtsbehörden für ihre Arbeit einen Geheimbereich beanspruchen, obwohl sie im öffentlichen Interesse andere private und öffentliche Stellen beaufsichtigen. In diesem Zusammenhang kann auf die positive Kehrtwende

der Eidgenössischen Finanzkontrolle (EFK) hingewiesen werden, welche diese im Jahr 2014 in Bezug auf das Öffentlichkeitsprinzip vollzogen hat. Sie, die auch Aufsichts- und Kontrollaufgaben wahrnimmt, zieht gemäss einer Medienmitteilung vom 23.06.2014 nach sieben Jahren BGÖ eine positive Bilanz und sieht sich durch das Gesetz nicht in ihrer Arbeit beeinträchtigt.

Interessant ist auch die Feststellung im Schlussbericht, wonach der Wechsel an der Spitze einer Behörde dazu geführt habe, dass das BGÖ umgesetzt wurde. Dies erstaunt den Beauftragten nicht, da er schon länger der Ansicht ist, dass sich die Haltung der Leitung einer Behörde entscheidend darüber auswirkt, ob und wie diese das Öffentlichkeitsprinzip lebt. Zudem stellt der Beauftragte immer wieder fest, dass der Wille, das BGÖ umzusetzen, stark von einzelnen Personen abhängig ist. Es ist davon auszugehen, dass es auch in anderen Departementen Stellen gibt (bspw. Generalsekretariate und Bundesämter, aber auch einzelne Abteilungs- oder Sektionsleitungen bzw. Kommunikationsdienste), welche die vom Gesetzgeber verlangte Umsetzung des Öffentlichkeitsprinzips zumindest nicht direkt anstreben. Wünschenswert wäre eine klare Unterstützung des Öffentlichkeitsprinzips durch alle Direktionsstufen der Bundesverwaltung.

Im Rahmen der Evaluation wurde auch das Schlichtungsverfahren unter die Lupe genommen. Nachfolgend werden einige interessante Aspekte herausgegriffen. Für den Evaluationsbericht wurden u.a. auch 106 Schlichtungsverfahren ausgewertet. Dabei zeigt sich u.a., dass 90 Prozent der vom Beauftragten durchgeführten Schlichtungsverfahren nicht zu einem Gerichtsverfahren führten. Damit konnte das in der Botschaft zum BGÖ formulierte Ziel, nämlich die Vermeidung von Verwaltungs- und Justizverfahren durch Schaffung eines Schlichtungsverfahren, erreicht werden (BBl 2003 2018).

Gleichwohl wurde im Rahmen der Evaluation ein Vergleich der Empfehlungen des Beauftragten mit den vorhandenen Urteilen vorgenommen. Die juristische Analyse der materiell relevanten Urteile des Bundesverwaltungsgerichts und des Bundesgerichts hat ergeben, dass die Empfehlungen des Beauftragten von den Gerichten gestützt werden und kein rechtskräftiges Urteil mit namhaften Abweichungen von den Empfehlungen existiert. Teilweise verweise das Bundesverwaltungsgericht in seinen Urteilen sogar explizit auf die Empfehlungen des Beauftragten, stellten die Evaluatoren fest. Vor diesem Hintergrund erstaunt es nicht, dass sie eine hohe Akzeptanz der Empfehlungen, insbesondere durch die Antragstellenden, in ihrem Bericht festhalten. Dies gilt selbst dann, wenn sich der Beauftragte zu ihren Ungunsten empfiehlt.

Die befragten Gesuchstellenden sind überdies einig darüber, dass bei einer Beschränkung des Zugangs durch Behörden ein kostenloses Schlichtungsverfahren möglich sein muss (91% positiv, 9% eher positiv). Ausserordentlich positiv werden

von ihnen die Empfehlungen des Beauftragten beurteilt: 91 Prozent der befragten Antragstellenden bewerten die Tatsache, dass der Beauftragte seine Empfehlungen begründet, als «positiv» und weitere acht Prozent beurteilen dies als «eher positiv». Mit anderen Worten schätzen fast 100 Prozent der Gesuchstellenden besonders die Abklärungstiefe und die ausführlichen Begründungen der Empfehlungen. Gleichzeitig bedauern sieben von zehn Befragten, dass die Empfehlungen des Beauftragten keine unmittelbare Rechtswirkung erzielen. Angesichts dieser Ergebnisse erstaunt nicht, dass die Antragstellenden die Arbeit des Beauftragten besonders positiv beurteilen.

