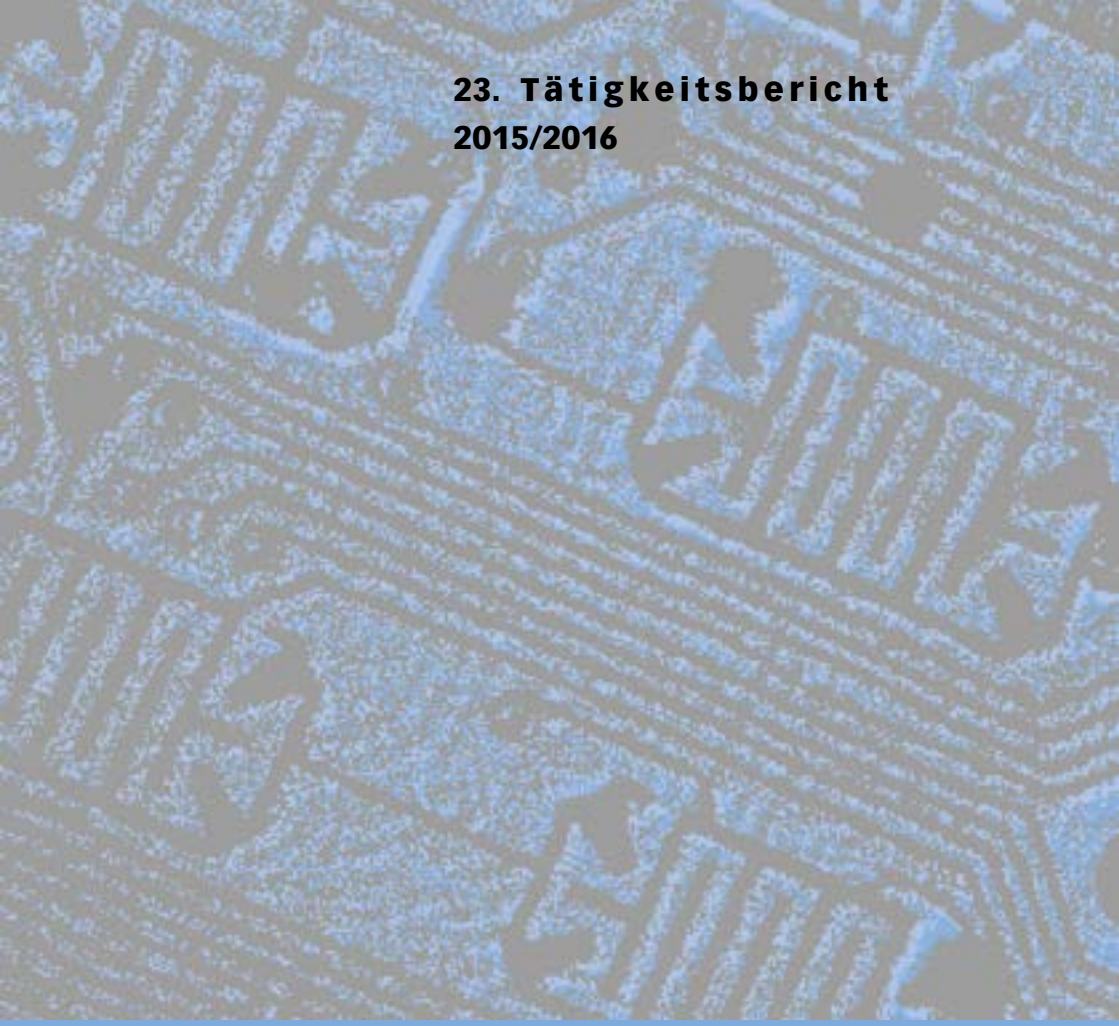


23. Tätigkeitsbericht 2015/2016

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Tätigkeitsbericht 2015/2016 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 2015 und 31. März 2016 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.bundespublikationen.admin.ch

Art.-Nr. 410.023.d/f

Inhaltsverzeichnis

Vorwort

Vor zehn Jahren, am 1. Juli 2006, ist das Öffentlichkeitsgesetz in Kraft getreten. Dieses Gesetz sollte eine entscheidende Rolle für das Funktionieren unseres Rechtsstaates spielen. Ziel war es, die Transparenz über den Auftrag, die Organisation und die Tätigkeit der Verwaltung zu fördern, indem es insbesondere den Zugang zu amtlichen Dokumenten gewährleistet. Transparente Entscheidungsprozesse in der Verwaltung tragen dazu bei, das Vertrauen der Bürgerinnen und Bürger in die öffentlichen Institutionen zu stärken. Das Öffentlichkeitsgesetz (BGÖ) trägt somit – genauso wie das Bundesgesetz über den Datenschutz – zum reibungslosen Funktionieren eines demokratischen Staates bei, in dem die grundlegenden Rechte und Freiheiten geachtet werden. Der Gesetzgeber hat deshalb zu Recht den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten damit beauftragt, die Anwendung der Gesetzesbestimmungen mittels Schlichtungsverfahren zu überwachen.

Die Umsetzung des Gesetzes verlief nicht ganz reibungslos. Es galt und gilt auch heute noch, gegen die Vorbehalte gewisser Behörden bezüglich der Bearbeitung der eingereichten Zugangsgesuche anzukämpfen. Zudem neigen Verwaltungen dazu, ohne weitere Abklärungen und ohne Begründung auf die im BGÖ aufgeführten Ausnahmebestimmungen zu verweisen. Unbefriedigend sind ausserdem die teils zu hohen Gebühren, die Personen davon abhalten, ein Zugangsgesuch einzureichen. Obschon der vom Gesetzgeber angestrebte Paradigmenwechsel immer stärker zum Tragen kommt, stellen sich bestimmte Interessenvertreter nach wie vor quer und versuchen, die Tragweite des Öffentlichkeitsprinzips mit spezialgesetzlichen Bestimmungen einzuschränken; dies insbesondere indem zusätzliche Ausnahmen für die Aufsichtstätigkeiten bestimmter Behörden eingeführt oder gewisse Typen amtlicher Dokumente vom BGÖ ausgeschlossen werden.

Angesichts der unrealistischen Fristen und der ungenügenden Ressourcen ist das reibungslose Durchführen der Schlichtungsverfahren nach wie vor eine Knacknuss für den Beauftragten. Derzeit wird das Öffentlichkeitsgesetz überarbeitet, wobei sich zeigen wird, wie ernst es der Verwaltung tatsächlich mit der Transparenz der Behörden ist. Es ist zu hoffen, dass im Rahmen der Revision die oben genannten Kinderkrankheiten des Gesetzes behoben werden und der Bundesrat zusätzliche Ressourcen zur Verfügung stellen wird, damit die Schlichtungsverfahren innert einer für die Zugangsgesuchsteller nützlichen Frist durchgeführt werden können.

Seit seinem Inkrafttreten hat das Öffentlichkeitsgesetz deutlich an Bekanntheit gewonnen. Die Anzahl der bei der Bundesverwaltung eingereichten Auskunftsbegehren und der beim Beauftragten eingegangenen Schlichtungsanträge steigt ständig. Das Gesetz erlaubt den Bürgerinnen und Bürgern, selbst zu bestimmen, welche Informationen sie erhalten möchten. Die Verwaltung entscheidet nicht mehr alleine,

was öffentlich gemacht wird. Heute sind die Bundesbehörden beispielsweise verpflichtet, bei Anfragen zur Verwendung der Steuern, zu gescheiterten Informatikprojekten oder zu Korruptionsaffären Auskunft zu erteilen und Dokumente vorzulegen. Das Öffentlichkeitsprinzip ist damit zu einem griffigen Instrument der Gesellschaft geworden.

2016 ist ein Schlüsseljahr für den Datenschutz: Zum einen wird in der Europäischen Union demnächst die neue Datenschutzgrundverordnung verabschiedet. Danach werden in allen Ländern der Europäischen Union und des Europäischen Wirtschaftsraums die gleichen Datenschutzbestimmungen gelten. Die Verordnung wird die Rechte der betroffenen Personen stärken und die Transparenz bei der Datenbearbeitung erhöhen. Zudem sieht sie strengere Pflichten für Datenbearbeiter vor sowie einen Ausbau der Umsetzungsmechanismen und der Zusammenarbeit zwischen den Datenschutzbehörden. Zum anderen wird die Revision des Übereinkommens 108 des Europarats abgeschlossen. Das neue Übereinkommen soll ebenfalls die Rechte der betroffenen Personen stärken und die Effektivität des Datenschutzes erhöhen. Um diese Ziele zu erreichen, werden die Pflichten für die Datenbearbeiter verschärft, die Zuständigkeiten und Befugnisse der Datenschutzbehörden sowie die Mechanismen für die Umsetzung des Übereinkommens ausgebaut.

Diese Reformen werden unweigerlich Auswirkungen auf die anstehende Revision des Bundesgesetzes über den Datenschutz (DSG) haben. Im Interesse der betroffenen Personen, aber auch der Ämter und der Unternehmen, die Daten bearbeiten, also im Interesse des Wirtschaftsplatzes Schweiz, erwarte ich, dass die Bestimmungen des Übereinkommens 108 im Rahmen der Totalrevision des DSG umgesetzt werden und dass zumindest eine starke Annäherung an den gesetzlichen Rahmen der Europäischen Union erfolgt, sofern dieser nicht direkt übernommen wird. Zudem erwarte ich, dass die Revision zu einer effektiven Stärkung des Rechts auf informationelle Selbstbestimmung führt und dass alle Bürgerinnen und Bürger selbst über ihre Daten bestimmen können. Dazu ist eine Ausweitung der Rechte der betroffenen Personen sowie die Einführung von Sammelklagen erforderlich. Die Umkehr der Beweislast, eine objektive Verantwortung für die Datenbearbeitung und Pflichten für die Datenbearbeitungsverantwortlichen, insbesondere die Pflicht, die Gesetzesbestimmungen einzuhalten, Datenschutzverstösse zu melden, Risiken zu evaluieren und Datenschutztechnologien zu nutzen, sind weitere Anliegen.

Mit der Gesetzesrevision sollten zudem die Kompetenzen und die Mittel des Beauftragten, insbesondere für Sachverhaltsabklärungen, erweitert werden. Das Strafmass im Falle einer Rechtsverletzung sollte abschreckend wirken. Datenbearbeitungen, die zu starken Eingriffen in die Privatsphäre führen, müssten strengen Bedingungen unterliegen, etwa einer vorherigen Genehmigung oder einer Zertifizierungspflicht. Dabei denke ich insbesondere an die Verwendung von Big Data

für das *Predictive Profiling* von Personen, aber auch an die Bearbeitung von Daten zur Personenüberwachung, insbesondere mittels invasiver Technologien wie etwa Drohnen oder biometrische Systeme. In einer Welt, in der sich Daten weder an das Souveränitäts- noch an das Territorialitätsprinzip halten, sollten die einzelnen Datenschutzsysteme keinesfalls zu stark voneinander abweichen. Die Schweiz hat ein Interesse daran, eine führende Rolle im Bereich der Datenbearbeitung und -aufbewahrung einzunehmen. So werden die Voraussetzungen für eine moderne Gesellschaft geschaffen, die offen für Fortschritt und technologische Innovation ist und gleichzeitig die grundlegenden Rechte und Freiheiten der Bürgerinnen und Bürger wahrt.

Ich setze mich für einen weltweit bindenden Rechtsrahmen ein. Ein wichtiger Schritt in diese Richtung kann mit der laufenden Revision des Übereinkommens 108 des Europarats gemacht werden und indem Staaten, die nicht Mitglied des Europarats sind, das Übereinkommen ratifizieren. In seinem Urteil vom 4. Oktober 2015 hält der Gerichtshofs der Europäischen Union fest, dass die «Safe Harbor»-Regelung angesichts des massiven und unkontrollierten Zugriffs der amerikanischen Behörden auf Daten, die amerikanischen Unternehmen übermittelt wurden, keinen angemessenen Schutz bietet. Dies verdeutlicht, wie wichtig ein breit abgestütztes System zur Gewährleistung des Datenschutzes bei der Weitergabe von Daten an Staaten ohne angemessenes Schutzniveau ist. Der Entscheid macht die Notwendigkeit eines globalen Datenschutzinstruments deutlich. Die Schaffung eines UNO-Sonderberichterstatters zur Überwachung des Rechts auf Privatsphäre dürfte zum Erreichen dieses Ziels beitragen.

Die Anpassung unseres Rechtsrahmens ist unumgänglich, allein aber nicht ausreichend. Die gesetzlichen Anforderungen müssen in den verschiedenen betroffenen Sektoren umgesetzt (Verhaltenskodex) und in die Informationssysteme und die Kommunikationstechnologien implementiert werden. Das Prinzip der datenschutzfreundlichen Voreinstellungen («privacy by default») sollte Standard werden. Technologisch ist dies kein Problem, gewisse Unternehmen sträuben sich jedoch dagegen. Daher plädiere ich dafür, dass die Politik echte Anreize für die Entwicklung und Nutzung datenschutzfreundlicher Technologien schafft. Mit solchen Technologien, insbesondere durch die Verwendung sicherer Datenverschlüsselungssysteme ohne «Hintertür», kann das Vertrauen der betroffenen Personen gewonnen werden. Die Sicherheit der Systeme ist auch für die Bekämpfung der Kriminalität wichtig.

Parallel dazu müssen Schulungsangebote im Bereich der digitalen Kompetenz zum festen Bestandteil nationaler Programme für sämtliche Bevölkerungsschichten werden. Nur wer die Technologie beherrscht und sich der damit verbundenen Vorteile und Risiken bewusst ist, kann sie Technologie verantwortungsvoll und kompetent nutzen.

Unsere Gesellschaft steht an einem Scheideweg: Der digitale und quantifizierte Mensch, die künstliche Intelligenz, das Internet der Dinge, das Aufkommen intelligenter Autos und Roboter, kontaktloses Bezahlen und das Verschwinden des Bargelds, die Auswertung von Big Data sowie die Verhaltensprofilierung und das *Predictive Profiling* sind allesamt Trends, die sich sowohl positiv als auch negativ auswirken können. Wenn ich lese, dass in Schweden eine Person alles, was sie in ihrer Tasche hat (Schlüssel, Mobiltelefon, Portemonnaie, Bankkarte), digitalisieren und auf einen Chip laden möchte, der ihr eingepflanzt wird, mache ich mir Sorgen um unsere liberale und demokratische Gesellschaft. Sie scheint sich – in den meisten Fällen mit unserer unbewussten Mitwirkung – in eine Überwachungsgesellschaft zu verwandeln, die zur Entmündigung und Manipulation der Menschen führt und somit das Ende der individuellen Freiheit und des freien Willens bedeutet. Wenn die neuen technologischen Entwicklungen die grundlegenden Werte der Gesellschaft, die Menschenrechte und insbesondere das Recht auf Würde und Nichtdiskriminierung nicht respektieren, besteht die Gefahr, dass sie rasch unwiderrufliche Schäden verursachen und in eine neue Form der Diktatur mündet. Die digitale Gesellschaft muss demokratisch bleiben und die grundlegenden Rechte und Freiheiten wahren.

Es müssen umgehend Verhaltensregeln definiert werden, damit nicht Algorithmen darüber entscheiden, was gut für uns ist. Die Zeit drängt, um die Grundlagen für eine Welt zu schaffen, in der die Technologie dem Wohl der Menschheit dient! Die Grundrechte in der digitalen Welt müssen über einen neuen Sozialvertrag sichergestellt werden, der auf Vertrauen und Zusammenarbeit der Menschen beruht. Zu diesem Zweck muss ein Gesetzesrahmen geschaffen werden, der dafür sorgt, dass die technologische Entwicklung das demokratische System respektiert und das Recht auf Datenschutz effektiv angewendet wird. Die Revision des DSG ist eine Chance, die genutzt werden muss, um dieses Ziel zu erreichen. Sie muss zum Anlass genommen werden, um eine breit angelegte demokratischen Debatte über die digitale Gesellschaft in der Schweiz zu führen.

Jean-Philippe Walter
Beauftragter ad interim

1. Datenschutz

1.1 Grundrechte

1.1.1 Datenschutz bei Unterschriftensammlungen

Wer Unterschriften für eine Volksinitiative oder ein Referendum sammelt, darf die erhalten Personendaten nur unter gewissen Voraussetzungen bearbeiten. So ist ihre Verwendung für den Versand eines Informationsschreibens o.Ä. nur zulässig, wenn die betroffene Person frei und ausdrücklich eingewilligt hat.

Die Abteilung für politische Rechte in der Bundeskanzlei bat uns im Berichtsjahr, die datenschutzrechtlichen Anforderungen zu erläutern, die gelten, wenn bei einer Unterschriftensammlung für eine Initiative oder ein Referendum erhobene Personendaten zu anderen Zwecken verwendet werden.

Bei einer solchen Unterschriftensammlung findet eine Bearbeitung von Personendaten statt, die dem Bundesgesetz über den Datenschutz (DSG) und seinen allgemeinen Grundsätzen unterliegt. Die bei der Ausübung der politischen Rechte gewonnenen Daten sind als besonders schützenswert im Sinne des DSG zu betrachten, da sie Angaben zu den politischen Meinungen oder Betätigungen der betroffenen Personen enthalten. Das DSG verlangt bei diesen Daten eine besonders strenge Anwendung der allgemeinen Datenschutzgrundsätze.

Die Unterstützung eines Referendums oder einer Volksinitiative beinhaltet eine Erhebung und Bearbeitung von Personendaten im Sinne des Gesetzes über die politischen Rechte, wobei dies im Wesentlichen die Prüfung der Gültigkeit der Unterschrift betrifft. Wenn eine Person mit ihrer Unterschrift ein Referendum oder eine Volksinitiative unterstützt, muss sie hingegen nicht mit der Verwendung ihrer Daten für den Versand von Informationen oder für Spendenkampagnen rechnen (Zweckbindungsprinzip). Eine solche Verwendung von Personendaten erfordert einen (neuen) Rechtfertigungsgrund, und zwar das Einverständnis der betroffenen Person, ein überwiegendes privates oder öffentliches Interesse oder ein Gesetz. Im vorliegenden Fall kommt nur die Zustimmung der Unterzeichner als Rechtfertigung infrage, wenn ihre Daten zu einem anderen Zweck als der Unterstützung der Initiative verwendet werden sollen.

Damit eine Einwilligung gültig ist, muss die betroffene Person ihren Willen frei und nach vorgängiger Information äussern (freie und aufgeklärte Einwilligung). Bei besonders schützenswerten Daten oder Persönlichkeitsprofilen muss die Zustimmung überdies ausdrücklich erfolgen. Die Verwendung der im Rahmen der Initiative

gewonnenen Personendaten, die als besonders schützenswerte Daten zu erachten sind, zu anderen Zwecken erfordert demnach ein freies, aufgeklärtes und ausdrückliches Einverständnis.

In dem von der Bundeskanzlei konkret vorgelegten Fall befand sich auf dem Formular für die Unterschriftensammlung ein kleines Feld (rechts von der Unterschrift), das anzukreuzen war, falls der Unterzeichner die Verwendung seiner Daten für die Zusendung von Informationen nicht wünscht (Opt-out). Über diesem Feld stand in kleiner Schrift: «Schickt mir bitte keine weiteren Infos (ankreuzen)». Es stellte sich also insbesondere die Frage, ob ein fehlendes Kreuzchen unter dem Gesichtspunkt des DSG als gültiges Einverständnis zum Zusenden von Informationen angesehen werden konnte.

Unseres Erachtens entsprach die Art, in der die Zustimmung eingeholt wurde, nicht den Anforderungen des DSG. Zum einen waren die Informationen bezüglich der Verwendung dieser besonders schützenswerten Daten nicht ausreichend klar. Zum anderen kann das Fehlen eines angekreuzten Feldes hier nicht als Einwilligung gelten, da die Bearbeitung von besonders schützenswerten Daten ein ausdrückliches Einverständnis erfordert. Die neben Namen und Adresse angebrachte Unterschrift bezieht sich nur auf die Unterstützung der betreffenden Initiative oder des fraglichen Referendums und nicht auf eine andere Verwendung der Personendaten.

Zudem halten wir auch ein anzukreuzendes Opt-in-Feld vor der Unterschrift nicht für geeignet, um Missbrauchsrisiken zu vermeiden, da ein solches Feld leicht von einer Drittperson angekreuzt werden kann. Diese Variante ist somit weder sicher noch datenschutzkonform. Tatsächlich macht es der Sicherheitsgrundsatz erforderlich, dass Personendaten durch angemessene organisatorische und technische Massnahmen gegen jegliche unerlaubte Bearbeitung geschützt werden. In diesem Kontext raten wir den Initiativ- oder Referendumskomitees, ein Vorgehen zu wählen, das gewährleistet, dass die betroffenen Personen der Verwendung ihrer Daten frei, ausdrücklich und nach vorgängiger Information zugestimmt haben. Eine Möglichkeit wäre es, die Einwilligung auf einem separaten Blatt oder mittels einer weiteren Unterschrift einzuholen.

1.1.2 Verwendung der AHV-Nummer als universelle Identifikationsnummer

Im Berichtsjahr haben wir den Bundesrat um eine Grundsatzentscheidung bezüglich der generellen Verwendung der AHV-Nummer ausserhalb des Sektors der Sozialversicherungen ersucht. Wir sind der Auffassung, dass nur eine sektoreigene Nummer in der Lage ist, die Risiken einer missbräuchlichen Datenverknüpfung zu begrenzen.

Am Rande unserer Mitwirkung an einer Arbeitsgruppe, die damit beauftragt war, die Ausarbeitung von Rechtsgrundlagen für die Verwendung eines administrativen Personenidentifikators im Bereich E-Government zu prüfen (vgl. unseren 22. Tätigkeitsbericht, Ziffer 1.1.7), haben wir beim Vorsteher des Eidgenössischen Departements des Innern (EDI) unsere Bedenken bezüglich der generellen Verwendung der AHV-Nummer ausserhalb des Sozialversicherungssektors angemeldet.

Angesichts der besorgniserregenden Entwicklung auf diesem Gebiet und der daraus entstehenden Risiken für die Privatsphäre der betroffenen Personen schien es uns angebracht, den Bundesrat auf diese Problematik aufmerksam zu machen. Wir haben ihn gebeten, sich klar für oder gegen die systematische Verwendung der AHV-Nummer ausserhalb des Sozialversicherungssektors auszusprechen beziehungsweise eine gesetzgeberische Überprüfung dieser Bestimmung zu erwägen, um ihren Geltungsbereich einzuschränken.

Das Bundesamt für Sozialversicherungen (BSV) wurde beauftragt, ein Aussprachepapier für den Bundesrat zu verfassen. In der Ämterkonsultation wiesen wir darauf hin, dass sich das Papier auf Vorschläge für Abänderungen des AHV-Gesetzes beschränke, mit denen die Bedingungen für die Verwendung der AHV-Nummer bei der Ausführung des kantonalen Rechts genauer festgelegt werden sollen (Status quo plus). Zudem bringe es keine echte Lösung zur Begrenzung der zunehmenden Verwendung der AHV-Nummer ausserhalb der Sozialversicherungen. Die empfohlenen Lösungen stellen den weit reichenden Einsatz dieser Nummer nicht in Frage. Wir erinnerten auch daran, dass ohne Massnahmen zur kontrollierten Verwendung dieser Nummer Zweifel an deren Verlässlichkeit aufkommen könnten.

Der Bundesrat nahm Kenntnis vom Aussprachepapier und beauftragte das EDI, die Frage der Verwendung der AHV-Nummer eingehender zu prüfen, insbesondere die Möglichkeit ihrer Verwendung als eindeutige Identifikationsnummer für den Bereich E-Government, und dem Bundesrat das Ergebnis seiner Analyse und die weiteren Arbeiten bis zum ersten Halbjahr 2016 zu unterbreiten.

Wir sind der Auffassung, dass nur eine sektoreigene Nummer in der Lage wäre, die Risiken einer missbräuchlichen Datenverknüpfung zu begrenzen und gleichzeitig den Bedürfnissen der Verwaltung und der Bürger zu entsprechen (hinsichtlich Richtigkeit der Daten, fehlende Verwechslungsgefahr, Qualität der Daten, usw.), da sie über die gleichen Funktionalitäten verfügt wie die AHV-Nummer. Im Gegensatz zu der von manchen vertretenen Meinung ist eine sektorielle Nummer leicht einzurichten und wenig kostspielig. Wie wir feststellten, wurde in mehreren Bereichen eine solche Nummer eingeführt, so etwa bei der elektronischen Patientenakte. Dies weil die Risiken richtig erkannt wurden und man mit ihr ein besseres Gleichgewicht zwischen dem Schutz der Privatsphäre und den Bedürfnissen der Verwaltung anstrebt. Zudem ist es im Zeitalter von Big Data und der Internet-Kriminalität unumgänglich,

die massive Verwendung der AHV-Nummer als Identifikator von Grund auf neu zu überdenken und in einer umfassenderen Betrachtungsweise als derjenigen der Bundesverwaltung oder der Kantone zu beleuchten.

1.1.3 Nationales Adressregister

Wir gehören einer Arbeitsgruppe an, die mit der Prüfung verschiedener Varianten für die Umsetzung des geplanten nationalen Adressregisters für die öffentlichen Verwaltungen betraut ist. Dabei geht es um die Analyse der vorgeschlagenen Lösungen, namentlich ihrer Realisierbarkeit, ihrer Kompatibilität mit dem Datenschutz, ihrer Kosten und ihrer Folgen.

Nach dem Verzicht auf einen automatischen Adressenaustausch zwischen der Post und den Einwohnerkontrollen prüft der Bundesrat derzeit die Möglichkeit der Schaffung eines zentralen Adressregisters für die Behörden. Mehrere Lösungsvarianten sind möglich. Das Zentralregister liesse sich im Rahmen der bestehenden staatlichen Strukturen einrichten: die Datenbank könnte durch die vorhandenen kantonalen Plattformen aufgebaut werden oder auf Plattformen des Bundes basieren, wie etwa die Datenbank für Bevölkerungsstatistik oder die von der Ausgleichszentrale der AHV betriebene Datenbank UPI (Unique Person Identification).

Der Bundesrat hat das Eidgenössische Justiz- und Polizeidepartement beauftragt, diese Varianten genauer zu untersuchen, namentlich ihre Realisierbarkeit, ihre Kompatibilität mit dem Datenschutz, ihre Kosten und ihre Folgen. Wir gehören der Arbeitsgruppe an, die zur eingehenden Prüfung der vorgeschlagenen Varianten eingesetzt wurde. Die Untersuchung begann mit einer Analyse der technischen Realisierbarkeit. Die Überlegungen werden mit der rechtlichen Prüfung der gewählten Varianten fortgesetzt. Wir werden uns weiter aktiv einbringen, um sicherzustellen, dass die Datenschutzanforderungen im Rahmen dieses Vorhabens berücksichtigt werden.

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

Während des Ämterkonsultationsverfahrens konnten wir Stellung nehmen zu zwei neuen Bestimmungen der Verordnung über die Krankenversicherung (KVV). Diese regeln die Details der Erhebung, Bearbeitung, Weitergabe und Veröffentlichung von Daten im Rahmen des Projekts MARS (Statistiken der ambulanten Gesundheitsversorgung).

Zur Erinnerung sei erwähnt, dass das Bundesamt für Statistik (BFS) aufgrund des Bundesstatistikgesetzes beauftragt ist, Statistiken von allgemeinem Interesse zu produzieren. Im Gesundheitsbereich hat das BFS die spezifische Aufgabe, die für die Prüfung der Funktionsweise und der Wirkungen des Bundesgesetzes über die Krankenversicherung (KVG) notwendigen statistischen Grundlagen zu erstellen. Die eidgenössischen statistischen Erhebungen müssen auf die ambulante Medizin ausgeweitet werden, damit Daten betreffend den Umfang der Versorgung in diesem Bereich, die Gründe für die Inanspruchnahme dieser Dienstleistungen (Diagnose) sowie die Leistungen und Kosten des ambulanten Sektors gewonnen werden können. Das BFS führt auch Erhebungen bei den Leistungserbringern durch, damit den von Gesetzes wegen mit der Aufsicht betrauten Stellen Daten übermittelt werden können.

Gemäss Artikel 59a KVG (beziehungsweise ehemals Art. 22a Absatz 4 KVG) erlässt der Bundesrat nähere Vorschriften zur Erhebung, Bearbeitung, Weitergabe und Veröffentlichung der Daten unter Wahrung des Verhältnismässigkeitsprinzips. Wir haben immer wieder auf der Notwendigkeit einer raschen Umsetzung dieses Artikels bestanden. Im Dezember 2014 legten uns das Bundesamt für Gesundheit (BAG) und das BFS den Entwurf der neuen Verordnungsbestimmungen (KVV) vor. Im Anschluss an ein Gespräch, das wir mit dem BAG, dem BFS und dem Bundesamt für Justiz (BJ) führten, wurde der Entwurf überarbeitet und danach im März 2015 in die Ämterkonsultation gegeben.

Unsere Stellungnahmen betrafen namentlich die Kategorien der bearbeiteten Daten, den Begriff der Datenverknüpfung und der Pseudonymisierung; wir brachten auch Bemerkungen zur Erwähnung der Datenempfänger und zur Angabe einer Aufbewahrungsfrist an. Überdies erinnerten wir daran, dass die im Rahmen des Projekts MARS durchgeführte Datenbearbeitung das Verhältnismässigkeitsprinzip einhalten und die Anonymität der Patienten gewährleisten muss.

Parallel zu den Änderungen an der KVV ist das BFS dabei, ein Bearbeitungsreglement zu erstellen; dieses regelt die technischen Aspekte der Verwendung der AHV-Nummer, der Datenverknüpfungen, der Pseudo- und Anonymisierung sowie des kryptologischen Verfahrens und des Key Management. Angesichts der besonderen Schutzwürdigkeit der erhobenen Personendaten verfolgen wir die Entwicklung des Projekts weiterhin mit grosser Aufmerksamkeit und achten darauf, dass die Datenschutzanforderungen vollumfänglich eingehalten werden.

