24. Tätigkeitsbericht 2016/17

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Tätigkeitsbericht 2016/2017
des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten

Der Eidgenössische 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 2016 und 31. März 2017 ab.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Vorwort

Aktuelle Herausforderungen und Schwerpunkte

I Veränderte technologische und gesellschaftliche Verhältnisse 6
II Ausdehnung und Beschleunigung der Kontrolltätigkeit des EDÖB 7
III Veränderte Erwartungen an den EDÖB 7
IV Nationale und internationale Kooperation des EDÖB 8
V Massnahmen des EDÖB zur Effizienzsteigerung 8

1 Datenschutz

1.1 Grundrechte 12
1.1.1 Verwendung der AHV-Nummer in Registern: Einheitsidentifikator versus sektorenspezifische Lösung 12
1.1.2 Vernichtung und Löschung der bei der Bevölkerungszählung erhobenen Daten 12
1.1.3 Nutzung der elektronischen Infrastruktur des Bundes: Sachverhaltsabklärungen beim Eidgenössischen Personalamt und beim Bundesamt für Bauten und Logistik 13
1.1.4 Nationaler Adressdienst 13
1.1.5 Videoaufnahmen in Schwimmbädern zu Trainingszwecken 14

1.2 Datenschutzfragen allgemein 15
1.2.1 Revision des Bundesgesetzes über den Datenschutz 15
1.2.2 Strategie «Digitale Schweiz» 16
1.2.3 Öffentlicher Verkehr: Umsetzung der Empfehlung in Sachen SwissPass und weitere Beratung 16
1.2.4 Elektronisches Ticketing 17

1.3 Internet und Telekommunikation 18
1.3.1 Abschluss der Sachverhaltsabklärung zu Windows 10 18
1.3.2 Neue Datenschutzbestimmungen von Swisscom 18
1.3.3 Datenschutzaspekte beim Internetprotokoll IPv6 19

1.4 Justiz, Polizei, Sicherheit 20
1.4.1 Gesetz zur elektronischen Identität 20
1.4.2 Überwachung des Post- und Fernmeldeverkehrs – Totalrevision der Verordnungen 20
1.4.3 Koordinationsgruppe der schweizerischen Datenschutzbehörden im Rahmen der Schengen-Abkommen 21

1.5 Gesundheit und Forschung 22
1.5.1 Ausführungsbestimmungen zum Bundesgesetz über das elektronische Patientendossier 22
1.5.2 Projekt BAGSAN des Bundesamts für Gesundheit 22
1.5.3 Auslagerung der Rechnungsstellung im medizinischen Bereich 23

1.6 Versicherungen 24
1.6.1 Die Entbindung von der Schweigepflicht im Rahmen eines IV-Verfahrens 24
1.6.2 Kontrolle der Datenannahmestellen der Krankenversicherer 25
1.6.3 Zentrales Informationssystem zur Bekämpfung von Versicherungsmissbrauch 25
1.6.4 Einsatz von Fitnesstrackern im Versicherungsbereich 26

1.7 Arbeitsbereich **27**
1.7.1 Sachverhaltsabklärung zu eRecruiting und Bewerbungsdossiers in der Bundesverwaltung 27

1.8 Handel und Wirtschaft **28**
1.8.1 Swiss-U.S. Privacy Shield 28
1.8.2 Wirtschaftsauskunftei Moneyhouse – Klage vor Bundesverwaltungsgericht 28
1.8.3 Verordnungen zur Energiestrategie 2050 29

1.9 Finanzen **31**
1.9.1 Bekanntgabe von Personendaten an ausländische Steuerbehörden 31

1.10 International **34**
1.10.1 Internationale Zusammenarbeit 34
1.10.2 Aufsichtskoordinationsgruppen SIS II, VIS und Eurodac 36
1.10.3 Arbeitsgruppe «Border, Travel & Law Enforcement» 36
1.10.4 Arbeitsgruppe für Datenschutz und internationale humanitäre Hilfe 37

2 Öffentlichkeitsprinzip

2.1 Zugangsgesuche **40**
2.1.1 Departemente und Bundesämter 40
2.1.2 Parlamentsdienste 40
2.1.3 Bundesanwaltschaft 40

2.2 Schlichtungsanträge **41**

2.3 Ämterkonsultationen **42**
2.3.1 Einschränkung des Öffentlichkeitsprinzips bei der Aufsicht über den öffentlichen Verkehr 42
2.3.2 Zugang zu Dokumenten über das öffentliche Beschaffungswesen 42
2.3.3 Verordnung über den Nachrichtendienst 43

2.4 Varia **44**
2.4.1 Neue Arbeitsmethode bei der Durchführung von Schlichtungsverfahren 44
2.4.2 Veranstaltung 10 Jahre Öffentlichkeitsgesetz 44

3 Der EDÖB

3.1 Aufgaben und Ressourcen **46**

3.2 11. Datenschutztag – Grenzen der Videoüberwachung **48**

3.3 Publikationen und Veranstaltungsteilnahmen **48**

3.4 Statistiken **49**
3.4.1 Statistiken über die Tätigkeiten des EDÖB vom 1. April 2016 bis 31. März 2016 49
3.4.2 Statistiken über eingereichte Zugangsgesuche nach Öffentlichkeitsgesetz vom 1. Januar 2016 bis am 31. Dezember 2016 50

3.5 Das Sekretariat des EDÖB **56**

Abkürzungsverzeichnis **58**

Vorwort

Fast jedes Land will zurzeit die Chancen der Digitalisierung packen und seine Bevölkerung daran teilhaben lassen. Unter anderen in den Bereichen Verkehr und Gesundheitswesen treibt auch die Schweiz Grossprojekte voran, für die wir als Bürgerinnen und Bürger in unseren alltäglichen Rollen als Kunden, Patienten oder Reisende eine Fülle von Daten verfügbar machen sollen.

Ob wir das wollen und dem digitalen Experiment unser Vertrauen schenken, hängt davon ab, ob sich transparente, faire und auf Minderheiten Rücksicht nehmende Online-Praktiken oder digitale Bevormundung, Aushorchung und Übertölpelung durchsetzen.

Letzterem wirken der behördliche und betriebliche Datenschutz entgegen, indem sie frühzeitig darauf Einfluss nehmen, dass Telematik und Robotik den grundrechtlichen Anspruch der Menschen auf ein freies und selbstbestimmtes Leben unterstützen, statt zu gefährden. Angesichts der experimentellen Realität der Digitalisierung braucht es dafür nach meiner Überzeugung nebst neuer Regulierung einen pragmatischen Datenschutz, der zuweilen auch unkonventionelle Wege gehen muss, um neuen rechtlichen und technischen Instrumenten zum Schutz der Privatsphäre und zur informationellen Selbstbestimmung Akzeptanz und Wirkung zu verleihen. Weiter braucht es glaubwürdige Befugnisse und Mittel, damit der Datenschutz Grossprojekte zufriedenstellend begleiten und eine angemessene Dichte an Kontrollen entfalten kann.

Adrian Lobsiger
Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter

Aktuelle Herausforderungen und Schwerpunkte

I Veränderte technologische und gesellschaftliche Verhältnisse

Am 21. Dezember 2016 schickte der Bundesrat den Vorentwurf zu einer Totalrevision des Bundesgesetzes über den Datenschutz (E-DSG) in die Vernehmlassung. Zur Begründung führte er an, dass er «den Datenschutz stärken und an die veränderten technologischen und gesellschaftlichen Verhältnisse anpassen» wolle. Diese Entwicklungen werden nachfolgend kurz skizziert.

Technologie und Wirtschaft

Seit dem Marktauftritt des ersten iPhones im Jahre 2007 akzentuiert sich die Dynamik der Informations- und Telekommunikationstechnologie (IKT). Nach den Smartphones werden immer mehr Alltagsgeräte mit leistungsfähigen Prozessoren, Sensoren und Netzwerkmodulen ausgestattet. Über das Internet tauschen diese Geräte teilweise sogar ohne Interaktionen der Benutzer grosse Datenmengen über die User und deren Umgebung aus. Die Bearbeitung erfolgt in weltweit verteilten Rechenzentren unter Einsatz von Prozeduren (Algorithmen) zu unterschiedlichsten Zwecken. Die Technologie ist soweit fortgeschritten, dass gewissen Systemen «künstliche Intelligenz» zugeschrieben wird, weil sie in der Lage sind, autonom von unmittelbaren Steuerimpulsen von Menschen in Echtzeit zu agieren.

Die technologischen Errungenschaften der IKT wären heute nicht allgegenwärtig ohne die globalisierte Wirtschaft, die aus der IKT-gestützten Erhebung, Analyse und Weitergabe von grossen Datenmengen (Big Data) ein Geschäftsmodell entwickelt hat und die Haushalte und Unternehmen mit leistungsfähigeren und preisgünstigeren IKT-Geräten versorgt.

Gesellschaft, Politik und Recht

Die Versorgung der Freizeit- und Arbeitswelten mit immer kompakterer IKT und ein durch das Smartphone geprägter Online-Lebensstil führten zum gesellschaftlichen Phänomen der Digitalisierung. Nebst den erwünschten Auswirkungen und Chancen führt der gesellschaftliche Umgang mit IKT zu Risiken, die von unerwünschten Eingriffen in die informationelle Selbstbestimmung und Privatsphäre der Individuen bis hin zu Kontrollverlusten über grosse Datenbestände reichen.

Die Digitalisierung wurde durch die weltweite Liberalisierung der Telekommunikationsmärkte und den Preiszerfall von elektronischen Komponenten beschleunigt, was zu einer Vielzahl von global tätigen IKT-Anbietern geführt hat. Mittlerweile gehören diese zu den kapitalkräftigsten Unternehmen weltweit und besitzen die wertvollsten Marken. Mit Ihren «Gratis-Angeboten» erreichen sie Leute rund um den Globus und generieren damit enorme Datenbestände, die sie gewinnbringend verwerten, sodass das Geschäftsmodell von «Big Data» immer mehr Nachahmer findet und sich allmählich in allen Branchen der Wirtschaft durchsetzt. Über die Verwertung riesiger und schnell wachsender Datenbestände generieren die Bearbeitungsverantwortlichen Erkenntnisse, die inzwischen Rückschlüsse auf Verhaltensweisen und Präferenzen von Milliarden von Menschen zulassen, die täglich deren Online-Dienste in Anspruch nehmen. Als Antwort auf diese Entwicklung haben der Europarat mit der Konvention 108 und die EU mit ihrer Datenschutz Grundverordnung (DSGVO) Schritte zu einem einheitlichen Datenschutzrecht eingeleitet, das über seine Instrumente zur Wahrung eines äquivalenten Schutzniveaus auch auf Drittstaaten wie die Schweiz oder die USA ausstrahlt. Im Kern zielen diese Regelwerke darauf ab,

- die Anbieter von datenhungrigen Online-Angeboten zu verpflichten, Art, Inhalt und Umfang der beschafften Daten offenzulegen. Die Kunden sollen wissen, welche Bearbeitungen über den betriebssicheren Gebrauch einer Applikation hinausgehen und diese demzufolge, falls nicht gewünscht, wegbedingen oder stoppen können;
- die Datenschutz-Kompetenzen der Verantwortlichen zu stärken und diese dazu zu verpflichten, nach Massgabe der Grundsätze von «privacy by design» (Einbezug des Datenschutzes in der Projektphase) und «privacy by default» (datenschutzfreundliche Voreinstellungen) frühzeitig das Risiko von Persönlichkeitsverletzungen zu verringern;
- das Zusammenwirken des internen Datenschutzes von Unternehmen und Behörden mit den Datenschutzbehörden zu fördern;
- die Befugnisse der Datenschutzbehörden auszubauen und deren Arbeitsmethoden an das verstärkte Zusammenwirken mit den Anwendungsverantwortlichen anzupassen.