Einzelne Medienexperten beurteilen das Schlichtungsverfahren als sinnvolle Institution. Die Empfehlungen des Beauftragten stossen bei ihnen auf eine hohe Akzeptanz, da sie in ihren Augen Richtlinien zur Umsetzung des Öffentlichkeitsgesetzes im Verwaltungsalltag darstellen. Der Beauftragte wird in gewissem Ausmass gar als der «Motor» des Öffentlichkeitsprinzips gesehen. Für andere ist das Verfahren zu schwerfällig und kompliziert. So wird u.a. auch vorgeschlagen, die Kompetenzen des Beauftragten auszubauen – dieser solle anstelle der Empfehlung direkt verfügen können.

Grossmehrheitlich sind auch die zwölf befragten Behörden der Ansicht, dass mit dem Schlichtungsverfahren Justizverfahren vermieden werden können. So haben die Empfehlungen des Beauftragten bei mindestens zwei Drittel von ihnen praxisbildende bzw. teilweise praxisbildende Wirkung. Von Behördenseite wird indes am meisten Kritik geäussert: Zwei Behörden erkennen keinen Bedarf an Schlichtungsverhandlungen, die auf das Schaffen von gegenseitigem Verständnis angelegt sind, denn es gehe einzig um den Vollzug des BGÖ und nicht um Befindlichkeiten. Gemäss einzelnen der befragten Behörden gewichte der Beauftragte die Transparenz grundsätzlich zu hoch; sie nehmen den Beauftragten in der Tendenz als zu «öffentlichkeitsfreundlich» und eher «behördenfeindlich» war.

Unbefriedigend wird von allen – auch vom Beauftragten selber – die lange Dauer des Schlichtungsverfahrens beurteilt. Sie stellt faktisch eine Begrenzung des Zugangs zu amtlichen Dokumenten dar und kann von Behörden dazu missbraucht werden, den Zugang zu den gewünschten Dokumenten aufzuschieben in der Hoffnung, dass das Interesse des Antragstellers mit der Zeit abnimmt. Interessant ist in diesem Zusammenhang, dass alle befragten Gruppen (auch Stimmen aus der Bundesverwaltung) der Ansicht sind, dass der Bundesrat dem Beauftragten endlich die notwendigen Ressourcen für eine effiziente Umsetzung des BGÖ und ein kürzeres Schlichtungsverfahren zusprechen sollte. Auch die Experten sehen als Ansatzpunkt für die Beschleunigung des Verfahrens die Erhöhung der Ressourcen des Beauftragten. Damit kommen sie zum gleichen Schluss wie die Evaluatoren 2009 und bestätigen damit die wiederholten Ressourcenanträge des Beauftragten an den Bundesrat, der diese bisher stets ablehnte.

Im Zusammenhang mit der Dauer von Schlichtungsverfahren hat der Beauftragte erneut darauf hingewiesen, dass eine Frist von 30 Tagen für die Durchführung des Schlichtungsverfahrens unrealistisch ist und letztlich jeglicher Logik des Verfahrens widerspricht. Es liegt in der Natur eines Mediationsverfahrens, dass eine zeitliche Limitierung jeder Einigungsfindung entgegensteht. Auch bei genügender Ressourcenausstattung ist die Einhaltung einer Frist zur Lösungsfindung für komplexere Fälle nicht möglich. In der Praxis zeigt sich immer wieder, dass etwa bereits die Vereinbarung eines Termins mit den Beteiligten Schwierigkeiten bereitet und ein Treffen nicht innerhalb eines Monats bewerkstelligt werden kann. Der Beauftragte bleibt daher bei seiner Forderung nach Aufhebung dieser Frist unter gleichzeitiger Zurverfügungstellung der notwendigen personellen Ressourcen.