1.1.5 Stellungnahme zu den rechtlichen Rahmenbedingungen von Open Government Data

Das Bundesarchiv hat uns im Rahmen einer Ämterkonsultation gebeten, zur Frage der rechtlichen Rahmenbedingungen für Open Government Data (OGD) aus datenschutzrechtlicher Perspektive Stellung zu nehmen.

Am 16. April 2014 hat der Bundesrat die OGD-Strategie Schweiz 2014-2018 verabschiedet. Diese wurde unter der Federführung des Informatiksteuerungsorgans des Bundes erarbeitet. Seit Anfang 2015 ist das Bundesarchiv federführend für die Umsetzung der OGD-Strategie und erarbeitet die notwendigen konzeptionellen Grundlagen. In diesem Rahmen wurden wir gebeten, zur Frage der datenschutzrechtlichen Rahmenbedingungen für OGD Stellung zu nehmen.

In OGD-Portalen werden typischerweise Sachdaten oder aggregierte und anonymisierte Daten publiziert. Unter Umständen kann jedoch die Abgrenzung zu Personendaten schwierig sein. In unserer Stellungnahme haben wir auf diese Problematik aufmerksam gemacht.

Keine anonymisierten Daten liegen beispielsweise dann vor, wenn zwar vordergründig keine direkt identifizierbaren Merkmale vorhanden sind, der Personenbezug aber ohne grossen Aufwand (zum Beispiel von Dritten) wieder hergestellt werden kann – insbesondere durch Verknüpfung mit weiteren Daten. Diese Daten stellen Personendaten im Sinne des Datenschutzgesetzes dar und es sind insbesondere die Voraussetzungen über die Bearbeitung von Personendaten durch Bundesorgane zu beachten. Dasjenige Bundesorgan, welches das OGD-Portal betreibt, muss dabei durch technische und organisatorische Massnahmen sicherstellen, dass keine Personendaten publiziert werden. Falls ausnahmsweise doch Personendaten in der OGD-Umgebung veröffentlicht werden sollen, muss das verantwortliche Bundesorgan die erforderliche Rechtsgrundlage abklären.

Die technologische Entwicklung und die damit verbundenen Möglichkeiten zur De-Anonymisierung haben zur Folge, dass der Inhaber eines OGD-Portals regelmässig neu beurteilen muss, ob seine publizierten Daten immer noch als anonym gelten. OGD-Projekte müssen solche Überprüfungsverfahren entsprechend vorsehen. - Unsere Bemerkungen aus Sicht des Öffentlichkeitsprinzips finden Sie in Ziffer 2.3.3 des vorliegenden Tätigkeitsberichts.

1.1.6 Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes

Unser Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes ist terminologisch überarbeitet worden. Die Personendaten werden entsprechend ihrer Schutzwürdigkeit klassifiziert, sodass sie in angemessener Weise bearbeitet und geschützt werden können. Die Klassifizierung der Daten in drei Stufen ist mit der Klassifizierung des Informationsschutzes vergleichbar und lässt sich auf die technischen und organisatorischen Massnahmen übertragen.

Wir haben den Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes (der nun auch in englischer Sprache vorliegt) terminologisch aktualisiert: ausgehend von den gesetzlichen Begriffsbestimmungen oder den mit ihrer Bearbeitung verbundenen Risikostufen wurden die Personendaten je nach Art in «nicht-sensible», «sensible» und «hochsensible» Daten eingeteilt. Bezüglich der Risikostufe gehören die besonders schützenswerten Daten und Persönlichkeitsprofile im Sinne des Bundesgesetzes über den Datenschutz (Art. 3 Bst. c und d DSG) in die Risikostufe «hoch» (Klasse «sensibel»), während die nicht-sensiblen Personendaten in den Risikostufen «mittel» und «gering» (Klasse «nicht-sensibel») erfasst sind. Die Risikostufe «sehr hoch» (Klasse «hochsensibel») ihrerseits ist für Daten vorbehalten, deren Missbrauch das Leben oder die körperliche Integrität der betroffenen Personen gefährden kann.

Diese Klassifizierung ist nicht zu verwechseln mit der Einstufung des Informationsschutzes (intern / vertraulich / geheim), der auf den Schutz nationaler Interessen gemäss der Informationsschutzverordnung und dem künftigen Gesetz über die Informationssicherheit abzielt. Die Verwendung der Kennzeichnung «vertraulich» für Personendaten der Klasse «sensibel» ist unangebracht und unbedingt zu vermeiden. Die beiden Klassifizierungsarten weisen indessen Ähnlichkeiten auf, sodass eine Parallelanwendung der technischen und organisatorischen Schutzmassnahmen zusammen mit jeder Klassifizierungsstufe (nicht-sensibel / intern, sensibel / vertraulich, hochsensibel / geheim) einen Gewinn an Einfachheit, Wirksamkeit und Klarheit bedeutet.

Ab der Klasse «sensibel» bzw. «vertraulich» ist somit eine Verschlüsselung der Übertragung und Speicherung zwingend erforderlich. Dies gilt für alle Datenmanagement-Systeme, wie etwa die Systeme der elektronischen Geschäftsverwaltung (GEVER), aber auch für die zusätzlichen Lösungen mit automatischer Unterstützung der Daten-/Informationsklassifizierung oder die durch Cloud Computing entstehenden Möglichkeiten des Hosting von Daten, insbesondere von Big Data.

Schliesslich ist festzuhalten, dass das Erfordernis der Klassifizierung der Daten und Informationen integrierender Bestandteil der meisten internationalen Normen für die Informations- und Datensicherheit ist. Als Beispiele zu erwähnen sind die Massnahme A8.2 (Klassifizierung der Information) der Norm ISO/IEC 27001:2013 und die Zusatzmassnahme 8.4 (Schutz des Informationsaustausches) der Zusatznorm ISO/IEC 27010:2015 (Sektor- und organisationsübergreifende Kommunikationen), deren Anhang das 'Traffic Light Protocol (TLP)' beschreibt. Auch bei der Massnahme P02.3 ('Data Classification Scheme') des Frameworks ISACA/COBIT 5:2012 und dem Prozess OSP-21 ('Information Quality and Compliance Assessment') des Frameworks The Open Group/O-ISM3:2011 gilt dies. Die amerikanische Regierung steht dem in nichts nach mit ihrem 'National Institute of Standards and Technology (NIST)', dessen Sonderpublikation SP 800-53R4:2013 den Anhang J mit dem Titel 'Privacy Control Catalogue' enthält, in dem beispielsweise die Massnahme SE-1 ('Inventory of Personally Identifiable Information') definiert wird. Die Anleitung SP 800-122:2010 ist überdies ganz dem Schutz der Vertraulichkeit von Personendaten gewidmet und umschreibt namentlich die Stufen der Auswirkung (gering/mittel/hoch) auf die Vertraulichkeit von Personendaten, für die gerade die Schutzwürdigkeit der betreffenden Daten einen der bestimmenden Faktoren darstellt.

Das Vereinigte Königreich hat ausserdem ab dem 2. April 2014 ein neues Klassifizierungsmodell, genannt 'Government Security Classifications', eingeführt, deren Grundklassifizierung official die Untergruppe official-sensitive (ex confidential) umfasst, ergänzt durch die Deskriptoren :personal oder :commercial, um die Präsenz besonders schützenswerter Daten von natürlichen oder juristischen Personen zu bestimmen. Theoretisch lässt sich die Klassifizierung sogar auf jeden Absatz des in seiner Gesamtheit klassifizierten Dokuments anwenden. Dadurch wird eine computergestützte Anonymisierung denkbar, beispielsweise im Rahmen eines Zugangsgesuchs gemäss dem Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung.

Im Wesentlichen in die gleiche Richtung geht schliesslich auch die künftige Datenschutz-Grundverordnung der Europäischen Union mit ihrem Datenfokus: sie beinhaltet unter anderem die Meldepflicht bei Datenschutzverletzungen, eine Folgenabschätzung betreffend den Datenschutz, das Recht auf Vergessen, härtere (finanzielle) Sanktionen für missbräuchliche Bearbeitungen, sowie eine Aufforderung zur Zertifizierung und Kennzeichnung gewisser Bearbeitungsformen.

1.2 Datenschutzfragen allgemein

1.2.1 Sachverhaltsabklärung Swiss Pass

Ende 2015 führten wir eine Sachverhaltsabklärung zum «Swiss Pass» der SBB und des Verbands öffentlicher Verkehr (VöV) durch. Wir kamen dabei zum Schluss, dass die bei den Fahrscheinkontrollen durchgeführten Datenbearbeitungen weder verhältnismässig waren noch auf einer genügenden gesetzlichen Grundlage beruhten. Folglich haben wir gegenüber dem VöV und den SBB eine Empfehlung zur Behebung der festgestellten Mängel erlassen.

Die SBB und der VöV setzten uns am 3. März 2015 über das Projekt Swiss Pass in Kenntnis – eine Woche vor der Orientierung der Medien. Dabei handelte es sich um eine reine Vorinformation, in welcher uns die wichtigsten Aspekte des Projekts präsentiert wurden.

Seit dem 1. August 2015 werden alle General- und Halbtaxabonnemente laufend durch den Swiss Pass ersetzt. Dieser bietet zusätzlich Zugang zu Partnerdiensten wie Mobility Carsharing, Publibike, SchweizMobil oder einigen Skigebieten.

Ende 2015 führten wir eine Sachverhaltsabklärung zum SwissPass und den damit zusammenhängenden Datenbearbeitungen durch. Dabei prüften wir insbesondere auch die Kontrolldatenbank. Wir konnten Folgendes feststellen:

Unmittelbar nach dem Kauf eines GA oder eines Halbtaxabonnements werden die Kundendaten in die zentrale Kunden- und Abonnementsdatenbank (KUBA) eingetragen. Bei den Kontrollen legt das Zugbegleitpersonal ein Lesegerät, das eine lokale Kopie der Abonnementsdaten enthält, auf den Swiss Pass, um diesen zu scannen. Dabei werden die Identitätsdaten, Art des Abonnements sowie dessen Gültigkeit (gültig, teilgültig, ungültig) auf dem Bildschirm des Lesegerätes angezeigt. Die Kontrolldaten, unter anderem bestehend aus Uhrzeit, Zug- und Kursnummer sowie der Verknüpfung zur Swiss-Pass-Ausweisnummer, werden anschliessend in die Kontrolldatenbank hochgeladen und dort während 90 Tagen aufbewahrt.

Die SBB wurden vom VöV mit der Marktbearbeitung und mit der Führung der Swiss-Pass-Datenbanken beauftragt und sind auch für die Behandlung von Auskunftsgesuchen zuständig. Die Kunden- und Leistungsdaten werden, sofern kein ausdrücklicher Einwand (Opt-out) der Kunden erfolgte, auch zu Marketingzwecken verwendet. Die Kontrolldaten selbst werden weder zu Marketingzwecken bearbeitet noch an Dritte bekannt gegeben.

Aufgrund unserer Abklärungen kamen wir zum Schluss, dass die in Zusammenhang mit der Kontrolldatenbank durchgeführten Datenbearbeitungen weder verhältnismässig sind noch auf einer genügenden gesetzlichen Grundlage beruhen. Folglich

erliessen wir gegenüber dem VöV und den SBB eine Empfehlung, in welcher wir die unverzügliche Löschung der Kontrolldaten und die Einstellung des Betriebs der Kontrolldatenbank verlangten. Weiter machten wir einen Verbesserungsvorschlag zur Formulierung der AGB zum GA und zum Halbtaxabonnement, um sicherzustellen, dass die Information zur Verwendung der Daten zu Marketingzwecken und zum Opt-out auf klare und angemessene Weise erfolgt.

Am 4. Januar 2016 haben wir unseren Schlussbericht dem VöV und den SBB geschickt. Sie haben unsere Empfehlung und die Verbesserungsvorschläge angenommen. Wir werden die Umsetzung noch in diesem Jahr prüfen.

1.2.2 Sachverhaltsabklärung zum kostenlosen Internet der SBB

In Zusammenhang mit dem kostenlos angebotenen WiFi der SBB führten wir eine Sachverhaltsabklärung durch. Dabei stellten wir verschiedene Mängel fest, weshalb wir Empfehlungen erliessen. In der Folge haben die SBB die Datenschutzbestimmungen des Dienstes und die Aufbewahrungsdauer der Userdaten angepasst.

Bereits im Herbst 2013 hatten wir die SBB wegen ihrem WLAN-Angebot «SBB-free» kontaktiert. Unserer Aufforderung, die Allgemeinen Geschäftsbedingungen (AGB) zu diesem Dienst anzupassen, kamen sie jedoch nicht nach (vgl. Ziffer 1.3.4 unseres 22. Tätigkeitsberichts). Daraufhin führten wir eine Sachverhaltsabklärung bei den SBB durch.

Um das kostenlose WLAN an den Bahnhöfen zu nutzen, müssen sich die Kunden registrieren lassen. Bei der Registrierung müssen sie ihre Mobiltelefonnummer angeben, die AGB annehmen und den Zugangscode anfordern. Die Registrierung ist abgeschlossen, sobald der per SMS zugestellte Code eingegeben wurde. Die AGB zu «SBB-free» und weiterführende Informationen haben die SBB auf ihrer Internetseite publiziert.

Zum Zeitpunkt unserer Sachverhaltsabklärung wurden die in Zusammenhang mit «SBB-free» erhobenen Daten einzig für die Erbringung des Dienstes, für die Behandlung von Auskunftsgesuchen sowie gestützt auf das Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) benutzt. Entgegen damals anderslautenden AGB wurden die Daten weder zur Optimierung der «Personenhydraulik» noch zur Analyse des Reiseverhaltens der Kunden, noch zur Generierung spezifischer Meldungen im Bereich der Kundeninformation bearbeitet. Die gestützt auf das BÜPF erhobenen Daten wurden erst nach neun Monaten gelöscht. Im Laufe unserer Abklärungen passten die SBB ihre AGB ein erstes Mal an.

Gestützt auf unsere Abklärungen machten wir zwei Empfehlungen, die beide die Datenbearbeitung in Zusammenhang mit dem BÜPF betrafen. Wir empfahlen den SBB, nur diejenigen Daten zu bearbeiten, die effektiv unter das BÜPF fallen und insbesondere die Daten «Ziel IP Adresse» und «Ziel Port» nicht mehr zu erheben. Weiter verlangten wir, die Nutzungs- und Randdaten nur so lange wie im Gesetz vorgesehen, nämlich sechs und nicht neun Monate, aufzubewahren. Zudem machten wir gegenüber den SBB zwei Verbesserungsvorschläge. Einerseits schlugen wir vor, für die Behandlung der Auskunftsgesuche ein dokumentiertes Verfahren auszuarbeiten. Andererseits forderten wir die SBB auf, ihre AGB an die effektiv getätigten Datenbearbeitungen anzupassen.

Die SBB nahmen unsere zweite Empfehlung sowie unsere beiden Verbesserungsvorschläge an. Gleichzeitig hielten sie fest, unserer ersten Empfehlung nicht folgen zu können, da ihnen der Dienst für die Überwachung des Post- und Fernmeldeverkehrs (Dienst ÜPF) dringend geraten habe, die obengenannten Daten für die Strafverfolgungsbehörden weiterhin zu speichern.

Wir sind allerdings der Auffassung, dass die Protokollierung von «Ziel IP Adresse» und «Ziel Port» im jetzigen BÜPF nicht vorgesehen ist. Aufgrund der zurzeit laufenden Revision des BÜPF sehen wir jedoch momentan davon ab, diesen Punkt durch die zuständigen Behörden beurteilen zu lassen. Folglich erklärten wir die Sachverhaltsabklärung für abgeschlossen, behielten uns jedoch ausdrücklich vor, die Frage der Protokollierung von «Ziel IP Adresse» und «Ziel Port» zu einem späteren Zeitpunkt nochmals aufzugreifen und gegebenenfalls gerichtlich durchzusetzen (vgl. auch Ziffer 1.4.1 des vorliegenden Tätigkeitsberichts).

1.2.3 Private Überwachung von Fussballfans auf öffentlichem Grund

Werden Fussballfans auf öffentlichem Grund heimlich gefilmt, verletzt dies möglicherweise deren Persönlichkeit widerrechtlich. Eine solche Massnahme könnte allenfalls dadurch legitimiert werden, dass sie entweder als Teil eines Polizeieinsatzes durchgeführt oder nur im Ereignisfall ergriffen wird.

Ein Projekt der Swiss Football League sorgte in diesem Frühjahr für Schlagzeilen: Fussballfangruppen sollen auf dem Weg zu Auswärtsspielen von Privatpersonen begleitet und heimlich gefilmt werden, um im Falle von Ausschreitungen, Sachbeschädigungen etc. Beweismittel zur Hand zu haben. Die Swiss Football League hat uns zu Beginn des Jahres zur Klärung einiger datenschutzrechtlicher Fragen kontaktiert. Wir haben in allgemeiner Weise wie folgt Stellung genommen:

Die geplante Massnahme, Fangruppen bei Auswärtsspielen durch Privatpersonen begleiten zu lassen, welche verdeckte Videoaufnahmen machen, ist aus datenschutzrechtlicher Sicht problematisch: Es handelt sich um eine private Videoüberwachung auf öffentlichem Grund, die insbesondere gegen das Verhältnismässigkeits- und das Transparenzprinzip verstösst. Es werden - unabhängig von konkreten Vorfällen - alle sich im Aufnahmebereich aufhaltenden Personen aufgenommen, auch wenn sich diese korrekt verhalten. Die Betroffenen wissen dabei nicht, dass sie gefilmt werden. So verletzt dieses Vorgehen möglicherweise die Persönlichkeitsrechte der betroffenen Personen widerrechtlich. Die Verwertbarkeit solcher Aufnahmen als Beweismittel in einem Strafverfahren ist damit zumindest fraglich. Zudem können die betroffenen Personen Zivilklage einreichen und dabei z.B. die Löschung der Aufnahmen und Schadenersatz verlangen. Dementsprechend ist die Massnahme wenig zielführend.

Die Situation ist möglicherweise anders zu beurteilen, wenn einer der folgenden Lösungsansätze verfolgt wird:

1. Die Massnahme wird mit der Polizei abgesprochen und direkt in deren Sicherheitsdispositiv integriert. Die aufnehmende Person übernimmt im Auftrag der Polizei eine polizeiliche Aufgabe. Ob dies möglich ist, hängt von den jeweiligen kantonalen oder kommunalen rechtlichen Grundlagen ab und muss mit dem jeweils zuständigen Polizeikorps geprüft werden.
2. Wird auf rein privater Basis, d.h. ohne Absprache mit der Polizei, gefilmt, darf die Kamera nur im Ereignisfall eingeschaltet und nur das Ereignis selbst gefilmt werden. Damit kann wenigstens verhindert werden, dass sich korrekt verhaltende Personen ohne Anlass gefilmt werden. Dieses Vorgehen wäre eher verhältnismässig und liesse sich vermutlich durch ein überwiegendes Interesse rechtfertigen.

1.2.4 Zentrale Speicherung von Kundenfotos bei Skistationen

Mit der PhotoCompare-Funktion der Firma Skidata wird bei Skipass-Kontrollen stärker in die Persönlichkeit der Kunden eingegriffen als mit herkömmlichen Verfahren. Deren Einsatz ist daher auf Abonnemente mit langer Gültigkeitsdauer zu beschränken. Die Kunden müssen speziell informiert und die Daten dürfen nur für kurze Zeit aufbewahrt werden.

Die in vielen Skistationen praktizierte Zutrittskontrolle mittels Fotoabonnementskarte wirft einige datenschutzrechtliche Fragen auf. Wir haben uns deshalb in der Vergangenheit wiederholt damit befasst (vgl. etwa unseren 22. Tätigkeitsbericht

2014/2015, Ziffer 1.2.3). In der Zwischenzeit wurden diese Systeme weiterentwickelt und durch zusätzliche Funktionen ergänzt. Insbesondere sollen die Skistationen die Möglichkeit erhalten, Abonnementsnutzungen auch nachträglich kontrollieren zu können.

Die PhotoCompare-Funktion der Firma Ski Data dient diesem Zweck. Bei jedem Passieren eines Drehkreuzes wird vom Gast ein Kontrollfoto erstellt. Es kann zu einem beliebigen Zeitpunkt mit dem zentral in der Abonnementsdatenbank hinterlegten Referenzfoto verglichen werden. Damit erhalten die Skistationen einerseits die Möglichkeit, in Zeiten mit hoher Besucherfrequenz Kontrollen aufzuschieben und diese in einem günstigeren Zeitpunkt nachzuholen. Andererseits ist es mit Hilfe dieser Funktion möglich, systematische und über einen längeren Zeitraum andauernde Missbräuche von Abonnementen zu entdecken und zu ahnden. Skistationen begründen den Einsatz dieser Funktion denn auch mit der offenbar gestiegenen Anzahl von Missbrauchsfällen. Wir haben die Funktion aufgrund diverser Anfragen betroffener Personen und auf Wunsch der Herstellerin analysiert und sind dabei zu folgendem Schluss gelangt:

Mit der PhotoCompare-Funktion wird stärker in die Persönlichkeitsrechte der Kunden eingegriffen als mit herkömmlichen Zutrittskontrollen. Überspitzt formuliert, werden sämtliche Gäste einem Generalverdacht unterstellt und Daten auf Vorrat gespeichert, was unter datenschutzrechtlichen Aspekten stets heikel ist. Daher ist bei deren Verwendung nebst den für Zutrittskontrollsysteme allgemein einzuhaltenden Rahmenbedingungen (vgl. unseren 22. Tätigkeitsbericht 2014/2015, Ziffer 1.2.3) insbesondere Folgendes zu beachten:

Der Einsatz von PhotoCompare rechtfertigt sich nur bei Abonnementen mit höherem Wert, also insbesondere bei Saison- oder Wochenkarten. Bei Karten mit kurzer Gültigkeitsdauer ist auf den Einsatz der Funktion hingegen zu verzichten. Das System von Skidata erlaubt entsprechende Einstellungen, damit nur bei bestimmten Abonnementskategorien Kontrollfotos erstellt werden.

Beim Einsatz von PhotoCompare müssen die Gäste vorab in den Allgemeinen Geschäftsbedingungen (AGB) oder spezifischen Datenschutzbestimmungen sowie vor Ort mit gut sichtbaren Hinweisschildern darüber informiert werden, dass sie beim Passieren der Drehkreuze fotografiert werden können. Dies dient nicht nur der Einhaltung des Transparenzgrundsatzes, sondern nach unseren Erfahrungen auch der Akzeptanz des Systems bei den betroffenen Personen.

Die Kontrollfotos dürfen nur für einige Tage aufbewahrt werden. Die Speicherdauer kann dabei im System individuell eingestellt werden. Die von einigen Skistationen praktizierte Speicherung der Vergleichsfotos während der gesamten Gültigkeitsdauer des Abonnements kann unter Umständen problematisch sein:

Bei Saison- oder Jahreskarten führt dies zu einer Speicherdauer von mehreren Monaten bis hin zu einem Jahr. Diese sehr lange Speicherdauer wird zwar damit begründet, dass Missbrauchs- und Betrugsfälle, die über einen längeren Zeitraum andauern, aufgedeckt und dokumentiert werden können. Hierfür würden aber die Daten sämtlicher (also auch aller sich korrekt verhaltender) Inhaber von Abonnementen mit längerer Gültigkeitsdauer gespeichert. Der daraus gewonnene Mehrwert wäre aus unserer Sicht deshalb fraglich.

Mit Hilfe der Fotovergleich-Funktion können die Abonnementsnutzungen täglich (oder zumindest alle paar Tage) detailliert kontrolliert und Missbrauchsfälle damit sofort entdeckt werden (was nach den uns bekannten Tarifbestimmungen der meisten Skistationen zu einem sofortigen Entzug des Abonnements führt). Deshalb ist eine längere Aufbewahrung der Bilder der sich korrekt verhaltenden Personen nicht notwendig. Die Betreiber müssen diese folglich löschen und dürfen einzig diejenigen Bilder weiterhin speichern, die einen allfälligen Missbrauch dokumentieren. Mit den übrigen Logdaten können auffällige Nutzungsmuster über einen längeren Zeitraum entdeckt und anschliessend gezielt abgeklärt werden, ohne derart stark in die Persönlichkeitsrechte sämtlicher Kunden einzugreifen.

1.2.5 Bekanntgabe von Personendaten ins Ausland zur Dopingbekämpfung

In der Schweiz besteht seit Inkrafttreten des Bundesgesetzes über die Förderung von Turnen und Sport eine ausreichende gesetzliche Grundlage zur Dopingbekämpfung. Das Gesetz regelt ebenfalls die Übermittlung von Personendaten zwischen den Dopingkontrollstellen. Erfolgt dabei eine Übermittlung in ein Land ohne genügendes Datenschutzniveau, muss der Schutz der Personendaten durch vertragliche Vereinbarungen sichergestellt werden.

In den vergangen Jahren haben wir mehrfach auf die Problematik von Datenlieferungen in Länder ohne angemessenes Datenschutzniveau hingewiesen (vgl. 20. Tätigkeitsbericht 2012/2013, Ziffer 1.2.6 mit weiteren Verweisen). Da die World Anti Doping Agency (WADA) in Montreal weder der kanadischen Datenschutzgesetzgebung noch derjenigen der Provinz Quebec unterstand, haben wir verlangt, dass die Datenlieferanten das Datenschutzniveau anderweitig, z.B. vertraglich, sicherstellen müssen. Die WADA kontaktierte uns betreffend dieser Anforderung und stellte uns ein Konzept zur Sicherstellung des Datenschutzniveaus vor. In den Beratungen haben wir gewisse Anpassungen gefordert, welche von der WADA übernommen wurden, sodass eine Übermittlung von Personendaten zur Dopingbekämpfung an die WADA in Lausanne unter Einhaltung der schweizerischen Gesetzgebung erfolgen kann.

Eine Vereinfachung der Datenbekanntgabe zur Dopingbekämpfung könnte auch die im vergangenen Jahr gemachten Anpassungen des kanadischen Datenschutzgesetzes mit sich bringen. Eine abschliessende Einschätzung dieser neuen kanadischen Bestimmungen steht momentan noch aus.

1.2.6 Revision der Energieverordnung und der Stromversorgungsverordnung

Im Rahmen unserer Stellungnahme zur Revision der Energie- und Stromversorgungsverordnungen haben wir die Publikation von Personendaten im Internet durch ein Bundesorgan auf die Verhältnismässigkeit geprüft. Wir kamen zum Schluss, dass mit der geplanten Ausweitung des betroffenen Personenkreises nur eine marginale Erhöhung der Transparenz erreicht werden kann. Daher forderten wir auf die Ausweitung zu verzichten.

Im Verordnungsentwurf war geplant, zu allen Stromproduktionsanlagen, die eine Vergütung erhalten, eine Liste mit folgenden Angaben zu publizieren:

Name des Produzenten, Standort der Anlage, verwendeter Energieträger, Anlagenkategorie und -typ, Leistung; erzielte Produktion, Höhe der Vergütung, Anmeldedatum, Inbetriebnahmedatum sowie Vergütungsdauer.

Nach geltendem Recht durften bislang nur Personendaten zu Anlagen mit Anschlussleistung von über 30 kVA publiziert werden, welche dem Obligatorium der Erfassung der Anlage, der produzierten Elektrizität sowie des Herkunftsnachweises unterstellt waren. Alle Anlagen mit einer kleineren Anschlussleistung wurden in anonymisierter Form mit Postleitzahl, Ort und Kanton auf der Liste aufgeführt.

Wir haben im Rahmen des Mitwirkungsverfahrens die geplante Ausweitung des Kreises der von einer Publikation betroffenen Personen auf die Verhältnismässigkeit geprüft. Bei der Beurteilung der Verhältnismässigkeit der Datenbearbeitung muss der Eingriff in die Persönlichkeit der Betroffenen dem Zweck der Bearbeitung gegenüber gestellt werden. Veröffentlicht ein Bundesorgan Personendaten im Internet, muss dies zur Zweckerreichung notwendig sein, da diese Bearbeitung nicht mit der Einwilligung der Betroffenen erfolgt, sondern über gesetzliche Bestimmungen. So pflegt ein Teil der Bevölkerung wegen dem Missbrauch von Daten im Internet einen restriktiven Umgang mit den eigenen Daten. Jedoch können die Betroffenen die gesetzlich vorgeschriebene Veröffentlichung durch Bundesorgane nicht beeinflussen.

Gemäss dem erläuternden Bericht soll die Publikation der Liste der Vergütungen samt Namen dem Zweck der Transparenz über die Verwendung des bei den Endverbrauchern erhobenen Netzzuschlags dienen. Aus datenschutzrechtlicher Sicht

erschien es fraglich, ob durch die zusätzliche Publikation der Personendaten von Produzenten, welche eine Vergütung im Bereich von Kleinbeträgen erhalten, eine Erhöhung der Transparenz zu erreichen ist. Die neue Regelung hätte bei der Liste der Bezüger der kostendeckenden Einspeisevergütung von 2013 zwar die Zahl der Personendatensätze mehr als vervierfacht, das Volumen der Beiträge, die bestimmten Personen zuordenbar sind, aber nur um acht Prozent gesteigert. Der Eingriff in die Persönlichkeitsrechte einer grossen Anzahl Betroffener mit einem solch geringen zusätzlichen Nutzen, war aus unserer Sicht nicht verhältnismässig. Daher haben wir das Bundesamt für Energie erfolgreich aufgefordert, auf die Ausweitung der Internetpublikation zu verzichten.