Wie nachfolgend gezeigt wird, führt das beschriebene technologische und gesellschaftliche Umfeld zu einer Reihe von behördenspezifischen Herausforderungen, mit denen die Datenschutzstelle des Bundes konfrontiert ist:

II Ausdehnung und Beschleunigung der Kontrolltätigkeit des EDÖB

Das Konzept von Big Data führt dazu, dass heute nicht nur die vom EDÖB zu beaufsichtigende Wirtschaft, sondern auch die Bundesverwaltung und Bundesbetriebe eine Vielzahl von Applikationen betreiben oder entwickeln, die auf grossen Datenbeständen beruhen, welche die Bürgerinnen und Bürger in ihren alltäglichen Rollen als Kunden, Patienten, oder Reisende speisen. Obwohl die Verantwortlichen die beschafften Datenbestände meist nicht oder nur teilweise personenbezogen auswerten, besteht aufgrund der Leistungsfähigkeit moderner Suchmaschinen das Risiko einer Re-Identifizierung einzelner Personen. Der EDÖB muss seine Aufsichtstätigkeit deshalb auf eine Vielzahl von Projekten der Bundesbehörden und der Wirtschaft ausdehnen, mit denen diese wissenschaftliche, statistische sowie technische oder administrative Zwecke ohne Personenbezug verfolgen. Er muss sich vergewissern, dass die erhobenen Informationen in einer Art und Weise anonymisiert werden, die eine Re-Identifizierung nach dem aktuellen Stand der Technik mit hinreichender Wahrscheinlichkeit ausschliesst. Weil anonymisierte Daten auch mit den über das Internet zugänglichen Informationen abgeglichen werden können, erweist sich diese Arbeit für den EDÖB als anspruchsvoll und zeitintensiv. Er muss die entsprechenden Projekte interdisziplinär, d.h. juristisch und technisch begleiten.

Applikationen zur Bearbeitung von Personendaten werden heute in der Regel nicht mehr zur lokalen Installation ausgeliefert, sondern über das Internet zugänglich gemacht und laufend weiterentwickelt und so z. B. online gegen Malware geschützt oder mit neuen Funktionen ausgestattet. Das bedeutet, dass die Kontrollen der sich laufend verändernden Applikationen anspruchsvoller geworden sind und auch rascher abgeschlossen werden müssen als früher.

III Veränderte Erwartungen an den EDÖB

Der digitale Lebensstil ist von einer Sorglosigkeit im Umgang mit IKT geprägt, die abrupt in öffentliche Entrüstung umzuschlagen pflegt, sobald Medien oder Konsumentenschutzorganisationen eine Massenapplikation wegen angeblich unerlaubter Eingriffe in die Privatsphäre kritisieren. Die Öffentlichkeit erwartet, dass der EDÖB zumindest bezüglich der aktuell gängigsten Applikationen, die oft gratis im Netz verfügbar sind, proaktiv über Risiken informiert. Gleichzeitig soll er Möglichkeiten zur Wahrung der Privatsphäre aufzeigen und im Rahmen von aufsichtsrechtlichen Verfahren die Datenschutzkonformität solcher Massenapplikationen durchsetzen.

Angesichts der grossen Zahl von Userinnen und Usern sind diese Erwartungen der Schweizer Öffentlichkeit berechtigt. Der EDÖB hat deshalb die Online-Kultur und Konsumenten-Apps in seine Informations- und Aufsichtstätigkeit einbezogen. Die Glaubwürdigkeit des EDÖB als Fachbehörde setzt dabei Abklärungen technologischer Wirkungsweisen voraus, welche in ihrer Tiefe über die von den Medien geschilderte Faktenlage hinausreichen. Mit dem Betrieb einer Hotline, der Stärkung seiner personellen IT-Kompetenz sowie dem Aufbau eines rudimentären IT-Labors, mit dem gängige Smartphone-Applikationen und andere Online-Angebote in Bezug auf ihre Datenschutzfreundlichkeit getestet werden, trägt der EDÖB den dringendsten Bedürfnissen Rechnung.

Auf Wunsch privater Unternehmen und staatsnaher Bundesbetriebe ist der EDÖB vermehrt dazu übergegangen, umfassende Projekte, welche die Bearbeitung grosser Mengen an Daten aus menschlichen Quellen zum Gegenstand haben, beratend zu begleiten. Dieses Bedürfnis nach möglichst frühzeitiger Projektberatung leitet sich aus der gewandelten Arbeitsweise der Rechts- und Datenschutzstellen dieser Betriebe ab, die Projekte von Beginn an auf ihre Datenschutzkonformität hin überprüfen, wie dies das vom E-DSG statuierte Prinzip von «privacy by design» vorschreibt.

Da Kontrollen des EDÖB bei bereits realisierten Applikationen zu kostspieligen und reputationsschädigenden nachträglichen Korrekturen führen können, findet «privacy by design» bei vielen Betrieben Anklang; insbesondere wenn diese Methode mit einer phasenweisen Beurteilung wichtiger Projektschritte durch die Datenschutzbehörde gekoppelt werden kann. Für den EDÖB ist eine beratende und beaufsichtigende Aufgaben kombinierende Arbeitsweise mit dem Vorteil einer frühzeitigen Minderung datenschutzrelevanter Risiken verbunden. So kann er auch auf kurzlebige Applikationen Einfluss nehmen, die sich über langwierige Verfügungs- oder gar Sanktionsverfahren nur beschränkt beeinflussen liessen.

Als aktuelle Beispiele lassen sich Grossprojekte wie Mobility Pricing der öffentlichen Verkehrsbetriebe und des UVEK, Sesam von Post und SBB, TWINT von Post und Banken oder Admeira von Swisscom, SRG und Ringier anführen.

IV Nationale und internationale Kooperation des EDÖB

Weil die Datenschutzbehörden von Bund und Kantonen in weiten Teilen mit den gleichen Entwicklungen und Technologien zur Bearbeitung von Personendaten konfrontiert sind, strebt der EDÖB vor dem Hintergrund der Digitalisierung eine Intensivierung seiner Kontaktpflege mit den kantonalen Datenschutzbehörden an. Deren Zusammenarbeit wird durch den Verein «privatim» interkantonal koordiniert.

Ein anschauliches Beispiel für die Notwendigkeit einer engen Zusammenarbeit ist die vom Bundesrat geplante Einführung der nicht sprechenden AHV-Nummer 13 als universeller Identifikator für die Verwaltungen von Bund, Kantonen und Gemeinden. Es liegt auf der Hand, dass dieses Vorhaben mit Blick auf die technologischen Risiken von unerwünschten Re-Identifikationen durch die Datenschutzstellen des Bundes und der Kantone gemeinsam beurteilt werden muss.

Im internationalen Bereich zeichnen sich folgende neuen Aufgaben ab:

Privacy Shield

Durch das Internet und die Dominanz der kalifornischen IT-Industrie, die gigantische Rechenzentren oder Clouds betreibt, in denen biometrische und andere Personendaten von Millionen von Schweizer Nutzern bearbeitet werden, ist die Beurteilung der Übermittlung von Personendaten ins Ausland zu einem wichtigen Teil der Aufsichtstätigkeit des EDÖB geworden. Damit sich die neue Regelung «Privacy Shield», die im Januar 2017 zwischen der Schweiz und den USA abgeschlossen wurde, im Gegensatz zu dem vom EuGH kassierten «Safe Harbor»-Abkommen etablieren und an die aktuellen Bedürfnisse anpassen kann, wurden mit den USA jährliche Evaluationen vereinbart. Diese werden vom SECO angeführt und durch den EDÖB begleitet und mit einer eigenständigen Berichterstattung abgeschlossen.

Vergemeinschaftung des Datenschutzes in der EU

Am 1. Mai 2018 wird die EU ihre Datenschutz Grundverordnung (DSGVO) in Kraft setzen, welche auch für Applikationsverantwortliche in der Schweiz zur Anwendung gelangt, soweit sie Daten von Bürgern in der EU bearbeiten. Mit diesem Regelwerk werden die Datenschutzgesetze der einzelnen EU-Mitgliedstaaten aufgehoben. Die nationalen Datenschutzbehörden werden ihre Aufsichtstätigkeiten inskünftig intensiver aufeinander abstimmen.

Angesichts der unionsweiten Bündelung des Datenschutzes und der extraterritorialen Anwendung der DSGVO ist davon auszugehen, dass die EU Einfluss darauf nehmen wird, wie Drittstaaten die in der DSGVO verankerten Prinzipien umsetzen. Ganz besonders dürfte dies gegenüber der Schweiz der Fall sein, die als assoziiertes Mitglied von Schengen-Dublin grosse Mengen sensibler Behördendaten mit der EU austauscht.

Vor diesem Hintergrund wird deutlich, dass der EDÖB als primäre Ansprechstelle für die ihrerseits unabhängigen Datenschutzorgane der EU und ihrer Mitgliedstaaten präsent und wahrnehmbar sein muss. Das bedingt, dass er auch an den diversen internationalen Veranstaltungen angemessen vertreten und in der Lage sein muss, den damit verbundenen Aufwand zu leisten. Dies auch mit Blick auf die EU-Richtlinie 2016/680, welche verlangt, dass der EDÖB in die Arbeiten des EU-Datenschutzkomitees eingebunden wird.

V Massnahmen des EDÖB zur Effizienzsteigerung

Zur Bewältigung der behördenspezifischen Herausforderungen und der damit einhergehenden Erwartungshaltungen der Wirtschaft und Behörden wie auch der Öffentlichkeit hat der EDÖB in der Berichtsperiode 2016/2017 eine Reihe von Massnahmen zum effizienten Einsatz seiner Mittel realisiert.

Aufgrund der dargelegten Herausforderungen hat der EDÖB folgende strategischen Schwerpunkte gesetzt:

- Stärkung der eigenen Kompetenzen bezüglich Technologien sowie Geschäfts- und Kommunikationsmodelle der digitalen Gesellschaft;
- Beratende Begleitung relevanter Projekte von Behörden und Wirtschaft;
- Wahrnehmbare Präsenz für die betroffenen Bürgerinnen und Bürger in der Schweiz.

Ausgehend von dieser Strategie wurde für das Jahr 2017 ein Plan erarbeitet, der die beratende Begleitung von zehn grösseren Projekten sowie acht umfassendere Kontrollen vorsieht (vgl. dazu Ziffer 3.1.1 des vorliegenden Tätigkeitsberichts).

Reorganisation der Behörde

Die strategische und operative Fokussierung auf die Digitalisierung wird durch eine finanzneutrale Reorganisation der Behörde unterstützt, die am 1. April 2017 in Kraft getreten ist. Sie zielt darauf ab, die technischen Kompetenzen der Behörde zu stärken und deren Leitung von alltäglichen Querschnittsaufgaben zu entlasten:

Alle traditionellen Stabs- und Querschnittsaufgaben wie Geschäftskontrolle, Kommunikation, Finanzen wurden in die neu gebildete Einheit Kompetenzzentren überführt (vgl. dazu das Organigramm des EDÖB: www.derbeauftragte.ch, Der EDÖB – Organisation). Dort werden u.a.:

- alle technischen Kompetenzen für die Unterstützung der datenschutzrechtlichen Verfahren und die eigene Weiterbildung gebündelt;
- aktuelle Entwicklungen der Digitalisierung analysiert.

Die beiden bisherigen Einheiten zum Vollzug des DSG wurden unter Bildung dreier Teams zusammengefasst.