Zusammenfassend sind die Resultate, welche die Evaluation in Bezug auf das Schlichtungsverfahren zu Tage gefördert hat, für den Beauftragten erfreulich. Das Verfahren hat sich in den nunmehr neun Jahren seit Inkrafttreten etabliert und wird von allen Beteiligten mehrheitlich positiv beurteilt. Zusammenfassend regen die Evaluatoren eine Verkürzung der Dauer des Schlichtungsverfahrens (durch Erhöhung der personellen Ressourcen des Beauftragten) bei gleichbleibender Gründlichkeit vor. Grundsätzlich befürworten sie eine Beschleunigung, ohne dass jedoch der aus der Sicht der Gesuchstellenden wichtige Vorteil des Schlichtungsverfahrens, nämlich die Abklärungstiefe und ausführliche Begründung der Empfehlung, verloren gehen soll. Es bleibt zu hoffen, dass sich der Bundesrat bei allfälligen Beschleunigungsmassnahmen auch an den Interessen der Gesuchstellenden und an diesem für sie wichtigen Vorteil orientieren wird. Der Beauftragte wird dies im Auge behalten.

2.3.2 Beziehungen zu kantonalen Öffentlichkeitsbeauftragten – Arbeitsgruppe Schlichtungswesen

Der Beauftragte und kantonale Öffentlichkeitsbeauftragte, welche auch Schlichtungsverfahren durchführen, trafen sich auch im Jahr 2014 zu vertieftem Erfahrungsaustausch. Im Rahmen der im Herbst 2011 gebildeten «groupe d'intervision sur la gestion consensuelle des conflits transparence» können so Fragen zur Schlichtungstätigkeit und zum Öffentlichkeitsprinzip diskutiert werden. Diese Zusammenarbeit ist für die Beteiligten wichtig und wertvoll, besonders da es sich bei der Öffentlichkeitsgesetzgebung um ein in der Schweiz junges Rechtsgebiet handelt. Infolge Mutationen erfuhr die Arbeitsgruppe im letzten Jahr eine Änderung in der Zusammensetzung. Gleichzeitig wurde beschlossen, die informellen Sitzungen jeweils alternierend durch die einzelnen Mitglieder zu organisieren und somit die Sitzungen auch in den Kantonen durchzuführen.

3. Der EDÖB

3.1 Neunter Datenschutztag

Zum neunten internationalen Datenschutztag vom 28. Januar 2015 haben wir eine Podiumsdiskussion über die Datenschutzproblematik von Gesundheitsapps und sensorgesteuerten Accessoires zur Vermessung von Körperfunktionen (Wearables) organisiert. Wir stellten ein grosses Interesse an der Thematik fest.

Die technologischen Innovationen im Gesundheitsbereich eröffnen neue Möglichkeiten für die medizinische Forschung und verändern die Gesellschaft nachhaltig. Mit dem zunehmenden Trend zur Selbstvermessung des eigenen Körpers (Quantified Self) steigt die Menge an Gesundheitsdaten exponentiell, und die kommerziellen Interessen an diesen Daten sind vielfältig. Die Gefahr des unbefugten Zugriffs auf teilweise hochsensible Informationen nimmt somit zu. In einem Podiumsgespräch mit Experten aus Politik, Wirtschaft und Forschung konnte der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte Hanspeter Thür verschiedene Aspekte kritisch beleuchten und das Bewusstsein für Datenschutz und informationelle Selbstbestimmung ins Zentrum der Debatte stellen. Der Anlass fand im Berner Generationenhaus statt.

In einer angeregten Diskussion beleuchtete die Expertenrunde das Thema Gesundheitsapps und Wearables facettenreich und hinterfragte es kritisch. Obschon die Vertreter aus Forschung und Wirtschaft der digitalen Selbstvermessung grundsätzlich positiv gegenüber stehen und darin Vorteile für den Menschen als Patienten sehen, sind sie sich des Gefahrenpotenzials im Umgang mit Gesundheitsdaten bewusst. Hanspeter Thür betonte, dass der Datenschutz bereits in der Entwicklungsphase neuer Technologien berücksichtigt werden sollte (Privacy by design) und fordert datenschutzfreundliche Voreinstellungen (Privacy by default). Auf der politischen Ebene steht deshalb eine Verschärfung des Datenschutzgesetzes an. Die Schweiz müsse ihre Vorbildfunktion im Bereich Datenschutz behalten und dürfe gegenüber der EU nicht ins Hintertreffen gelangen, weil dies auch negative Folgen für die Schweizer Wirtschaft mit sich bringen würde.