1.2.7 Verfahren zur Abklärung des Sachverhalts: Strafanzeigen bei Verletzung der Mitwirkungspflicht

Datenbearbeiter haben bei Verfahren, die der EDÖB zur datenschutzrechtlichen Abklärung des Sachverhalts einleitet, eine Mitwirkungspflicht. Deren Verletzung ist strafbar. Wir haben gegen fehlbare Personen Strafanzeige eingereicht.

Nachdem wir durch Bürgeranfragen auf eine möglicherweise rechtswidrige Datenbearbeitung aufmerksam gemacht wurden, eröffneten wir in der Sache ein Verfahren zur Feststellung des Sachverhalts nach Artikel 29 des Datenschutzgesetzes (DSG). Dies wurde dem Datenbearbeiter schriftlich mitgeteilt. Nach Erhalt des Eröffnungsschreibens kontaktierte uns der Datenbearbeiter zwar zunächst telefonisch. Die von uns eingeforderte schriftliche Stellungnahme inklusive weiterer Dokumente reichte er in der Folge jedoch nie ein und reagierte auf unsere Mahnschreiben nicht mehr. Er brach jeglichen Kontakt zu uns ab, eine zuletzt per Einschreiben versendete letzte Mahnung wurde als «nicht abgeholt» retourniert.

Ein solches Verhalten verunmöglicht uns eine wirksame Aufsichtstätigkeit und muss als Verweigerung der Mitwirkung bei der Abklärung eines Sachverhalts eingestuft werden. Wir haben daher gestützt auf das Datenschutzgesetz Strafanzeige gegen die Verantwortlichen eingereicht (Art. 34 Abs. 2 Bst. b).

Durch das eingeleitete Strafverfahren aufgeschreckt, hat sich der Datenbearbeiter doch noch bei uns gemeldet und die geforderten schriftlichen Unterlagen eingereicht. Wir konnten somit die Sachverhaltsabklärung doch noch durchführen und abschliessen. Nachdem wir eine Desinteresse-Erklärung abgaben, stellte die zuständige Strafverfolgungsbehörde das Strafverfahren ein.

1.2.8 Herausgabe der Fahrgestellnummer durch das ASTRA

In Zusammenhang mit einer Anfrage des ASTRA kamen wir zum Schluss, dass es sich bei Fahrgestellnummern (VIN) um Personendaten im Sinne des Datenschutzgesetzes handelt. Folglich braucht das ASTRA für die Bekanntgabe der VIN eine gesetzliche Grundlage. Zuvor müsste sorgfältig abgeklärt werden, ob die allgemeinen Datenschutzgrundsätze eine solche Bekanntgabe rechtfertigen.

Das Bundesamt für Strassen (ASTRA) wollte von uns wissen, ob die Vehicle Identification Number (VIN; auf Deutsch: Chassis- oder Fahrgestellnummer) als Personendatum im Sinne des Datenschutzgesetzes zu qualifizieren sei oder nicht. Das ASTRA selbst hatte verschiedene Anfragen erhalten, in welchen die Bekanntgabe von ganzen VIN-Listen verlangt wurde.

Jeder Personenkraftwagen (PKW) erhält vom Fahrzeughersteller eine eigene VIN, die das Fahrzeug sowie jedes Bestandteil des Fahrzeugs eindeutig bestimmen lässt. Bei landwirtschaftlichen Fahrzeugen oder Anhängern kann, in seltenen Fällen, die VIN mehrmals vergeben werden. Sie dient in erster Linie der Identifikation eines Fahrzeugs.

Es stellte sich die Frage, welchen Aufwand der Datenbearbeiter oder ein Dritter objektiv hätte, um anhand der vom ASTRA erhaltenen VIN die Fahrzeughalter bestimmen zu können. Dabei war auch zu berücksichtigen, welches Interesse der Datenbearbeiter oder ein Dritter an der Identifizierung hat.

Beim ASTRA sind die VIN im Informationssystem MOFIS (automatisiertes Fahrzeug- und Fahrzeughalterregister), zusammen mit den Halterangaben, gespeichert. Auch wenn das Amt nur die VIN, ohne Angabe des Halters, herausgibt, weiss der Empfänger, dass es sich um in der Schweiz zugelassene Fahrzeuge handelt. Aufgrund der heute zur Verfügung stehenden technischen Mittel ist insbesondere bei Empfängern aus dem Automobilgewerbe davon auszugehen, dass sie einen Bezug zu einer bestimmbaren Person, in diesem Fall zum Halter, herstellen können. So verfügen insbesondere die Importeure und Garagisten bereits über die VIN ihrer Fahrzeuge oder können auch beim Hersteller selbst nachfragen. Auch ein Interesse des Empfängers an einer Identifizierung des Halters lässt sich nicht ausschliessen. Zur Qualifizierung als Personendaten ist es zudem ausreichend, wenn die Bestimmbarkeit in Bezug auf einen Teil der Informationen (vorliegend VIN) gegeben ist.

Anhand der VIN kann der Fahrzeughersteller eindeutig identifiziert werden, da ein Teil der Nummer aus einem Code besteht, der ihm zugeteilt ist. Welche VIN zu welchem Hersteller gehört, kann mittels der Suche auf verschiedenen Websites sehr schnell herausgefunden werden.

Daraus folgerten wir, dass die VIN als Personendatum im Sinne des DSG gilt. Folglich braucht das ASTRA für die Bekanntgabe dieser Nummer eine gesetzliche Grundlage. Vor der allfälligen Schaffung einer solchen Grundlage müsste das ASTRA allerdings sorgfältig abwägen, ob die allgemeinen Datenschutzgrundsätze (Verhältnismässigkeit, Zweckbindung, usw.) eine solche Bekanntgabe rechtfertigen.

1.3 Internet und Telekommunikation

1.3.1 Sachverhaltsabklärung zu Windows 10

Microsoft lancierte im vergangenen Jahr das Betriebssystem Windows 10. Im Rahmen dieser Einführung wurden wir auf die damit einhergehenden Datenbearbeitungen aufmerksam und haben diese in der Folge näher betrachtet. Ein Hauptaugenmerk lag dabei auf der Information der Betroffenen und deren Einwilligung.

Nach der Lancierung von Windows 10 betrachteten wir die Datenbearbeitung durch Microsoft näher. So haben wir festgestellt, dass im Rahmen des Installationsprozesses von Windows 10 den Benutzern im Fenster «Schnell einsteigen» sogenannte «Express-Einstellungen» angeboten werden, mit welchen standardmässig fast alle Datenübermittlungen und -zugriffe aktiviert werden. Unter anderem werden damit Standortdaten, die in der Umgebung der Benutzer von Windows 10 erkannten WLAN-Netzwerke, der Browser- und Suchverlauf, die Sprach-, Freihand- und Tastatureingaben sowie Feedback- und Diagnosedaten an Microsoft übermittelt.

Basierend auf diesen Erkenntnissen haben wir eine Sachverhaltsabklärung eröffnet und Microsoft einen Fragekatalog zu den Datenbearbeitungen im Rahmen von Windows 10 zugestellt. Hierbei geht es um den Umfang der übermittelten Daten und die damit zusammenhängende Frage, ob die Betroffenen genügend transparent informiert werden und deren Einwilligung zur Datenbearbeitung vorliegt. - Die Abklärungen waren bei Redaktionsschluss noch in Gang.

1.3.2 Kundendatenanalyse bei Telekomanbieter zwecks personalisierter Angebote

Die Firma Cablecom hat ihre Allgemeinen Geschäftsbedingungen (AGB) überarbeitet. Da einzelne Bestimmungen unklar formuliert waren, haben wir bei dem Unternehmen Abklärungen vorgenommen und Verbesserungen verlangt.

Im September 2015 hat die upc cablecom GmbH (nachfolgend Cablecom) die AGB für ihre Unterhaltungs- und Telekommunikationsdienste geändert. Die Kunden wurden aufgefordert, sich innerhalb einer bestimmten Frist zu melden, falls sie mit den neuen Geschäftsbedingungen nicht einverstanden wären. In den neuen AGB stand, dass Cablecom Nutzungsdaten für die bedarfsgerechte Gestaltung und Entwicklung der Dienste sowie für personalisierte Angebote bearbeiten darf.

In der Folge haben wir Cablecom aufgefordert, schriftlich mitzuteilen, welche Daten das Unternehmen im Detail bearbeitet und welche Dienste und personalisierten

Angebote konkret gemeint sind. Gleichzeitig haben wir das Unternehmen darauf aufmerksam gemacht, dass unter Umständen Persönlichkeitsprofile im Sinne des Datenschutzgesetzes bearbeitet werden und diese Daten gemäss den Geschäftsbedingungen für einen neuen Zweck genutzt werden sollen. In diesem Fall muss die Einwilligung einer betroffenen Person ausdrücklich sein, eine stillschweigende Annahme eines Kunden auf die neuen AGB genügt in der Regel nicht.

Unsere Abklärungen haben ergeben, dass mit Nutzungsdaten diejenigen Daten gemeint sind, welche im Zusammenhang mit der Nutzung der TV-Box «Horizon» anfallen. Wenn die Kunden die Box zuhause installieren, werden sie im Laufe dieses Vorgangs auf ihrem Fernsehbildschirm darüber informiert, dass bei der Verwendung gewisser Dienste Daten anfallen. Diese würden namentlich dazu verwendet, den Kunden Sendungen oder Filme vorzuschlagen, die ihren persönlichen Vorlieben entsprechen. Da die Kunden die Datenbearbeitung in den TV-Box-Einstellungen jederzeit ablehnen und später wieder aktivieren können, wird dem Transparenzerfordernis unseres Erachtens genüge getan. Die Kunden können sich eindeutig für oder gegen diese Datenbearbeitung aussprechen.

Die betreffenden Ziffern der neuen AGB sind jedoch unklar und zu knapp formuliert. Wir haben deshalb Verbesserungen verlangt. Cablecom hat die Präzisierungen zur Verwendung der Nutzungsdaten in einem separaten Merkblatt vorgenommen, welches mit den AGB verlinkt ist. In einer nächsten Revision der AGB sollen die wesentlichen Klarstellungen direkt darin vorgenommen werden.

1.3.3 Datenzugriffe durch Apps

Es lohnt sich, bei der Installation einer Smartphone-App kurz inne zu halten und nachzusehen, welche Berechtigungen verlangt werden. Sie sind meist mit Datenzugriffen verbunden.

Vor der Installation einer Smartphone-App werden die Nutzer aufgefordert, verschiedene Berechtigungen zu erlauben. Teilweise sind diese für das Funktionieren der Applikation erforderlich. Es werden aber auch oft Berechtigungen verlangt, die nicht zwingend notwendig oder sogar komplett überflüssig sind.

Dass eine Navigations-App nur dann funktionieren kann, wenn diese Standortinformationen zur Verfügung hat, ist leicht nachvollziehbar. Andere Apps nutzen den Standort allenfalls um ortsabhängige Werbung anzuzeigen oder andere Zwecke, die eher für den App-Anbieter als den User von Nutzen sind. Ganz generell muss man sich bewusst sein, dass man bei (vordergründig) kostenlosen oder kostengünstigen Apps häufig mit seinen Daten bezahlt.

Manche Apps verlangen z.B. Zugriff auf die Kamera des Gerätes. Oft ist der Zweck auf den ersten Blick nicht ersichtlich. Vielleicht gibt es eine durchaus sinnvolle Funktion etwa zum Lesen von Strichcodes, die über die Kamera erfolgt. Die erteilte Berechtigung erlaubt jedoch der App theoretisch jederzeit die Kamera zu aktivieren und Aufnahmen zu machen.

Der EDÖB hat exemplarisch eine App im Bereich medizinischer Vorsorgeuntersuchungen näher angeschaut. Aufgrund der Eingabe von Werten des Benutzers wird eine Risikoanalyse erstellt und allenfalls weitere Abklärungen empfohlen. Wir haben auf Anfrage von den Entwicklern Begründungen für die aus unserer Sicht weit gehenden verlangten Berechtigungen erhalten. Diese waren an und für sich nachvollziehbar. Die App muss z.B. Speicherinhalte lesen, ändern und löschen können, weil die Resultate in Form einer PDF-Datei an eine E-Mail-Adresse geschickt werden können. Die App hätte aber auch ohne diese Funktion programmiert werden können, indem das Resultat lediglich auf dem Display des Gerätes erscheinen würde.

Wir raten Nutzerinnen und Nutzern, genau hinzusehen, welche Berechtigungen eine App verlangt und abzuschätzen, ob diese notwendig erscheinen. Auch die AGB bzw. Privacy Policy sind aufmerksam zu lesen. Die Bearbeitungen von Personendaten, die von einer App vorgenommen werden, müssen gegenüber dem Nutzer transparent sein. Werden Berechtigungen für nicht nachvollziehbare Zwecke verlangt und ist der Herausgeber nicht vertrauenswürdig, sollte auf eine Installation der App verzichtet werden.

1.3.4 Revision des Fernmeldegesetzes

Im Rahmen der Revision des Fernmeldegesetzes wurden wir vom Bundesamt für Kommunikation zur Stellungnahme eingeladen. Unsere Bemerkungen zum Gesetzesvorschlag betrafen unter anderem die Verzeichnis- und die Notrufdienste.

Der Gesetzesvorschlag zu den Telefonverzeichnissen sieht vor, dass die Kunden nur zwischen der Publikation oder keiner Publikation des Verzeichniseintrages wählen können, jedoch nicht den Publikationskanal. Kunden, die nicht wollen, dass ihre Adresse und Telefonnummer im Internet publiziert werden, haben momentan einzig die Möglichkeit, ihre Adresse komplett zu sperren, obschon sie bereit wären, über die anderen Kanäle auffindbar zu sein. Die Publikation der Verzeichnisdaten im Internet wird oftmals als Freipass zur Personendatenbearbeitung zu diversen Zwecken angesehen. So existieren im Internet diverse unseriöse, anonyme Website-Betreiber, welche die Verzeichnisdaten der «offiziellen» Anbieter abgreifen und veraltete oder falsche Verzeichnisdaten publizieren. Eine Korrektur oder Löschung der Verzeichnisdaten ist bei diesen Betreibern nicht möglich. Wir haben daher

gefordert, im Gesetz eine Wahlmöglichkeit für den Publikationskanal zu verankern. Das Bundesamt für Kommunikation (BAKOM) sah jedoch keine Notwendigkeit, unsere Begehren umzusetzen.

Wie wir dem BAKOM bereits in mehreren Ämterkonsultation mitgeteilt haben, dürfen die Verzeichniseinträge, insbesondere solche mit Sterneintrag, aufgrund des Zweckbindungsprinzips nicht für die direkte Werbung verwendet werden. Dies wurde auch schon in der Botschaft zur Änderung des Fernmeldegesetzes von 2003 festgehalten: «Der Begriff der auf den Verzeichnissen basierenden Dienste schliesst hingegen die Verwendung von Verzeichnisdaten für direkte Werbung aus.» Wir stellen fest, dass die heutige Umsetzung des Werbewiderspruchs durch den sogenannten Sterneintrag im Telefonverzeichnis unbefriedigend ist, da sich Werbetreibende teilweise nicht daran halten und über die Tragweite des Sterneintrags Uneinigkeit herrscht. Um zu verhindern, dass der Verzeichniseintrag für direkte Werbung verwendet wird, haben die Kundinnen und Kunden nur die Möglichkeit, ihre Kontaktdaten nicht im Verzeichnis publizieren zu lassen. Dies entspricht aber nicht einer echten Wahlfreiheit und führt dazu, dass sich immer weniger Leute in die Verzeichnisse eintragen lassen. Wir forderten daher ein ausdrückliches Verbot der Verwendung von Verzeichniseinträgen für direkte Werbung im Fernmeldegesetz. Leider wollte das BAKOM keine solch ausdrückliche Einschränkung im Gesetz festschreiben.

Bei den Notrufdiensten unterstützen wir die Bestrebungen, dass die Anbieterinnen des öffentlichen Telefondienstes die Pflicht haben, die Leitweglenkung der Notrufe und die Standortidentifikation der Anrufenden sicherzustellen, denn nur dann ist eine effiziente und effektive Aufgabenerfüllung möglich. Sollten Notfalldienste in der Zukunft aber möglicherweise sogar selbst den «Location Manager» des Anrufers aktivieren, würde dies zu Problemen mit dem Grundrecht auf Schutz der Privatsphäre führen. Wir haben daher vorgeschlagen, dem Bundesrat die Kompetenz zu übertragen, einerseits die Verwendung resp. Ausgestaltung einer Notfall-App zu standardisieren und anderseits zu regeln, in wie weit auf das Gerät zur Standortidentifikation zugegriffen werden darf. Das BAKOM wollte die Möglichkeit zur Festlegung einer standardisierten Notfall-App nicht im Gesetz aufnehmen, hat jedoch die Bestimmung für den Zugriff auf die Ortungsfunktionen ohne Einwilligung des Benutzers vorgesehen. Wir werden die Umsetzung in der Verordnung entsprechend verfolgen, damit die Privatsphäre der Benutzer geschützt bleibt.

1.4 Justiz/Polizei/Sicherheit

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

Im Berichtsjahr wurden wir von den Kommissionen für Rechtsfragen beider Räte eingeladen, an den Sitzungen zur Totalrevision des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) teilzunehmen. Thema war dabei unter anderem die Aufbewahrungsdauer von Randdaten sowie die Aufzeichnung des Internet-Nutzungsprotokolls.

Im vergangenen Jahr lud uns sowohl die Kommission für Rechtsfragen des Nationalrats als auch die des Ständerates zu den Sitzungen zum Entwurf des totalrevidierten BÜPF ein. Dabei riefen wir unsere bereits mehrfach geäusserte Haltung in Erinnerung, wonach es für den Eingriff in ein verfassungsmässig geschütztes Grundrecht formelle und materielle gesetzliche Grundlagen braucht, die zudem genügend bestimmt sind.

In diesem Zusammenhang wiesen wir auch darauf hin, dass die vorgeschlagene Bestimmung für Auskünfte zur Identifikation der Täterschaft bei Straftaten über das Internet zu wenig bestimmt ist und dazu führen kann, dass Internet-Nutzungsprotokolle über die gesamte Dauer der Kundebeziehung erfasst und gespeichert werden könnten. Mit einer solchen unverhältnismässigen Ausdehnung der Aufbewahrungsdauer liesse sich der Grundrechtseingriff nicht mehr rechtfertigen.

Bezüglich der Aufbewahrungsdauer der Randdaten hielten wir zudem erneut fest, dass die Ausdehnung der Speicherdauer auf zwölf Monate nicht nötig sei, da mit einer Aufbewahrungsdauer von sechs Monaten schon sehr weitgehende Voraussetzungen für die Strafverfolgung bestehen (vgl. 22. Tätigkeitsbericht 2014/2015, Ziffer 1.4.4). Wir gehen mit dem Antrag der Kommission des Ständerates einig, der die bisherige Aufbewahrungsdauer von sechs Monaten sowohl für den Post- als auch für den Fernmeldebereich beibehalten will.

Mit Sorge verfolgen wir Bestrebungen, welche die Randdaten auch für die Verfolgung von zivilrechtlichen Verletzungen nutzen möchten (vgl. Ziffer 1.8.4 des vorliegenden Tätigkeitsberichts). Im Rahmen der Diskussionen zur Totalrevision des BÜPF wurde uns immer wieder versichert, dass die Randdaten einzig zum Zweck der Strafverfolgung gespeichert und verwendet würden. Diese Beschränkung ist aus unserer Sicht unabdingbar, da die Randdaten unter das verfassungsmässig geschützte Grundrecht des Post- und Fernmeldegeheimnisses fallen.

1.4.2 Bundesgesetz über den Nachrichtendienst

Das revidierte Bundesgesetz über den Nachrichtendienst sieht Kontrollen auf mehreren Ebenen und spezifische Verfahren für die Beschaffung bewilligungspflichtiger Informationen und für die Kabelaufklärung vor. Es bleibt zu prüfen, ob die erwähnten Kontrollen einen Schutz der Grundrechte der betroffenen Personen tatsächlich ermöglichen. Das neue Gesetz enthält auch einige datenschutzrechtlich problematische Elemente.

Wir haben verschiedentlich angemerkt, dass der Entwurf des Nachrichtendienstgesetzes noch datenschutzrechtlich problematische Elemente enthält (vgl. u.a. unseren 22. Tätigkeitsbericht 2014/2015, Ziffer 1.4.2). Im Bundesgesetz über den Nachrichtendienst vom 25. September 2015 sind folgende Punkte weiterhin bedenklich: das Gesetz erlaubt es dem Nachrichtendienst des Bundes (NDB), Flugzeuge und Satelliten zur Beobachtung von Ereignissen und Anlagen an öffentlichen und frei zugänglichen Orten einzusetzen und dort Aufzeichnungen in Bild- und Tondokumenten vorzunehmen. Der NDB hat auch die Möglichkeit, Computersysteme und -netzwerke zu infiltrieren, um den Zugang zu Informationen zu stören, zu verhindern oder zu verlangsamen. Ausserdem ist die Informationsbeschaffung durch den Nachrichtendienst vom Öffentlichkeitsgesetz ausgenommen, womit der Zugang zu entsprechenden amtlichen Dokumenten verhindert wird.

Während die oben erwähnten Punkte zu heiklen Eingriffen in die Privatsphäre führen und deshalb besonderer Aufmerksamkeit bedürfen, begrüssen wir die im neuen Gesetz vorgesehenen mehrgleisigen Kontrollmassnahmen. So sieht das Nachrichtendienstgesetz in Sachen Kontrolle und Beaufsichtigung des NDB vor, dass der Bundesrat eine unabhängige Aufsichtsbehörde und ein unabhängiges Kontrollorgan für die Funk- und Kabelaufklärung einsetzt. Die Tätigkeiten des NDB werden auch vom Bundesrat überwacht und kontrolliert. Die parlamentarische Oberaufsicht schliesslich wird von der Geschäftsprüfungsdelegation und der Finanzdelegation ausgeübt. Der NDB ist eines der meistkontrollierten Organe des Bundes. Dieser Rahmen sollte den Schutz der Grundrechte der betroffenen Personen ermöglichen. Ansonsten wären weitere Massnahmen zur Beaufsichtigung einzuführen.

Schliesslich muss eine bewilligungspflichtige Ermittlungsmassnahme vor ihrer Umsetzung durch das Bundesverwaltungsgericht genehmigt und vom Vorsteher des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport (VBS) gebilligt werden. Der Vorsteher des VBS beschliesst die Durchführung nach Absprache mit den Vorstehern des Eidgenössischen Departements für auswärtige Angelegenheiten (EDA) und des Eidgenössischen Justiz- und Polizeidepartements (EJPD). Dieses Verfahren gilt auch für die Überwachung des Kabelnetzes.

Auch diese Mechanismen sollten den Schutz der Grundrechte der betroffenen Personen möglich machen.

1.4.3 Informationssysteme der Eidgenössischen Zollverwaltung

Mit der Teilrevision des Zollgesetzes erhalten die Informationssysteme der Eidgenössischen Zollverwaltung zur Bearbeitung von besonders schützenswerten Daten und Persönlichkeitsprofilen eine ausreichende Gesetzesgrundlage.

Die geltenden Bestimmungen über die Informationssysteme der Eidgenössischen Zollverwaltung (EZV), die besonders schützenswerte Daten enthalten oder die Erstellung von Persönlichkeitsprofilen ermöglichen, erfüllen nicht alle Erfordernisse einer Gesetzesgrundlage im formellen Sinn (vgl. auch unseren 21. Tätigkeitsbericht 2013/2014, Ziffer 1.4.7). Im Rahmen der Teilrevision des Zollgesetzes hat das Eidgenössische Finanzdepartement mit der Datenschutzgesetzgebung konforme Rechtsvorschriften für die Informationssysteme der EZV ausgearbeitet. Diese Vorschriften gelten für folgende Informationssysteme: Informationssystem in Strafsachen, für die Bewirtschaftung der Resultate von Zollkontrollen, für die Erstellung von Risikoanalysen, für die Führungsunterstützung, für die Dokumentation der Tätigkeit des Grenzwachtkorps sowie für Bildaufnahme-, Bildaufzeichnungs- und andere Überwachungsgeräte.

1.4.4 Bekanntgabe von Daten über Flugreisende an den Nachrichtendienst des Bundes

Wir überprüften im Berichtsjahr die Bekanntgabe von Daten über Flugreisende durch das Sekretariat für Migration an den Nachrichtendienst des Bundes. Während dieses Vorgehen datenschutzkonform ist, müssen die Durchführungsbestimmungen hingegen ergänzt werden.

Das Staatssekretariat für Migration (SEM) übermittelt Daten von Flugreisenden an den Nachrichtendienst des Bundes (NDB). Auf Ersuchen der Geschäftsprüfungsdelegation haben wir geprüft, ob für diesen Vorgang eine ausreichende Rechtsgrundlage besteht. Um den datenschutzrechtlichen Anforderungen zu genügen, benötigen Bundesorgane eine gesetzliche Grundlage für die Bekanntgabe von Personendaten. Im Rahmen unserer Analyse stellten wir fest, dass einzig die Bestimmungen des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit (BWIS) als solche in Betracht kommen. Die bekannt gegebenen Daten an sich

sind nicht besonders schützenswert. Ihre Bearbeitung im Kontext der inneren und äusseren Sicherheit des Staates verleiht ihnen aber eine besondere Schutzwürdigkeit und könnte in gewissen Fällen zur Erstellung von Persönlichkeitsprofilen führen. Aus diesem Grunde müssen die Erhebung der Daten von Flugreisenden durch den NDB und ihre Bekanntgabe durch das SEM auf einer Gesetzesgrundlage im formellen Sinn beruhen. Laut BWIS beschafft der NDB die Informationen, welche zur Erfüllung der Aufgaben nach dem BWIS notwendig sind, und das selbst wenn dies für die betroffenen Personen nicht erkennbar ist (Art. 14 Abs. 1). Auch sieht das Gesetz vor, dass der NDB Personendaten durch Nachforschen nach der Identität oder dem Aufenthalt von Personen und durch Feststellen ihrer Bewegungen und Kontakte beschaffen kann (Art. 14 Abs. 2 BWIS). Diese Bestimmung des BWIS bezeichnet die Kategorie der erhobenen Daten wie auch den Zweck dieser Beschaffung. Artikel 14 Absatz 1 und 2 bildet somit eine Gesetzesgrundlage im formellen Sinn, die den NDB zur Beschaffung von Daten über Flugreisende berechtigt.

Überdies ist das SEM aufgrund von Artikel 13 Absatz 1 BWIS zu Auskünften an den NDB verpflichtet. Absatz 2 dieser Bestimmung verlangt, dass das SEM dem NDB unaufgefordert Meldung erstattet, wenn es konkrete Gefährdungen der inneren oder der äusseren Sicherheit feststellt, und dass es weitere Meldungen aufgrund der allgemeinen Informationsaufträge in Anwendung von Artikel 11 BWIS oder aufgrund von Aufträgen des NDB im Einzelfall erstattet. Artikel 11 Absatz 2 BWIS erteilt dem Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) die Kompetenz, in einer vertraulichen Liste die Vorgänge festzuhalten, die dem NDB zu melden sind, die jedoch aus Geheimhaltungsgründen nicht veröffentlicht werden dürfen. Die Bekanntgabe von Daten über Flugreisende durch das SEM an den NDB beruht ebenfalls auf einer ausreichenden Gesetzesgrundlage im formellen Sinn.

Nachdem nun das Vorliegen von Gesetzesgrundlagen im formellen Sinn festgestellt wurde, ist eine Analyse der Durchführungsbestimmungen erforderlich. Diese müssen genügend präzise sein, damit die vorgesehene Bearbeitung insbesondere dem Verhältnismässigkeitsprinzip gerecht wird. In Anwendung von Artikel 4 Absatz 2 der Verordnung über den Nachrichtendienst des Bundes hat das SEM dem NDB unaufgefordert und ohne Verzug die in der vertraulichen Liste des VBS nach Artikel 11 Absatz 2 BWIS genannten Vorgänge zu melden. Diese vertrauliche Liste wird dem Bundesrat jährlich zur Genehmigung und anschliessend der Geschäftsprüfungsdelegation zur Kenntnisnahme unterbreitet (Art. 11 Abs. 7 BWIS). Nach der bundesrätlichen Genehmigung kann diese Liste als Durchführungsbestimmung auf einer mit einer bundesrätlichen Verordnung vergleichbaren Stufe betrachtet werden. Die vertrauliche Liste des VBS muss die Liste der dem NDB bekanntzugebenden Personendaten enthalten. Wir haben festgestellt, dass in der Liste des VBS nicht

ausdrücklich sämtliche Bekanntgaben von Daten über Flugreisende erwähnt sind und sie daher ergänzt werden muss, damit eine ausreichende gesetzliche Grundlage gegeben ist.

1.4.5 Kontrolle der Logfiles beim Grenzwachtkorps als Endnutzer des Schengener Informationssystems

Im Rahmen der Schengen-Assoziierungsabkommen haben wir eine Kontrolle der Logfiles beim Grenzwachtkorps (GWK) als Endnutzer des Schengener Informationssystems (SIS) durchgeführt. Die Auswertung der Logfiles ergab, dass der SIS-Zugang dieses Organs datenschutzkonform erfolgt.

Im Rahmen der Schengen-Assoziierungsabkommen nehmen wir jährliche Kontrollen bei den Endnutzern des SIS vor. So haben wir auch den Zugang der Mitarbeiterinnen und Mitarbeiter der Region IV des GWK einer Kontrolle unterzogen.

Bei unserer Analyse gingen wir von den Logfiles des N-SIS aus, die uns vom Bundesamt für Polizei übermittelt wurden. Wir überprüften die Zugriffe von 30 Mitarbeiterinnen und Mitarbeitern der Region IV des GWK über eine Woche. Diese Kontrolle ergab, dass offenbar keine Suche missbräuchlich oder unverhältnismässig erfolgt war. Wir haben die Kontrolle daher ohne Abgabe von Empfehlungen abgeschlossen.