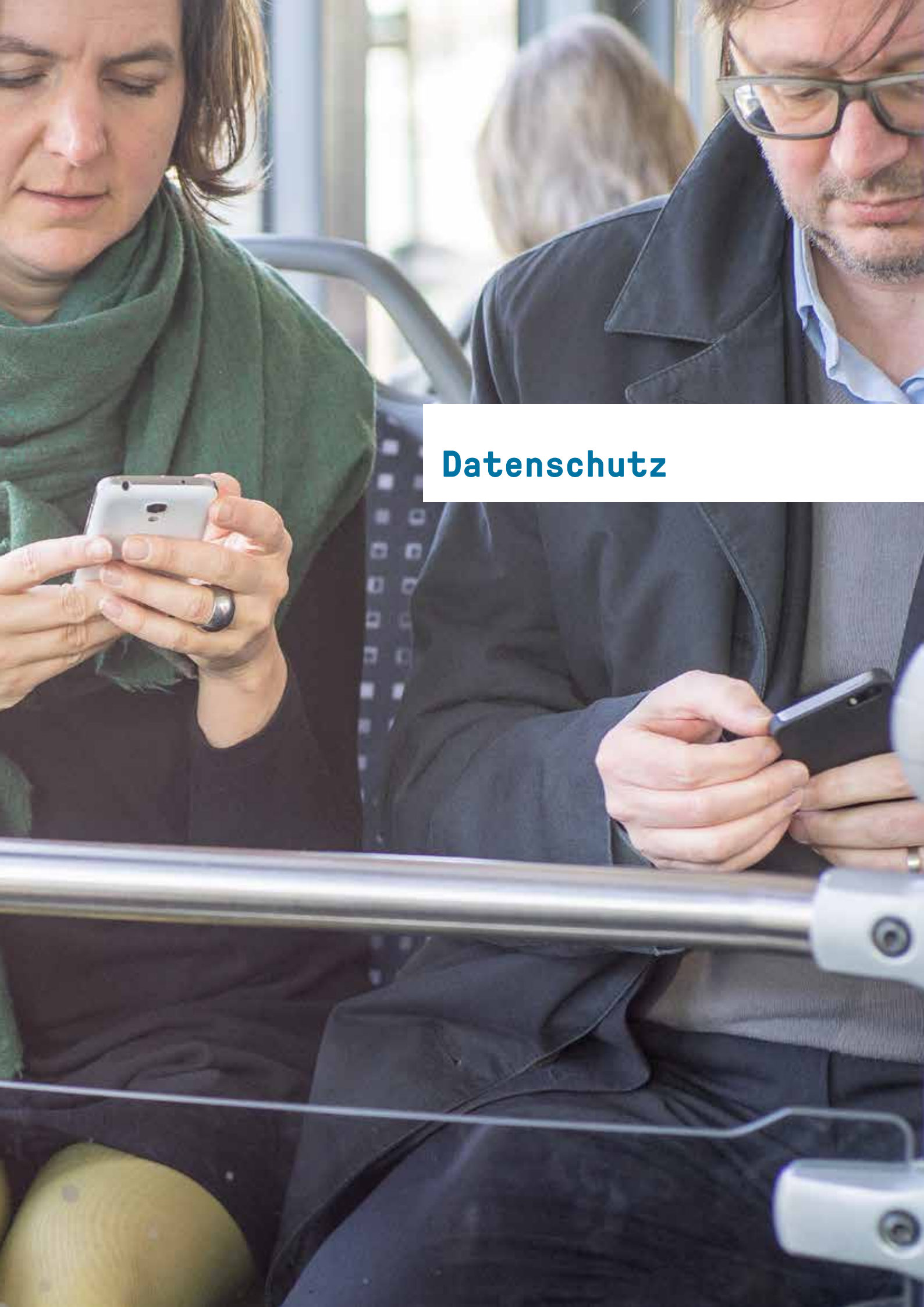
Eine erneuerte Laborumgebung ermöglicht das Austesten von Consumer-Apps, IKT-Produkten oder sozialen Netzwerken. Bei besonderen technischen Fragestellungen kann der EDÖB das BAKOM und den ISB (MELANI) amtshilfeweise um fachliche Unterstützung angehen.

Konzeptionelle Erneuerung des Informationsangebots

Der EDÖB beantwortete 2016 rund 3500 mündliche und schriftliche Anfragen von Bürgerinnen und Bürgern, Firmen und Organisationen. Zudem veröffentlichte er auf seiner Webseite ein breites Angebot von Informationen über technologische Entwicklungen mit praktischen Ratschlägen sowie sämtliche formellen Empfehlungen, die er im Zuge seiner Aufsichtstätigkeit erlässt. Dieses Angebot wurde zusammen mit dem Geschäftsbericht einer konzeptionellen Überarbeitung unterzogen. Damit will der EDÖB dem gesteigerten öffentlichen Bedürfnis nach proaktiver Information über gängige technische Applikationen bestmöglich Rechnung tragen.

Angepasstes Verfahren im Bereich des Öffentlichkeitsgesetzes (BGÖ)

In der Einheit BGÖ sind in den letzten Jahren erhebliche Arbeitsrückstände bei der Behandlung von Schlichtungsanträgen entstanden. Um zu vermeiden, dass zu deren Abbau wie in den Vorjahren Personal aus dem Datenschutz-Bereich abgezogen werden muss, ist der EDÖB ab dem 1. Januar 2017 zu einem beschleunigten und summarischen Verfahren übergegangen, das sich dadurch charakterisiert, dass in der Regel mündliche Schlichtungsverhandlungen durchgeführt werden (vgl. dazu Ziffer 3.1 des vorliegenden Tätigkeitsberichts).



Datenschutz

1.1 Grundrechte

1.1.1 Verwendung der AHV-Nummer in Registern: Einheitsidentifikator versus sektorenspezifische Lösung

Im Berichtsjahr haben wir die Rechtskommissionen des National- und Ständerates hinsichtlich der Einführung der AHV-Versichertennummer für das Handelsregister und Grundbuch beraten. Zudem äusserten wir uns zum Vorhaben des Bundesrats, die Verwendung der AHV-Nummer auch ausserhalb des Sozialversicherungsbereichs systematisch zu ermöglichen.

Wir setzen uns seit Jahren für die Verwendung von sektorenspezifischen Identfikatoren ein (vgl. u.a. unseren Tätigkeitsbericht 2014/2015, Ziffern 1.1.2 und 1.1.3). Einen solchen haben Bundesrat und Parlament denn auch bei der Patientenidentifikationsnummer nach dem Bundesgesetz über das elektronische Patientendossier vorgesehen. Auch mit der Verabschiedung der revidierten Bestimmungen zum Handelsregister im Obligationenrecht hat der Gesetzgeber am 17. März 2017 einen sektoriellen Identifikator geschaffen, der im Verkehr der Register gegen aussen sichtbar ist. Damit wird einerseits die sichere Identifikation der im Register eingetragenen Personen gewährleistet; andererseits wird unseren datenschutzrechtlichen Bedenken betreffend die missbräuchliche Verknüpfung von Personendaten Rechnung getragen. Das Eidgenössische Amt für das Handelsregister wird die Ableitung der Nummer vornehmen.

Im Berichtsjahr wurden wir in den Rechtskommissionen des National- und des Ständerats nicht nur zur Handelsregistervorlage, sondern auch zur Revision des Grundbuchrechts konsultiert. Nachdem sich der Ständerat in Anlehnung an das Handelsregisterrecht auch für das Grundbuch für die Verwendung einer sektorenspezifischen Nummer aussprach, wird diese Frage nun im Frühsommer 2017 von der Rechtskommission des Nationalrats behandelt.

Nachdem im Gesundheits- und Registerrecht sektorenspezifische Identifikatoren eingeführt wurden, hat der Bundesrat am 1. Februar 2017 das Eidgenössische Departement des Innern damit beauftragt, eine Gesetzesvorlage auszuarbeiten, welche die systematische Verwendung der AHV-Nummer durch Behörden des Bundes, der Kantone und der Gemeinden über den Sozialversicherungsbereich hinaus erleichtern soll. Wir sehen darin einen Richtungswechsel oder zumindest eine Inkonsistenz zu den vorerwähnten, sektorenspezifischen Lösungen.

Wir wiesen stets darauf hin, dass die Verwaltungen von Bund, Kantonen und Gemeinden bei einer einheitlichen Verwendungen der AHV-Nummer ausserhalb des Sozialversicherungsbereichs integral und gleichzeitig betroffen wären, wenn es zu unberechtigten Datenabflüssen oder -manipulationen käme. Weiter äusserten wir Zweifel daran, ob als sektorenübergreifender Identifikator ausgerechnet die AHV-Nummer als sichere Lösung gelten könne, obwohl diese über alle privaten Betriebe verbreitet ist.

Dem hält die Verwaltung entgegen, dass die Risiken für den Datenschutz angesichts der Leistungen moderner Suchprogramme bei Verwendung sektorenspezifischer Identifikatoren nicht geringer seien als bei einheitlicher Verwendung der AHV-Nummer. Wie wir auch anlässlich seiner Anhörungen durch parlamentarische Kommissionen darlegten, verschliessen wir uns dieser Argumentation nicht generell. Ob aufgrund des technischen Fortschritts tatsächlich eine Neueinschätzung der Risiken angezeigt ist, hat die Verwaltung als Verursacherin dieser Risiken indessen mit wissenschaftlich untermauerten Fakten belegen zu lassen. Weil vom angestrebten Systemwechsel alle Gemeinwesen der Schweiz und die Personendaten von Millionen von Menschen betroffen wären, fordern wir die Erstellung einer Risikofolgenabschätzung durch eine unabhängige Fachstelle. Die Datenschutzorgane von Bund und Kantonen sollen dann zu gegebener Zeit zu dieser Studie Stellung nehmen können.

1.1.2 Vernichtung und Löschung der bei der Bevölkerungszählung erhobenen Daten

Im Berichtsjahr haben wir beim Bundesamt für Statistik (BFS) eine Sachverhaltsabklärung eröffnet. Im Fokus der Untersuchung steht namentlich die Kontrolle der Vernichtung und Löschung der Daten, die anlässlich der Bevölkerungszählung erhoben werden.

Uns interessierte, wie das BFS die Volkszählungsdaten nach der Erfassung, Bereinigung sowie Kontrolle löscht bzw. vernichtet. Wir erachteten es als notwendig, die in diesem Zusammenhang stehenden Prozesse vertiefter anzuschauen und auf ihre Konformität mit dem Datenschutzgesetz (DSG) zu überprüfen. Einen Augenschein vor Ort beim BFS haben wir bereits vorgenommen. Als nächstes werden wir die vom BFS erhaltenen Unterlagen und Antworten auf unsere Rückfragen analysieren und prüfen, ob die genannten Prozesse den Anforderungen des DSG genügen.

1.1.3 Nutzung der elektronischen Infrastruktur des Bundes: Sachverhaltsabklärungen beim Eidgenössischen Personalamt und beim Bundesamt für Bauten und Logistik

Wir haben zwei Kontrollen beim Eidgenössischen Personalamt (EPA) und beim Bundesamt für Bauten und Logistik (BBL) betreffend einen Teil der Nutzung der elektronischen Infrastruktur des Bundes durchgeführt und sind zum Schluss gekommen, dass die angewendete Dauer der Datenaufbewahrung den gesetzlichen Anforderungen entspricht.

Im Berichtsjahr überprüften wir im Rahmen unserer Aufsichtstätigkeit, ob die Daten, die bei der Nutzung der elektronischen Infrastruktur des Bundes anfallen, rechtzeitig und korrekt vernichtet werden. Bei dieser Kontrolle ging es darum zu verstehen, wie die Vernichtung dieser Daten konkret erfolgt, und zu beurteilen, ob die Aufbewahrungsdauer eingehalten wird. In diesem Kontext eröffneten wir zwei Sachverhaltsabklärungen: Die erste erfolgte beim EPA und betraf die Daten über die Arbeitszeiten des Personals im Sinne des Regierungs- und Verwaltungsorganisationsgesetzes (RVOG) mit einer Aufbewahrungsdauer von höchstens fünf Jahren. Das zweite Verfahren wurde beim BBL eingeleitet und bezog sich auf die Daten über das Betreten oder Verlassen von Gebäuden und Räumen der Bundesorgane und über den Aufenthalt darin. Diese Daten dürfen während maximal drei Jahren aufbewahrt werden.

Da unsere Lageanalyse keine Hinweise auf mögliche Verfehlungen betreffend die in der Verordnung über die Bearbeitung von Personendaten vorgesehene Aufbewahrungsdauer ergab, haben wir die Kontrollen ohne Abgabe von Empfehlungen abgeschlossen. Wir stellten fest, dass die Aufbewahrungsdauer die in der Verordnung vorgegebenen Fristen nicht überschreitet und demnach die Anforderungen des Datenschutzgesetzes erfüllt.

1.1.4 Nationaler Adressdienst

Wir haben im Rahmen einer Ämterkonsultation zur Schaffung eines nationalen Adressregisters Stellung genommen. Unseren Bemerkungen wurde im Wesentlichen Rechnung getragen. Wir werden das Projekt weiterhin aufmerksam verfolgen.

Am 12. November 2014 beauftragte der Bundesrat das Eidgenössische Justiz- und Polizeidepartement (EJPD), die verschiedenen Möglichkeiten zur Schaffung eines nationalen Adressregisters zu prüfen und ihm vor Ende 2016 einen Vorschlag zu unterbreiten (vgl. unseren 23. Tätigkeitsbericht 2015/2016, Ziff. 1.1.3).

Diese Studie unter der Leitung eines vom Bundesamt für Justiz (BJ) beauftragten Experten gelangte zum Schluss, dass die optimale Lösung in der Einrichtung eines Registers auf Bundesebene (Nationaler Adressdienst – NAD) liegt, das die derzeit vom Bundesamt für Statistik (BFS) zu statistischen Zwecken erhobenen Adressdaten verwendet. Dafür müsste eine Überleitung geschaffen werden, um den Datentransfer vom BFS zum NAD sicherzustellen. Die Organisation des NAD soll von dem bisher durch das BFS geführten Register unabhängig sein. Die Kosten könnten durch die Erhebung einer Gebühr gedeckt werden. Rechtlich gesehen kann die Schaffung des NAD im Anschluss an eine Änderung des Registerharmonisierungsgesetzes (RHG) erfolgen. Die technischen und organisatorischen Details des NAD sind noch zu präzisieren.