Die abschliessende Diskussionsrunde unter Einbezug des Publikums ging auch auf ethische Aspekte im Umgang mit Gesundheitsdaten ein und schnitt dabei die thematisch verwandten Bereiche eHealth und Big Data an.

3.2 Publikationen des EDÖB im laufenden Geschäftsjahr

Umfassende Informationen zu aktuellen Datenschutzthemen finden interessierte Bürgerinnen und Bürger auf unserer Website www.derbeauftragte.ch. Im Berichtsjahr kamen insbesondere folgende neuen Beiträge hinzu: Erläuterungen zu Big Data, Recht auf Vergessen, Einsatz von Drohnen, Datenschutz in der Forschung sowie Zutrittskontrollsysteme in Freizeitanlagen. Ausserdem publizierten wir im Bereich des Öffentlichkeitsgesetzes eine Reihe von Empfehlungen.

Big Data bietet neue Chancen für soziale oder wissenschaftliche Erkenntnisse und für die kommerzielle Nutzung durch Unternehmen. Big Data kann aber auch eine Bedrohung für die Privatsphäre sein, wenn die bearbeiteten Personendaten nicht oder ungenügend anonymisiert wurden. Zum Schutz der Persönlichkeit fordern wir deshalb eine datenschutzfreundliche Ausgestaltung der technischen Voreinstellungen (privacy by default). Der Datenschutz muss schon in der konzeptionellen Phase berücksichtigt und die Datensicherheit gewährleistet werden (privacy by design). Zudem sind hohe Transparenz- und Verfahrensanforderungen an Big Data zu stellen (www.derbeauftragte.ch, Datenschutz – Internet und Computer – Big Data).

Das Urteil des Europäischen Gerichtshofs vom 13. Mai 2014 zum «Recht auf Vergessen», das die Suchmaschinenbetreiber für die Bearbeitung der Personendaten auf ihren Websites verantwortlich macht und verlangt, dass sie auf Gesuch hin und unter bestimmten Voraussetzungen Links auf diesen Seiten löschen, hat auch die öffentliche Diskussion in der Schweiz angeregt. Um der technologischen Entwicklung und zunehmenden Digitalisierung Rechnung zu tragen, strebt die EU eine Revision des rechtlichen Rahmens an. Auch bei uns müssen effektive Lösungen gefunden werden, um die Würde der Betroffenen und das Recht auf Privatsphäre im Internet besser zu schützen (www.derbeauftragte.ch, Datenschutz – Internet und Computer – Recht auf Vergessen).

Im Zuge des technologischen Fortschritts sind Drohnen immer kleiner und leichter, preiswerter und einfacher bedienbar geworden. Sie werden deshalb immer häufiger sowohl zu privaten als auch zu gewerblichen Zwecken eingesetzt. Da Drohnen heute in der Regel mit Kameras bestückt sind, können sie zur Videoüberwachung eingesetzt werden. Personen, die solche Drohnen fliegen lassen, müssen deshalb die Voraussetzungen des Datenschutzes einhalten, sobald auf den Aufnahmen Personen erkennbar sind. Auf unserer Website beschreiben wir ausführlich und anschaulich, worauf beim Einsatz von Drohnen zu achten ist (www.derbeauftragte.ch, Datenschutz – Technologien – Videoüberwachung – Drohnen).

Auch Personentrackingsysteme finden zunehmende Verbreitung. Sie werden z.B. zur Optimierung von Verkehrs- und Personenströmen oder für die Analyse von Kundenverhalten zu Marketing- und anderen Zwecken eingesetzt. Da mit solchen Systemen zum Teil auch besonders schützenswerte Personendaten erhoben oder gar Persönlichkeitsprofile generiert werden, ist bei ihrem Betrieb Vorsicht geboten. Auf unserer Website werden die wichtigsten datenschutzrechtlichen Aspekte erläutert, die bei Personentracking zu beachten sind (www.derbeauftragte.ch, Datenschutz – Technologien – Personentracking).