1.5 Gesundheit und Forschung

1.5.1 Ausführungsbestimmungen zum Bundesgesetz über das elektronische Patientendossier

Das Bundgesetz über das elektronische Patientendossier (EPDG) wurde vom Parlament am 19. Juni 2015 verabschiedet. Die Referendumsfrist ist am 8. Oktober 2015 abgelaufen. Der sektorielle Identifikator für das elektronische Patientendossier ist damit Realität. Zahlreiche heikle Punkte müssen noch geklärt werden.

Das EPDG soll Mitte 2017 in Kraft treten. Es regelt die Grundsätze wie zum Beispiel, dass für die Identifikation von Patientinnen und Patienten nicht die Sozialversicherungsnummer, sondern ein sektorieller eHealth-Identifikator verwendet wird. Für diesen wichtigen Schritt haben wir mehrere Jahre Überzeugungsarbeit geleistet. Doch viele entscheidende Punkte werden erst in den zugehörigen Verordnungen geklärt. Im Berichtsjahr haben wir uns im Rahmen der Ämterkonsultation ausführlich zu den vorgelegten Entwürfen geäussert. Zu den wichtigsten Punkten unserer Stellungnahme zählen das für eHealth- und Stammgemeinschaften geltende Datenschutzrecht, die Zertifizierungsvoraussetzungen und die Zugangsberechtigungen.

In Bezug auf das für Gemeinschaften und Stammgemeinschaften geltende Datenschutzrecht sind wir der Ansicht, dass für das Bearbeiten von Personendaten das Bundesgesetz über den Datenschutz (DSG) zur Anwendung gelangt und wir die zuständige Aufsichtsbehörde sind. Dies muss in den Erläuterungen zur Verordnung festgehalten sein. Die Gemeinschaften müssen sich, unabhängig von der Art der Teilnehmer, als juristische Personen des Zivilrechts konstituieren und zudem ist das Verhältnis zwischen Patienten und Gemeinschaften bzw. Stammgemeinschaften zivilrechtlicher Natur. Somit gelangt hier das DSG zur Anwendung.

Unabhängig von dieser formaljuristischen Begründung drängt sich die Anwendung des DSG auch aus praktischen Gründen auf. Im Sinne der Rechtssicherheit für die Patientinnen und Patienten und auch für die übrigen Teilnehmer am System eHealth Schweiz ist es wichtig, dass für das elektronische Patientendossier an allen Standorten in der Schweiz die gleichen datenschutzrechtlichen Bestimmungen gelten und eine Aufsichtsbehörde deren einheitliche Anwendung gewährleistet. In diesem Sinne dienen die Anwendung des DSG und die Aufsicht durch uns den Gemeinschaften und Stammgemeinschaften sowie deren Betreiberorganisationen auch als Investitionsschutz. Das Bundesamt für Gesundheit (BAG) wird als sogenannter Zertifizierungsschema-Eigentümer auftreten und in Zusammenarbeit mit den akkreditierten Zertifizierern für das Einhalten der Zertifizierungsvorgaben sorgen müssen. Wir bleiben aber für die datenschutzrechtliche Aufsicht zuständig.

In Bezug auf die technischen und organisatorischen Zertifizierungsvoraussetzungen für Gemeinschaften und Stammgemeinschaften haben wir bemängelt, dass der Fokus zu stark auf die Datensicherheit gerichtet ist und die Aspekte des Datenschutzes zu wenig berücksichtigt werden. Dies steht einerseits im Widerspruch zur massgeblichen Bestimmung im EPDG, welche eine Zertifizierung vorsieht, die sowohl den Datenschutz als auch die Datensicherheit berücksichtigt. Zudem stellt das Einhalten des Datenschutzes eine zentrale Vorgabe für das elektronische Patientendossier dar. Dem ist mit einer ausreichenden Gewichtung im Rahmen der Zertifizierungsvorgaben Rechnung zu tragen.

Auch zur Möglichkeit, Gruppen von Gesundheitsfachpersonen Zugang zum elektronischen Patientendossier zu gewähren, nahmen wir Stellung. Wir wiesen darauf hin, dass die Verordnungsbestimmungen den Zugang dieser Gruppen nicht, wie von uns gefordert, restriktiv konkretisieren. Vielmehr soll es zu eigentlichen globalen Gruppenberechtigungen kommen. Die Berechtigungsvergabe stellt gemäss unserer Auffassung eine Willenserklärung dar, die nur eine Rechtswirkung entfalten kann, wenn sie gegenüber einer Person oder Stelle mit einer Rechtspersönlichkeit abgegeben wird. Eine Willenserklärung an eine Gruppe von Personen, z.B. den Mitarbeiterinnen und Mitarbeitern einer bestimmten Abteilung in einem Krankenhaus, stellt aber gemäss unserer Auffassung keine rechtsgültige Berechtigungsvergabe dar, da die Gruppe an sich keine Rechtspersönlichkeit hat.

In diesem Sinne hätten wir erwartet, dass in der Verordnung die Berechtigung von Gruppen dahingehend konkretisiert wird, dass es sich im Grundsatz um eine Berechtigungsvergabe an einzelne Personen handelt. Diese würden sodann als Gruppe in den entsprechenden Verzeichnissen der Gemeinschaft oder der Stammgemeinschaft dargestellt. Der Verordnungsentwurf geht nun aber genau in die entgegengesetzte Richtung. Er hält ausdrücklich fest, dass Patientinnen und Patienten Gruppen von Gesundheitsfachpersonen Berechtigungen erteilen können. Die Zusammensetzung der Gruppen muss lediglich jederzeit nachvollziehbar sein.

Offenbar ist sich das BAG bewusst, dass es hier zu einem problematischen Vorgang kommen kann. Denn einerseits sollen die Gemeinschaften dafür sorgen, dass die Gruppen nicht unverhältnismässig gross sind. Andererseits wird im Kommentar zu den technischen und organisatorischen Zertifizierungsvoraussetzungen vermerkt, dass nicht unverhältnismässige viele Gesundheitsfachpersonen ohne Behandlungskontext mitberechtigt werden sollen. Die Vorgabe, dass die Gruppen nicht zu gross sein dürfen, erscheint uns als wenig tauglich. Niemand wird hier einen Massstab für die Grösse der Gruppe definieren können, welcher für die Beurteilung der Verhältnismässigkeit herangezogen werden kann. Eine Vorgabe hierfür wäre im Prinzip der Behandlungskontext. Gerade diese Vorgabe wird durch die Verordnung und den erwähnten Hinweis völlig aufgeweicht. Eine nicht von der Patientin oder

dem Patienten explizit vorgenommene Berechtigungsvergabe an Gesundheitsfachpersonen, die nicht im Behandlungskontext stehen, müsste eigentlich gänzlich ausgeschlossen sein.

Ein für eHealth Schweiz definierter Grundsatz besagt, dass nur im Behandlungskontext stehende Gesundheitsfachpersonen einen Zugriff auf das elektronische Patientendossier haben sollen. Der Hinweis des BAG, dass die Anzahl der nicht im Behandlungskontext stehenden Gesundheitspersonen, welche zum Zugriff berechtigt werden, nicht zu gross sein darf, ist daher nicht nachvollziehbar. Weiter akzentuiert wird diese Problematik dadurch, dass es sich auch um dynamische Gruppe handeln darf. So wird davon ausgegangen, dass eine Gesundheitsfachperson, welche neu in die Gruppe eintritt, automatisch die entsprechenden Zugriffsberechtigungen erhalten soll. Hier kann von einer Berechtigungserteilung durch die Patientin oder den Patienten keine Rede mehr sein.

Besonders zu beachten ist auch die Rolle der Hilfspersonen der Gesundheitsfachpersonen. Diese sollen, obwohl weder im Bundgesetz noch im Verordnungsentwurf genannt, ebenfalls Zugriff auf das elektronische Patientendossier erhalten. Damit wird der Kreis der Zugriffberechtigten nochmals vergrössert. Deshalb muss für die Patienten anhand der Protokolldaten erkennbar sein, welche Hilfspersonen auf das elektronische Patientendossier zugreifen und für welche Gesundheitsfachperson diese arbeiten. Denn es ist letztlich die Gesundheitsfachperson, die für ihre Hilfspersonen verantwortlich ist.

Insgesamt haben wir bei der Analyse der uns vorgelegten Ausführungsbestimmungen zum EPDG den Eindruck erhalten, dass die klare Trennung von Primär- (z.B. Patienteninformationssystem eines Spitals oder einer Praxis) und Sekundärsystemen (z.B. Abfragedienst der Gemeinschaft) nicht mehr eindeutig angestrebt wird. Möglicherweise zeigt sich damit schon jetzt, dass sich das elektronische Patientendossier zu einer Art Primärsystem entwickeln wird.

1.5.2 Sachverhaltsabklärung beim ärztlichen Dienst des Bundes

Die Sachverhaltsabklärung beim ärztlichen Dienst der Bundesverwaltung und der bundesnahen Betriebe (MedicalService AeD) hat ergeben, dass dieser die datenschutzrechtlichen Anforderungen einhält. Das Verfahren wurde abgeschlossen.

Im Rahmen unserer Aufsichtstätigkeit haben wir ab Herbst 2014 eine Sachverhaltsabklärung bei Medical Service betreffend die Bearbeitung von Gesundheitsdaten im Arbeitsbereich durchgeführt (siehe unseren 22. Tätigkeitsbericht 2014/2015, Ziffer 1.5.4). Anlass dazu waren Anfragen mehrerer Bürger.

Wir prüften zunächst die Prozesse und Datenbearbeitungen anhand der von Medical Service eingereichten Unterlagen und nahmen dann im Januar 2015 einen Augenschein vor Ort vor. Im Vordergrund standen dabei das Geschäftsverwaltungssystem, die Organisation des MedicalServices und dessen Zugriffsrechte, die Datenaufbewahrung und -bekanntgabe an die Bundesverwaltung sowie die Datensicherheit und die Archivierung. Medical Service informiert die Bundesverwaltung lediglich über die «Schlussfolgerungen aus den ärztlichen Feststellungen» und gibt keine Diagnosen oder Resultate aus seinen Untersuchungen betreffend die gesundheitliche Eignung eines Bewerbenden bekannt.

Die Sachverhaltsabklärung hat gezeigt, dass die Organisation und die Datenbearbeitungen von MedicalService die Voraussetzungen des Bundespersonalgesetzes erfüllen und den Anforderungen des Datenschutzgesetzes entsprechen. Angesichts dieser Ergebnisse haben wir unsere Kontrolle abgeschlossen.

1.5.3 Verweigern der Auskunft über Gesundheitsdaten eines Kindes

In diesem Berichtsjahr wurden wir angefragt, ob eine Krankenkasse beim gemeinsamen Sorgerecht die Auskunft über die Gesundheitsdaten eines urteilsunfähigen Kindes an einen Elternteil verweigern darf, wenn sich das Kind nach der Scheidung oder Trennung in der Obhut des anderen Elternteils befindet.

Gemäss Artikel 8 des Bundesgesetzes über den Datenschutz (DSG) kann der gesetzliche Vertreter das Auskunftsrecht an Stelle der unmündigen und urteilsunfähigen Person stellvertretend für diese ausüben. Dies sind im Normalfall die Eltern. Unabhängig davon, wer beim gemeinsamen Sorgerecht die Obhut des Kindes hat, können beide Elternteile dieses Auskunftsrecht geltend machen und es muss beiden gewährt werden.

Die Situation ist anders zu beurteilen in Fällen, in denen zum Schutz des Kindeswohls dem einen Elternteil gewisse Informationen nicht mehr gegeben werden dürfen. Es ist jedoch nicht an der Krankenkasse eine solche, strittige Situation zu beurteilen. Auch darf sie sich nicht nach den Anweisungen des einen Elternteils richten. Sie hat sich im Streitfall an offizielle Entscheide eines Gerichts bzw. an eine Verfügung der Kindes- und Erwachsenenschutzbehörde (KESB) zu halten.

1.6 Versicherungen

1.6.1 Kontrolle der Datenannahmestellen der Krankenversicherer

Wie bereits im Tätigkeitsbericht 2014/2015 erwähnt, muss seit dem 1. Januar 2014 jeder Krankenversicherer über eine zertifizierte Datenannahmestelle (DAS) für den Empfang der Rechnungen des Typus «Diagnosis Related Groups» (DRG) verfügen. Unsere diesjährigen Kontrollen von Datenannahmestellen haben gezeigt, dass die Umsetzung der DAS gut funktioniert. In einigen Fällen haben wir Mängel festgestellt, die wir der jeweiligen Zertifizierungsstelle gemeldet haben.

Im Berichtsjahr haben wir im Rahmen von Sachverhaltsabklärungen sieben zertifizierte DAS kontrolliert. Dabei wurden auch Schnittstellen zu verschiedenen anderen Akteuren geprüft (z.B. die Schnittstelle zwischen Intermediär und DAS). Bei diesen Kontrollen stellten wir mehrheitlich dieselben Probleme fest wie im Jahr zuvor. Es sei deshalb an dieser Stelle auf die Ausführungen des 22. Tätigkeitsberichts verwiesen (Kapitel 1.6.1).

Im Laufe des Berichtsjahres fanden erneut mehrere Koordinationssitzungen mit dem Bundesamt für Gesundheit (BAG) statt. Das Ziel dieser Sitzungen war es, die sich teilweise überschneidenden Aufsichtstätigkeiten der beiden Behörden zu koordinieren und offene Fragen bezüglich DAS und damit verbundene Themen zu diskutieren.

Zudem fanden in diesem Berichtsjahr zwei Sitzungen mit den Zertifizierern der DAS sowie der Akkreditierungsstelle (SAS) statt. Auch in diesem Jahr dienten diese Sitzungen der konstruktiven Diskussion betreffend Zertifizierung, Umsetzung und Funktion der DAS, Schnittstellen zwischen den verschiedenen Akteuren (Spitäler, Intermediäre usw.) sowie auch der Klärung von Meinungsverschiedenheiten.

Rückblickend können wir feststellen, dass die Umsetzung des Artikels 59a der Verordnung über die Krankenversicherung nach wie vor erfolgreich und mehrheitlich gesetzeskonform verläuft. Die Zusammenarbeit mit den Zertifizierern, den Versicherern und den Betreibern von elektronischen DAS verlief äusserst konstruktiv.

1.6.2 Rechnungsstellung nach SwissDRG – Was muss zum Vertrauensarzt?

Im Rahmen der Rechnungstellung im Bereich SwissDRG gelangen sehr detaillierte Gesundheitsangaben mit der Rechnung und dem Medical Data Set (MCD) zum Krankenversicherer. Es stellt sich die Frage, ob diese zu den medizinischen Angaben gehören, die auch an den Vertrauensarzt übermittelt werden dürfen.

Seit 1. Januar 2012 werden die Leistungen der Spitäler und Geburtshäuser im stationären Bereich über einheitliche, an Diagnosen geknüpfte Fallpauschalen vergütet (Swiss DRG). Die Leistungserbringer müssen dazu der Datenannahmestelle des Krankenversicherers gleichzeitig mit der Rechnung das Minimal Clinical Data Set (MCD) übermitteln. Das MCD enthält die Hauptdiagnose, allfällige Nebendiagnosen und die Prozeduren in codierter Form. Die Angaben im MCD sind klarerweise als medizinische Angaben zu qualifizieren. Die eigentliche Rechnung, der sogenannte Invoice, enthält neben einigen administrativen Daten zum Leistungserbringer und zum Patienten aber auch Tarifziffern. Bei diesen handelt es sich unserer Auffassung nach um medizinische Angaben. Dies gilt insbesondere für den eigentlichen DRG-Code, der eine Tarifziffer ist, aber klare Hinweise auf den Gesundheitszustand des Patienten gibt.

Der DRG-Fallpauschalenkatalog ist so differenziert, dass die überwiegende Zahl der DRG-Codes der konkreten Diagnose schon sehr nahe kommt. Deshalb haben wir uns im Berichtsjahr intensiv mit den Fällen befasst, wo entweder der Patient die Übermittlung aller medizinischen Angaben an den Vertrauensarzt verlangt oder dies der Leistungserbringer im begründeten Fall basierend auf die entsprechende Bestimmung im Krankenversicherungsgesetz (KVG) vornimmt. Wir prüften besonders die Frage, ob auch die Rechnung mit dem DRG-Code von der Datenannahmestelle an den Vertrauensarzt und nicht an die Leistungsabteilung weitergeleitet werden muss. Grundsätzlich muss hier festgehalten werden, dass die vom «Forum Datenaustausch» vorgegebene Formatvorlage (XML 4.4) eine Kennzeichnung der Rechnung (Invoice) als «für den Vertrauensarzt bestimmt» (flag confidential) derzeit nicht zulässt. Lediglich das MCD kann vom Leistungserbringer mit dem entsprechenden Vermerk gekennzeichnet werden. Da die Formatvorlage aber ohnehin nicht den gesetzlichen Vorgaben entspricht, kann daraus nicht abgeleitet werden, dass die Rechnung nicht auch an den Vertrauensarzt adressiert sein kann.

Wie wir im Rahmen unserer Abklärungen feststellten, kennzeichnet eine grosse Anzahl von Leistungserbringern alle MCD als für den Vertrauensarzt bestimmt. Es kann aber nicht davon ausgegangen werden, dass in diesen Spitälern immer die gesetzlichen Voraussetzungen für eine Übermittlung des MCD an den Vertrauensarzt erfüllt waren. Eine ebenfalls grosse Anzahl von Spitälern kennzeichnet die MCD

nie als für den Vertrauensarzt bestimmt. Auch hier kann nicht davon ausgegangen werden, dass in diesen Spitälern kein Patient die Übermittlung der medizinischen Angaben an den Vertrauensarzt verlangt hat. Zudem erhielten wir den Eindruck, dass in einem Teil der Spitäler das confidential flag nicht im Sinne der gesetzlichen Bestimmungen verwendet wird. Sehr wahrscheinlich gelangen so zu viele MCD, aber nicht alle, die sollten, zum Vertrauensarzt.

Basierend auf den festgestellten Unklarheiten kontaktierten wir auch das Bundesamt für Gesundheit (BAG) und erkundigten uns nach dem korrekten Vorgehen in Bezug auf die Rechnung. Dem BAG zufolge handelt es sich beim DRG-Code primär um eine Tarifziffer, welche für den Versicherer (Leistungsabteilung) bestimmt ist, auch wenn der DRG-Code bis zu einem gewissen Grad auch Angaben zur Gesundheit enthält. Aufgrund einer vertieften Analyse der massgeblichen gesetzlichen Bestimmungen und weiteren Abklärungen sahen wir uns veranlasst, den Vorsteher des zuständigen Eidgenössischen Departments des Innern (EDI) über die Sachlage zu informieren.

Zu diesem Schritt bewegte uns insbesondere die Tatsache, dass die Ausweitung der Fallpauschalen und damit der Abrechnung mit Rechnungen des Typus SwissDRG auf die Bereiche stationäre Rehabilitation und stationäre Psychiatrie bevorsteht. Die bestehenden Unklarheiten sollten durch den Gesetzgeber beseitigt werden, bevor diese Ausweitung erfolgt. Der gegenwärtige Zustand ist aus der Sicht des Datenschutzes und der Patientenrechte unbefriedigend. Es macht keinen Sinn, dass der Patient oder der Leistungserbringer eine Übermittlung der medizinischen Angaben an den Vertrauensarzt veranlassen kann, wenn die Leistungsabteilung des Versicherers durch die Angaben in der Rechnung über den Gesundheitszustand des Patienten informiert wird.

In diesem Sinne ist unsere Forderung klar: Bei der Weiterentwicklung der Formatvorlage für die Rechnungen des Typus SwissDRG ist sicherzustellen, dass auch die Rechnung mit dem flag confidential gekennzeichnet werden kann. Auch die relevanten Bestimmungen im KVG und in der zugehörigen Verordnung müssen konkretisiert werden. Insbesondere muss der Inhalt der Rechnung präziser definiert werden. Die Krankenversicherer sollten die notwendigen Informationen für die Rechnungskontrolle bekommen, ohne dass das Recht des Patienten auf Übermittlung von medizinischen Angaben an den Vertrauensarzt beschnitten wird. Weiter muss mittels geeigneter Information sichergestellt werden, dass die Leistungserbringer das flag confidential korrekt einsetzen, damit eine unnötige Belastung der Vertrauensärzte der Krankenversicherer verhindert wird. Offenbar hat das EDI die Problematik erkannt und uns deshalb zugesichert, dass unsere Überlegungen bei der weiteren Gesetzgebung einbezogen werden.

1.6.3 Datenlöschung bei Unfallversicherern

Zahlreiche Bürgerinnen und Bürgern haben uns kontaktiert, da sie nicht damit einverstanden waren, dass Unfallversicherer auch jahrzehntealte Daten über sie weiterhin speichern. Das Vorgehen der Unfallversicherer ist jedoch korrekt.

Im Berichtsjahr wurden wir über unsere Beratungs-Hotline erstaunlich oft von Bürgerinnen und Bürgern kontaktiert, welche bei einem Unfallversicherer (obligatorische Unfallversicherer gemäss Bundesgesetz über die Unfallversicherung, UVG) ein Datenlöschungsgesuch gestellt hatten. Sie machten geltend, dass es sich zum Teil nur um Bagatellunfälle gehandelt habe und dass die Informationen auch schon sehr alt seien (20 Jahre und mehr).

Hier gilt es zu berücksichtigen, dass das Gesetz für Unfallversicherer keine maximalen Aufbewahrungsfristen kennt. Der Grund dafür liegt in der Erfordernis der adäquaten Kausalität zwischen dem Schadensereignis und dem eingetretenen Schaden, welche für die Leistungspflicht eines Unfallversicherers entscheidend ist. Dieser wird im Schadensfall der Frage nachgehen, ob der eingetretene Schaden adäquat kausal durch den Unfall verursacht wurde. Er wird insbesondere prüfen, ob bei der versicherten Person nicht Vorschädigungen oder Krankheitsmerkmale bestanden, welche den eingetretenen Schaden mitverursacht oder sogar bewirkt haben. Deshalb muss der Versicherer im Schadensfall auch auf alte Informationen zurückgreifen können. Die sehr lange Aufbewahrungsdauer verstösst in diesem Sinne auch nicht gegen den Grundsatz der Verhältnismässigkeit. Selbstverständlich kann ein Unfallversicherer für sich entscheiden, dass er Informationen, welche ein gewisses Alter erreicht haben, nicht mehr aufbewahren will und deshalb löscht oder vernichtet. Ein genereller Anspruch auf Löschung lässt sich daraus aber nicht ableiten.

1.6.4 Verordnung betreffend die Aufsicht über die soziale Krankenversicherung – Projekt BAGSAN

Für die Aufsicht über die sozialen Krankenversicherer verlangt das Bundesamt für Gesundheit von den Krankenversicherern sehr detaillierte Angaben zu jeder versicherten Person. Im Rahmen der Ämterkonsultation zur Verordnung betreffend die Aufsicht über die soziale Krankenversicherung haben wir uns hierzu geäussert. Die nun geltenden gesetzlichen Vorgaben sind unbefriedigend.

Am 1. Januar 2016 ist das neue Bundesgesetz betreffend die Aufsicht über die sozialen Krankenversicherer (KVAG) in Kraft getreten. Für die Ausführungsbestimmungen

auf Verordnungsstufe (KVAV) wurde im Berichtsjahr eine Ämterkonsultation durchgeführt. Aus der Sicht des Datenschutzes von besonderer Bedeutung waren hier die Bestimmungen bezüglich der Übermittlung von Individualdatensätzen zu jeder versicherten Person durch die Krankenversicherer an das Bundesamt für Gesundheit (BAG). Diese Individualdatensätze möchte das BAG für die neuen respektive konkretisierten Aufsichtsaufgaben verwenden. In diesem Zusammenhang steht auch das Projekt BAGSAN, ein Statistikprojekt zur Umsetzung der Strategie «Gesundheit 2020» des Bundesrates. Es soll die Grundlagen für eine effizientere Steuerung des Gesundheitssystems liefern.

Im Rahmen der Ämterkonsultation haben wir uns intensiv mit den zu liefernden Individualdatensätzen und insbesondere mit dem Übermittlungsprozess an das BAG befasst. Aufgrund dieser Analyse haben wir das BAG darauf hingewiesen, dass der vorgesehene Übermittlungsprozess im Widerspruch steht zur Verpflichtung der Krankenversicherer, die Anonymität der Versicherten zu wahren. Dieser würde nämlich zu einer Übermittlung von pseudonymisierten Personendaten führen. Unserer Ansicht nach ist das Wahren der Anonymität der Versicherten unter diesen Umständen primär eine Aufgabe des datenempfangenden und weiterbearbeitenden Bundesamtes, in diesem Fall des BAG. Das ergibt sich auch aus dem Umstand, dass es das Recht bekommen sollte, die hier angesprochenen Daten mit Daten aus anderen Quellen zu verknüpfen. Weiter haben wir das BAG darauf hingewiesen, dass ein Teil der zu übermittelnden Angaben als besonders schützenswerte Personendaten eingestuft werden muss und die Krankenversicherer, als Bundesorgane im obligatorischen Versicherungsbereich, für deren Weiterleitung an das BAG eine gesetzliche Grundlage in einem Bundesgesetz benötigen.

Wie wir bei einer zweiten Ämterkonsultation sodann feststellten, wurden die Bestimmungen betreffend Übermittlung von Versichertendaten aus der KVAV gestrichen. Hingegen wurde die Verordnung zur Krankenversicherung (KVV) so angepasst, dass die von den Versicherern gemäss dieser Verordnung zu liefernden Aufsichtsdaten auch für die Zwecke des KVAG genutzt werden dürfen. Dieses Vorgehen erachten wir aus zwei Gründen als problematisch. Der erste Grund ist gesetzgebungstechnischer Natur. Ein Teil der Ausführungsbestimmungen des KVAG befindet sich jetzt nicht in der zugehörigen KVAV sondern in der KVV. Dies dürfte für Verwirrung sorgen. Zweitens ist die Bedeutung der jetzigen Bestimmungen in der KVV hoch umstritten, da sie derzeit auf einer sehr unklaren Bestimmung im KVG beruhen. Deshalb sollte der Gesetzgeber sie bei nächster Gelegenheit konkretisieren und auf der korrekten Normenebene erlassen. Wir haben dies dem BAG im Rahmen unserer Beratungstätigkeit mitgeteilt. Bis zum Erlass neuer Bestimmungen haben die Krankenversicherer die geltenden Vorgaben der KVV zu respektieren und bei der Datenübermittlung an das BAG die Anonymität der Versicherten zu wahren.

1.6.5 Verordnung über den Risikoausgleich in der Krankenversicherung

Die Verfeinerung des Risikoausgleichs soll die Krankenversicherungen mit schlechter Risikostruktur weiter entlasten. Notwendig dafür sind neue Lieferungen von Individualdaten mit Angaben zu den bezogenen Arzneimitteln von den Krankenversicherern an die Gemeinsame Einrichtung KVG.

Im Rahmen der Ämterkonsultation haben wir uns zur Revision der Verordnung über den Risikoausgleich in der Krankenversicherung geäussert. Die Revision dient der Verfeinerung des Risikoausgleichs und damit einer weiteren Entlastung von Krankenversicherern mit einer schlechten Risikostruktur. Zwecks Berechnung des Risikoausgleichs liefern die Krankenversicherer der Gemeinsamen Einrichtung KVG die Daten, welche eine Gruppierung der Versicherten nach mehreren Risikoindikatoren erlaubt. Neben den bereits vorhandenen Indikatoren Alter, Geschlecht und Aufenthalt in einem Spital oder Pflegeheim sollen neue Indikatoren eingeführt werden. Es handelt sich dabei um die Pharmazeutische Kostengruppe (PCG), welche mit Daten aus dem ambulanten Bereich gebildet wird, und die Arzneimittelkosten.

Damit wird berücksichtigt, dass ein erheblicher Anteil der Kosten im Krankenversicherungsbereich durch kostenintensive medikamentöse Behandlungen entsteht. Da hierfür erstmals Individualdaten der einzelnen Versicherten mit Angaben zu den von ihnen bezogenen Arzneimitteln geliefert werden müssen, erhält die Datenübermittlung der Krankenversicherer an die gemeinsame Einrichtung KVG aus datenschutzrechtlicher Sicht eine neue Qualität.

Zum Zeitpunkt der Ämterkonsultation war noch nicht klar, wie die Datenlieferung konkret erfolgen soll, da die Gemeinsame Einrichtung KVG hierfür noch ein neues Erhebungstool entwickeln (lassen) muss und die Übermittlung laut Verordnung gemäss den Weisungen der Gemeinsamen Einrichtung KVG zu erfolgen hat. Lediglich in den Erläuterungen zum Verordnungsentwurf war festgehalten, dass die Daten in anonymisierter Form geliefert werden müssen. Zudem waren die zu liefernden Datensätze in der Verordnung nicht klar definiert. Deshalb sollte eigentlich das Bundesamt für Gesundheit die Vorgaben für die Datenübermittlung erlassen und die Datensätze in der Verordnung klar definieren.

Wir hielten auch fest, dass es hier nicht zu einer Übermittlung von anonymisierten Daten, sondern von pseudonymisierten Personendaten kommen wird. Soweit uns bekannt ist, wurden in der Folge die zu liefernden Datensätze in den Verordnungsentwurf entsprechend unseren Hinweisen integriert und präzisiert, dass es sich um eine Übermittlung in pseudonymisierter Form handelt. Hingegen wurde daran

festgehalten, dass die Gemeinsame Einrichtung die Vorgaben für die Datenübermittlung erlässt. Das BAG wird bezüglich der Weisungen aber von ihr konsultiert werden und muss ihre Weisungen genehmigen. So übernimmt hier das zuständige Bundesorgan richtigerweise die Verantwortung für die zu befolgenden Übermittlungsmodalitäten.