Der Bundesrat muss sich zur Schaffung des NAD äussern und das EJPD beauftragen, ihm mit der technischen Unterstützung des BFS bis Ende 2018 einen Entwurf zwecks externer Vernehmlassung zu unterbreiten.

Im Rahmen der Ämterkonsultation wurden wir aufgefordert, Stellung zu nehmen zum Fortschrittsbericht über den Adressdatenaustausch zwischen den Einwohnerregistern und anderen Dateninhabern. Unsere Bemerkungen sind im Wesentlichen berücksichtigt worden. Sie betrafen die genauen Zwecke eines solchen Dienstes, die Rolle des BFS – Garant der statistischen Geheimhaltung und einer seinem gesetzlichen Auftrag entsprechenden Datennutzung -, die Aufbewahrungsdauer der Adressen, den Kreis der Nutzungsberechtigten, die Verhältnismässigkeit der Datenerhebung, die Genauigkeit der Daten im Falle einer nicht unmittelbaren Aktualisierung, die Organisation des NAD und der Aufsichtsbehörde sowie die technischen und organisatorischen Massnahmen, die zur Gewährleistung des Datenschutzes getroffen werden.

Als Mitglieder der Arbeitsgruppe werden wir das Projekt weiter aufmerksam verfolgen und sicherstellen, dass angesichts der in der Folge noch anzubringenden technischen und organisatorischen Präzisierungen die vorgeschlagene Variante dem Datenschutz gerecht wird.

1.1.5 Videoaufnahmen in Schwimmbädern zu Trainingszwecken

Videoaufnahmen in Schwimmbädern können die Intimsphäre der Badegäste tangieren. Deswegen muss bei Trainingseinheiten, bei denen Videoanalysen zum Einsatz kommen, sichergestellt werden, dass sich keine unbeteiligten Badegäste im Aufnahmebereich aufhalten.

Videoanalysen haben sich als Trainingsinstrument in diversen Sportarten etabliert und leisten beispielsweise bei der Optimierung von Bewegungsabläufen wertvolle Dienste. So ist es nicht weiter verwunderlich, dass auch Schwimmtrainer gerne darauf zurückgreifen. Wenn das Schwimmtraining dabei in einem öffentlichen Bad durchgeführt wird, kann dies jedoch zu heiklen Situationen für den Persönlichkeitsschutz führen.

Unterwasseraufnahmen in öffentlichen Schwimmbädern können die Intimsphäre der Betroffenen tangieren, was sich durch Trainingszwecke allein nicht rechtfertigen lässt. Dementsprechend dürfen solche Aufnahmen nur mit der expliziten Einwilligung aller Betroffenen erstellt werden. Das Einholen einer solchen Einwilligung bei den gefilmten Sportlerinnen und Sportler bereitet vergleichsweise wenig Probleme. Ein vom Bundesamt für Sport (BASPO) zum Thema veröffentlichtes Informationsblatt gibt hier weiter Auskunft (www.mobilesport.ch).

Bei unbeteiligten Badegästen hingegen kann die explizite Einwilligung nur sehr schwer eingeholt werden. Eine gültige Einwilligung setzt voraus, dass die betroffenen Personen über alle wesentlichen Aspekte der Videoaufzeichnung informiert worden sind. Dies beinhaltet nebst der Tatsache, dass solche Aufnahmen gemacht werden, insbesondere auch deren Zweck, deren Aufbewahrungsdauer und wer die Aufnahmen ansehen kann. Die Einwilligung muss zudem freiwillig erfolgen, das heisst, die Betroffenen müssen das Schwimmbad nutzen können, ohne dabei gefilmt zu werden.

Es dürfte sich als kaum praktikabel erweisen, bei Normalbetrieb des Bades sämtliche sich zufällig im Aufnahmebereich aufhaltenden Badegäste ausreichend zu informieren und den allfällig geäusserten Willen, nicht gefilmt zu werden, zu berücksichtigen. Dementsprechend muss der Datenbearbeiter sicherstellen, dass sich nur Teilnehmer der Trainingseinheit im fraglichen Bereich aufhalten. Dies lässt sich zum Beispiel erreichen, indem man Videoanalysen nur ausserhalb der offiziellen Öffnungszeiten des Bades durchführt.

1.2 Datenschutzfragen allgemein

1.2.1 Revision des Bundesgesetzes über den Datenschutz

Am 21. Dezember 2016 hat der Bundesrat den Vorentwurf für die Revision des Bundesgesetzes über den Datenschutz in die Vernehmlassung geschickt. Ziel dieser Revision sind die Anpassung unserer Gesetzgebung an die neuen Technologien, die Verstärkung des Datenschutzes und der Attraktivität der Schweiz für das digitale Zeitalter. Die Revision soll es der Schweiz insbesondere ermöglichen, sich den neuen europäischen Standards anzunähern und weiterhin über ein angemessenes Datenschutzniveau zu verfügen. Für uns ist es wichtig, dass die Revision rasch zum Abschluss gebracht wird.

Das Bundesgesetz über den Datenschutz (DSG) gehört zu den Datenschutzgesetzen der ersten Generation. Es stammt aus der Zeit vor dem Internet, den Smartphones und dem Internet der Dinge. Eine Revision ist unumgänglich, um den neuen Herausforderungen der digitalen Gesellschaft gerecht zu werden und die Achtung der Rechte und Grundfreiheiten der Menschen bei der Bearbeitung sie betreffender Daten besser zu gewährleisten. Mit der Revision soll auch der Reform des europäischen Rechtsrahmens und insbesondere der Modernisierung des Übereinkommens des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen 108) Rechnung getragen werden. Im Auftrag des Bundesrates hat das Bundesamt für Justiz einen Entwurf zur Totalrevision des DSG ausgearbeitet. Diesen Entwurf hat der Bundesrat am 21. Dezember 2016 in die Vernehmlassung gegeben.

Wir haben an den Revisionsarbeiten mitgewirkt und unseren Standpunkt in der Arbeitsgruppe und im Ämterkonsultationsverfahren eingebracht. Der Entwurf entspricht unseren Erwartungen weitgehend. Einige Punkte müssen indes erneut geprüft werden, damit unsere Gesetzgebung im Einklang mit dem revidierten Übereinkommen 108 steht und sich dem europäischen Rechtsrahmen stärker annähert. Eine solche Annäherung würde eine grössere Rechtssicherheit bieten, was nicht nur den betroffenen Personen, sondern auch den Datenbearbeitern und dem Wirtschaftsstandort Schweiz zum Vorteil gereicht.

Die Revision soll das Recht auf Datenschutz stärken, damit jedermann eine bessere Kontrolle über die ihn betreffenden Informationen erlangt. Dies erfordert eine grössere Transparenz der Bearbeitungen und die Gewährung neuer Rechte, etwa das Recht, seinen Standpunkt vor einer automatischen Entscheidung geltend machen zu können oder das Recht zu erfahren, auf welche Weise solche Entscheidungen getroffen werden. Die Revision zielt auch auf eine Verstärkung und Konkretisierung der Verpflichtungen der Verantwortlichen für die Bearbeitung ab. Sie sieht namentlich die Pflicht vor, Datenschutzverletzungen zu melden, Datenschutz-Verträglichkeitsprüfungen durchzuführen und die Bearbeitungen zu dokumentieren. Sie führt auch den Grundsatz des Datenschutzes bereits bei der Planung als Standard ein (Privacy by Design).

Mit der Revision sollen zudem die Kompetenzen des EDÖB erweitert werden, indem er eine Entscheidungsbefugnis erhält. Er sollte künftig auch Empfehlungen der guten Praxis abgeben können, die in Zusammenarbeit mit den betroffenen Kreisen ausgearbeitet werden; ausserdem wird er zwingende Vorschriften für Unternehmen im Rahmen eines Datentransfers ins Ausland genehmigen oder anerkennen können. Er wird befähigt, Standardvertragsklauseln zu erlassen, anzuerkennen oder zu genehmigen. Dagegen wird es in Zukunft Aufgabe des Bundesrates sein, Beschlüsse betreffend das angemessene Schutzniveau eines Drittstaates zu fassen.

Die Möglichkeiten der Zusammenarbeit mit anderen Datenschutzbehörden in der Schweiz und im Ausland und der Amtshilfe werden verbessert. Um seine derzeitigen und künftigen Aufgaben glaubwürdig und effektiv wahrnehmen zu können, wird der EDÖB indessen zusätzliche Ressourcen und Mittel benötigen, wie der erläuternde Bericht zum Vorentwurf betont. Er sollte über ein eigens dafür vorgesehenes Budget verfügen, ähnlich dem für die eidgenössische Finanzkontrolle gewählten Modell. Ausserdem strebt die Revision eine bedeutende Erweiterung der strafrechtlichen Sanktionen an, wenngleich die Höhe der Sanktionen gegenüber der europäischen Verordnung geringer ausfällt. Schliesslich wird die Pflicht zur Anmeldung von Datensammlungen oder -bearbeitungen im Privatsektor abgeschafft. Das Register der Datensammlungen wird künftig nur noch die Bearbeitungen durch Bundesorgane erfassen.

Wir anerkennen die Qualität der Revisionsvorlage, sind aber der Ansicht, dass sie ergänzt werden müsste. So haben wir im Ämterkonsultationsverfahren unter anderem vorgeschlagen, die Stellung der betroffenen Personen zu stärken, namentlich mit einem Widerspruchsrecht gegen die Bearbeitung, einem Recht auf Datenübertragbarkeit sowie einem Auslistungsrecht als Ergänzung zum Recht auf Löschung. Die Verantwortlichen von Bearbeitungen, die ein besonderes Risiko für die Privatsphäre darstellen, sollten zur Ernennung eines Datenschutzberaters verpflichtet werden. Diese Aufgabe

wird in zahlreichen Unternehmen bereits umfassend wahrgenommen, ist Gegenstand von Lehrgängen und bildet ein wirksames Instrument zur Umsetzung des Datenschutzes in Unternehmen und in der Verwaltung.

Schliesslich sollte das DSG auch für Datenbearbeiter gelten, die keinen Sitz in der Schweiz haben, deren Bearbeitungen aber ihre Wirkung in der Schweiz entfalten und hier niedergelassene Personen betreffen. Diese Unternehmen sollten verpflichtet werden, einen Ansprechpartner in der Schweiz zu haben, insbesondere um die Wahrnehmung der Rechte der betroffenen Personen zu erleichtern. Das Verhältnis zwischen unserer Gesetzgebung und der europäischen Verordnung, namentlich ihre Auswirkungen in der Schweiz oder für schweizerische Bearbeitungsverantwortliche mit Bearbeitungstätigkeiten in Europa, wirft in der Schweiz und in Europa zahlreiche legitime Fragen auf. In diesem Sinne begrüssen wir die Motion 16.3752 der FDP-liberalen Fraktion «Gegen Doppelspurigkeiten im Datenschutz», in welcher der Bundesrat beauftragt wird, mit der Europäischen Union eine Vereinbarung zur Koordinierung der Anwendung des jeweils geltenden Rechts anzustreben.

Wir werden die Entwicklung der Revisionsvorlage auch im Anschluss an das externe Vernehmlassungsverfahren aktiv verfolgen.

1.2.2 Strategie «Digitale Schweiz»

Im Rahmen von Ämterkonsultationen und Arbeitsgruppen haben wir zur Umsetzung der Strategie «Digitale Schweiz» des Bundesrates Stellung genommen und dabei die datenschutzrechtlichen Anforderungen erläutert. Wir setzen uns dafür ein, dass Persönlichkeitsverletzungen bereits im Voraus verhindert werden. Dazu müssen bereits bei der Planung eines Projektes angemessene Schutzmassnahmen eingebaut werden.

Mit der Strategie «Digitale Schweiz» hat der Bundesrat 2014 eine neue Datenpolitik genehmigt. Diese zielt darauf ab, die Chancen der Digitalisierung konsequent zu nutzen, damit sich die Schweiz u.a. als innovativer, zukunftsorientierter Wirtschafts- und Forschungsstandort positionieren kann. Die einzelnen Massnahmen der Strategie werden in einem Aktionsplan definiert.

Eine Massnahme der Strategie umfasst die zentralen Rahmenbedingungen für die digitale Wirtschaft, welche in einem Bericht ausgeführt werden. Bei der Ämterkonsultation zu diesem Bericht wiesen wir darauf hin, dass datenschutzrechtliche Aspekte bereits in der Planungs- und Entwicklungsphase von digitalen Wirtschaftsprojekten berücksichtigt werden müssen. So sollen bereits zu Beginn eines Projektes angemessene Schutzmassnahmen eingebaut werden, um allfällige Gesetzesverstösse zu verhindern. Ein effektiver Datenschutz setzt allerdings voraus, dass der Datenbearbeiter weiss, welche Daten er wie bearbeitet. Deshalb haben wir angeregt, die Projektträger zu verpflichten, die geplanten Datenbearbeitungen angemessen zu dokumentieren und eine Analyse zu ihren potenziellen Auswirkungen auf die Rechte der betroffenen Personen vorzunehmen.