Forscherinnen und Forscher sind bei der Bearbeitung von Personendaten für deren Schutz verantwortlich. Daten, die zur medizinischen Forschung gesammelt werden, dürfen nur bearbeitet werden, wenn die betroffenen Personen vorgängig zugestimmt haben oder eine gesetzliche Grundlage vorliegt. Auch wenn jeder Einzelfall im Forschungskontext und im Lichte seiner Besonderheiten betrachtet werden muss, sollten in Forschungsprojekt wenn möglich anonymisierte Daten verwendet werden. Das Forschungsergebnis ist ebenfalls in anonymisierter Form zu publizieren (www.derbeauftragte.ch, Datenschutz – Statistik, Register und Forschung – Datenschutz und Forschung im Allgemeinen).

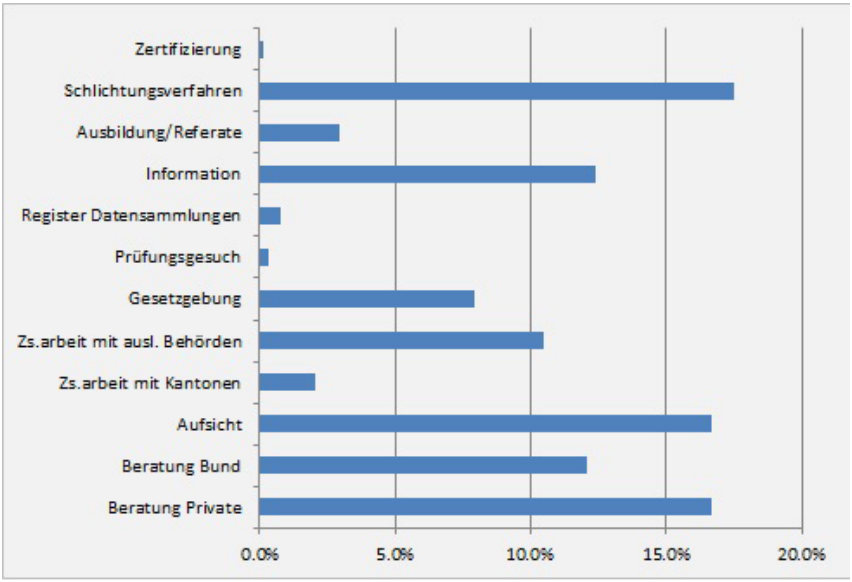
Die medizinische Forschung ist ganz besonders auf Informationen angewiesen, mit deren Hilfe die betroffenen Personen identifiziert werden können und erfüllt in der Regel ein wichtiges öffentliches und/oder privates Interesse. Da dabei besonders schützenswerte Personendaten bearbeitet werden, ist es verständlich, dass Menschen zögern, gegenüber Dritten Angaben zu ihrer Gesundheit zu machen. (www.derbeauftragte.ch, Datenschutz – Statistik, Register und Forschung – Medizinische Forschung).

Für Firmen, die ihre Mitarbeitenden die eigenen mobilen Geräte für ihre Arbeit nutzen lassen («Bring Your Own Device», kurz BYOD), stehen Vorteile wie Kostenteilung, Erreichbarkeit oder Gerätekenntnisse im Vordergrund, doch ergeben sich aus datenschutzrechtlicher Sicht für beide Seiten verschiedene Probleme. Einerseits besteht die Gefahr, dass der Arbeitgeber Zugriff auf persönliche Daten des Arbeitnehmenden erhält, wenn diese nicht klar von seiner geschäftlichen Tätigkeit getrennt sind. Andererseits das Risiko, dass unbefugte Dritte Zugriff auf Geschäftsdaten erhalten, wenn das Gerät in der Freizeit z.B. von Familienmitgliedern genutzt wird. Auch die Gefahr des Verlusts oder Missbrauchs von geschäftlichen Daten kann durch die private Nutzung höher sein (www.derbeauftragte.ch, Datenschutz – Arbeitsbereich – Bring Your Own Device).