1.7 Arbeitsbereich

1.7.1 Personensicherheitsprüfung von Mitarbeitenden (im Privatbereich)

Aufgrund verschiedener Anfragen haben wir die Anforderungen für die Personensicherheitsüberprüfungen im Privatbereich abgeklärt und Erläuterungen zu diesem Thema verfasst.

Wir wurden von Dienstleistungserbringern für Finanzinstitute angefragt, inwiefern es datenschutzrechtlich erlaubt sei, bestimmte Daten ihrer Mitarbeitenden, wie z.B. Auszüge aus dem Betreibungs- oder Strafregister, an die Auftrag gebenden Finanzinstitute weiterzuleiten. Die Finanzinstitute würden diese Informationen benötigen, um sich zu vergewissern, dass die Datensicherheit gewährleistet ist.

Aufgrund dieser Anfragen haben wir uns vertieft mit dieser Problematik auseinandergesetzt. Dazu haben wir uns einerseits mit Finanzinstituten und andererseits mit der entsprechenden Aufsichtsbehörde getroffen, um die verschiedenen Anforderungen und Bedürfnisse im Bereich der Überprüfung von Mitarbeitenden zu kennen. So wurde uns beschrieben, wie die Überprüfung je nach Risikopotential der Mitarbeitenden variiert und welche bereichsspezifischen Vorschriften gelten. Zudem wurde uns erläutert, dass eine unterschiedliche Handhabung von internen und externen Mitarbeitenden nicht zweckmässig sei.

Wir haben danach unter Berücksichtigung der relevanten Bestimmungen des Datenschutzgesetzes und des Obligationenrechts die Sachlage analysiert. Besondere Beachtung wurde dabei der Verhältnismässigkeit geschenkt, die jedoch nur im Einzelfall konkret überprüft werden kann. Für die privaten Arbeitgeber und die betroffenen Mitarbeitenden haben wir Erläuterungen mit datenschutzrechtlichen Vorgaben verfasst, die bei der Risikoprüfung beachtet werden sollten. Diese Erläuterungen wurden auf unserer Website veröffentlicht.

1.7.2 Whistleblowing-Meldestelle des Bundes

Das Bundesgericht hat in der Angelegenheit Whistleblowing-Meldestelle des Bundes auf Nichteintreten entschieden, weshalb das Urteil des Bundesverwaltungsgerichts nun in Kraft getreten ist.

Wie wir im 22. Tätigkeitsbericht 2014/2015 (Ziffer 1.7.3) berichteten, hat die Eidgenössische Finanzkontrolle (EFK), welche die Meldestelle betreibt, das Urteil des Bundesverwaltungsgerichts in Sachen Whistleblowing-Meldestelle an das Bundesgericht weitergezogen. Mit Urteil vom 12. November 2015 hat dieses auf Nichteintreten

entschieden. Als Begründung führte das Gericht aus, dass die EFK als Beschwerdeführerin keine Beschwerdelegitimation besitze. Es trat demnach mangels Legitimation bzw. Erfüllung der Begründungsanforderungen nicht auf die Beschwerde ein. Somit tritt das Urteil des Bundesverwaltungsgerichts vom 16. Dezember 2014 in Kraft und verpflichtet die EFK, ihre Datensammlung bei uns anzumelden und ein Bearbeitungsreglement zu erstellen.

1.8 Handel und Wirtschaft

1.8.1 Urteil des Europäischen Gerichtshofs zu Safe Harbor und die Folgen für die Schweiz

In seinem Urteil vom 6. Oktober 2015 hat der Europäische Gerichtshof das Datenschutzabkommen Safe Harbor zwischen der EU und den USA für ungültig erklärt. Das Gericht hielt fest, dass die Übermittlung personenbezogener Daten in die USA unter dem Regime des Safe-Harbor-Abkommens problematisch ist. Was bedeutet dieses Urteil für die Schweiz?

Der Gerichtshof der Europäischen Union (EuGH) hat in seinem Urteil vom 6. Oktober 2015 in der Rechtssache C-362/14 (Schrems) die Entscheidung der Kommission, wonach die Vereinigten Staaten von Amerika ein angemessenes Schutzniveau übermittelter personenbezogener Daten gewährleisten, für ungültig erklärt. Wie der EuGH dabei festhält, bestehe für Daten, die im Rahmen des sogenannten Safe-Harbor-Abkommens in die USA übermittelt werden, kein genügender Schutz gegen unverhältnismässige Behördenzugriffe. Auch existiere für Personen ausserhalb der USA kein wirksamer Rechtsschutz vor solchen Zugriffen.

Die Schweiz hat mit den USA im Jahre 2008 ein vergleichbares und inhaltlich sehr ähnliches Abkommen, das U.S.-Swiss Safe Harbor Framework (nachfolgend Safe-Harbor-Abkommen Schweiz-USA) abgeschlossen. Wir haben daher die aktuelle Situation für Datenübermittlungen in die USA analysiert und sind zum Schluss gelangt, dass die vom EuGH aufgezeigten Schwachstellen auch auf das Safe-Harbor-Abkommen Schweiz-USA zutreffen:

Letzteres ist ein System mit Selbstzertifizierung für Unternehmen, welche Daten aus der Schweiz in die USA importieren möchten. Die darin enthaltenen Datenschutzgarantien binden jedoch nur die zertifizierten Unternehmen selbst, nicht aber staatliche Behörden. Es existieren keine anderweitigen innerstaatlichen oder vertraglichen Regelungen, welche Behördenzugriffe auf diese Daten einschränken. Dagegen lassen gewisse innerstaatliche Regelungen die generelle Speicherung von Personendaten durch US-Behörden ohne Differenzierung, Einschränkung, Ausnahme oder Beschränkung des Zugangs oder der Nutzung zu. Damit besteht kein angemessener Schutz gegen unverhältnismässige Zugriffe auf aus der Schweiz in die USA übermittelte Personendaten durch US-Behörden.

Dieser Umstand stand bei der Prüfung nötiger Garantien im Abkommen zwischen der Schweiz und den USA im Jahre 2008 noch nicht im Zentrum. Damals konnte in guten Treuen davon ausgegangen werden, dass die Behördenpraxis bei der Bearbeitung von Personendaten in beiden Ländern vergleichbar ist, weshalb

hier kein Regelungsbedarf erkannt wurde. Durch die Enthüllungen von Edward Snowden haben sich nun aber deutliche Diskrepanzen in der Auffassung der beiden Länder darüber gezeigt, was zur Wahrung der nationalen Sicherheit zulässig sein soll. So bestehen heute zumindest ernsthafte Zweifel daran, ob die durch US-Geheimdienste praktizierten Zugriffe auf Personendaten von Nicht-US-Bürgern nach Schweizer Auffassung noch als verhältnismässig eingestuft werden können. Zudem hat sich gezeigt, dass die zertifizierten US-Unternehmen Zugangsgesuchen von US-Behörden in der Regel sofort nachkommen, ohne dass die Garantien des Safe-Harbor-Abkommens berücksichtigt würden.

Auch die im Abkommen vorgesehenen Massnahmen zum Rechtsschutz der betroffenen Personen binden stets nur die zertifizierten Unternehmen selbst. Ein wirksamer Rechtsschutz gegen Behördenzugriffe existiert dagegen für Personen ausserhalb der USA nicht. Diese haben damit keine Möglichkeiten, sich in einem rechtsstaatlichen Verfahren gegen die Bearbeitung ihrer Daten durch US-Behörden zu wehren.

Auch wenn der Entscheid des EuGH, das europäische Safe-Harbor-Abkommen für ungültig zu erklären, das Schweizer Abkommen nicht direkt betrifft, kann die Schweiz in der Sache keine andere Haltung vertreten. Würde sie unverändert am eigenen Abkommen festhalten, könnte ein solches Vorgehen, nebst den oben ausgeführten Risiken für die Grundrechte betroffener Personen aus der Schweiz, auch zur Konsequenz haben, dass die EU ihre Angemessenheitserklärung zum Datenschutzniveau in der Schweiz aufhebt. Dies insbesondere deshalb, da bei Beibehalten des ursprünglichen Abkommens eine Umgehung allfälliger neuer, strengerer Vereinbarungen mit den USA durch einen Datentransfer EU-Schweiz-USA möglich wäre. Eine Aufhebung der Angemessenheitserklärung hätte schwerwiegende Konsequenzen für den freien Austausch von Personendaten mit EU-Staaten und könnte zur Isolation der Schweiz führen.

Auch die verbleibende Möglichkeit, ein angemessenes Schutzniveau beim Datenaustausch mit den USA mit vertraglichen Garantien sicherzustellen (gemäss Art. 6 Abs. 2 des Datenschutzgesetzes), kann einen unverhältnismässigen Zugriff auf Personendaten durch U.S.-Behörden nicht verhindern, da ein solcher Vertrag zwischen Exporteur und Importeur für die Behörde nicht bindend ist.

Eine Klärung dieser Situation kann nur auf politischer Ebene erwirkt werden. Wir haben daher dem Bundesrat empfohlen, das U.S.-Swiss Safe Harbor Framework zu sistieren oder zu kündigen. Es soll neu verhandelt werden, um die Anforderungen des Schweizer Datenschutzrechts zu erfüllen. Da nur ein gemeinsames Vorgehen mit der EU und ihren Mitgliedsstaaten zielführend ist, soll die Schweiz ihr Vorgehen mit den zuständigen Behörden der Europäischen Union koordinieren.

Der Bundesrat hat die Situation aufgrund unserer Empfehlungen sowie entsprechender parlamentarischer Interpellationen analysiert und den von uns aufgezeigten Handlungsbedarf bestätigt. Er hat erklärt, das Vorgehen der EU zu beobachten und seine Massnahmen mit ihr zu koordinieren.

Da der Datenaustausch mit Unternehmen in den USA bis zur Klärung der Lage nicht einfach unterbrochen werden kann, müssen sich betroffene Unternehmen für die Zwischenzeit zusätzlich absichern. Dabei stehen ergänzende vertragliche Garantien im Vordergrund. Auch wenn damit, wie bereits ausgeführt, das Problem unverhältnismässiger Behördenzugriffe nicht vollständig gelöst werden kann, sollte auf diesem Weg das Datenschutzniveau im Vergleich zu den Garantien des Safe-Harbor-Abkommen Schweiz-USA immerhin verbessert werden, indem zusätzlich folgendes geregelt wird:

Wenn der Zugriff auf Personendaten durch US-Behörden schon nicht eingeschränkt oder verhindert werden kann, so muss dieser Mangel durch erhöhte Anforderungen an die Transparenz der Datenbearbeitung wenigstens ansatzweise kompensiert werden. Dementsprechend müssen die betroffenen Personen klar und möglichst umfassend darüber informiert werden, dass ihre Daten in die USA übermittelt werden und dass die dortigen Behörden darauf zugreifen können. Betroffene Personen müssen bei der Geltendmachung ihrer Rechte in den USA im zumutbaren Rahmen unterstützt werden. Zugangsgesuche von U.S.-Behörden dürfen nicht unbesehen erfüllt werden. Vielmehr müssen die Unternehmen die ihnen offenstehenden Verfahren zur Verhinderung solcher Zugriffe tatsächlich durchführen und darauf ergehende Urteile akzeptieren. Dabei gilt es zu beachten, dass die betroffenen Personen in der Schweiz stets die Möglichkeit haben, eine geplante Datenlieferung in die USA durch ein Zivilgericht beurteilen zu lassen. In diesen Fällen sollte mit der Datenlieferung bis zum Vorliegen eines rechtskräftigen Urteils zugewartet werden.

Weiterführende Informationen dazu können auf unserer Website nachgelesen werden.

1.8.2 Gesetzliche Grundlagen für Smart Metering in der Schweiz

Im Rahmen der Vorbereitung von gesetzlichen Grundlagen zur schweizweiten Einführung von «intelligenten Stromzählern» (Smart Meter) nahmen wir an der Begleitgruppensitzung des Bundesamtes für Energie (BFE) teil. Basierend auf den Ergebnissen haben wir das BFE bei der Ausarbeitung der gesetzlichen Bestimmungen beraten.

Das Bundesamt für Energie hat uns zur Begleitgruppe Datensicherheit und Datenschutz beim Smart Metering eingeladen, welche die Grundlagen für eine

schweizweite einheitliche Regelung dieser Technologie erarbeitete. Wir konnten uns zu den datenschutzrechtlichen Anforderungen an die Datenbearbeitung im Rahmen des Smart Meterings äussern, insbesondere zur Zweckbindung und der Aufbewahrung der erfassten Daten.

Basierend auf diesen Grundlagen hat uns das BFE Gesetzesbestimmungen unterbreitet, welche eine einheitliche Regelung des Datenschutzes bei Smart Metering in der Schweiz darstellen sollen. Das BFE konnte die überarbeiteten Bestimmungen noch in die laufenden parlamentarischen Beratungen zur Energiestrategie 2050 einfliessen lassen, damit die Voraussetzung für die schweizweite Einführung des Smart Meterings geschaffen werden können (vgl. 22. Tätigkeitsbericht 2014/2015, Ziffer 1.8.1 und 21. Tätigkeitsbericht 2013/2013, Ziffer 1.8.1).

1.8.3 Kundenkarte im Detailhandel

Einwilligungsklauseln in Allgemeinen Geschäftsbedingungen (AGB) können problematisch sein. Mit der Einführung der Warenkorbanalyse bei Coop Supercard ging eine AGB-Änderung einher, mit der Coop die Zustimmung zur Analyse der Einkaufsdaten einholte. Die Kunden haben die neuen AGB durch Setzen eines Häkchens akzeptieren können und wurden dort nochmals kurz auf die Warenkorbanalyse und auf die relevanten Ziffern in den AGB hingewiesen.

Coop bietet ihre Kundenkarte Supercard seit dem Jahr 2000 an. Heute benutzen rund drei Millionen Haushalte in der Schweiz eine Supercard. Im Jahr 2005 haben wir die Datenbearbeitung im Zusammenhang mit dieser Kundenkarte kontrolliert und verschiedene Verbesserungsvorschläge und Empfehlungen im Schlussbericht erlassen. Gegenstand der neuen Kontrolle war einerseits die Umsetzung unserer damaligen Vorschläge und Empfehlungen. Andererseits wollten wir die wesentlichen Veränderungen im Zusammenhang mit dem Supercard-Programm festhalten und datenschutzrechtlich beurteilen.

Unsere Abklärungen ergaben, dass Coop sämtliche Vorschläge und Empfehlungen aus dem Schlussbericht von 2005 umgesetzt hat. Die bedeutsamste Neuerung bei Supercard stellt die im September 2012 eingeführte Analyse der Einkaufsdaten (Warenkorbanalyse) zur gezielten Kundenansprache dar. Dazu hat Coop die Allgemeinen Geschäftsbedingungen (AGB) zur Supercard angepasst. Darin wird transparent über Art und Zweck der Datenbearbeitung und die Rechte der betroffenen Personen informiert. Bestehende Kunden wurden beispielsweise an den sogenannten «Superboxen» in den Coop-Filialen auf die AGB-Änderungen hingewiesen und aufgefordert, ihre Zustimmung zu erteilen. Auch ohne diese Zustimmung ist eine Nutzung der Supercard ohne übermässige Nachteile weiterhin möglich.

Neue Teilnehmer am Supercard-Programm müssen die neuen Bestimmungen und damit die Warenkorbanalyse akzeptieren. Da die Umstellung der Datenbearbeitung zur Warenkorbanalyse für bestehende Kunden eine grosse Änderung bedeutet, kann eine einseitige Änderung der AGB trotz Akzeptanz durch den Kunden an der «Superbox» problematisch sein: Einzelne Kunden waren sich unter Umständen der Tragweite der Datenbearbeitung nicht bewusst oder haben die neuen AGB bloss flüchtig gelesen. Coop hat dieses Problem entschärft, indem sie am Ort der Zustimmung zu den neuen AGB nochmals auf die Warenkorbanalyse und die relevanten Ziffern hinwies. Die Warenkorbanalyse war im Zeitpunkt unserer Kontrolle noch nicht vollständig umgesetzt.

Wir konnten jedoch feststellen, dass Coop sich der datenschutzrechtlichen Problematik in diesem Zusammenhang bewusst ist und sich bemüht, die entsprechende Umsetzung in den Systemen sorgfältig auszuarbeiten. Besonders hervorzuheben ist dabei die transparente Information gegenüber den Kunden, sei es auf der Website von Supercard oder in entsprechenden Medienartikeln in ihrer Kundenzeitschrift. Trotz des insgesamt positiven Gesamtbilds formulierten wir in unserem Schlussbericht Verbesserungsvorschläge bezüglich Transparenzerfordernissen und Auskunftserteilung. Coop hat diese allesamt angenommen und Umsetzungsvarianten zugesichert.

1.8.4 Internet-Tauschbörsen und Urheberrecht – Revision des Urheberrechtsgesetzes

Der mit der Revision des Urheberrechts geplante Informationsanspruch im Zivilverfahren, die Zustellung von Warnhinweisen sowie das für bestimmte Fälle vorgesehene Stay-Down-Verfahren sind aus Datenschutzsicht problematisch.

Das Bundesgesetz über das Urheberrecht und verwandte Schutzrechte (URG) wird revidiert. Mit der Revision sollen insbesondere die von der Arbeitsgruppe AGUR12 vorgeschlagenen Massnahmen zur Verbesserung des Urheberrechtsschutzes im Internet umgesetzt werden (vgl. unseren 21. Tätigkeitsbericht 2013/2014, Ziffer 1.3.1). Einige dieser Massnahmen werfen aus Sicht des Datenschutzes Fragen auf:

Mit dem revidierten URG soll im Rahmen der zivilrechtlichen Leistungsklage ein Informationsanspruch eingeführt werden. Wer als Rechteinhaber gegen einen Rechteverletzer klagen möchte, von dem er nur die IP-Adresse kennt (was z.B. regelmässig bei via Peer-to-Peer-Netzwerken zum Download angebotenen Werken der Fall ist), soll von den Internetanbietern Auskunft darüber erhalten, welche Person im fraglichen Zeitpunkt Inhaber besagter IP-Adresse war.

Diese Information muss von den Internetanbietern heute aufgrund des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) während eines halben Jahres gespeichert werden und ist durch das Fernmeldegeheimnis geschützt. Die Speicherpflicht wurde zur Bekämpfung schwerer Straftaten eingeführt und ist rechtsstaatlich heikel: Sie stellt einen schweren Eingriff in die Persönlichkeitsrechte der Internetnutzer dar. Deren Daten werden ohne konkreten Anlass auf Vorrat gespeichert, was im Grunde genommen als unverhältnismässige Datenbearbeitung einzustufen ist. Bei der Einführung des BÜPF wie auch in den Diskussionen zur laufenden BÜPF-Revision (vgl. Kap. 1.4.1 des vorliegenden Tätigkeitsberichts) wurde denn auch immer wieder betont, dass nur die Aufklärung schwerer Straftaten diesen Eingriff rechtfertigte. Es wurde stets bekräftigt, dass eine Beschränkung der Verwendung der Vorratsdaten auf den Strafprozess notwendig sei. Auch der Europäische Gerichtshof (EuGH) verlangt in seinem Urteil vom 8. April 2014 zur Vorratsdatenspeicherung, dass Strafverfolgungsbehörden nur unter strengen Voraussetzungen Zugang zu den Randdaten erhalten dürfen. In diesem eng gesteckten Rahmen hat denn auch der EDÖB die Vorratsdatenspeicherung als gerechtfertigt eingestuft.

Trotzdem sollen diese Daten nun zur Durchsetzung zivilrechtlicher Ansprüche im Zusammenhang mit Urheberrechtsverletzungen verwendet und den Rechteinhabern zugänglich gemacht werden. Damit entfernt man sich weit vom ursprünglichen Zweck der Vorratsdatenspeicherung und widerspricht zum einen den bei ihrer Einführung gemachten Beteuerungen. Zum anderen verlässt man auch den vom EuGH im erwähnten Urteil gesteckten engen Rahmen. Da sich eine Privilegierung urheberrechtlicher Ansprüche gegenüber anderen zivilrechtlichen Forderungen kaum objektiv begründen liesse, kann zudem davon ausgegangen werden, dass solche Daten über kurz oder lang in sämtlichen zivilrechtlichen Forderungsprozessen zugänglich wären.

Da die Vorratsdatenspeicherung schwere Eingriffe in die Persönlichkeitsrechte sämtlicher Internetnutzer verursacht, vertreten wir klar die Auffassung, dass sich die damit einhergehende Verletzung des Fernmeldegeheimnisses mit der Durchsetzung zivilrechtlicher Forderungen nicht rechtfertigen lassen. Eine derartige Bestimmung würde gegen die Grundsätze der Verhältnismässigkeit und der Zweckbindung verstossen.

Gleichermassen beurteilen wir die ebenfalls geplante Massnahme, dass Internetanbieter ihren Kunden Warnhinweise zustellen müssen, wenn von deren Anschluss aus Urheberrechtsverletzungen begangen werden und die Rechteinhaber dies verlangen. Auch diese Massnahme greift auf die ursprünglich zur Verfolgung schwerer Straftaten gesammelten Daten zurück, weshalb das bisher Gesagte auch dafür gilt.

Neu sollen Hosting-Provider zudem künftig nicht nur dazu verpflichtet werden, Urheberrechte verletzende Inhalte zu löschen, was aus datenschutzrechtlicher Sicht unbedenklich ist. Vielmehr sollen sie in gewissen Fällen auch dafür sorgen, dass diese Inhalte nicht erneut hochgeladen werden. Ein solches Stay-Down-Verfahren ist unseres Erachtens nur mit einer Überwachung der fraglichen Nutzer wirksam durchsetzbar, also mit einer Massnahme, welche noch tiefer in die Persönlichkeitsrechte der Betroffenen eingreift als der Informationsanspruch der Rechteinhaber. Die verfolgten Interessen wiegen im Vergleich zu wenig schwer, als dass sich ein solcher Eingriff rechtfertigen liesse. Wir beurteilen die Massnahme daher als unverhältnismässig. Zudem würde diese Überwachung auf Veranlassung Privater durch Private (d.h. durch die Provider) durchgeführt, so dass sie auch aus rechtsstaatlichen Überlegungen problematisch ist.

Aus diesen Gründen haben wir uns im laufenden Revisionsverfahren gegen diese Massnahmen ausgesprochen.

1.8.5 Sachverhaltsabklärung zur Kredit- und Wirtschaftsauskunftei Moneyhouse

Wir haben gegen die Auskunftei Moneyhouse Klage vor Bundesverwaltungsgericht eingereicht, weil diese nicht alle unsere Empfehlungen angenommen hatte. Unter anderem erwarten wir eine Klärung des Begriffs des Persönlichkeitsprofils und hoffen, dass ein Entscheid noch in diesem Jahr gefällt wird.

In unseren zwei letzten Tätigkeitsberichten haben wir über unsere Sachverhaltsabklärung und die Empfehlungen betreffend die von itonex AG betriebene Plattform www.moneyhouse.ch berichtet (vgl. insbesondere 22. Tätigkeitsbericht 2014/2015, Ziffer 1.8.3). itonex AG hat übrigens im Berichtsjahr den Namen des Unternehmens in Moneyhouse AG geändert (nachfolgend Moneyhouse). Da das Unternehmen gewisse Empfehlungen nicht annahm, legten wir die strittigen Fragen nun dem Bundesverwaltungsgericht zum Entscheid vor.

Unsere Klage betrifft insbesondere folgende Punkte:

- Moneyhouse veröffentlicht Personendaten der eigenen Datensammlung und verknüpft diese mit Daten von anderen Dienstleistungsanbietern. Wir sind der Meinung, dass schon die Zusammenstellung der eigenen Daten Persönlichkeitsprofile darstellen und Moneyhouse zudem den Besuchern der Plattform die weitere Zusammenstellung von noch umfassenderen Profilen ermöglicht. Die Persönlichkeit der betroffenen Personen wird durch diese Bearbeitung verletzt. Die Verletzung kann nur durch das Einholen der Einwilligung gerechtfertigt werden. Wir möchten mit unserer Klage erreichen, dass Moneyhouse

entweder die angebotenen Dienstleistungen so anpasst, dass keine Persönlichkeitsprofile mehr bearbeitet werden oder dass die Einwilligung aller Personen eingeholt wird, deren Persönlichkeitsprofile von Moneyhouse selber oder von Besuchern der Plattform bearbeitet werden.

- Die Suchmaschinenindexierung aller Inhalte der Datensammlung durch Moneyhouse verstösst gegen das Verhältnismässigkeitsprinzip. Wir fordern deshalb vom Unternehmen, die Auffindbarkeit von im Handelsregister eingetragenen Personen so anzupassen, dass sie der vom Eidgenössischen Amt für Handelsregister mit der Website www.zefix.ch aktuell verfolgten Praxis entspricht.
- Da Moneyhouse bei der Auskunftserteilung nur die in der eigenen Datensammlung gespeicherten Daten bekannt gibt, wollen wir, dass das Unternehmen erhaltene Auskunftsgesuche an die Partner der Plattform weiterleitet. Damit wird es betroffenen Personen erleichtert, ihre weiteren Rechte auszuüben, wie zum Beispiel ihre Daten berichtigen oder löschen zu lassen.
- Schliesslich soll Moneyhouse die Qualität der Daten verbessern, indem das Unternehmen vermehrt überprüft, ob diese richtig sind. Im Bereich der Bonitätsabfragen soll Moneyhouse häufiger kontrollieren, ob abfragende Kunden tatsächlich einen Interessensnachweis vorweisen können. D.h. das Unternehmen muss prüfen, ob die Abfrage der Bonität einer Person durch den Kunden der Plattform im Rahmen von Vertragsverhandlungen gemacht wird.

Wir hoffen, dass das Bundesverwaltungsgericht im Laufe dieses Jahres entscheiden wird und erwarten durch den Entscheid eine Klärung der Rechtslage, insbesondere durch die Auslegung des Begriffs des Persönlichkeitsprofils.

1.8.6 Umsetzung der Auskunfts- und Widerspruchsrechte bei einem Adresshändler – Verfahren vor dem Bundesverwaltungsgericht

Im letzten Berichtsjahr erliessen wir eine Empfehlung gegenüber einem Adresshändler, der die Auskunfts- und Löschungsgesuche mehrerer Personen nicht beantwortet hatte (siehe unser 22. Tätigkeitsbericht 2014/2015, Ziffer 1.8.4). Das fragliche Unternehmen reagierte nicht auf unsere Empfehlung und setzte die darin enthaltenen Vorgaben auch nicht um. Nachdem sich weitere Personen bei uns in dieser Angelegenheit beschwerten, legten wir die Sache im Sommer 2015 dem Bundesverwaltungsgericht zur Beurteilung vor. Das Verfahren ist noch hängig.

Die betroffenen Personen wiesen wir darauf hin, dass sie zur Durchsetzung ihrer Auskunfts- und Widerspruchsrechte nach Datenschutzgesetz eine Zivilklage einreichen können.

1.8.7 Unzulässige Werbeanrufe eines Call Centers

Mehrere Personen haben sich im Berichtsjahr bei uns über unerwünschte Werbeanrufe eines Call Centers beschwert. Das Call Center habe angegeben, eine Umfrage im Auftrag des Schweizerischen Datenschutzes durchzuführen. Das eigentliche Ziel des Telefonats war es, ein Werbesperre-Angebot zu verkaufen. Angerufen wurden auch Personen mit Sterneintrag im Telefonbuch.

Wir haben die Firma aufgefordert, Werbeanrufe bzw. Umfragen mit Bezug auf unsere Behörde umgehend zu unterlassen und die Sterneinträge zu beachten. Da das geschilderte Vorgehen gegen das Bundesgesetz gegen den unlauteren Wettbewerb (UWG) verstösst, meldeten wir den Fall zusätzlich dem Staatssekretariat für Wirtschaft.

1.9 Finanzen

1.9.1 Bearbeitung von Kundendaten bei Postfinance

Die Integration von zusätzlichen Finanzinstrumenten in eine bestehende E-Banking-Plattform stellt unter Umständen eine Zweckänderung der Datenbearbeitung dar, welche der Zustimmung der Kunden bedarf. Im Rahmen unserer Sachverhaltsabklärung bei Postfinance hat das Unternehmen mehrere Verbesserungen akzeptiert, um den Kunden Wahlmöglichkeiten zu bieten.

Postfinance hat im vergangenen Jahr ihre E-Banking-Plattform überarbeitet und in diesem Zusammenhang die Teilnahmebestimmungen angepasst. Darin wurde festgelegt, dass das sogenannte E-Cockpit, ein Instrument, das grundsätzlich jede Transaktion eines Kunden automatisch einer bestimmten Datenkategorie zuteilt, zwingend in die E-Banking-Oberfläche integriert wird. Desweitern sollte ein Tool eingeführt werden, das den Kunden aufgrund ihrer Transaktionen Werbeangebote von Dritten anzeigt. Eine nachträgliche Abmeldung der Kunden (Opt-out) für Werbeangebote von Dritten sollte im Gegensatz zu E-Cockpit möglich sein.

Die Postfinance-Kunden wurden nach ihrer Anmeldung auf dem Portal aufgefordert, die neuen Bestimmungen zu akzeptieren, damit sie weiterhin Zugang zum E-Banking haben. Wir haben die Datenbearbeitung im Zusammenhang mit diesen Neuerungen im Rahmen einer Sachverhaltsabklärung untersucht. Gleichzeitig verlangten wir von Postfinance, ihren Kunden auch nach Inkraftsetzung der neuen Teilnahmebestimmungen weiterhin Zugang zu E-Finance zu gewähren. Dies – mindestens für die Dauer unserer Abklärungen – auch dann, wenn sie die neuen Bedingungen nicht akzeptiert haben. Die darauf folgenden Gespräche mit Postfinance ergaben, dass die Kunden bereits auf der Zwischenseite nach dem Einstieg in die E-Banking-Plattform eine Option zum Abmelden von Werbeangeboten von Dritten erhalten.