Als weitere Massnahme der Strategie wurde eine Arbeitsgruppe geschaffen, welche ein Aussprachepapier zur Datenpolitik der Schweiz erstellen soll. Wir sind in dieser Arbeitsgruppe vertreten und haben insbesondere betont, dass der Daten- und Persönlichkeitsschutz auch langfristig sichergestellt werden muss. Ebenfalls regten wir an, den betroffenen Personen auch künftig ein Wahlrecht in Bezug auf die Verwendung ihrer Daten einzuräumen. Zudem konnten wir die Wichtigkeit der Unterscheidung zwischen Personen- und Sachdaten betonen, welche entscheidend ist für die Anwendung der Schutzbestimmungen des DSG.

Nicht zuletzt haben wir zum Bericht zur Aussenwirtschaftspolitik 2016 und den Botschaften zu Wirtschaftsvereinbarungen sowie zum Bericht über zolltarifarische Massnahmen im Jahr 2016 Stellung genommen. Der Bericht setzt sich mit den Chancen und Herausforderungen der Globalisierung und Digitalisierung auseinander, ohne aber den in diesem Zusammenhang wichtigen Schutz der Persönlichkeit der betroffenen Personen zu erwähnen. Wir haben darauf hingewiesen, dass dies gerade wegen den aktuellen Verhandlungen zu Freihandelsabkommen notwendig wäre.

1.2.3 Öffentlicher Verkehr: Umsetzung der Empfehlung zum SwissPass und weitere Beratung

Im Rahmen einer Sachverhaltsabklärung haben wir im Berichtsjahr die Umsetzung unserer Empfehlung zum SwissPass überprüft. Wir werden der Transportbranche weiterhin beratend zur Seite stehen.

Im Verlauf des Jahres haben wir die Umsetzung unserer Empfehlung und der Verbesserungsvorschläge in Sachen SwissPass überprüft (vgl. Ziff. 1.2.1 unseres 23. Tätigkeitsberichts 2015/2016). Dabei ging es vor allem darum sicherzustellen, dass die Kontrolldaten in Zusammenhang mit dem SwissPass einerseits gelöscht und andererseits nicht mehr erhoben werden. In diesem Zusammenhang führten wir zwei Nachkontrollen vor Ort durch, an denen sowohl die SBB als auch der Verband öffentlicher Verkehr (VöV) anwesend waren. Zur Umsetzung der Empfehlung wurde insbesondere die Software der Lesegeräte angepasst. Die verschiedenen Transportunternehmen mussten diese übernehmen und herunterladen. Gleichzeitig löschten die Verantwort-

lichen die bereits erhobenen SwissPass-Kontrolldaten rückwirkend. Weiter übernahmen alle Transportunternehmen die Allgemeinen Geschäftsbedingungen (AGB) für die Halbtax- und Generalabonnemente, die im Sinne unseres Verbesserungsvorschlags auf den 1. Juni 2016 angepasst wurden.

Da unsere Empfehlung vom 4. Januar 2016 somit umgesetzt wurde, schlossen wir die Sachverhaltsabklärung ab.

Wir stehen weiterhin in Kontakt mit dem VöV und der gesamten Transportbranche und begleiten diese im Rahmen unserer Beratungsfunktion. Dabei gilt es auch sicherzustellen, dass die weitere Entwicklung des SwissPass in Einklang mit dem Datenschutz erfolgt. Auch mit dem Bundesamt für Verkehr (BAV), das die Schaffung einer gesetzlichen Grundlage prüft, stehen wir in Kontakt.

1.2.4 Elektronisches Ticketing

Das elektronische Ticketing wirft viele datenschutzrechtliche Fragen auf. Es muss insbesondere freiwillig und nach angemessener Information des Reisenden erfolgen. Aber auch die übrigen datenschutzrechtlichen Voraussetzungen sind zu berücksichtigen.

Einzelne Transportunternehmen gelangten in Zusammenhang mit der Einführung des elektronischen Ticketing an uns. Das elektronische Ticketing kann unterschiedlich ausgestaltet sein. Um das Angebot nutzen zu können, muss die reisende Person vorgängig die entsprechende App auf ihr mobiles Gerät herunterladen und sich anmelden. Die Erfassung der Reise erfolgt automatisch, in gewissen Fällen müssen Start und Ende der Reise per Knopfdruck bestätigt werden. Von den Reisenden werden Bewegungsprofile erhoben, die zur Rechnungstellung benötigt werden.

Jedes elektronische Ticketing-System ist daraufhin zu prüfen, ob es datenschutzkonform ist. Nachfolgend wird lediglich auf die wichtigsten Punkte hingewiesen. Zentral ist, dass es auf freiwilliger Basis erfolgt, die reisende Person über die Datenbearbeitungen informiert ist und dazu ihre Einwilligung abgibt. Ein Widerruf muss jederzeit möglich sein. Es muss klar sein, wer Dateninhaber ist; diese Information kann über die AGB erfolgen. Die betroffene Person muss insbesondere wissen, wer welche Daten über sie bearbeitet und wie lange diese aufbewahrt werden. Dabei sind nur diejenigen Daten zu bearbeiten, die tatsächlich geeignet sind und benötigt werden (Verhältnismässigkeitsprinzip).

Grundsätzlich dürfen Transportunternehmen keine Bewegungsdaten an Dritte bekannt geben. So dürfen sie beispielsweise einem für die Rechnungstellung beauftragten Kreditkartenunternehmen nur den Gesamtbetrag, nicht aber die gemachten Fahrten oder Bewegungsdaten angeben. Sollen die Daten nicht nur für die Berechnung des Fahrpreises und die Rechnungstellung, sondern für weitere Zwecke, wie Marketing erfolgen, braucht es auch hierfür eine angemessene Information und Einwilligung der Person. Auf unübliche Datenbearbeitungen ist speziell hinzuweisen. Die Bearbeitung von Bewegungsprofilen erfordert zudem eine ausdrückliche Einwilligung (z. B. in Form eines Opt-in anstelle eines Opt-out). Die erhobenen Personendaten gilt es verschlüsselt zu übermitteln.

Die Transportbetriebe müssen zudem technische und organisatorische Massnahmen zum Schutz der Daten ergreifen. Die Bewegungsdaten sind möglichst zu pseudonymisieren oder zu anonymisieren. Für die Regulierung von Personenaufkommen und der Auslastung des Rollmaterials genügen anonymisierte Daten. Sobald die Daten nicht mehr für Abrechnungszwecke benötigt werden, sind diese zu löschen resp. zu anonymisieren. Weiter dürfen nur diejenigen Mitarbeitenden und Personen Zugang zu den Daten haben, die diese für die Erfüllung ihrer Aufgaben benötigen. Diese Personen sind datenschutzrechtlich zu schulen und zu sensibilisieren. Schliesslich muss die korrekte Handhabung von Auskunftsgesuchen betroffener Personen sichergestellt sein, sodass sie erfahren, ob und welche Daten über sie bearbeitet werden.

1.3 Internet und Telekommunikation

1.3.1 Abschluss der Sachverhaltsabklärung zu Windows 10

Der EDÖB hat im Berichtsjahr die Sachverhaltsabklärung zum Betriebssystem Windows 10 von Microsoft abgeschlossen. Das Unternehmen hat unsere Empfehlungen zur Verbesserung der Transparenz der Datenbearbeitung und der diesbezüglichen Wahlmöglichkeiten umgesetzt.

Bei der 2015 eröffneten Abklärung zu Windows 10 (vgl. 23. Tätigkeitsbericht 2015/2016, Ziffer 1.3.1), stellten wir fest, dass die Datenbearbeitung im Rahmen von Windows 10 teilweise nicht datenschutzkonform verlief. So genügten der Seitenaufbau und der Inhalt der Seiten «Schnell einsteigen» und «Einstellungen anpassen» nur beschränkt den Anforderungen an eine transparente Information. Aus inhaltlicher Sicht fehlten Informationen zur Speicherdauer der übermittelten Daten, zum Inhalt von Browserdaten sowie zum Inhalt von Feedback- und Diagnosedaten. Zudem war es für die Nutzer umständlich, bei den einzelnen Datenbearbeitungen weitergehende Informationen, z. B. aus den relevanten Passagen der Datenschutzerklärung, nachzuschlagen. Wir erliessen deshalb mehrere Empfehlungen.

Microsoft hat uns in der Folge Vorschläge zur Behebung der festgestellten Mängel vorgelegt. Unsere Rückmeldungen wurden von Microsoft eingearbeitet, so dass eine datenschutzkonforme Umsetzung der Empfehlungen erreicht und auf ein Verfahren vor dem Bundesverwaltungsgericht verzichtet werden konnte. Mit den nun festgelegten Anpassungen werden die Angaben zu den Datenbearbeitungen präzisiert. Zudem werden die Nutzer mit der neuen Einstellungsseite während dem Installationsprozess klar darauf hingewiesen, dass sie die Datenbearbeitungen und -übermittlungen im Rahmen von Windows 10 festlegen und in diese einwilligen müssen.

Die technische Umsetzung der von uns geforderten Anpassungen erfolgt weltweit über die beiden für 2017 geplanten Softwarereleases von Windows 10. Im ersten Release werden allen Benutzern bei der Neuinstallation bzw. bei einem Update auf dieses Betriebssystem die Einstellungsmöglichkeiten der Datenübermittlungen mit umfangreicheren Informationen angezeigt. Im zweiten Release können die Benutzer beim Installationsprozess zusätzlich direkt auf die entsprechende Passage in der Datenschutzerklärung zugreifen. Die Verlinkung zu weiterführenden Informationen in der Datenschutzerklärung erhöht die Transparenz und erleichtert es den Benutzern, sich in der umfangreichen und ausführlichen Erklärung zurecht zu finden.

Unabhängig von der Anpassung des zukünftigen Installationsprozesses haben die Nutzer von Windows 10 die Möglichkeit, die Datenbearbeitung und -übermittlungen jederzeit in den Systemeinstellungen anzupassen.

Wir erachten die erreichte Lösung, insbesondere die direkte Verlinkung zu den relevanten Passagen der Datenschutzerklärung und die Wahlmöglichkeiten, als Mindeststandard für Anwendungen und Dienste anderer Unternehmen. Bei künftigen Abklärungen werden wir die zu überprüfenden Datenbearbeitungen an der mit Microsoft erzielten Lösung messen.

1.3.2 Neue Datenschutzbestimmungen von Swisscom

Im Berichtsjahr hat uns Swisscom über geplante neue Datenbearbeitungen informiert. In der anschliessenden Beratung erläuterten wir dem Unternehmen die gesetzlichen Pflichten in Zusammenhang mit der Information und der Einwilligung der Kunden.

Das Telekommunikationsunternehmen Swisscom hat 2016 verschiedene Änderungen in der Kundendatenbearbeitung vorgenommen. Diese zielen darauf ab, den Kunden persönlich zugeschnittene Werbeangebote zustellen zu können. Zudem sollen gewisse nicht-personenbezogene Daten dem Werbenetzwerk Admeira zur Verfügung gestellt werden. Die Firma beabsichtigte, ihre Kundschaft in einer separaten Datenschutzerklärung über diese Umstände zu informieren und die allgemeinen Geschäftsbedingungen entsprechend anzupassen. Sie bat uns, zu den geplanten Neuerungen Stellung zu nehmen.