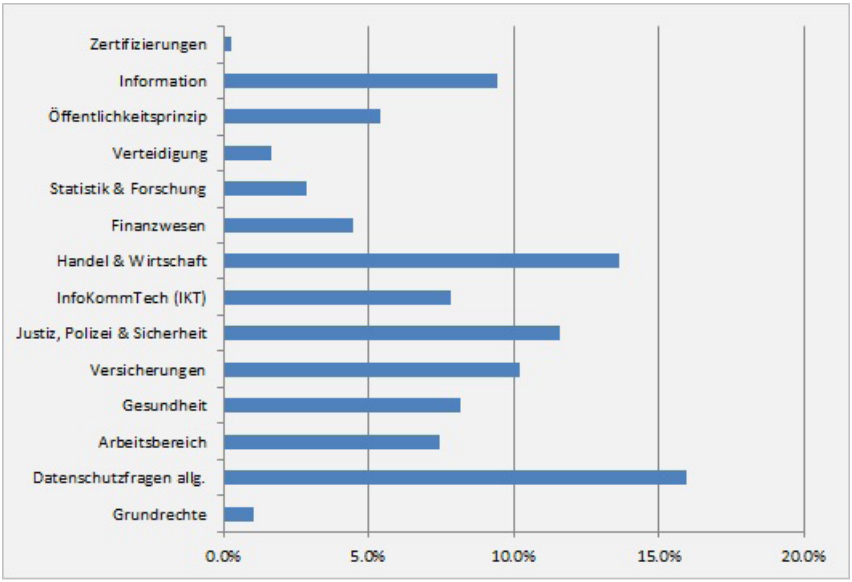
Auf unserer Website befindet sich schliesslich auch ein neues Merkblatt zum datenschutzkonformen Betrieb von Zutrittskontrollsystemen in Freizeitanlagen, die neben Skistationen auch von Tennisclubs, Fitnesscentern und anderen Freizeitanbietern betrieben werden. Auf unserem Merkblatt erfahren Sie, welche Daten erhoben werden dürfen, wer Zugang zu ihnen haben darf, zu welchem Zweck die Daten verwendet werden dürfen usw. (www.derbeauftragte.ch, Datenschutz – Dokumentation – Merkblätter – Zutrittskontrollsysteme in Freizeitanlagen).

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

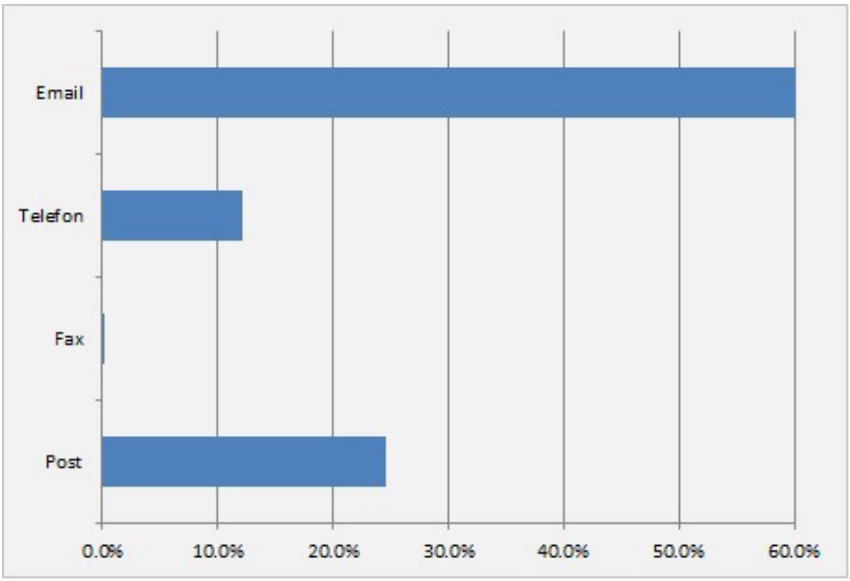
Aufwand nach Aufgabengebiet



Aufwand nach Sachgebiet



Herkunft der Anfragen



3.4 Statistik über die bei den Departementen eingereichten Zugangsgesuche nach Art. 6 des Öffentlichkeitsgesetzes (Zeitraum: 1. Januar 2014 bis 31. Dezember 2014)