Nach weiteren Sitzungen mit Postfinance konnten Anfang April 2015 zwei weitere wesentliche Verbesserungen erzielt werden: Die Kunden erhielten die Möglichkeit, die Datenbearbeitung bei E-Cockpit zu deaktivieren und die bereits kategorisierten Daten zu löschen. Was die Werbeangebote von Dritten betrifft, wird Postfinance die Einwilligung bei denjenigen Kunden, die den neuen Teilnahmebestimmungen bereits vor der Einführung der neuen Wahlmöglichkeiten zugestimmt haben, nochmals einholen.

Im Schlussbericht konnten wir festhalten, dass Postfinance mit diesen Nachbesserungen ihren datenschutzrechtlichen Pflichten nachkommt. Insbesondere ist sichergestellt, dass sich die Kunden von Werbeangeboten von Dritten abmelden

können, ohne den Verlust des elektronischen Zugangs zu ihren Konten befürchten zu müssen. Die Umsetzung der Massnahmen wird zu einem späteren Zeitpunkt im Rahmen einer Nachkontrolle von uns überprüft.

1.9.2 Bekanntgabe von Personendaten an ausländische Steuerbehörden

Die Schweiz setzt die neuen Standards in der weltweiten Bekämpfung von Steuerbetrug und Steuerhinterziehung um. Damit die erforderlichen Rechtsgrundlagen bis 2017 bereit sind, läuft der Gesetzgebungsprozess auf vollen Touren. Für den Bund geht es darum, seine politischen und wirtschaftlichen Interessen angesichts der internationalen Herausforderungen zu wahren, ohne dabei die Persönlichkeitsrechte der Steuerzahler zu vernachlässigen.

a. Übereinkommen der OECD und des Europarats über die gegenseitige Amtshilfe in Steuersachen

Im Berichtsjahr wurden wir im Rahmen verschiedener Vernehmlassungsverfahren zur internationalen Zusammenarbeit in Steuersachen angehört. Seit die Schweiz sich im März 2009 zur Übernahme der internationalen Rechtsvorschriften auf diesem Gebiet verpflichtete, (vgl. 19. Tätigkeitsbericht 2011/2012, Ziffer 1.9.1) hat sich die Lage stark verändert. Am 15. Oktober 2013 unterzeichnete der Bund das Übereinkommen der OECD und des Europarats über die gegenseitige Amtshilfe in Steuersachen (Übereinkommen). Dieses stammt aus dem Jahr 1988 und bildet ein multilaterales Kooperationsinstrument, mit dem sich die Parteien auf eine Amtshilfe für eine Vielzahl von Steuern einigen können.

Mehrere Formen der Zusammenarbeit sind vorgesehen, einschliesslich des automatischen Informationsaustausches. Die Umsetzung dieser Form einer neuartigen Amtshilfe im Landesrecht erfordert die Schaffung von Gesetzesgrundlagen und die Revision gewisser Normen. Der Bundesrat hat daher vorgeschlagen, im Bundesgesetz über die internationale Amtshilfe in Steuersachen (StAhiG) punktuelle Weichenstellungen vorzunehmen. Darüber hinaus wurde ein Entwurf für ein Spezialgesetz ausgearbeitet, das die Einzelheiten des automatischen Informationsaustausches regeln soll (siehe b. «Internationaler automatischer Austausch von Steuerinformationen»).

Auf die Unterzeichnung des Übereinkommens folgte die Vorbereitung eines Bundesbeschlusses betreffend seine Genehmigung. Die Teilrevision des StAhiG, die im Anhang dieses Beschlusses vorgesehen ist, bildete das Hauptziel unserer Bemerkungen. Daher lenkten wir bei der Ämterkonsultation die Aufmerksamkeit

des Eidgenössischen Finanzdepartements (EFD) besonders auf Fragen betreffend die Regelungsdichte, die Verfahrensrechte der Steuerzahler und die Probleme im Zusammenhang mit der Verwendung der AHV-Nummer zur internationalen Steueridentifikation. Das EFD hat unseren Bemerkungen teilweise Rechnung getragen, namentlich in Bezug auf die Schaffung einer sektoreigenen Identifikationsnummer an Stelle der AHV-Nummer.

Gewisse Divergenzen mit dem EFD blieben auch nach der Ämterkonsultation bestehen und wurden unsererseits Gegenstand eines Mitberichtsverfahrens beim Bundesrat. Der Entwurf zur Revision des StAhiG sieht beispielsweise die Möglichkeit einer Weitergabe von Personendaten an andere schweizerische Behörden (abgesehen von den Steuerbehörden) und zu nicht steuerlichen Zwecken vor. Dies ist problematisch hinsichtlich des Spezialitätsprinzips und der Wahrung des Bearbeitungszwecks, der im vorliegenden Fall rein steuerlicher Natur sein sollte. Gemäss unserem Vorschlag wäre deshalb zu präzisieren, an welche weiteren Behörden Personendaten gegebenenfalls weitergegeben werden dürfen. In einem solchen Szenario müssen die Verfahrensrechte und insbesondere das rechtliche Gehör der betroffenen Personen ausdrücklich gewährleistet sein. Bei den Beratungen vom 5. Juni 2015 beschloss der Bundesrat indes, den Vorschlag des EFD unverändert anzunehmen.

b. Internationaler automatischer Austausch von Steuerinformationen

In unserem letzten Tätigkeitsbericht (vgl. 22. Tätigkeitsbericht 2014/2015, Ziffer 1.9.2) erwähnten wir die Arbeitsgruppe, die eingesetzt wurde, nachdem die OECD im Juli 2014 den Standard für den automatischen Informationsaustausch im Steuerbereich (Common Reporting Standard; CRS oder Standard) beschlossen hatte. Wir wurden zu verschiedenen Punkten in Verbindung mit dem Datenschutz angehört. Heikle Themen konnten so im Voraus aufgegriffen und erörtert werden. Angesichts des bedeutenden Umfangs des Dossiers und seines doch sehr ambitionierten Zeitplans war dieses Vorgehen zu begrüssen. Tatsächlich wurde im Laufe des Jahres 2015 eine erhebliche Anzahl Gesetzeserlasse in die Vernehmlassung geschickt, um den neuen Standard umzusetzen und die von der OECD vorgeschriebenen Fristen einzuhalten.

Der Standard sieht für die Staaten einen automatischen Informationsaustausch (AIA) über Steuerzahler vor, die Konten bei einem Finanzinstitut im Ausland besitzen. Er ist auch mit einem verbindlichen völkerrechtlichen Instrument für die multilaterale Umsetzung des automatischen Austauschs ausgestattet. Gemeint ist die Multilaterale Vereinbarung der zuständigen Behörden über den automatischen

Informationsaustausch über Finanzkonten (Multilateral Competent Authority Agreement; MCAA), welche die Schweiz am 19. November 2014 unterzeichnet hat. Damit die Bestimmungen dieser Vereinbarung sowie des CRS angewendet werden können, müssen sie mit einem Ausführungsgesetz einhergehen. Diese Rolle wird dem neuen Gesetz über den internationalen automatischen Informationsaustausch in Steuersachen (AIAG) zukommen, dessen Inkraftsetzung für 2017 vorgesehen ist. Es wird Bestimmungen über die Organisation, das Verfahren, die Rechtsmittel sowie Strafbestimmungen enthalten.

Bei der Ämterkonsultation sprachen wir uns im Wesentlichen für eine grössere Regelungsdichte aus, das heisst für eine klarere und detailliertere Formulierung gewisser Bestimmungen. Darüber hinaus verlangten wir, dass die durch eine automatische Deklaration betroffenen Steuerzahler ausdrücklich informiert werden. Dies bietet die Gewähr, dass das Transparenzprinzip und der Grundsatz von Treu und Glauben bei der Bearbeitung eingehalten werden. Diese Prinzipien setzen voraus, dass die betroffene Person vorgängig die Richtigkeit der an das Ausland weitergegebenen Informationen überprüfen kann. Ohne diesen Mechanismus müsste der Steuerzahler systematisch ein Auskunftsgesuch bei einem Finanzinstitut stellen. Eine generelle und abstrakte Information beispielsweise über die allgemeinen Geschäftsbedingungen ist nicht ausreichend.

Wie schon in der Ämterkonsultation zum Bundesbeschluss über die Genehmigung des Übereinkommens gab es auch beim Entwurf des AIAG weiterhin Divergenzen. Das EFD trug sie indes dem Bundesrat nicht vor. Wir unterbreiteten sie ihm daher im Mitberichtsverfahren. In diesem Rahmen machten wir unter Anderem erneut unseren Standpunkt deutlich, wonach Personen, die von einer Meldung betroffen sind, einzeln und konkret informiert werden sollten. Bei den Beratungen vom 5. Juni 2015 beschloss der Bundesrat jedoch, den Vorschlag des EFD unverändert anzunehmen.

Anlässlich des parlamentarischen Verfahrens stellte sich die Frage der Steueridentifikation mit der AHV-Nummer erneut, obwohl der Bundesrat beschlossen hatte, eine sektoreigene Nummer einzuführen. In der Herbstsession hatte sich der Nationalrat als erstbehandelnder Rat zunächst unserem Standpunkt angeschlossen (siehe zu diesem Thema das Rechtsgutachten des Bundesamtes für Justiz vom 5. August 2015, veröffentlicht auf: www.parlament.ch). Der Ständerat entschied sich indes für die Verwendung der AHV-Nummer. Diese Divergenz endete schliesslich bei der Schlussabstimmung in der Wintersession mit der Annahme des ursprünglichen Beschlusses des Ständerats. Damit hat sich das Parlament für die internationale Steueridentifikation mit der AHV-Nummer im Rahmen des automatischen Informationsaustausches ausgesprochen.

c. Verfahren für die zwischenstaatliche Umsetzung des AIA

Die Anwendung des Standards zwischen den Staaten kann auf zwei Arten erfolgen: entweder über ein bilaterales Abkommen wie das am 27. Mai 2015 zwischen der Schweiz und der Europäischen Union unterzeichnete Abkommen (siehe E: «Bundesbeschluss über die Genehmigung eines Protokolls zur Änderung des Zinsbesteuerungsabkommens zwischen der Schweiz und der EU»); oder auf der Basis der MCAA, die wiederum auf dem Übereinkommen beruht. Diese zweite Lösung wurde namentlich für die Einführung des AIA zwischen der Schweiz und Australien bevorzugt (siehe d. «Bundesbeschluss über die Einführung des AIA mit Australien»). Eine Aktivierung auf der Grundlage der MCAA muss die folgenden vier Voraussetzungen erfüllen:

- das Übereinkommen muss für beide Staaten in Kraft sein;
- beide Staaten müssen die MCAA unterzeichnet haben;
- beide Staaten müssen bestätigt haben, dass sie über die für die Umsetzung des Standards notwendigen Gesetze verfügen;
- beide Staaten müssen dem Sekretariat der Koordinationsstelle ihre Absicht mitgeteilt haben, den AIA gegenseitig anzuwenden.

Ganz allgemein richtet sich die Wahl der Partnerstaaten der Schweiz nach anderen Kriterien. Insbesondere sind dies das Bestehen wirtschaftlicher und politischer Beziehungen, eines Verfahrens für die Regularisierung der Vergangenheit, mittels der die Steuerzahler im Bedarfsfall ihre steuerlichen Verhältnisse bereinigen können, eines Marktzugangs und eines ausreichenden Datenschutzniveaus. Das Staatssekretariat für internationale Finanzfragen (SIF) überprüft diese Anforderungen und hat schon mehrmals unsere Meinung zu Fragen des Datenschutzes eingeholt. Wir wiesen es darauf hin, dass keinerlei zusätzliche Garantien erforderlich sind im Rahmen der bilateralen Aktivierung eines AIA mit einer ausländischen Rechtsordnung, in der gemäss der auf unserer Website veröffentlichten Staatenliste ein angemessenes Schutzniveau gilt. Bezüglich der Länder, die nicht unter diese Kategorie fallen, sind indes zusätzliche Garantien vorzusehen.

Ein Panel bestehend aus zwölf Experten, hauptsächlich Informatikern, wurde von der OECD beauftragt, die Vertraulichkeit und die Einhaltung des Spezialitätsprinzips in verschiedenen ausländischen Rechtsordnungen namentlich auf der Basis von Modellfragebogen im Anhang 4 des CRS zu beurteilen. Diese befassen sich im Wesentlichen mit den technischen Erfordernissen und den Aspekten der Informationssicherheit. Generell stehen Kontrollen vor Ort in diesem Kontext nicht zur Debatte. Überdies werden darin die aus dem Grundrecht auf Privatsphäre

abgeleiteten Rechte wie das Recht auf Berichtigung, das Auskunftsrecht und das Recht auf Löschung der Daten nicht geprüft. Der Fragebogen ist daher ein unvollständiges Instrument, das eine Gesamtbeurteilung des Schutzniveaus für Personendaten in einem ausländischen Rechtssystem nicht ermöglicht. Wir wiesen das SIF darauf hin, dass die Aktivierung eines AIA mit einem Drittstaat ohne die Einführung zusätzlicher Garantien trotz einer guten Bewertung durch das Expertenpanel mit Risiken verbunden ist.

d. Bundesbeschluss über die Einführung des AIA mit Australien

Wie oben erwähnt bestimmen die MCAA und der Entwurf des AIAG die Rechtsgrundlagen des AIA, ohne die Staaten zu beschreiben, mit denen dieser eingeführt werden soll. Australien ist einer der Partner, mit denen die Schweiz den AIA mit einem für 2018 geplanten ersten Austausch einführen möchte. Die Vorlage ist im Laufe des Jahres 2015 in die Vernehmlassung gegangen, und wir hatten die Gelegenheit, einige Bemerkungen zu dem Thema anzubringen. Wir hoben insbesondere hervor, dass zu prüfen sei, ob die australische Gesetzgebung über das Recht auf Privatsphäre den Steuerbereich abdeckt und ob sie gegebenenfalls auch die Daten von Ausländern und juristischen Personen erfasst.

Laut der Auswertung des EFD in seinem Vorschlag an den Bundesrat bietet die australische Gesetzgebung angemessene datenschutzrechtliche Garantien im Rahmen der Einführung des AIA mit Australien.

e. Bundesbeschluss über die Genehmigung eines Protokolls zur Änderung des Zinsbesteuerungsabkommens zwischen der Schweiz und der EU

Die bilaterale Aktivierung des AIA mit der EU wurde am 27. Mai 2015 unterzeichnet. In diesem Fall ist das Vorgehen anders als bei einer Aktivierung über die MCAA, wie sie für Australien gilt. Hier konnte das bisherige Zinsbesteuerungsabkommen zwischen der Schweiz und der EU für die Umsetzung des AIA genutzt werden. Dafür wurde ein Änderungsprotokoll vorgesehen. Dieses wandelt inhaltlich das Abkommen über die Zinsbesteuerung fast vollständig in ein Abkommen über den AIA um.

In der Ämterkonsultation betrafen unsere Bemerkungen insbesondere die Einhaltung des Zweckbindungsprinzips, das eine ausschliessliche Bearbeitung zu Steuerzwecken gewährleisten muss. Dem hat das EFD teilweise Rechnung getragen.

1.9.3 Lockerung der Amtshilfe in Bezug auf gestohlene Daten

Wir sind der Ansicht, dass das Bearbeiten von Amtshilfegesuchen, die auf gestohlenen Daten beruhen, gegen das Rechtmässigkeitsprinzip verstösst. Entsprechend kritisch haben wir uns in der Vernehmlassung zu einer weiteren Änderung des Steueramtshilfegesetzes geäussert.

Neben der unter Ziffer 1.9.2 des vorliegenden Tätigkeitsberichtes besprochenen Änderung des Steueramtshilfegesetzes ist noch eine weitere Änderung desselben geplant. Da wir in der ordentlichen Ämterkonsultation nicht begrüsst wurden, haben wir uns im Rahmen der Vernehmlassung zu der Vorlage geäussert. Unserer Meinung nach ist die geplante Änderung aus datenschutzrechtlicher Sicht höchst problematisch. Werden Daten rechtswidrig beschafft und danach weitergegeben, so verstösst der Empfänger der Personendaten, der diese ebenfalls bearbeitet, gegen den Grundsatz der Rechtmässigkeit und verletzt die Persönlichkeit der betroffenen Person. Diese Unrechtmässigkeit kann unserer Meinung nach nicht dadurch rechtfertigt werden, dass zwischen aktivem und passivem Handeln des Empfängerstaates unterschieden wird. Nimmt ein Staat die ihm angebotenen gestohlenen Daten an, so akzeptiert er damit deren deliktische Vergangenheit. Bearbeitet er diese und leitet sie weiter, so handelt er ebenfalls unrechtmässig und beteiligt sich an den Persönlichkeitsverletzungen. Wir baten das SIF deshalb, die Gesetzesvorlage zu streichen oder zu ändern, was jedoch nicht berücksichtigt wurde.

1.9.4 Banken und das Auskunftsrecht

Wir erhalten vermehrt Anfragen betreffend die Auskunftserteilung durch Banken. Gewisse Banken verlangen dafür eine Gebühr, die die datenschutzrechtlich zulässige Höhe von 300 Franken deutlich übersteigt.

Wir erhalten vermehrt Anfragen, die das Recht auf Auskunft gemäss Artikel 8 des Datenschutzgesetzes (DSG) betreffen. Insbesondere scheinen gewisse Finanzinstitute entsprechende Anfragen entweder nicht oder nur unter Auferlegung von hohen Gebühren beantworten zu wollen.

Das Auskunftsrecht ist der Ausgangspunkt zur Durchsetzung anderer datenschutzrechtlicher Ansprüche wie desjenigen der Berichtigung, Sperrung oder Löschung von Personendaten. Es kann nur unter engen Voraussetzungen eingeschränkt werden. Falls eine Bank die Auskunft einschränkt, muss sie den Grund dafür kommunizieren. Sie macht sich ausserdem strafbar, wenn sie vorsätzlich falsche

oder unvollständige Auskünfte erteilt. Die Auskunft kann zum Beispiel dann eingeschränkt werden, wenn die betroffene Person rechtsmissbräuchlich handelt. Das Bundesgericht hat in BGE *138* II 425 die Hürden für die Annahme einer rechtsmissbräuchlichen Geltendmachung des Auskunftsrechts hoch angesetzt. Eine Bank wurde durch diesen Entscheid dazu verpflichtet, Auskunft zu erteilen, auch wenn diese Informationen nicht nur aus persönlichkeitsrechtlichen Gründen gewünscht wurden, sondern um diese eventuell in einem nachfolgenden haftungsrechtlichen Prozess geltend zu machen.

Der Ausweg aus diesem Dilemma scheint nun für gewisse Finanzinstitute darin zu bestehen, die Auskunftserteilung nur unter Auflage exorbitant hoher Gebühren zu erteilen. In Bezug auf die Höhe der Gebühren, die gestützt auf das DSG gefordert werden können, besteht eine klare Rechtslage: Der Dateninhaber, also die Bank, kann als Kostenbeteiligung maximal 300 Franken fordern. In diesem Sinne beraten wir betroffene Personen, die ihren Anspruch auf Auskunft beim Zivilrichter geltend machen können.

1.10 International

1.10.1 Internationale Zusammenarbeit

Die internationale Zusammenarbeit zwischen den Datenschutzbehörden ist weiterhin eine wesentliche Komponente, wenn es darum geht, eine möglichst breit abgestützte Verankerung des Datenschutzrechts sicherzustellen. Der EDÖB bringt sich aktiv in die Arbeiten des Europarats, der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD), der europäischen und der internationalen Konferenz der Datenschutzbeauftragten sowie in der französischsprachigen Vereinigung der Datenschutzbehörden (AFAPDP) ein. Im Rahmen der Assoziierungs-Abkommen Schengen-Dublin beteiligt er sich an den Arbeiten verschiedener Koordinationsgruppen innerhalb der Europäischen Union (EU).

Europarat

Die Arbeiten zur Modernisierung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen 108), die zur Annahme eines Änderungsprotokolls führen soll, gehören zu den vorrangigen Zielen der Organisation im Bereich des Datenschutzes. Diese Arbeiten wurden jedoch seit Ende 2014 in Erwartung der Vollendung des neuen Rechtsrahmens der EU auf Eis gelegt. Mit der Anfang 2016 erfolgten Annahme des Entwurfs der europäischen Datenschutzverordnung und der Richtlinie für die Datenübermittlung zu polizeilichen und gerichtlichen Zwecken sollte der Abschluss der Revision möglich werden. Parallel dazu führt der Europarat seine Politik zur Förderung des Übereinkommens 108 bei Drittstaaten fort. Ausser Uruguay, das im Jahre 2013 beigetreten ist, wurden Marokko, Mauritius, Senegal und Tunesien nach einer positiven Stellungnahme des Beratenden Ausschusses (T-PD) vom Ministerkomitee des Europarats zum Beitritt aufgefordert. Mit dem Urteil des Gerichtshofs der Europäischen Union vom 6. Oktober 2015, in dem die Entscheidung 200/520 der Europäischen Kommission zum Safe-Harbor-Abkommen mit den Vereinigten Staaten für ungültig erklärt wurde, erscheint es notwendiger denn je, dass jeder Staat ein wirksames, auf gemeinsame und universell anerkannte Grundsätze abgestütztes Schutzsystem einführt. Das Übereinkommen 108 mit seinem universellen Anspruch bietet hier dem Europarat eine Gelegenheit, seine Pionierrolle in der internationalen Datenschutzgemeinschaft zu stärken.

Der T-PD hielt seine 32. Plenartagung vom 1. Juli bis 3. Juli 2015 in Strassburg ab. Er prüfte insbesondere die Empfehlung 2067 (2015) der parlamentarischen Versammlung zu Massenüberwachungseinsätzen und gab eine Stellungnahme ab. Darin fordert er den Europarat zu einer Intensivierung seiner Bemühungen zur Förderung

des Übereinkommens 108 im Hinblick auf den Beitritt von Drittstaaten auf, namentlich der Staaten, die bereits dem Übereinkommen über die Internetkriminalität beigetreten sind. Er erinnert daran, dass das Grundrecht der Achtung der Privatsphäre durch das Übereinkommen 108 und sein Zusatzprotokoll geschützt ist. Die Modernisierungsarbeit sollte die Wirksamkeit dieses Instruments weltweit verstärken. Er unterstützt die Aufforderung, eine Empfehlung an die Mitgliedstaaten zu richten, die auf die Gewährleistung des Schutzes der Privatsphäre im Zeitalter der Digitalisierung und der Internetsicherheit im Lichte der mit den Massenüberwachungstechniken verbundenen Gefahren ausgerichtet ist. Er ist auch erfreut über die Aufforderung zur Prüfung der mit den Massenüberwachungsmassnahmen verbundenen Sicherheitsprobleme im Internet sowie über die Aufforderung, die aus diesen Praktiken entstehenden Gefahren zu prüfen. In dieser Hinsicht weist er darauf hin, dass ohne jeglichen Kontrollmechanismus die Bearbeitung von Personendaten die Ausübung anderer Grundrechte sowie die Wahrnehmung anderer legitimer Interessen gefährden könnte. Der Ausschuss unterstützt schliesslich den Vorschlag zur Schaffung eines Kodexes für Nachrichtendienste und wird gegebenenfalls seinen Beitrag zu allen künftigen Arbeiten leisten.

Der T-PD hat überdies Arbeiten im Hinblick auf die Entwicklung eines praktischen Leitfadens zum Datenschutz im Polizeisektor aufgenommen. Er befasst sich auch mit der Überarbeitung der Empfehlung R (97) 5 über den Schutz der medizinischen Daten. Dabei geht es insbesondere darum, den technologischen Fortschritten Rechnung zu tragen, namentlich der Entwicklung der elektronischen Patientenakten, den Fernkonsultationen, der Entstehung des Internets der Dinge und der digitalen Selbstvermessung mit Akteuren, die nicht dem herkömmlichen Gesundheitswesen und dem medizinischen Bereich angehören. Der Ausschuss erörterte die Bedeutung der Megadaten für den Datenschutz und beschloss, Leitlinien dazu auszuarbeiten. Er prüfte einen Bericht über die Passagierdaten (PNR) und beauftragte sein Büro mit der Abfassung eines Gutachtens. Schliesslich hält er es für notwendig, die Untersuchung der Datenschutzfragen im Zusammenhang mit dem automatischen Datenaustausch zu Verwaltungs- und Steuerzwecken fortzuführen.

Europäische Konferenz der Datenschutzbeauftragten

Die europäische Konferenz der Datenschutzbeauftragten fand auf Einladung des Amtes des Informationsbeauftragten für das Vereinigte Königreich vom 18. bis 20. Mai 2015 in Manchester statt. Die Konferenz bot den Teilnehmern die Gelegenheit zu einem Meinungsaustausch über die Datenschutzpraktiken in der digitalisierten Welt (namentlich in den Bereichen Sensibilisierung, Behandlung von Beschwerden und Zusammenarbeit). Die Konferenz nahm dabei Kenntnis von einer Studie über die Rechte der betroffenen Personen und die Erwartungen der Öffentlichkeit gegenüber den Datenschutzbehörden.

Besonders wichtig ist laut der Studie, dass die Behörden für eine wirkungsvolle Tätigkeit die Erwartungen der Öffentlichkeit im Bereich des Datenschutzes kennen und wissen, wie die Personen ihre Rechte verstehen und sie ausüben möchten. Es geht diesen Personen namentlich darum, die Kontrolle über die sie betreffenden Daten zu behalten, sie erwarten eine grössere Transparenz bei der Bearbeitung und sie möchten die mit dem Datenaustausch angestrebten Ziele und seinen Nutzen besser verstehen. Die breite Öffentlichkeit erwartet insbesondere von den Datenschutzbehörden, dass sie völlig unabhängig vorgehen, für Transparenz sorgen und ihre Befugnisse für die Durchsetzung der Datenschutzvorschriften nutzen, was auch die Veröffentlichung ihrer Untersuchungsberichte voraussetzt. Die Behörden sollten vermehrt der Entwicklung neuer Technologien vorgreifen. Mehrere Behörden verwiesen auf den Mangel an Ressourcen und die Unmöglichkeit, sämtlichen an sie gerichteten Gesuchen und Beschwerden nachzugehen.

Internationale Konferenz der Datenschutzbeauftragten

Die 37. Internationale Konferenz der Datenschutzbeauftragten fand auf Einladung der niederländischen Datenschutzbehörde vom 26. bis 29. Oktober 2015 in Amsterdam statt. Unter dem Motto «Brücken schlagen» befasste sich die offene Konferenz, zu der sich rund 700 Teilnehmer aus den Datenschutzbehörden und der Wirtschaft, aus öffentlichen Verwaltungen, internationalen Organisationen, der Zivilgesellschaft und akademischen Kreisen versammelt hatten, mit einem von amerikanischen und europäischen Experten vorbereiteten Bericht . Dieser zeigt zehn Wege zu einer Verbesserung des Datenschutzes in den transatlantischen Beziehungen auf. Der Bericht stiess bei mehreren Teilnehmern auf wenig Begeisterung, bedauerten sie doch insbesondere seine allzu atlantische Ausrichtung und das Fehlen von Vorschlägen für Gesetzesänderungen. Für seine Urheber hingegen sind diese Vorschläge unter Einhaltung des bisherigen Datenschutzrahmens anwendbar und können auch auf andere Regionen der Welt übertragen werden. Diese verschiedenen Vorschläge sollen eingehender geprüft werden und könnten sich künftig in konkreten Projekten niederschlagen.

In dem den Datenschutzbehörden vorbehaltenen Konferenzteil erörterten diese die Frage, wie auf die weltweiten Veränderungen in einem besonders von Sicherheitsdenken geprägten Umfeld zu reagieren ist. Es geht vor allem darum, das Vertrauen der Öffentlichkeit zu sichern, namentlich indem bei den Nachrichtendienstaktivitäten Transparenz gefordert wird. Die Nachrichten- und Sicherheitsdienste müssen unter Beachtung der Gesetze handeln und insbesondere Eingriffe in die Privatsphäre im Rahmen ihrer Befugnisse auf das strikt notwendige Minimum beschränken. Die Datenschutzbehörden befassten sich auch mit der Frage der Bearbeitung der genetischen Daten. Obwohl der Austausch genetischer Daten zahlreiche Vorteile mit

sich bringt, ist die Verwendung solcher Daten mit vielen Risiken verbunden, die weitgehend vom Kontext, in dem diese Daten bearbeitet werden, und von den bei ihrer Bearbeitung geltenden Garantien abhängen.

So erscheint es unerlässlich, dass die betroffenen Personen die Kontrolle über ihre Daten behalten können, dass sie angemessen informiert werden und dass ihre Entscheidungen respektiert werden. Das lässt sich dank verschiedener Mittel erreichen, mit denen ein dynamischer Umgang mit dem Einverständnis der Betroffenen über den gesamten Lebenszyklus der Daten, ergänzt durch zusätzliche Garantien, gewährleistet werden kann. Es ist auch zu bedenken, dass die genetischen Daten Informationen über andere offenbaren, die zu ihrer Identifizierung und Charakterisierung beitragen. Zwar darf Innovation nicht durch den Datenschutz gebremst werden, doch muss sie in einem Rahmen erfolgen, der die Rechte und Grundfreiheiten der betroffenen Personen gewährleistet.

Die Datenschutzbehörden verabschiedeten vier Resolutionen über die strategische Ausrichtung der Konferenz, die Zusammenarbeit mit dem UNO-Sonderberichterstatter für das Recht auf Privatsphäre, das Öffentlichkeitsprinzip und die internationale humanitäre Tätigkeit. Mit der letzten Resolution verpflichten sich die Datenschutzbehörden, die Anforderungen im Kontext der humanitären Tätigkeit zu analysieren und dem Wunsch zur Zusammenarbeit von Seiten der humanitären Organisationen nachzukommen, um unter Berücksichtigung der Besonderheiten der internationalen humanitären Tätigkeit Leitlinien auszuarbeiten. Für diese Aufgabe wurde eine Ad-hoc-Arbeitsgruppe eingesetzt. Diese wird gemeinsam durch die spanische Datenschutzbehörde und den EDÖB koordiniert. Sie wird anlässlich der nächsten internationalen Konferenz der Datenschutzbeauftragten, die 2016 in Marrakesch in Marokko stattfindet, über ihre Arbeiten berichten.