Wie unsere Prüfung der Unterlagen ergab, fallen durch den Ausbau der Datenbearbeitung Persönlichkeitsprofile im Sinne des Datenschutzgesetzes an. Da die Daten zu einem neuen Zweck (Marketing) bearbeitet werden, ist ein Rechtfertigungsgrund erforderlich. Im hier zu beurteilenden Fall kommt nur die Einwilligung der betroffenen Personen in Frage. Gemäss Datenschutzgesetz ist die Bearbeitung von Persönlichkeitsprofilen nur zulässig, wenn die betroffenen Personen ausdrücklich zugestimmt haben. Dem Datenbearbeiter obliegt eine erweiterte Informationspflicht: Er muss zusätzlich am Ort, wo der Kunde seine Zustimmung schriftlich oder elektronisch kundtut, über die Beschaffung von Persönlichkeitsprofilen informieren, damit eine gültige Einwilligung vorliegt. Er kann dabei auf die betreffenden Ziffern in der separaten Datenschutzerklärung verweisen und dort die relevanten Informationen weiter ausführen. Die Kunden haben das Recht, der Bearbeitung ihrer

Daten zu Marketingzwecken und deren Weitergabe an Dritte auch nachträglich zu widersprechen. Das Unternehmen muss dafür sorgen, dass der Widerspruch möglichst einfach mitgeteilt werden kann. Swisscom schlug vor, ihre bisherigen Kunden in einem separaten Schreiben über die neuen Geschäftsbedingungen und die separate Datenschutzerklärung in Kenntnis zu setzen. In diesem Schreiben sollte auch transparent aufgezeigt werden, wie sich die Kunden auch gegen die geplante Datenbearbeitung wehren können. Im Sinne der Transparenz und Information haben wir diesen Vorschlag begrüsst. Für Neukunden ist das Telekomunternehmen daran, eine entsprechend transparente Umsetzung der neuen Datenschutzerklärung und die ausdrückliche Einwilligung für die Online- und Offline-Varianten vorzubereiten. Jeder Kunde hat zudem die Möglichkeit, online in einem sogenannten Kundencenter oder per Telefon der Bearbeitung von Personendaten für Marketingzwecke zu widersprechen resp. die Zustimmung zu widerrufen.

Mit diesen, erst teilweise umgesetzten Massnahmen wird den gesetzlichen Anforderungen entsprochen. Wir bleiben mit dem Unternehmen in Kontakt und werden die definitive Umsetzung unserer Anregungen begleiten.

1.3.3 Datenschutzaspekte beim Internetprotokoll IPv6

Da die IP-Adressen des bisherigen IPv4 Protokolls erschöpft sind, wird momentan das Nachfolgeprotokoll (Version 6) eingeführt. Im Vergleich zu IPv4 bietet IPv6 eine Reihe praktischer Vorteile, birgt aber auch gewisse Risiken für den Datenschutz und die Privatsphäre. Diese Risiken können mit geeigneten technischen und organisatorischen Massnahmen minimiert werden.

Das Internet Protokoll definiert grundlegende Regeln, wie Rechner und Geräte im Internet miteinander kommunizieren. Das bisherige IPv4 mit nur 32 Bit kurzen Adressen ist an seine Grenzen gestossen, weshalb das Nachfolgeprotokoll IPv6 entwickelt wurde. Neben der Vergrösserung des Adressraums auf 128 Bit bietet IPv6 auch neue Funktionen, die der Datensicherheit dienen. Wegen der grundsätzlich möglichen Nachverfolgbarkeit der IP-Adressen ergeben sich Datenschutzrisiken, die es zu kontrollieren gilt. Eine (bisher durch Adressmangel bedingte) dynamische Adressvergabe an die Endbenutzer soll weiterhin ermöglicht werden, um das Tracking zu verhindern. Allerdings besteht auch dann noch eine Verfolgungsmöglichkeit über den sog. Interface Identifier. Dieser ist identisch mit der festen Hardware-Adresse (MAC). Mit Privacy Extentions, einem Verfahren zur Anonymisierung von IPv6-Adressen, kann mithilfe regelmässig generierter Zufallswerte eine «Verwischung» erreicht werden.

Wesentlich ist, dass ein Internetuser nicht unbemerkt über die IP-Adresse identifiziert wird. Eine Identifizierung muss erkennbar und beabsichtigt sein (z. B. durch Einloggen in seinen persönlichen E-Mail- oder Social-Network-Account oder Akzeptieren von Cookies).

Unser Merkblatt zu IPv6 sowie eine Linksammlung befindet sich auf unserer Website www.derbeauftragte.ch in der Rubrik Datenschutz – Internet und Computer.

1.4 Justiz, Polizei, Sicherheit

1.4.1 Gesetz zur elektronischen Identität

Der Entwurf des Gesetzes zur elektronischen Identität (E-ID-Gesetz) enthält eine angemessene Datenschutzbestimmung. Wir haben uns jedoch gegen die geplante Verwendung der AHV-Nummer als eindeutigen Personenidentifikator ausgesprochen.

Das Bundesamt für Justiz hat den Entwurf für ein Bundesgesetz über staatlich anerkannte elektronische Identifizierungsmittel (E-ID-Gesetz) in die Ämterkonsultation gegeben. Die Vorlage enthält eine Bestimmung betreffend den Schutz von Personendaten, welche vorsieht, dass die anerkannten elektronischen Identitätsdienstleister die vom Staat bescheinigten Personenidentifizierungsdaten nur für Identifizierungen und Authentifizierungen bearbeiten dürfen. Überdies dürfen sie Personenidentifizierungsdaten nur an Beteiligte übermitteln, die das erforderliche Sicherheitsniveau bieten, und unter der Voraussetzung, dass der Inhaber der E-ID sein Einverständnis gibt. Die Bestimmung sieht auch vor, dass die elektronischen Identitätsdienstleister und die Beteiligten keinen Handel mit staatlich anerkannten Personenidentifizierungsdaten oder mit den aufgrund dieser Daten erstellten Nutzerprofilen treiben dürfen.

In unserer Stellungnahme haben wir uns erneut gegen die Verwendung der AHV-Nummer als universellen Personenidentifikator in der gesamten Verwaltung und auch ausserhalb ausgesprochen. Wir haben auch darauf hingewiesen, dass die elektronischen Identitätsdienstleister eine Bundesaufgabe erfüllen und somit datenschutzrechtlich als Bundesorgane gelten müssen. Die Vernehmlassung zum E-ID-Gesetzesentwurf ist für das erste Halbjahr 2017 geplant. Zur Verwendung der AHV-Nummer ist eine neue Diskussionsnotiz für den Bundesrat in Vorbereitung, der zufolge die AHV-Nummer offenbar als universeller Personenidentifikator in der Verwaltung des Bundes, der Kantone und der Gemeinden verwendet werden soll.

1.4.2 Überwachung des Post- und Fernmeldeverkehrs – Totalrevision der Verordnungen

Wir haben im Berichtsjahr zu den Verordnungen zum totalrevidierten Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs Stellung genommen. Wir äusserten uns insbesondere zum Recht auf Auskunft, zur Protokollierung sowie zum Antennensuchlauf.

Im März 2016 verabschiedete das Parlament das totalrevidierte Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF). Im Rahmen der Kommissionsitzungen äusserten wir unser Verständnis für die Bestrebungen, die Speicherung der Randdaten in der Schweiz spezialgesetzlich zu regeln, obschon das Datenschutzgesetz bereits Anforderungen für die Auslagerung von Personendaten ins Ausland vorsieht. Mit einer solchen Regelung können die Risiken von Zugriffen ausländischer Behörden reduziert werden.

In unserer Stellungnahme zu den Entwürfen der Ausführungserlasse äusserten wir uns unter anderem zum Recht auf Auskunft, zur Protokollierung, zum Antennensuchlauf sowie zu den Randdaten beim Roaming.

- Wir forderten, dass die Einzelheiten des Rechts auf Auskunft und Akteneinsicht auf Verordnungsstufe geregelt werden, wie dies im Bundesgesetz festgelegt ist. Insbesondere sollte in der Verordnung die Weiterleitung der Auskunfts- und Einsichtsbegehren an die anordnende Behörde vorgesehen werden.

  Bei den Zugriffs- und Bearbeitungsprotokollen war eine kürzere Aufbewahrungsfrist als die Speicherdauer der jeweiligen Daten vorgesehen. Dies war aus unserer Sicht unbefriedigend. Die Protokolle können ihre Kontrollfunktion nur ausüben, wenn sie über die gesamte Speicherdauer der jeweiligen Daten vorliegen. Daher haben wir für die Protokolle die gleiche Aufbewahrungsdauer wie für die entsprechenden Daten gefordert.
- Gemäss der Verordnung können Antennensuchläufe über einen Zeitraum von bis zu zwei Stunden für eine bestimmte Mobilzelle resp. WLAN-Zugangspunkt beantragt werden. Wie wir bereits in der Ämterkonsultation zum Bundesgesetz ausführten, kann ein Antennensuchlauf ohne die Bildung einer genügend kleinen Schnittmenge zu einer Rasterfahndung führen. Werden die Daten aller im fraglichen Zeitpunkt an den angegebenen Standorten anwesenden Personen übermittelt, kann dies zu einem unverhältnismässigen Eingriff

in die Grundrechte einer Vielzahl von Personen führen. Unserer Auffassung nach genügt es, wenn die Strafverfolgungsbehörden die Daten basierend auf der resultierenden Schnittmenge herausverlangen können, was zudem auch den Umfang der zu liefernden Daten reduziert. Eine denkbare Lösung wäre, dass der Dienst ÜPF die Bildung der Schnittmenge im Rahmen der Auskünfte zu den standardisierten Antennensuchläufen anbietet.

- Bei den Ausführungsbestimmungen zum Roaming war aus unserer Sicht nicht klar geregelt, welche Daten die Schweizer Anbieter herausgeben müssen. Wir sind der Auffassung, dass die Fernmeldedienstanbieter in der Schweiz einzig die Daten liefern können, welche beim Roaming technisch bedingt bei ihnen anfallen oder an sie übermittelt werden sowie die standardmässig übermittelten Daten zur Rechnungsstellung. Weitergehende Pflichten sind aus unserer Sicht nicht im Gesetz vorgesehen. Wir forderten daher eine Konkretisierung der entsprechenden Bestimmung.

Da die Verordnungen inhaltlich sehr technisch sind, schlugen wir zum besseren Verständnis vor, auch die Erläuterungen zu den einzelnen Ausführungserlassen zu publizieren.

1.4.3 Koordinationsgruppe der schweizerischen Datenschutzbehörden im Rahmen der Schengen-Abkommen

Der EDÖB beaufsichtigt die im Bereich Migration, Polizei und Justiz in der Schweiz vorgenommenen Datenbearbeitungen in Anwendung der Schengen-Kooperation. Wir koordinieren unsere Aufsichtstätigkeiten mit den kantonalen Datenschutzbehörden.

Die Koordinationsgruppe der Schweizerischen Datenschutzbehörden ist im Berichtsjahr zweimal zusammengetreten. Anlässlich des ersten Treffens wurde die Arbeitsgruppe «koordinierte Kontrollen» gebildet. Ihr Ziel ist es, das Kontrollkonzept zu überprüfen und ein an alle schweizerischen Datenschutzbehörden gerichtetes Dokument auszuarbeiten, um die Kontrollen im Bereich Schengen zu erleichtern. Die Gruppe wird sich unter anderem an den Dokumenten des kürzlich von der Kontrollkoordinationsgruppe des SIS II in Brüssel verabschiedeten Audits orientieren.

Beim zweiten Treffen haben wir die kantonalen Datenschutzbehörden über die wichtigsten Punkte informiert, die von der Kontrollkoordinationsgruppe des SIS II behandelt wurden. Wir haben unsere kantonalen Kollegen auch über unsere geplanten Kontrollen und über den Beginn der Arbeiten im Hinblick auf die Schengen-Evaluation 2018 in Kenntnis gesetzt. Die Kantone ihrerseits trugen die Ergebnisse ihrer Kontrolltätigkeiten vor. Schliesslich präsentierte die Arbeitsgruppe «koordinierte Kontrollen» den Fortschritt ihrer Arbeiten.

1.5 Gesundheit und Forschung

1.5.1 Ausführungsbestimmungen zum Bundesgesetz über das elektronische Patientendossier

Die Ausführungsbestimmungen zum Bundesgesetz über das elektronische Patientendossier regeln auf Verordnungsstufe zahlreiche für den Datenschutz und die Datensicherheit relevante Vorgaben. Von zentraler Bedeutung sind die technischen und organisatorischen Zertifizierungsvoraussetzungen. Mit dem Inkrafttreten des Bundesgesetzes über das elektronische Patientendossier fallen für unsere Behörde neue Aufgaben an.

Die Arbeiten an den gesetzlichen Grundlagen für das elektronische Patientendossier wurden im Berichtsjahr durch das Bundesamt für Gesundheit (BAG) vorangetrieben. Nachdem das Parlament das Bundesgesetz über das elektronische Patientendossier (EPDG) gutgeheissen hatte und die Referendumsfrist ungenutzt abgelaufen war, standen die auf Stufe Verordnung angesiedelten Ausführungsbestimmungen und die technischen und organisatorischen Zertifizierungsvoraussetzungen auf dem Programm. Da hier zahlreiche konkrete Vorgaben in Bezug auf Datenschutz und -sicherheit zu erarbeiten waren, beteiligten wir uns im Rahmen von Veranstaltungen, Sitzungen und Ämterkonsultationen intensiv an diesen Arbeiten.