Departement	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt / aufgeschoben	Zugangsgesuch hängig	Zugangsgesuch zurückgezogen
BK	18	12	2	4	0	0
EDA	101	87	8	6	0	0
EDI	95	31	22	30	10	2
EJPD	67	23	21	20	2	1
VBS	33	8	13	11	1	0
EFD	71	41	12	16	0	2
WBF	84	37	24	20	0	3
UVEK	106	58	20	17	4	7
Total 2014 (in %)	575 (100 %)	297 (51 %)	122 (21 %)	124 (22 %)	17 (3 %)	15 (3 %)
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 %)	-	-

Bundeskanzlei BK

Betroffener Fachbereich	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt / aufgeschoben	Zugangsgesuch hängig	Zugangsgesuch zurückgezogen
BK	9	4	2	3	0	0
EDÖB	9	8	0	1	0	0
Total	**18**	**12**	**2**	**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	101	87	8	6	0	0
Total	**101**	**87**	**8**	**6**	**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	14	4	4	5	0	1
EBG	0	0	0	0	0	0
BAK	3	2	0	1	0	0
BAR	2	2	0	0	0	0
METEO CH	0	0	0	0	0	0
NB	0	0	0	0	0	0
BAG	32	9	8	11	4	0
BFS	6	2	0	4	0	0
BSV	10	5	2	2	1	0
BLV	6	1	2	3	0	0
SNM	0	0	0	0	0	0
SWISS-MEDIC	21	5	6	4	5	1
SUVA	1	1	0	0	0	0
Total	**95**	**31**	**22**	**30**	**10**	**2**

Eidgenössisches Justiz- und Polizeidepartement EJPD

Betroffener Fachbereich	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt / aufgeschoben	Zugangsgesuch hängig	Zugangsgesuch zurückgezogen
GS	7	2	1	2	2	0
BJ	3	2	1	0	0	0
FEDPOL	8	3	2	3	0	0
METAS	2	1	0	1	0	0
BFM	33	9	14	10	0	0
SIR	7	2	1	4	0	0
IGE	3	2	1	0	0	0
ESBK	2	2	0	0	0	0
ESchK	0	0	0	0	0	0
RAB	1	0	1	0	0	0
ISC	1	0	0	0	0	1
NKVF	0	0	0	0	0	0
Total	**67**	**23**	**21**	**20**	**2**	**1**

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	10	3	3	4	0	0
Verteidig. / Armee	2	2	0	0	0	0
NDB	13	2	4	6	1	0
armasuisse	7	0	6	1	0	0
BASPO	1	1	0	0	0	0
BABS	0	0	0	0	0	0
Total	**33**	**8**	**13**	**11**	**1**	**0**

Eidgenössisches Finanzdepartement EFD

Betroffener Fachbereich	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt / aufgeschoben	Zugangsgesuch hängig	Zugangsgesuch zurückgezogen
GS	9	6	2	1	0	0
ISB	3	1	0	2	0	0
EFV	0	0	0	0	0	0
EPA	3	2	1	0	0	0
ESTV	12	4	4	2	0	2
EZV	7	4	2	1	0	0
EAV	0	0	0	0	0	0
BBL	3	2	0	1	0	0
BIT	2	2	0	0	0	0
EFK	28	18	1	9	0	0
SIF	2	0	2	0	0	0
PUBLICA	0	0	0	0	0	0
ZAS	2	2	0	0	0	0
TOTAL	**71**	**41**	**12**	**16**	**0**	**0**