Ausserdem ist am 27. Oktober 2015 die auf der 36. Konferenz abgeschlossene Vereinbarung über die Zusammenarbeit zwischen den Datenschutzbehörden in Kraft getreten. Der EDÖB war bisher nicht in der Lage, sich dieser nicht-verbindlichen Absichtserklärung anzuschliessen, da das Bundesamt für Justiz in einer negativen Vormeinung die Auffassung vertrat, dass wir nicht zur Unterzeichnung einer solchen Verpflichtung befugt seien.

Am Ende der Konferenz wurde eine Schlusserklärung veröffentlicht.

Französischsprachige Vereinigung der Datenschutzbehörden

Die französischsprachige Vereinigung der Datenschutzbehörden (AFAPDP) trat am 25. und 26. Juni 2015 zu ihrer Konferenz in Brüssel zusammen. Bei diesem Anlass diskutierten die Teilnehmer über die Überwachung und die digitalen Rechte. Zur

Überwachung erinnerten die Behörden daran, dass ein Interessenausgleich zwischen Datenschutz und Sicherheit unbedingt beibehalten werden muss. Dieses Gleichgewicht setzt die Annahme eines gemeinsamen Rahmens und eine unabhängige Kontrolle der Überwachungstätigkeiten voraus.

Zu den Rechten des Individuums im digitalen Universum präsentierten wir die Regelung des Rechts auf Vergessen im europäischen Recht und insbesondere das Urteil des Gerichtshofs der Europäischen Union vom 13. Mai 2014. Im Zuge der Diskussionen zeichnete sich die Notwendigkeit ab, den Personen eine echte Kontrolle über ihre Daten zu bieten, ohne damit in Richtung einer Patrimonialiserung der Personendaten zu gehen. Es geht auch um die Förderung des kollektiven und individuellen Bewusstseins der Wichtigkeit des Schutzes der eigenen Personendaten. Die Teilnehmer wirkten zudem in verschiedenen Workshops mit, die sich namentlich mit der Kontrolle der Konformität der Bearbeitungen, der verbesserten Behandlung von Beschwerden und der Zusammenarbeit befassten.

Die Mitglieder AFAPDP verabschiedeten zwei Resolutionen über die Massenüberwachung und über die Rolle der Ethik in der Bearbeitung von Gesundheitsdaten und genetischen Daten.

Internationale Zusammenarbeit – Aufsichtskoordinationsgruppen SIS II, VIS und Eurodac sowie Schengenevaluation von Österreich und Liechtenstein

2015 fanden zwei Sitzungen der Aufsichtskoordinationsgruppen SIS II, VIS und Eurodac statt. Zudem nahmen wir als Experten an den Evaluationen von Österreich und Liechtenstein teil.

Die Aufsichtskoordinationsgruppen über das Schengener Informationssystem (SIS II), über das Visa-Informationssystem (VIS) und über die europäische Datenbank zur Speicherung von Fingerabdrücken (Eurodac) haben sich vom 25. bis 26. März 2015 und vom 7. bis 8. Oktober 2015 in Brüssel getroffen. In der Märzsitzung wurde das Vereinigte Königreich (GB) als volles Mitglied in die Aufsichtskoordinationsgruppe SIS II aufgenommen, da GB neu bei einem Teil von Schengen (Teilnahme am Informationssystem SIS II) mitmacht. Die Aufsichtskoordinationsgruppe SIS II hat zudem den Leitfaden zum Auskunftsrecht (guide of access) angepasst. Die Aufsichtskoordinationsgruppe VIS hat ihren Tätigkeitsbericht 2012-2014 erstellt. In der Aufsichtskoordinationsgruppe Eurodac wurde unter anderem das Inkrafttreten der neuen europäischen Eurodac-Verordnung, aufgrund welcher die Strafverfolgungsbehörden Zugriff auf Eurodac erhalten, thematisiert. Eine Untergruppe der Aufsichtskoordinationsgruppen hat im September 2015 die Informationssysteme

SIS II, VIS und Eurodac in Strassburg besucht, wobei sie vor allem die datensicherheitsrelevanten Aspekte prüfte.

Auch 2015 Jahr nahmen wir als Experten an Schengenevaluationen im Bereich Datenschutz teil: im März an der Evaluation von Österreich und im November an derjenigen des Fürstentums Liechtenstein. Österreich war das erste Land, das nach dem neuen Mechanismus evaluiert wurde. Dieser bringt verschiedene Änderungen mit sich. Neu gibt es zwei «leading experts», einer der Europäischen Kommission und ein Vertreter der Mitgliedstaaten. Der Bericht kann in den verschiedenen Punkten zu folgenden Ergebnissen kommen: konform (compliant), nichtkonform (non-compliant) oder konform aber verbesserungsbedürftig (compliant but improvement necessary). Die Empfehlungen sind neu nicht mehr im Bericht selber, sondern in einem separaten Dokument aufgeführt.

Arbeitsgruppe «Border, Travel & Law Enforcement»

Die «Border, Travel & Law Enforcement subgroup» (BTLE) ist eine von der Arbeitsgruppe «Artikel 29» über den Datenschutz eingesetzte Untergruppe. Diese ist beauftragt, die gesetzgeberischen Entwicklungen in den Sektoren Polizei, Grenzen und Strafjustiz, insbesondere betreffend den Schengen-Besitzstand, zu verfolgen. In diesem Kontext bereitet sie Gutachten und Stellungnahmen vor, die danach von der Arbeitsgruppe «Artikel 29» verabschiedet werden. Wir haben im Laufe des Berichtsjahres an den verschiedenen Tagungen teilgenommen.

Im Anschluss an das Urteil des Gerichtshofs der Europäischen Union vom 6. Oktober 2015 in der Sache Nr. C-362/14, Schrems c. Data Protection Commissioner, erhielt die Unterarbeitsgruppe den Auftrag, die amerikanische Gesetzgebung zu analysieren und die Mindestanforderungen zu ermitteln, die im Falle einer Verletzung der Privatsphäre im Rahmen der nachrichtendienstlichen Aktivitäten einzuhalten sind.

Die Unterarbeitsgruppe setzte ausserdem die Prüfung des Gerichtsurteils der Europäischen Union betreffend die Aufbewahrung von Personendaten für den Kampf gegen das organisierte Verbrechen und den Terrorismus fort. In diesem Kontext hat sie einen Fragebogen zur Ermittlung der Praktiken in den verschiedenen Mitgliedstaaten ausgearbeitet.

Mit besonderer Aufmerksamkeit beobachtet die Untergruppe den Fortschritt des Projekts «intelligente Grenzen». Die EU-Kommission hat einen Verordnungsentwurf angenommen, der die Einrichtung eines Systems zur Ein- und Ausreiseregistrierung von Angehörigen von Drittstaaten beim Grenzübertritt an den Aussengrenzen der Mitgliedstaaten der Europäischen Union vorsieht. Auch eine Verordnung über die

Schaffung eines Programms für die Registrierung von Reisenden hat die Kommission angenommen.

Schliesslich begleitet die Unterarbeitsgruppe die Schaffung eines europäischen Rahmens für die Bekanntgabe von PNR-Daten an Drittstaaten und für ihre Verwendung zu Strafverfolgungszwecken. Sie beobachtet auch die Entwicklung des Vorschlags für eine Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Bearbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung und Aufklärung von Straftaten, der strafrechtlichen Ermittlung, Verfolgung und Ahndung sowie zum freien Verkehr dieser Daten.

Koordinationsgruppe der schweizerischen Datenschutzbehörden im Rahmen der Schengen-Abkommen

Über die «Koordinationsgruppe der schweizerischen Datenschutzbehörden im Rahmen der Umsetzung des Schengen-Assoziierungsabkommens» beaufsichtigen wir in Koordination mit den kantonalen Datenschutzbehörden die in der Schweiz durchgeführten Datenbearbeitungen im Bereich Migration, Polizei und Justiz in Anwendung der Schengen-Zusammenarbeit.

Die Koordinationsgruppe trat 2015 zwei Mal zusammen. Das erste Treffen fand im Rahmen eines Schulungsprogramms statt, das wir in Form eines Besuchs des SIRENE-Büros (Nationale Kontaktstelle für den Austausch zusätzlicher Informationen) organisiert hatten. Bei dieser Gelegenheit konnten die Teilnehmer ihre Fragen an die Datenschutzberaterin und an den Leiter des Büros richten.

Bei der zweiten Zusammenkunft informierten wir die kantonalen Datenschutzbehörden über die wichtigsten Punkte, welche die Koordinationsgruppe zur Kontrolle von SIS II angesprochen hatte, sowie über die verschiedenen von uns geplanten Kontrollen. Die Kantone ihrerseits stellten die Ergebnisse ihrer Kontrolltätigkeiten vor. Zur Vereinfachung der Auswertung der SIS-Logfiles haben wir den kantonalen Behörden ein von uns geschaffenes Informatik-Tool zur Verfügung gestellt.

Internationale Arbeitsgruppe für Datenschutz in der Telekommunikation

Der EDÖB hat am 13. und 14. Oktober 2015 an der 58. Sitzung der Internationalen Arbeitsgruppe für Datenschutz in der Telekommunikation (International Working Group on Data Protection in Telecommunications, IWGDPT) teilgenommen. Unter dem Vorsitz des Berliner Beauftragten für Datenschutz und Informationsfreiheit wurden unter anderen folgende Themen erörtert: Biometrische Authentifikationssysteme, Datenschutz auf e-learning Plattformen, Web Tracking (Do-Not-Track

Problematik), Datenschutz in Sozialen Netzwerken sowie bei Smart TVs. Arbeitspapiere und gemeinsame Positionen der Gruppe können auf folgender Website abgerufen werden (englisch): www.datenschutz-berlin.de

Weiter haben wir anlässlich eines Workshops der Europäischen Akademie für Informationsfreiheit und Datenschutz (EAID) am 14. Oktober 2015 ebenfalls in Berlin über die Entwicklungen und Diskussionen zur Vorratsdatenspeicherung insbesondere in den USA, Kanada, Grossbritannien und Deutschland informiert.

2. Öffentlichkeitsprinzip

2.1 Zugangsgesuche

Gemäss den uns mitgeteilten Zahlen sind im Jahr 2015 bei den Bundesbehörden insgesamt 597 Zugangsgesuche eingereicht worden (inklusive Bundesanwaltschaft und Parlamentsdienste sind es 600 Zugangsgesuche, siehe dazu Ziffer 2.1.2 f.). Dies entspricht erneut einem Höchstwert seit Inkrafttreten des Öffentlichkeitsgesetzes im Jahr 2006. In 319 Fällen (54%) gewährten die Behörden einen vollständigen, in 127 (21%) einen teilweisen Zugang. Bei 98 Gesuchen (16%) wurde die Einsichtnahme vollständig verweigert, 31 Zugangsgesuche wurden zurückgezogen und 22 Fälle meldeten die Behörden Ende Jahr als noch hängig. Mit Blick auf den kontinuierlichen Anstieg an Zugangsgesuchen ist davon auszugehen, dass der Bekanntheitsgrad und die Nutzung des BGÖ weiter zunehmen werden.

Was die Gesamtzahl der Zugangsgesuche und die Praxis der Behörden im Umgang mit Gesuchen anbelangt, zeigen die Zahlen mit Blick auf die vergangenen Jahre insgesamt ein stabiles Bild. Demnach wird der Zugang durchschnittlich in knapp der Hälfte aller Fälle vollständig gewährt sowie in je einem Viertel der Fälle teilweise oder vollständig verweigert.

2.1.1 Departemente und Bundesämter

Am meisten Zugangsgesuche für das Jahr 2015 auf Stufe Amt meldete uns die EFK mit 43 Gesuchen. Danach folgen das BAFU (31), das BLW und die WEKO (je 23) sowie das BAG und das GS-VBS (je 22). Bei den Departementen liegen das EDA (134 Gesuche), das UVEK (101) und das EFD (84) an der Spitze. Besonders transparenzfreundlich fallen die Quoten beim EDA aus, welches von insgesamt 134 Gesuchen 110 vollständig positiv beantwortete, in 17 Fällen den Zugang teilweise gewährte oder aufschob und bei lediglich sieben Gesuchen den Zugang vollständig verweigerte. 17 von 71 Behörden meldeten uns für 2015, dass bei ihnen kein einziges Zugangsgesuch eingegangen sei. Der Beauftragte selbst sah sich im Berichtsjahr mit sieben Zugangsgesuchen konfrontiert, wobei er den Zugang in allen Fällen vollständig gewährte.

Der im Berichtsjahr für den Zugang zu amtlichen Dokumenten erhobene Gebührenbetrag ist mit einem Gesamtumfang von 13 663 Franken deutlich höher als in den letzten Jahren ausgefallen (2012: Fr. 6 322; 2013: Fr. 6 502; 2014: Fr. 2 600). Dieser Gesamtbetrag entfällt auf lediglich 17 von insgesamt 597 gemeldeten Zugangsgesuchen. Wie bereits in den Vorjahren werden damit weiterhin in den meisten Fällen (durchschnittlich 97% aller Gesuche) keine Gebühren in Rechnung gestellt. Auffällig

sind dabei die nach wie vor bestehenden Unterschiede in der Gebührenhandhabung zwischen den verschiedenen Behörden. Während die Bundeskanzlei und drei Departemente überhaupt keine Gebühren erhoben, verrechneten vier Departemente ihren Zeitaufwand den jeweiligen Gesuchstellern zumindest teilweise. Der Hauptteil der erhobenen Gebühren entfiel dabei auf das VBS (Fr. 5 663 für 5 Gesuche), das UVEK (Fr. 4 150 für 3 Gesuche) und das WBF (Fr. 3 650 für 8 Gesuche). Nicht im oben erwähnten Gesamtbetrag für das Jahr 2015 enthalten sind diejenigen Fälle, in denen ein allfälliger Gebührenbetrag im Berichtsjahr noch nicht definitiv festgesetzt worden ist. Dies betrifft etwa einen vom Bundesverwaltungsgericht beurteilten Fall, in welchem das Gericht den von der Behörde für die Bearbeitung des Zugangsgesuch geschätzten Gebührenbetrag von 16 500 Franken auf eine Obergrenze von 8 500 Franken reduzierte (Urteil A-2589/2015 vom 4. November 2015).

Was den Zeitaufwand für die Bearbeitung von Zugangsgesuchen anbelangt, weist der Beauftragte einmal mehr 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 gegenüber den Vorjahren deutlich zugenommen (2012: 2155 Stunden; 2013: 1707 Stunden; 2014: 1642 Stunden; 2015: 2912 Stunden). Der Zeitaufwand für die Mitwirkung in Schlichtungsverfahren hat hingegen von 1436 Stunden im 2014 auf 1148 Stunden im 2015 abgenommen. Nicht bzw. nicht gesondert erfasst wird dagegen der Zeitaufwand für den Erlass einer Verfügung sowie ein allfälliges Beschwerdeverfahren.

2.1.2 Parlamentsdienste

Die Parlamentsdienste meldeten uns für das Jahr 2015 zwei Zugangsgesuche, wobei der Zugang einmal vollständig gewährt und einmal vollständig verweigert wurde.

2.1.3 Bundesanwaltschaft

Die Bundesanwaltschaft meldete uns für das Jahr 2015 ein einziges Zugangsgesuch. Der Zugang wurde dabei teilweise gewährt.

2.2 Schlichtungsanträge

Im 2015 wurden insgesamt 98 Schlichtungsanträge eingereicht, was einer Zunahme um knapp 9 Prozent entspricht (2014: 90). Die meisten Schlichtungsanträge wurden wiederum von Medienschaffenden (26) sowie Privatpersonen (23) eingereicht.

Diese Zahlen lassen folgende Schlüsse und Bemerkungen zu:

In 225 Fällen verweigerte die Bundesverwaltung den Zugang vollständig (98) respektive teilweise (127). Dem stehen 98 bei uns eingereichte Schlichtungsanträge gegenüber. Im Berichtsjahr wurde somit in gut 43 Prozent aller Fälle von ganz oder teilweise abgelehnten Zugangsgesuchen ein Schlichtungsantrag eingereicht (2014: 36%).

Insgesamt konnten im Berichtsjahr 134 Schlichtungsanträge abgeschlossen werden. Davon stammen 59 Anträge aus dem Berichtsjahr selbst, 52 aus dem Jahr 2014, 21 aus dem Jahr 2013 und zwei noch aus dem Jahr 2012. In 35 Fällen konnte zwischen den Beteiligten eine Schlichtung erzielt werden, wovon es in 19 Fällen zu einer Schlichtung im eigentlichen Sinne kam und in den übrigen 16 Fällen zu einer gütlichen Erledigung des Verfahrens aufgrund einer Intervention des Beauftragten. In vier Fällen wurde der Zugang nach Eröffnung des Schlichtungsverfahrens ohne Mitwirkung des Beauftragten gewährt. Insgesamt erliess der Beauftragte 58 Empfehlungen. Dies in denjenigen Fällen, in denen eine einvernehmliche Lösung nicht möglich oder von vornherein nicht ersichtlich war. Mit diesen 58 Empfehlungen konnten 83 Schlichtungsanträge erledigt werden. Vier Schlichtungsanträge wurden zurückgezogen und in zwei Fällen waren die Voraussetzungen für die Anwendung des Öffentlichkeitsgesetzes nicht gegeben. In fünf Fällen wurde der Schlichtungsantrag nicht fristgerecht eingereicht. Ein Schlichtungsverfahren wurde sistiert.

Im Berichtsjahr konnten deutlich mehr Schlichtungsverfahren als bisher abgeschlossen werden. Dies ist in erster Linie auf den Umstand zurückzuführen, dass zwei zusätzliche, bis Ende 2015 befristete Stellen zur Verfügung standen. Dennoch konnten die bestehenden grossen Rückstände in der Bearbeitung der hängigen Schlichtungsverfahren nicht vollständig abgebaut werden.

Alle im Berichtsjahr erlassenen Empfehlungen finden Sie auf der Website des Beauftragten.

2.3 Ämterkonsultationen und weitere Stellungnahmen

2.3.1 Mitwirkung in der Arbeitsgruppe Transparenz und Teilrevision des Öffentlichkeitsgesetzes

Der Bundesrat will eine Verbesserung der Umsetzung des Öffentlichkeitsgesetzes. Im Nachgang zur Evaluation hat der Bundesrat daher zum einen eine Teilrevision des Öffentlichkeitsgesetzes beschlossen und zum andern eine interdepartementale Arbeitsgruppe eingesetzt. Die Arbeitsgruppe soll einen besseren Austausch innerhalb der Bundesverwaltung sicherstellen und ist auch in die Erarbeitung des Vorentwurfs involviert.

Der Beauftragte hat in seinem letzten Tätigkeitsbericht über die vom Bundesamt für Justiz BJ durchgeführte Evaluation des Öffentlichkeitsgesetzes berichtet (22. Tätigkeitsbericht 2014/2015, S. 89ff.), deren Ergebnisse der Bundesrat im Berichtsjahr zur Kenntnis genommen hat. Der Bundesrat will die Umsetzung des Öffentlichkeitsprinzips in der Bundesverwaltung verbessern und hat zu diesem Zweck das Eidgenössische Justiz- und Polizeidepartement (EJPD) mit der Erarbeitung eines Vorentwurfs für eine Teilrevision des Öffentlichkeitsgesetzes (BGÖ) beauftragt. So sollen u.a. Unternehmen, deren Geschäfts- und Fabrikationsgeheimnisse durch Zugangsgesuche betroffen sind oder betroffen sein können, beim Zugangsgesuchsverfahren besser einbezogen werden. Weiter soll geprüft werden, wie das Verhältnis zwischen dem Datenschutzgesetz (DSG) und dem BGÖ geklärt werden kann. Schliesslich soll das EJPD Lösungen prüfen, um die Dauer des Schlichtungsverfahrens zu verkürzen.

Weiter hat der Bundesrat beschlossen, eine interdepartementale Arbeitsgruppe unter Führung des BJ zu schaffen. Die Arbeitsgruppe «Transparence» soll den Austausch zwischen den Öffentlichkeitsberatenden der Bundesverwaltung sicherstellen und die Umsetzung des BGÖ verbessern helfen. Nebst den Öffentlichkeitsberatenden der Departemente, der Bundeskanzlei, der Parlamentsdienste, des Bundesarchivs sowie einer Vertretung der Konferenz der Informationsdienste KID ist auch der Beauftragte in dieser Arbeitsgruppe vertreten.

Im Berichtsjahr fanden zwei Sitzungen statt, in denen die vom BJ ausgearbeiteten Lösungsvorschläge zu einzelnen Revisionsbestimmungen diskutiert wurden. Der Beauftragte hat sich auch in diesem Gremium gegen Beschränkungen des Öffentlichkeitsprinzips ausgesprochen. So ist er gegen die Ausnahme von Aufsichts-, Inspektions-, Audit oder Kontrollberichten der entsprechenden Bundesbehörden vom Geltungsbereich des BGÖ. Weiter vertritt der Beauftragte der Ansicht, dass die Koordination von BGÖ und DSG bereits heute ausreichend klar geregelt ist. Zur Klärung des Zugangs zu amtlichen Dokumenten mit Personendaten tragen nicht

zuletzt die Praxis mit den Empfehlungen des Beauftragten und die zunehmende Zahl von Entscheiden der Bundesgerichte zum Verhältnis von Öffentlichkeitsprinzip und Datenschutz bei.

Seit Inkrafttreten des BGÖ gibt die 30-tägige Frist für die Durchführung des Schlichtungsverfahrens Anlass zu Diskussionen. Der Beauftragte kann diese Frist in der Mehrheit der Fälle nicht einhalten und wurde daher auch schon wegen Rechtsverzögerung vom Bundesverwaltungsgericht gerügt. Die Erfahrung zeigt, dass die Frist von 30 Tagen praxisfremd und unrealistisch ist. Nach Ansicht des Beauftragten widerspricht die Vorgabe einer Frist grundsätzlich der Natur von Mediationsverfahren. Klar ist die Meinung des Beauftragte auch in Bezug auf den vom Bundesrat erteilten Auftrag, Lösungen für eine kürzere Dauer von Schlichtungsverfahren zu prüfen: Eine reelle Verkürzung der Dauer von Schlichtungsverfahren kann einzig über ausreichende Ressourcen erreicht werden kann (siehe dazu Ziffer 2.1 des vorliegenden Tätigkeitsberichts). Jegliche anderen gesetzlichen Neuregelungen für eine kürzere Schlichtungsdauer laufen Gefahr, auf Kosten des Öffentlichkeitsprinzips und zulasten der Gesuchstellenden zu gehen.

2.3.2 Organisation Bahninfrastruktur

Der Beauftragte hat im Rahmen der Ämterkonsultation zur Vorlage «Organisation Bahninfrastruktur (OBI)» des Bundesamtes für Verkehr (BAV) Stellung genommen. Vorgesehen war die weitgehende Einschränkung des Öffentlichkeitsprinzips im Bereich der gesetzlichen Aufsicht des BAV. Er hat sich gegen die vorgesehenen Gesetzesbestimmungen ausgesprochen.

Vorgesehen waren vom BAV vier identische Spezialbestimmungen im Eisenbahngesetz (EBG), im Bundesgesetz über Seilbahnen zur Personenbeförderung (SebG), im Bundesgesetz über die Personenbeförderung (PBG) und im Bundesgesetz über die Binnenschifffahrt (BSG). Gemäss diesen Bestimmungen soll das Öffentlichkeitsgesetz (BGÖ) nicht mehr gelten für Berichte betreffend Audits, Betriebskontrollen und Inspektionen des BAV sowie für alle anderen amtlichen Dokumente, welche die technische oder betriebliche Sicherheit betreffen, soweit sie Personendaten enthalten.

Der Beauftragte hat die vorgesehenen Bestimmungen abgelehnt, weil das BGÖ keine Kategorien amtlicher Dokumente kennt, welche von vornherein nicht zugänglich sind (wie z.B. Audit- oder Inspektionsberichte). Das BGÖ bietet ausserdem mit seinen Ausnahmebestimmungen genügend Möglichkeiten, um dem erhöhten Schutzbedürfnis für bestimmte amtliche Dokumente gebührend Rechnung zu tragen. Darüber hinaus erinnerte er an die Mitwirkungspflichten der beaufsichtigten

Unternehmen im Rahmen der gesetzlichen Aufsicht des BAV, welche durch das BGÖ nicht durchbrochen werden. So habe der Gesetzgeber die Vertraulichkeit zwischen Aufsichtsbehörde und Beaufsichtigten bewusst nicht als Ausnahmebestimmung des BGÖ vorgesehen.

Schliesslich lehnte der Beauftragte die vorgesehenen Bestimmungen auch deshalb ab, weil das BAV neben den eigentlichen Audit-, Kontroll- und Inspektionsberichten auch alle übrigen amtlichen Dokumente, welche die technische oder betriebliche Sicherheit eines Unternehmens betreffen, soweit sie Personendaten enthalten, vom Recht auf Zugang ausnehmen wollte. Die gesamte Aufsichtstätigkeit des BAV würde sich damit integral dem BGÖ entziehen und sich in einen vom Gesetz gerade nicht gewollten Geheimbereich staatlichen Handelns verabschieden.

Der Beauftragte stellt mit Sorge fest, dass auch andere Verwaltungseinheiten (insbesondere Aufsichtsbehörden) Bestrebungen verfolgen, anlässlich von Gesetzesrevisionen Teilbereiche ihres Handelns bzw. bestimmte Dokumentenkategorien vom BGÖ auszunehmen.

2.3.3 Freier Zugang zu Behördendaten / Open Government Data (OGD)

Am 16. April 2014 hat der Bundesrat die Open-Government-Data-Strategie Schweiz 2014-2018 verabschiedet, mit der er den freien Zugang zu Behördendaten ausbauen will. Die Strategie wurde unter der Federführung des Informatiksteuerungsorgans des Bundes erarbeitet. Seit Anfang 2015 ist das Bundesarchiv für die Umsetzung dieser Strategie verantwortlich und erarbeitet die notwendigen konzeptionellen Grundlagen. In diesem Rahmen wurden wir gebeten, zur Frage der rechtlichen Rahmenbedingungen für OGD aus der Sicht des Öffentlichkeitsprinzips Stellung zu nehmen.

Der Beauftragte begrüsst alle politischen Bestrebungen in Richtung eines einfachen, freien Zugangs zu Behördendaten. Insbesondere sieht er in der Einführung einer bundesweiten OGD-Plattform eine nützliche und notwendige Erweiterung der Informationsrechte der Bevölkerung. Ein weitgehender Zugang zu behördlichen Informationen stärkt das Vertrauen in staatliche Institutionen und macht eine sinnvolle Mitwirkung am politischen Entscheidungsprozess erst möglich.

Aus der Perspektive des Öffentlichkeitsprinzips haben wir darauf hingewiesen, dass OGD als aktive behördliche Informationstätigkeit (freiwillige oder von Gesetzes wegen vorgesehene Information) strikte vom Öffentlichkeitsgesetz (BGÖ) zu trennen ist, welches lediglich die passive behördliche Informationstätigkeit (Information auf Gesuch hin) regelt. Aus dieser klaren Zweiteilung behördlicher Informationsmodi geht auch hervor, dass das BGÖ nicht als gesetzliche Grundlage für

OGD herangezogen werden kann. - Die datenschutzrechtlichen Bemerkungen zur OGD-Strategie finden Sie in Ziffer 1.1.2 des vorliegenden Tätigkeitsberichts.

2.3.4 Revision der Energieverordnung und der Stromversorgungsverordnung

Das Bundesamt für Energie hat seine Praxis bei der Veröffentlichung von Daten über Anlagen, die eine Vergütung erhalten, präzisiert. Der Beauftragte hat im Rahmen des Vernehmlassungsverfahrens zum Entwurf einer Revision der Energieverordnung (EnV) und der Stromversorgungsverordnung (StromVV) Stellung genommen.

Der Revisionsentwurf sah eine Klärung der Situation vor, indem die bisherige Praxis der Veröffentlichung einer Anzahl Daten betreffend vergütungsberechtige Anlagen ausdrücklich geregelt wurde, so etwa der Name der Produzenten, der Standort der Anlage, die Energiequelle, die Leistung, die Produktion, die Höhe der Vergütung usw. Für Anlagen mit einer Leistung unter 30 kW bleibt die Veröffentlichung anonym. Der Beauftragte begrüsst den Willen des Bundesamtes für Energie, die aktive Veröffentlichung gewisser Daten von Anlagen, die eine Vergütung beziehen, in der Verordnung vorzusehen. Er ist jedoch der Ansicht, dass im Interesse des Öffentlichkeitsprinzips diese Veröffentlichung verbindlich vorgeschrieben werden sollte. Sodann erinnerte er im Zusammenhang mit der anonymisierten Veröffentlichung der Daten für Anlagen mit einer Leistung unter 30 KW daran, dass ein auf das Öffentlichkeitsgesetz gestützter Antrag auf Zugang immer noch möglich ist und dass dies in der Erläuterung präzisiert werden sollte.

Das Bundesamt teilte dem Beauftragten daraufhin mit, dass es mit sämtlichen Bemerkungen einverstanden sei und es den Revisionsentwurf sowie die Erläuterung in diesem Sinne ändern werde. Die revidierte Fassung ist am 1. Januar 2016 in Kraft getreten.