Zentrales Anliegen war für uns, dass die Vorgaben ein möglichst hohes Schutzniveau garantieren und dabei die Praktikabilität gewährleistet bleibt. Hier mussten wir zum Teil Abstriche machen. Zum Beispiel wird das Prinzip der Einzelermächtigung von Gesundheitsfachpersonen für den Zugriff auf ein elektronisches Patientendossier durch Gruppenberechtigungen aufgeweicht. Jedoch haben wir erreicht, dass für Patientinnen und Patienten die Zusammensetzung einer Gruppe von Gesundheitsfachpersonen jederzeit nachvollziehbar sein muss. Dies erachten wir als besonders wichtig, da eine neu in eine Gruppe eintretende Gesundheitsfachperson automatisch deren Zugriffsberechtigungen erhalten soll.

Im Bereich der technischen und organisatorischen Zertifizierungsvoraussetzungen betrachten wir es als wichtigen Schritt, dass die Datenspeicherung in den Gemeinschaften (Zusammenschlüsse von Gesundheitsfachpersonen und deren Einrichtungen) weitestgehend verschlüsselt erfolgen muss. Damit wird das Risiko des Datenmissbrauchs durch externe Angreifer signifikant verringert.

Für unsere Behörde werden in diesem Bereich neue Aufgaben erwachsen, für die wir dem Bundesrat zusätzliche Mittel beantragt haben. Mit dem Inkrafttreten des EPDG werden wir die zuständige Datenschutzaufsichtsbehörde für eHealth-Gemeinschaften und die Herausgeber von Identifikationsmitteln sein. Das BAG wird hier zwar als Inhaberin des Zertifizierungsschemas auftreten und das Einhalten der Vorgaben in Zusammenarbeit mit den Zertifizierern überwachen, doch bleiben wir die zuständige Aufsichtsbehörde für Datenschutz und -sicherheit. Es wird sich noch zeigen müssen, wie die konkrete Arbeitsteilung zwischen dem BAG und uns aussehen wird und wie gross der zusätzliche Arbeitsaufwand sein wird. Da Datenschutz und -sicherheit aber als zentrale Punkte für den Erfolg des elektronischen Patientendossiers anerkannt sind, werden wir hier einen erheblichen Kontroll- und Beratungsaufwand haben.

1.5.2 Projekt BAGSAN des Bundesamts für Gesundheit

Im Projekt BAGSAN des Bundesamtes für Gesundheit wurden mit unserer Beratung wichtige Massnahmen zur Wahrung der Anonymität der Versicherten ergriffen. Das Projekt zeigt klar auf, dass bei Big-Data-Projekten das Risiko einer Re-Identifizierung laufend überwacht werden muss.

Im Projekt BAGSAN (Statistik auf Grundlage von Versichertendaten) haben die Krankenversicherer dem Bundesamt für Gesundheit (BAG) jedes Jahr für jede versicherte Person mehrere Datensätze abzuliefern. Mittels eines Anonymisierungsverfahrens wird sichergestellt, dass das Bundesamt für jeden Datensatz einen Identifikator erhält, der die Verknüpfung der Datensätze über die Berichtsjahre hinweg ermöglicht und doch keinen Personenbezug herstellt. Diese Daten (sogenannte Nutzdaten) stehen dem BAG somit für umfangreiche statistische Auswertungen zur Verfügung und ermöglichen eine verbesserte Kontrolle, Steuerung und Planung im Krankenversicherungsbereich.

Besonderes Augenmerk legten wir in diesem Projekt auf den Umstand, dass auch bei reinen Nutzdaten durch deren Detailierungsgrad, Einzigartigkeit, Akkumulierung und Verknüpfung eine Re-Identifizierung möglich sein kann. Dem muss in einem Big-Data-Projekt mittels eines risikobasierten Überwachungsverfahrens Rechnung getragen werden. Im Rahmen unserer Beratungstätigkeit haben wir uns mit dem BAG vertieft zu diesem Punkt ausgetauscht. Es konnte uns mit einem

innovativen Ansatz die statistischen Risiken von Re-Identifizierungen aufzeigen. Dieser Ansatz ermöglicht es, auch über die weiteren Projektphasen eine Risikoeinschätzung vorzunehmen und mit den geeigneten Mitteln, wie zum Beispiel der Datenverarmung, die Wahrscheinlichkeit einer Re-Identifizierung sehr gering zu halten. Eine vollständige Eliminierung des Risikos lässt sich aber nicht erreichen. Deshalb ist es wichtig, dass wir auch in den kommenden Projektphasen die Massnahmen zur Wahrung der Anonymität der versicherten Personen begleiten.

1.5.3 Auslagerung der Rechnungsstellung im medizinischen Bereich

Die Auslagerung der Rechnungsstellung im medizinischen Bereich ist nicht neu. Schon lange erledigen spezialisierte Anbieter die Rechnungsstellung und das Inkasso. Trotzdem scheinen gewisse Vorgaben hinsichtlich der Transparenz gegenüber den Patienten noch nicht genügend umgesetzt zu sein. Besonders heikel wird es, wenn die Dienstleister die Patientendaten für eigene Zwecke, wie eine Bonitätsdatenbank oder Scoring, verwenden.

Gesundheitsfachpersonen sorgen sich in erster Linie um das Wohl ihrer Patientinnen und Patienten. Es ist deshalb wenig erstaunlich, dass sie die Rechnungsstellung und das Inkasso gerne an spezialisierte Unternehmen auslagern. Der zunehmende Kostendruck ist sicherlich auch ein Grund dafür, dass hier eine möglichst weitgehende Auslagerung von administrativen Aufgaben angestrebt wird. Hierbei sind aber gewisse datenschutzrechtliche Grundsätze, kantonale Bestimmungen und nicht zuletzt auch das Strafgesetzbuch zu beachten.

Im Rahmen einer Auslagerung der Rechnungsstellung ist es unumgänglich, dass Informationen, die dem strafrechtlichen Berufsgeheimnis oder kantonalen Geheimhaltungsvorschriften unterstehen, an den Dienstleister übermittelt werden. Sowohl die administrativen als auch die medizinischen Patientendaten unterliegen diesen Vorschriften. Um nicht dagegen zu verstossen, wird zwingend die ausdrückliche Einwilligung der Patientin oder des Patienten für die Datenbekanntgabe an den Dienstleister benötigt. Damit die Einwilligung rechtsgültig ist, müssen die Patienten angemessen über die Weitergabe ihrer Daten an den Dienstleister, den Zweck der Weitergabe und die Datenbearbeitungen durch den Dienstleister informiert werden. Aus Beweisgründen hat die Einwilligung schriftlich zu erfolgen. Gerade Datenbearbeitungen des Dienstleisters, welche über die eigentliche Rechnungsstellung und das Inkasso hinausgehen, müssen hier kritisch betrachtet werden.
So konnten wir feststellen, dass es Anbieter gibt, die einen Teil der Rechnungs- und Inkassodaten auch für die eigene Bonitätsdatenbank und ein Scoring verwenden und diese Daten auch an Dritte verkaufen wollen. Auch hier muss gegenüber den Patientinnen und Patienten Transparenz herrschen. Es erscheint uns für das notwendige Vertrauen in einem Behandlungsverhältnis aber als wenig förderlich, wenn eine Gesundheitsfachperson der Patientin oder dem Patienten auch noch erklären muss, dass ihre Daten durch den mit der Rechnungsstellung beauftragten Dienstleister zusätzlich für Zwecke wie Kreditscoring verwendet und sogar an Dritte verkauft werden dürfen.

Klar ist, dass eine derartige Verwendung der Daten durch den Dienstleister nicht mit einer allgemeinen Information in den Praxisräumlichkeiten gerechtfertigt werden kann. Auch ein diesbezüglicher Hinweis im Kleingedruckten auf dem Anmeldeformular, wo die Patientinnen und Patienten üblicherweise ihre Einwilligung zur Weitergabe ihrer Daten für die Rechnungsstellung und das Inkasso abgeben, erscheint uns heikel. Aufgrund der gesetzlichen Geheimhaltungspflichten sind die Gesundheitsfachpersonen gut beraten, wenn sie hier für klare Verhältnisse sorgen und die Patientinnen und Patienten deutlich auf die vorgesehenen Datenbearbeitungen des Dienstleisters einschliesslich des möglichen Verkaufs an Dritte hinweisen und die ausdrückliche Einwilligung auch hierzu einholen. Dies liegt auch im Reputationsinteresse des Dienstleisters. Unabhängig davon, ob eine zivilrechtliche Klage von Patientinnen und Patienten gegen den Dienstleister wegen Persönlichkeitsverletzungen Erfolg haben könnte, verfolgen wir die weiteren Entwicklungen in diesem Bereich aufmerksam und behalten uns aufsichtsrechtliche Massnahmen ausdrücklich vor.

1.6 Versicherungen

1.6.1 Entbindung von der Schweigepflicht im Rahmen eines IV-Verfahrens

Der Austausch von Gesundheitsdaten von Versicherten im Rahmen eines IV-Verfahrens geht relativ weit. Dasselbe gilt auch in Bezug auf die Entbindung von der Schweigepflicht. Gleichzeitig setzen aber die allgemeinen Datenschutzprinzipien Grenzen, die die Behörden zu beachten haben.

Im Berichtsjahr erhielten wir wiederholt Anfragen von Personen, die in ein IV-Verfahren gemäss Bundesgesetz über die Invalidenversicherung (IVG) involviert waren. Manche befanden sich im Stadium der frühzeitigen Erfassung von arbeitsunfähigen Versicherten. Bei anderen standen Massnahmen zur Frühintervention oder eine Abklärung ihrer Berechtigung für eine IV-Rente zur Debatte bzw. eine Rentenrevision bevor.

Bei den Bürgeranfragen ging es praktisch immer um die Rechtmässigkeit des Austausches von Personen- bzw. Gesundheitsdaten innerhalb einer Behörde und zwischen Amtsstellen. Gesundheitsdaten sind gemäss Datenschutzgesetz (DSG) als besonders schützenswerte Personendaten einzustufen, bei deren Bearbeitung erhöhte Anforderungen zu beachten sind. Es stellte sich deshalb häufig die Frage, wie weit die Ermächtigung der versicherten Person zur Entbindung der Schweigepflicht innerhalb einer Behörde geht. Dürfen z. B. sämtliche Mitarbeiter einer IV-Stelle die Akten des jeweiligen Falles konsultieren? An welche Leistungsträger dürfen Akten einer versicherten Person gesendet werden, wenn es etwa um die Abklärung des IV-Grades oder um eine Rentenrevision geht?

Beim IVG und der dazugehörigen Verordnung (IVV) handelt es sich zwar um Bundeserlasse. Allerdings sind für die Durchführung der Invalidenversicherung kantonale Stellen zuständig, d.h. die kantonalen IV-Stellen mit ihren regionalen ärztlichen Diensten (RAD) und die AHV-Ausgleichskassen. Diese kantonalen Stellen unterstehen in datenschutzrechtlichen Belangen nicht unserer Aufsicht, und das DSG ist nicht anwendbar. In diesen Fällen kommt das jeweilige kantonale Datenschutzgesetz zur Anwendung. Zudem ist der Datenschutzverantwortliche des Kantons, in dem das IV-Verfahren durchgeführt wird, für die datenschutzrechtliche Aufsicht zuständig. Im Wissen, dass wir für die fraglichen Fallkonstellationen nicht zuständig sind, gaben wir den Rechtssuchenden dennoch jeweils eine kurze Einschätzung der Rechtslage.

Der Austausch von Personendaten, und Gesundheitsdaten, im Rahmen eines IV-Verfahrens innerhalb einer IV-Stelle und zwischen Behörden betrifft, so kann dieser relativ weit gehen. Dies wird verständlich, wenn man sich vor Augen führt, welche mannigfaltigen Aufgaben die IV-Stellen zu erfüllen haben. So sind sie u.a. zuständig für die Früherfassung von arbeitsunfähigen Versicherten und für die Frühintervention, um eine drohende Invalidität abzuwenden. Ferner müssen die IV-Stellen die versicherungsmässigen Voraussetzungen abklären, d.h. der Frage nachgehen, ob die IV in einem konkreten Fall überhaupt leistungspflichtig ist. Hierbei sind die IV-Stellen auch auf die Unterlagen der AHV-Ausgleichskassen angewiesen, bzw. auf deren Mitwirkung bei der Abklärung. Weiter sind die IV-Stellen zuständig für die Abklärung der Eingliederungsfähigkeit der versicherten Personen, ordnen Eingliederungsmassnahmen an und überwachen diese. Sie setzen den Invaliditätsgrad sowie den Grad der Hilflosigkeit fest und erlassen Verfügungen über die Leistungen der IV.