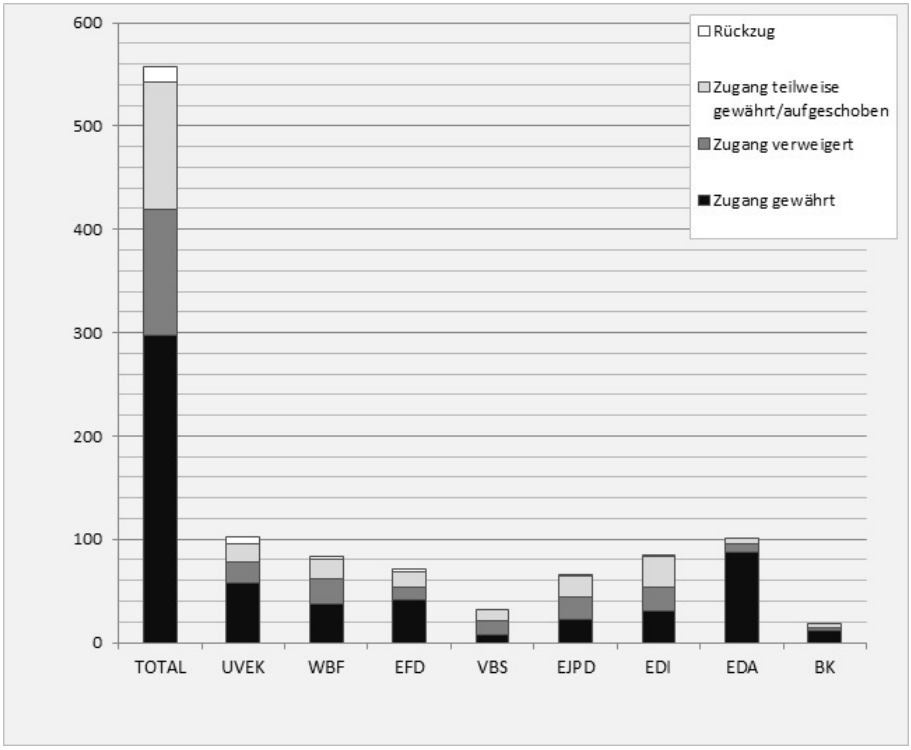
Eidgenössisches Departement für Wirtschaft, Bildung und Forschung WBF

Betroffener Fachbereich	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt / aufgeschoben	Zugangsgesuch hängig	Zugangsgesuch zurückgezogen
GS	2	1	1	0	0	0
SECO	20	4	12	4	0	0
SBFI	8	4	3	1	0	0
BLW	25	10	5	10	0	0
BWL	0	0	0	0	0	0
BWO	0	0	0	0	0	0
PUE	0	0	0	0	0	0
WEKO	13	8	0	3	0	2
ZIVI	2	1	0	1	0	0
BFK	2	1	0	1	0	0
SNF	0	0	0	0	0	0
EHB	0	0	0	0	0	0
ETH Rat	12	8	3	0	0	1
Total	**84**	**37**	**24**	**20**	**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	8	5	1	2	0	0
BAZL	14	2	7	4	1	0
BFE	12	8	2	1	0	1
ASTRA	6	3	0	1	0	2
BAKOM	11	8	2	4	0	3
BAFU	31	25	2	4	0	0
ARE	1	0	0	1	0	0
ComCom	1	1	0	0	0	0
ENSI	17	2	5	4	2	4
PostCom	1	0	1	0	0	0
UBI	4	4	0	0	0	0
Total	**106**	**58**	**20**	**17**	**4**	**7**

Behandlung der Zugangsgesuche



3.5 Statistik über die bei der Bundesanwaltschaft eingereichten Zugangsgesuche nach Art. 6 des Öffentlichkeitsgesetzes (Zeitraum: 1. Januar 2014 bis 31. Dezember 2014)

Bundesanwaltschaft BA

Betroffener Fachbereich	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt / aufgeschoben	Zugangsgesuch hängig	Zugangsgesuch zurückgezogen
BA	6	5	1	0	0	0
Total	**6**	**5**	**1**	**0**	**0**	**0**

3.6 Statistik über die bei den Parlamentsdiensten eingereichten Zugangsgesuche nach Art. 6 des Öffentlichkeitsgesetzes (Zeitraum: 1. Januar 2014 bis 31. Dezember 2014)

Parlamentsdienste PD

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

3.7 Anzahl Schlichtungsgesuche nach Kategorien der Antragsteller (Zeitraum: 1. Januar 2014 bis 31. Dezember 2014)

Kategorie Antragsteller	**2014**
Medien	44
Privatpersonen (bzw. keine genaue Zuordnung möglich)	19
Interessenvertreter (Verbände, Organisationen, Vereine usw.)	9
Rechtsanwälte	7
Unternehmen	8
Universitäten	1
Gemeinwesen	2
Total	**90**

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:	6 Personen (davon 2 Praktikantinnen)
Kanzlei:	2 Personen