2.3.5 Gesetz über die Information und den Zugang zu Dokumenten des Kantons Freiburg

Der Beauftragte hat im Rahmen der Vernehmlassung zum Vorentwurf des Kantons Freiburg zur Änderung des Gesetzes über die Information und den Zugang zu Dokumenten (InfoG) Stellung genommen. Er begrüsst jegliche Schritte zu mehr Transparenz und spricht sich für den Hauptantrag aus.

Mit der Änderung will der Kanton Freiburg das Gesetz an die Aarhus-Konvention anpassen. Die Konvention, in der Schweiz seit 1. Juni 2014 in Kraft, setzt sich aus drei Grundpfeilern zusammen. Erstens verleiht sie jeder Person das Recht, Zugang

zu Informationen über Umweltangelegenheiten zu erhalten. Zweitens darf sich jeder an umweltbezogenen Entscheidungsverfahren beteiligen. Zum Beispiel ist man berechtigt, an Verfahren betreffend den Bau einer Autobahn mitzuwirken. Drittens hat jeder das Recht Zugang zu einem Gericht zu erhalten, wenn ihm z.B. umweltrelevante Informationen verweigert werden oder die Tätigkeit einer Behörde oder Privatperson gegen Umweltvorschriften verstösst. Um eine Übereinstimmung mit der Konvention zu gewährleisten, müssen auch andere Kantone ihre Gesetze anpassen.

Der Kanton Freiburg hat in seinem Vorentwurf zur Revision des InfoG einen Hauptantrag sowie eine Variante ausgearbeitet und in der Vernehmlassung auch den Beauftragten um eine Stellungnahme gebeten. Bei der Variante beschränkt man sich auf die Anpassungen, die streng notwendig erscheinen. Das heisst, es werden lediglich Anpassungen für den Umweltbereich vorgenommen. Der Hauptantrag hingegen nimmt die Anliegen der Konvention auf, ohne sich auf den Bereich der Umwelt zu beschränken und verzichtet dadurch in gewissen Punkten auf die Einschränkung des Zugangsrechts. Ein Teil der vorgeschlagenen Gesetzesbestimmungen würde somit auch für behördliche Dokumente gelten, die nicht die Umwelt betreffen.

In seiner Stellungnahme hat sich der Beauftragte klar für den Hauptantrag ausgesprochen, da er im Vergleich zur Variante zu einer grösseren Transparenz der Behörden führt. Dies weil er vorsieht, den Kreis der Privaten, bei denen man Informationen einholen kann, zu erweitern. Bisher mussten diese eine öffentliche Aufgabe wahrnehmen (Bsp. privates Wasserwerk) sowie eine Verfügungskompetenz innehaben. Neu fiele die Verfügungskompetenz als Voraussetzung weg. Zudem würde die aktuelle Gesetzesbestimmung, welche Dokumente aufgrund ihres Erstellungs- oder Zustellungsdatums vom Zugang ausnimmt, ersatzlos gestrichen. Damit wäre auch der Zugang zu Dokumenten möglich, die vor Inkrafttreten des InfoG erstellt wurden.

Der Beauftragte hob schliesslich die vorausschauende Sichtweise des Hauptantrags hervor für den Fall des Beitritts der Schweiz zur Tromsø-Konvention. Diese enthält ähnliche Bestimmungen wie die Aarhus-Konvention, gilt jedoch nicht nur für Dokumente in Umweltangelegenheiten, sondern für sämtliche Verwaltungsdokumente. Würde der Kanton Freiburg jetzt bloss die Vorschriften im Zusammenhang mit Umweltangelegenheiten anpassen, müsste er diese in ein paar Jahren aufgrund der Tromsø-Konvention möglicherweise wieder ändern. Zusammenfassend kann nach Ansicht des Beauftragten gesagt werden, dass der Kanton Freiburg mit seinem Vorentwurf ein starkes Zeichen für eine offene und transparente Verwaltung setzt.

2.4 Varia

2.4.1 Internationale Konferenz der Informationsbeauftragten 2015

Die neunte Internationale Konferenz der Informationsbeauftragten ICIC fand vom 21. bis 23. April 2015 in Santiago de Chile, Chile, statt. Der Anlass, der vom chilenischen Rat der Transparenz (consejo para la transparencia) organisiert wurde, bestand in einer nicht öffentlichen, eintägigen Arbeitssitzung an der 33 Delegierte aus 25 Ländern teilnahmen sowie aus einem öffentlichen Teil mit zahlreichen Vorträgen und Debatten zur Informationsfreiheit.

An der privaten Arbeitssitzung wurde entsprechend dem Vorschlag der Gastgeberbehörde vier Themen in Arbeitsgruppen vertieft diskutiert und bearbeitet. Ihre Schlussfolgerungen und Vereinbarungen werden ebenso wie eine Abschlusserklärung in einer gemeinsamen Resolution festgehalten. Darin äussern die Beauftragten ihre Besorgnis über die Entwicklung im Zusammenhang mit dem Recht auf Informationszugang. Sie verweisen dabei auf die Rückschritte bei der Informationsfreiheit aufgrund der Billigung von Gesetzgebungen und öffentlicher Politiken, die im Widerspruch zu diesem Recht stehen, sowie auf die fehlende angemessene Finanzierung und Unterstützung der Beauftragten bzw. entsprechender Aufsichtsorgane.

Die Resolution der neunten ICIC befindet sich auf der Website des Beauftragten.

2.4.2 Beziehungen zu kantonalen Öffentlichkeitsbeauftragten

Der Beauftragte und kantonale Öffentlichkeitsbeauftragte, welche Schlichtungsverfahren durchführen, treffen sich seit dem Jahr 2011 ein bis zweimal im Jahr zu einem vertieften Erfahrungsaustausch. Aufgrund mehrerer Mutationen in den Kantonen tagte die Gruppe im Jahr 2015 in neuer Zusammensetzung. Wie im Jahr 2014 vereinbart, werden die informellen Sitzungen jeweils alternierend von den einzelnen Mitgliedern der Arbeitsgruppe organisiert. 2015 trafen sich die Mitglieder auf Einladung der jeweiligen kantonalen Öffentlichkeitsbeauftragten in Fribourg und in Solothurn.

In der Praxis finden sich mitunter Fragen, die sich aufgrund der nicht zahlreichen Rechtsprechung und Lehre nicht einfach beantworten lassen. Darüber hinaus haben die Kantone und der Bund eine Vielfalt unterschiedlicher Regelungen im Bereich Datenschutz und Öffentlichkeitsprinzip. Für die Teilnehmer der Arbeitsgruppe ist daher der berufliche Austausch ihrer Erfahrungen wertvoll. Zum einen werden Fragen aus den beiden Rechtsgebieten Datenschutz und Öffentlichkeitsprinzip

diskutiert. Zum anderen dient es dem Austausch von Erfahrungen und dem gegenseitigen Lernen im Bereich der Schlichtungstätigkeit. Im nächsten Jahr wird die Arbeitsgruppe ihr fünfjähriges Bestehen feiern können.

3. Der EDÖB

3.1 Zehnter Datenschutztag

Ende Januar fand die zehnte Ausgabe des Internationalen Datenschutztages statt, den der EDÖB dieses Jahr dem Thema «Cloud Computing: sicherer Umgang mit Personendaten nach Safe-Harbor-Urteil» gewidmet hat. Wir organisierten eine öffentliche Veranstaltung mit Kurzvorträgen und einer Podiumsdiskussion an der Universität Lausanne.

Privatpersonen und Firmen verwenden vermehrt Clouddienste, weil diese praktische Vorteile gegenüber physischen Speichermedien bieten: Persönliche Daten sind jederzeit online abrufbar und können mit wenigen Klicks vom einen zum anderen Gerät übertragen werden. Weil Speicherplatz im Internet zudem kostengünstig ist, lagern auch immer mehr Schweizer Unternehmen und KMU ihre Datenbearbeitung an externe Clouddienste aus. Da sich die Daten dann nicht mehr im firmeneigenen Netzwerk befinden, sondern in einer «Datenwolke» oftmals in Ländern mit ungenügendem Datenschutzniveau gespeichert werden, betrachten wir diese Entwicklung kritisch.

Seit der Europäische Gerichtshof am 6. Oktober 2014 das Safe-Harbor-Abkommen zwischen der EU und den USA für ungültig erklärt hat, ist die Diskussion um Clouddienste stärker entfacht, da diese ihren Standort oftmals in den USA haben. In der Schweiz fehlt unserer Ansicht nach zurzeit eine angemessene Rechtsgrundlage für die Übermittlung personenbezogener Daten in die USA. Astrid Epiney, Inhaberin des Lehrstuhls für Europarecht, Völkerrecht und Öffentliches Recht der Universität Freiburg, erörterte in ihrem Vortrag die aktuellen datenschutzrechtlichen Probleme in diesem Zusammenhang. IT-Experten der Universitäten Genf und Lausanne beleuchteten in ihren Kurzvorträgen die technologischen Chancen und Risiken des Cloudcomputing.

Im Anschluss an die Vorträge und Präsentationen diskutierte Jean-Philippe Walter, Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter ad interim, mit Politikern und IT-Spezialisten in einer Podiumsdiskussion über die Gefahren, welche die Auslagerung von Datenbearbeitungen an externe Clouddienste mit sich bringt. Die Veranstaltung war gut besucht, und es ergab sich eine rege Diskussion mit kritischen Fragen aus dem Publikum. Interessierte Bürgerinnen und Bürger hatten die Möglichkeit, ihre Meinung zum Thema «Die Kehrseite des Cloud Computing» auf unserem Blog zu äussern. Die Präsentationen zur Veranstaltung sowie eine Videobotschaft von Jean-Philippe Walter befinden sich auf www.derbeauftragte.ch.

3.2 Publikationen des EDÖB im laufenden Geschäftsjahr

Auf der Website des EDÖB finden interessierte und betroffene Bürgerinnen und Bürger, aber auch Medienschaffende und Juristen umfassende Informationen zu unseren Themen- und Zuständigkeitsbereichen: www.derbeauftragte.ch. Im Berichtsjahr publizierten wir aus dem Bereich des Öffentlichkeitsgesetzes eine Vielzahl von Empfehlungen. Im Bereich Datenschutz kamen neue Erläuterungen zur Personensicherheitsprüfung sowie zum digitalen Erbe hinzu.

Unternehmen haben ein Interesse daran, nur Mitarbeiter zu beschäftigen, von denen keine Gefahr für die Sicherheit ausgeht. Gerade in Branchen wie der IT, dem Bankenwesen oder der Spitzentechnologie, bei denen Angestellte Zugang zu sensiblen Einrichtungen und Daten erhalten, besteht das Bedürfnis, Personensicherheitsprüfungen durchzuführen. In den Erläuterungen auf unserer Website steht, welche datenschutzrechtlichen Vorgaben private Arbeitgeber dabei zu beachten haben.

Weil unser Leben zunehmend online stattfindet, wird die Datenmenge, die wir in Form von Kontakten, persönlichen Profilen, Benutzerkonti, Fotos, Videos, Tweets und Likes im Internet speichern, immer grösser. Damit wir das Recht auf informationelle Selbstbestimmung über unseren Tod hinaus wahrnehmen und mitbestimmen können, was mit unseren Daten geschieht, sollten wir uns frühzeitig Gedanken zu unserem digitalen Erbe machen. Wir erläutern nicht nur die rechtlichen Rahmenbedingungen, sondern geben auch wichtige Tipps für Internetanwender, -anwenderinnen und deren Angehörige.

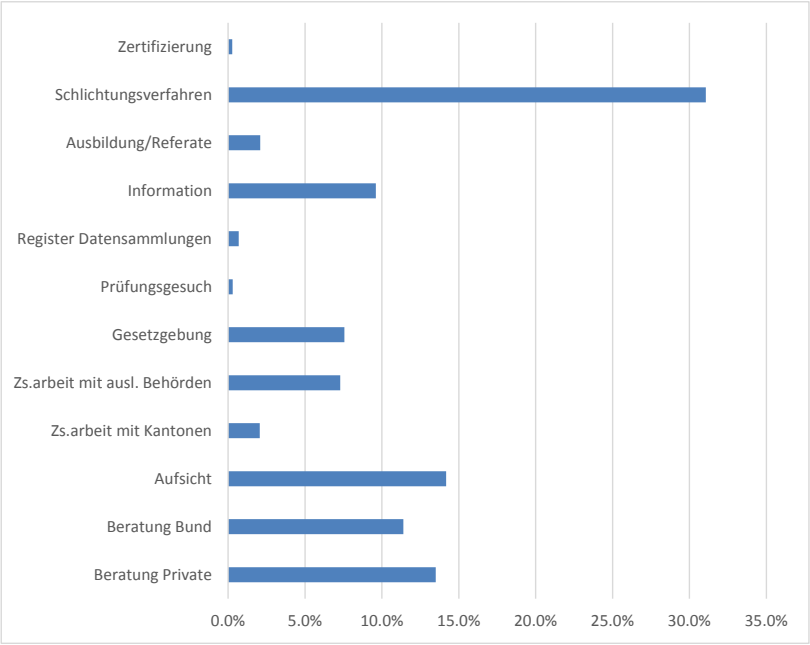
Unter dem Namen «Pay as you drive» (PAYD) evaluieren immer mehr Motorfahrzeugversicherungen Verhaltensdaten ihrer Kundinnen und Kunden, um ihnen massgeschneiderte Risikoprämien anzubieten. Sobald sich jemand in der Wahl eines solchen Versicherungsmodells nicht mehr frei fühlt (beispielsweise infolge grosser Preisunterschiede), wird es datenschutzrechtlich problematisch. Wir haben deshalb unsere Erläuterungen zu risikobasierten Prämienmodellen für Versicherungen aktualisiert.

Nach dem Safe-Harbor-Urteil des Europäischen Gerichtshofs hat der EDÖB eine Stellungnahme verfasst und die Hinweise zur Datenübermittlung in die USA aktualisiert. Bis ein neues Abkommen mit den USA ausgehandelt ist, empfehlen wir, beim Datenaustausch mit US-Unternehmen vertragliche Garantien im Sinne des DSG zu vereinbaren. Obwohl damit ein Zugriff auf die Daten durch US-Behörden nicht ausgeschlossen ist, kann das Datenschutzniveau auf diesem Weg verbessert werden.

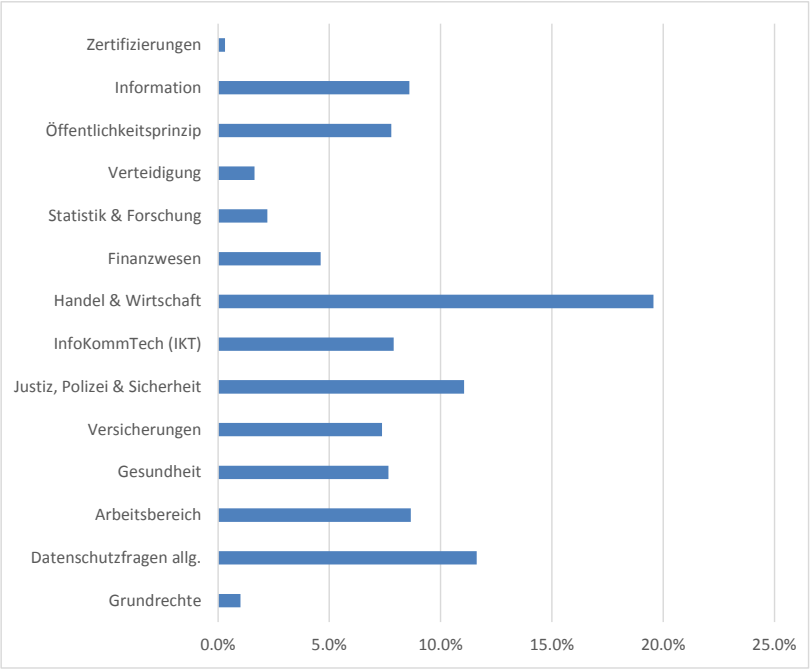
Das Bundesamt für Kommunikation BAKOM hat zusammen mit dem EDÖB und weiteren Partnern die Publikation «Geschichten aus dem Internet» veröffentlicht. Anhand von 15 Comic-Geschichten über Erlebnisse einer Familie im Internet sollen insbesondere Jugendliche für einen vernünftigen, sicherheitsbewussten Umgang mit den Informations- und Kommunikationstechnologien sensibilisiert werden. Die Comics sind im Internet publiziert und können als Broschüre kostenlos bestellt werden.

3.3 Statistik über die Tätigkeit des EDÖB vom 1. April 2015 bis 31. März 2016

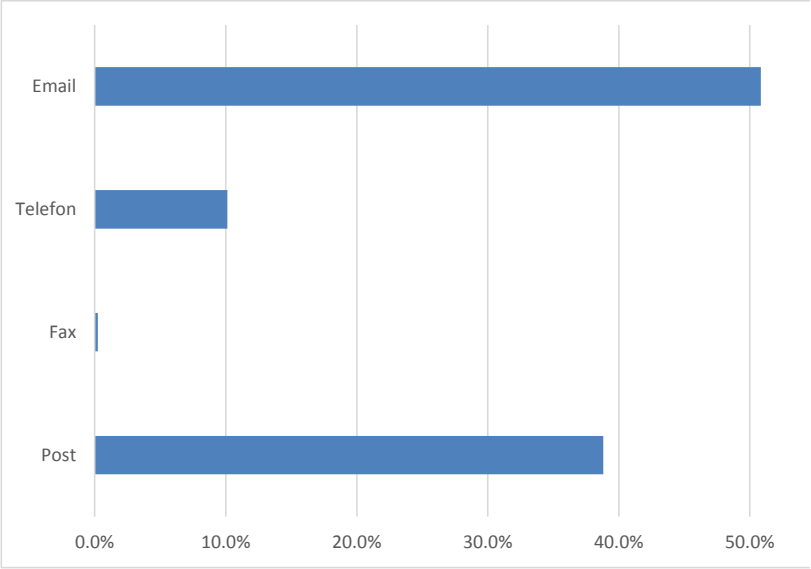
Aufwand nach Aufgabengebiet



Aufwand nach Sachgebiet



Herkunft der Anfragen



3.4 Statistik über die bei den Departementen eingereichten Zugangsgesuche nach Art. 6 des Öffentlichkeitsgesetzes (Zeitraum: 1. Januar 2015 bis 31. Dezember 2015)

Departement	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt / aufgeschoben	Zugangsgesuch hängig	Zugangsgesuch zurückgezogen
BK	17	7	4	3	3	0
EDA	134	110	7	17	0	0
EDI	77	23	10	28	4	12
EJPD	46	16	13	13	3	1
VBS	63	20	22	12	6	3
EFD	84	53	20	11	0	0
WBF	75	34	9	22	4	6
UVEK	101	56	13	21	2	9
Total 2015 (in %)	597 (100 %)	319 (54 %)	98 (16 %)	127 (21 %)	22 (4 %)	31 (5 %)
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 %)	-	-

Bundeskanzlei BK

Betroffener Fachbereich	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt / aufgeschoben	Zugangsgesuch hängig	Zugangsgesuch zurückgezogen
BK	10	1	4	2	3	0
EDÖB	7	6	0	1	0	0
Total	**17**	**7**	**4**	**3**	**3**	**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	134	110	7	17	0	0
Total	**134**	**110**	**7**	**17**	**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	3	1	0	1	0	1
EBG	0	0	0	0	0	0
BAK	1	1	0	0	0	0
BAR	6	6	0	0	0	0
METEO CH	0	0	0	0	0	0
NB	0	0	0	0	0	0
BAG	22	3	4	11	2	2
BFS	4	0	0	2	0	2
BSV	21	10	0	10	1	0
BLV	4	1	0	2	0	1
SNM	0	0	0	0	0	0
SWISS-MEDIC	13	0	4	2	1	6
SUVA	3	1	2	0	0	0
Total	**77**	**23**	**10**	**28**	**4**	**12**

Eidgenössisches Justiz- und Polizeidepartement EJPD

Betroffener Fachbereich	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt / aufgeschoben	Zugangsgesuch hängig	Zugangsgesuch zurückgezogen
GS	9	5	0	1	3	0
BJ	2	0	2	0	0	0
FEDPOL	6	2	3	1	0	0
METAS	2	1	0	1	0	0
SEM	19	3	6	9	0	1
SIR	5	3	1	1	0	0
IGE	2	2	0	0	0	0
ESBK	0	0	0	0	0	0
ESchK	0	0	0	0	0	0
RAB	0	0	0	0	0	0
ISC	1	0	1	0	0	0
NKVF	0	0	0	0	0	0
Total	**46**	**16**	**13**	**13**	**3**	**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	22	13	4	4	1	0
Verteidig. / Armee	16	4	7	2	3	0
NDB	15	0	7	6	1	1
armasuisse	8	1	4	0	1	2
BASPO	2	2	0	0	0	0
BABS	0	0	0	0	0	0
Total	**63**	**20**	**22**	**12**	**6**	**3**

Eidgenössisches Finanzdepartement EFD

Betroffener Fachbereich	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt / aufgeschoben	Zugangsgesuch hängig	Zugangsgesuch zurückgezogen
GS	18	10	6	2	0	0
ISB	4	2	0	2	0	0
EFV	1	0	0	1	0	0
EPA	1	0	1	0	0	0
ESTV	5	0	5	0	0	0
EZV	3	1	1	1	0	0
EAV	4	0	1	3	0	0
BBL	1	0	0	1	0	0
BIT	2	1	0	1	0	0
EFK	43	39	4	0	0	0
SIF	1	0	1	0	0	0
PUBLICA	0	0	0	0	0	0
ZAS	1	0	1	0	0	0
TOTAL	**84**	**53**	**20**	**11**	**0**	**0**

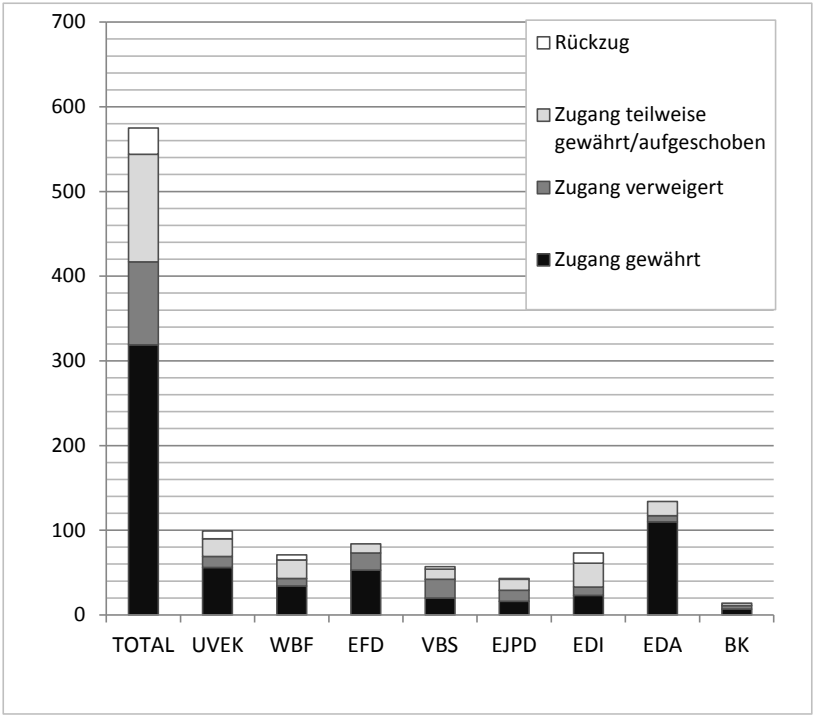
Eidgenössisches Departement für Wirtschaft, Bildung und Forschung WBF

Betroffener Fachbereich	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt / aufgeschoben	Zugangsgesuch hängig	Zugangsgesuch zurückgezogen
GS	6	1	2	0	3	0
SECO	6	1	2	3	0	0
SBFI	4	1	1	1	0	1
BLW	23	13	1	9	0	0
BWL	0	0	0	0	0	0
BWO	0	0	0	0	0	0
PUE	2	0	2	0	0	0
WEKO	23	14	1	3	1	4
ZIVI	0	0	0	0	0	0
BFK	1	1	0	0	0	0
SNF	0	0	0	0	0	0
EHB	0	0	0	0	0	0
ETH Rat	10	3	0	6	0	1
Total	**75**	**34**	**9**	**22**	**4**	**6**

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	6	3	1	0	2	0
BAV	5	2	0	0	0	3
BAZL	6	2	2	2	0	0
BFE	13	7	4	1	0	1
ASTRA	4	1	1	1	0	1
BAKOM	11	2	1	4	0	4
BAFU	31	26	1	4	0	0
ARE	4	4	0	0	0	0
ComCom	0	0	0	0	0	0
ENSI	17	5	3	9	0	0
PostCom	0	0	0	0	0	0
UBI	4	4	0	0	0	0
Total	**101**	**56**	**13**	**21**	**2**	**9**

Behandlung der Zugangsgesuche



3.5 Statistik über die bei der Bundesanwaltschaft eingereichten Zugangsgesuche nach Art. 6 des Öffentlichkeitsgesetzes (Zeitraum: 1. Januar 2015 bis 31. Dezember 2015)

Bundesanwaltschaft BA

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

3.6 Statistik über die bei den Parlamentsdiensten eingereichten Zugangsgesuche nach Art. 6 des Öffentlichkeitsgesetzes (Zeitraum: 1. Januar 2015 bis 31. Dezember 2015)

Parlamentsdienste PD

Betroffener Fachbereich	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt / aufgeschoben	Zugangsgesuch hängig	Zugangsgesuch zurückgezogen
PD	2	1	1	0	0	0
Total	**2**	**1**	**1**	**0**	**0**	**0**

3.7 Anzahl Schlichtungsgesuche nach Kategorien der Antragsteller (Zeitraum: 1. Januar 2015 bis 31. Dezember 2015)

Kategorie Antragsteller	**2015**
Medien	26
Privatpersonen (bzw. keine genaue Zuordnung möglich)	23
Interessenvertreter (Verbände, Organisationen, Vereine usw.)	14
Rechtsanwälte	14
Unternehmen	21
Total	**98**

3.8 Das Sekretariat des EDÖB

Eidgenössischer Datenschutz-und Öffentlichkeitsbeauftragter:

bis 30. November 2015:	Thür Hanspeter
ab 1. Dezember 2015:	Walter Jean-Philippe (ad interim)

Sekretariat:

Leiter:	Walter Jean-Philippe
Stellvertreter:	Buntschu Marc
Einheit 1:	11
Einheit 2:	14
Einheit 3:	5 (davon 1 Praktikantin)
Kanzlei:	2

4. Abkürzungsverzeichnis

ARE	Bundesamt für Raumentwicklung
armasuisse	Bundesamt für Rüstung
ASTRA	Bundesamt für Strassen
BABS	Bundesamt für Bevölkerungsschutz
BAFU	Bundesamt für Umwelt
BAG	Bundesamt für Gesundheit
BAK	Bundesamt für Kultur
BAKOM	Bundesamt für Kommunikation
BAR	Schweizerisches Bundesarchiv
BASPO	Bundesamt für Sport
BAV	Bundesamt für Verkehr
BAZL	Bundesamt für Zivilluftfahrt
BBL	Bundesamt für Bauten und Logistik
BFE	Bundesamt für Energie
BFK	Eidgenössisches Büro für Konsumentenfragen
BFS	Bundesamt für Statistik
BGE	Bundesgerichtsentscheid
BIT	Bundesamt für Informatik und Telekommunikation
BJ	Bundesamt für Justiz
BK	Bundeskanzlei
BLW	Bundesamt für Landwirtschaft
BLV	Bundesamt für Lebensmittelsicherheit und Veterinärwesen
BSV	Bundesamt für Sozialversicherungen
BWL	Bundesamt für wirtschaftliche Landesversorgung
BWO	Bundesamt für Wohnungswesen
ComCom	Eidgenössische Kommunikationskommission
EAV	Eidgenössische Alkoholverwaltung
EBG	Eidgenössisches Büro für die Gleichstellung von Frau und Mann
EFK	Eidgenössische Finanzkontrolle
EFV	Eidgenössische Finanzverwaltung
EHB	Eidgenössisches Hochschulinstitut für Berufsbildung
ENSI	Eidgenössische Nuklearsicherheitsinspektorat

EPA	Eidgenössisches Personalamt
ESBK	Eidgenössische Spielbankenkommission
ESchK	Eidgenössische Schiedskommission für die Verwertung von Urheberrechten und verwandten Schutzrechten
ESTV	Eidgenössische Steuerverwaltung
EZV	Eidgenössische Zollverwaltung
fedpol	Bundesamt für Polizei
IGE	Eidgenössisches Institut für Geistiges Eigentum
ISB	Informatiksteuerungsorgan des Bundes
ISC	Informatik Service Center
METAS	Eidgenössisches Institut für Metrologie
METEO CH	Bundesamt für Meteorologie und Klimatologie
NB	Schweizerische Nationalbibliothek
NDB	Nachrichtendienst des Bundes
NKVF	Nationale Kommission zur Verhütung von Folter
PostCom	Eidgenössische Postkommission
PUBLICA	Pensionskasse des Bundes
PUE	Preisüberwacher
RAB	Eidgenössische Revisionsaufsichtsbehörde
SBFI	Staatssekretariat für Bildung, Forschung und Innovation
SECO	Staatssekretariat für Wirtschaft
SEM	Staatssekretariat für Migration
SIF	Staatssekretariat für internationale Finanzfragen
SIR	Schweizerisches Institut für Rechtsvergleichung
SNF	Schweizerischer Nationalfonds
SNM	Schweizerisches Nationalmuseum
SUVA	Schweizerische Unfallversicherungsanstalt
SWISSMEDIC	Schweizerisches Heilmittelinstitut
UBI	Unabhängige Beschwerdeinstanz für Radio und Fernsehen
WEKO	Wettbewerbskommission
ZAS	Zentrale Ausgleichsstelle
ZIVI	Vollzugsstelle für den Zivildienst