Bei der Erfüllung ihrer Aufgaben können die kantonalen IV-Stellen eine ganze Reihe von anderen Diensten, wie z. B. Medizinische Abklärungsstellen (MEDAS) und Spezialisten für die Abklärung der Leistungspflicht der IV, beiziehen. In diesem Zusammenhang dürfen und müssen die IV-Stellen Gesundheitsdaten von Versicherten austauschen und weitergeben, da sie verpflichtet sind, den jeweiligen Fall umfassenden abzuklären. Hierzu brauchen sie verschiedenste Daten, welche Aufschluss geben können über die medizinischen und anderen Gründe, die beim jeweiligen Versicherten zu einer Arbeitsunfähigkeit führten. Wären die IV-Stellen nicht befugt, Personen- bzw. Gesundheitsdaten von Gesuchstellern zu bearbeiten und an andere Stellen weiterzuleiten, könnten sie die ihnen obliegenden Aufgaben nicht erfüllen. Die Datenschutzregelungen dienen nämlich auch den Interessen der Gesuchsteller, die bei der IV um Leistungen ersuchen. Es dürfen aber nur diejenigen Daten bearbeitet bzw. bekannt und weitergegeben werden, welche für die Beurteilung des Einzelfalls notwendig und für den in Frage stehenden Zweck erforderlich sind. Somit sind den Datenbearbeitungen durch die am IV-Verfahren beteiligten Stellen durch die Prinzipien der Verhältnismässigkeit und Zweckgebundenheit Grenzen gesetzt.

Dasselbe gilt auch in Bezug auf die Entbindung der Schweigepflicht. Wiederholt erhielten wir Anfragen von Personen, die im Rahmen der Abklärung von Ansprüchen auf IV-Eingliederungsmassnahmen oder einer Rente eine Ermächtigung zur Erteilung von Auskünften unterschrieben. In diesem Zusammenhang entbanden sie verschiedene Stellen und Personen von ihrer Schwei-

gepflicht (siehe Art. 6a IVG). Auch diese Ermächtigung geht nur so weit, als dies zur Abklärung der persönlichen Situation des Gesuchstellers in medizinischer, beruflicher und sozialer Hinsicht nötig ist. Hier setzen die Grundsätze der Verhältnismässigkeit und Zweckbindung den Datenbearbeitungen Schranken. Es dürfen nur die Auskünfte erteilt und diejenigen Unterlagen bearbeitet bzw. zur Verfügung gestellt werden, die für die Klärung des Falles erforderlich sind. Die Einsicht in die Unterlagen ist auf diejenigen Personen zu beschränken, die aufgrund der jeweiligen Sachlage darin Einsicht nehmen müssen. Die Frage, was im konkreten Fall erforderlich ist, entscheidet die zuständige kantonale IV-Stelle.

1.6.2 Kontrolle der Datenannahmestellen der Krankenversicherer

Seit dem 1. Januar 2014 muss jeder Krankenversicherer über eine zertifizierte Datenannahmestelle (DAS) für den Empfang der Rechnungen des Typus «Diagnosis Related Groups» (DRG) verfügen. Unsere Kontrollen von Datenannahmestellen in diesem Berichtsjahr haben gezeigt, dass die Umsetzung der DAS gut funktioniert. In einigen Fällen stellten wir Mängel fest.

Im Berichtsjahr haben wir im Rahmen von Sachverhaltsabklärungen drei zertifizierte DAS kontrolliert. Dabei wurden auch Schnittstellen zwischen den verschiedenen anderen Akteuren geprüft.

Bei diesen Kontrollen stellten wir mehrheitlich dieselben Probleme fest wie im Berichtsjahr 2014/2015. Es sei deshalb an dieser Stelle auf diese Ausführungen verwiesen (vgl. unseren 22. Tätigkeitsbericht, Kap. 1.6.1).

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

Erneut fand in diesem Berichtsjahr eine Sitzung mit den Zertifizierern der DAS sowie der Akkreditierungsstelle (SAS) statt. Auch in diesem Jahr diente sie der konstruktiven Diskussion betreffend Zertifizierung, Umsetzung und Funktion der DAS, Schnittstellen zwischen den verschiedenen Akteuren (Spitäler, Intermediäre usw.) sowie der Klärung von Meinungsverschiedenheiten.

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

1.6.3 Zentrales Informationssystem zur Bekämpfung von Versicherungsmissbrauch

Motorfahrzeugversicherungen verfügen über eine gemeinsame Datenbank zur Bekämpfung von Missbräuchen. Dieses Modell soll nun auf weitere Versicherungsbereiche ausgedehnt werden. Wir haben die Branche diesbezüglich beraten.

Die Motorfahrzeugversicherungen betreiben eine elektronische Datenplattform zur Bekämpfung des Versicherungsmissbrauchs (Car Claims Information). Im Rahmen einer Prüfung konnten wir feststellen, dass das System grundsätzlich datenschutzkonform angelegt ist (vgl. 18. Tätigkeitsbericht 2010/2011, Ziff. 1.6.1). Es bestehen aktuell Bestrebungen zur Entwicklung eines Schadenpools, welcher die Missbrauchsbekämpfung auf weitere Versicherungsbereiche ausdehnen soll.

Anlässlich einer Beratungsanfrage wiesen wir auf die neuen datenschutzrechtlichen Rahmenbedingungen hin, welche dabei zu beachten sind. Wir haben insbesondere betont, dass der Zweck der Datensammlung genügend bestimmt sein muss und die Datenbearbeitung verhältnismässig zu erfolgen hat. Weiter sind die betroffenen Personen, in der Regel die Versicherungsnehmer, genügend zu informieren, und es ist ein besonderes Augenmerk auf die Richtigkeit der Daten zu legen.

1.6.4 Einsatz von Fitnesstrackern im Versicherungsbereich

Weil eine Vielzahl der Fitness-Apps und sogenannten Wearables, d. h. Sensoren in Fitnessarmbändern oder Smartwatches, die wir auf unserem Köper tragen, keinen genügenden Datenschutz bieten, haben wir die Problematik dieser neuen Technologie in Form von Erläuterungen auf unserer Website ausführlich beleuchtet.

Die spielerische Messung der eigenen Körperfunktionen und Leistungen mittels Fitness-Apps oder Wearables kann motivierend sein und einen positiven Effekt auf die Gesundheit und das allgemeine Wohlbefinden haben. Bei der digitalen Selbstvermessung fallen jedoch gewaltige Datenmengen an, die sich kaum mehr überblicken lassen. Es droht ein Kontrollverlust, der das Grundrecht auf informationelle Selbstbestimmung infrage stellt.

Daten, die Aufschluss über unsere Gesundheit oder bestehende Krankheiten geben, werden im Datenschutzgesetz (DSG) als besonders schützenswert eingestuft, da ihre Weitergabe und Bearbeitung einen massiven Eingriff in die Privatsphäre darstellen. Mit der Nutzung von Fitnesstrackern geben wir nicht nur vielfältige Informationen über unsere Gesundheit preis, sondern kreieren auch ein aufschlussreiches Persönlichkeitsprofil. An diesen Daten haben nebst den Akteuren im Gesundheitsbereich auch andere Wirtschaftszweige ein grosses Interesse. Wenn Dritte an Informationen zu unserer Gesundheit gelangen und entgegen den Interessen der Betroffenen verwenden, können diesen gravierende Nachteile entstehen.

Inzwischen haben auch die Krankenversicherer den Trend erkannt und bieten vermehrt Prämienrabatte an für Personen, die bereit sind, ihre Körperfunktionen zu messen und die Versicherung mit diesen Informationen zu versorgen. Dies kann heikel sein, da Angaben zu Fettanteil, Schlafverhalten, Herz- oder Atemfrequenz Rückschlüsse auf den Gesundheitszustand und allfällige Krankheiten einer Person zulassen und dieser zum Nachteil werden können (z. B. Prämienerhöhungen oder Ausschluss gewisser Risiken beim Versicherungsabschluss).

Wenn Krankenversicherer über Gesundheitsdaten verfügen, besteht die Gefahr, dass diese persönlichen Informationen auch noch für weitere Zwecke verwendet werden. Deshalb muss insbesondere das Transparenzprinzip gewährleistet sein (Art. 4 DSG). Zur Bearbeitung sensibler Personendaten braucht es die ausdrückliche Einwilligung, die freiwillig und ohne (finanziellen) Druck erfolgen muss. Im Rahmen der freiwilligen Zusatzversicherung sind solche Angebote denkbar, jedoch nicht bei der obligatorischen Grundversicherung.

Wir haben detaillierte Erläuterungen zum Einsatz von Fitnesstrackern auf unserer Website publiziert (www.derbeauftragte.ch, Datenschutz – Gesundheit – Kranken- und Unfallversicherungen). Bürgerinnen und Bürger finden dort auch wertvolle Tipps, worauf sie beim Einsatz von Fitnesstrackern achten müssen.

1.7 Arbeitsbereich

1.7.1 Sachverhaltsabklärung zu eRecruiting und Bewerbungsdossiers in der Bundesverwaltung

Im Berichtsjahr haben wir die Datenbearbeitungen im Bewerbungsprozess bei der Bundesverwaltung kontrolliert. Wie unsere Sachverhaltsabklärung ergab, werden die Personendaten der Bewerberinnen und Bewerber sowohl im eRecruiting-System, als auch auf Papier mit wenigen Ausnahmen datenschutzkonform bearbeitet.

Um einen Überblick zu erhalten, wie die Bundesämter die Daten im Rahmen des Rekrutierungsprozesses bearbeiten, wählten wir pro Departement ein Amt aus, bei welchem wir nähere Abklärungen vornahmen. Bei der Auswahl der Ämter stützten wir uns auf ihre Grösse und auf die Anzahl der Stellenausschreibungen.

Nach einer Analyse der verlangten Dokumentation und Antworten führten wir Augenscheine vor Ort durch. Gestützt auf die erhaltenen Erkenntnisse sandten wir allen Ämtern eine Sachverhaltsfeststellung und einen Schlussbericht zu. Wir haben in unseren Schlussberichten festgehalten, dass die Bearbeitung der Daten im eRecruiting-System grundsätzlich datenschutzkonform verläuft. Verbesserungsmöglichkeiten sahen wir u.a. bei der Überprüfung von Zugriffsberechtigungen und der Regelung des Umgangs mit Papierdossiers. Wir teilten diese den Ämtern mit und schlossen die Abklärungen damit ab.

Bei einem Amt haben wir eine Empfehlung erlassen. Wir forderten es auf, gewisse Daten von Bewerberinnen und Bewerbern zu löschen, da deren Aufbewahrung nicht verhältnismässig sei und keine gesetzliche Grundlage für eine solche Speicherung vorliege. Das Amt hat die Empfehlung abgelehnt und sie an das zuständige Departement weitergezogen.

Da das Eidgenössische Personalamt (EPA) für das eRecruiting-System verantwortlich ist, haben wir unsere Abklärungen auf dieses Amt ausgedehnt. Wir haben im Rahmen von zwei Sitzungen verschiedene Verbesserungsmöglichkeiten angeschaut, zum Beispiel in Bezug auf die Löschung des eigenen Dossiers durch die Bewerberinnen und Bewerber. Das EPA wird die von uns kritisierten Punkte im System anpassen. Wir werden diese Verbesserungen bei einer Nachkontrolle überprüfen.

1.8 Handel und Wirtschaft

1.8.1 Swiss-U.S. Privacy Shield

Der Bundesrat hat im Januar 2017 von der Einrichtung eines neuen Rahmens für die Übermittlung von Personendaten aus der Schweiz in die USA Kenntnis genommen. Der sogenannte Privacy Shield ersetzt das vom EDÖB für ungenügend erklärte und nun auch vom Bundesrat formell aufgehobene Safe-Harbor-Abkommen zwischen der Schweiz und den USA. Wir haben die Verhandlungen zum Swiss-US Privacy Shield in beratender Funktion begleitet.

In unserem 23. Tätigkeitsbericht 2015/2016 haben wir über das Urteil des Europäischen Gerichtshofs zu Safe Harbor und die Folgen für die Schweiz berichtet (Ziffer 1.8.1). Im Januar 2016 passten wir unsere Staatenliste an und befanden, dass Datenübermittlungen in die Vereinigten Staaten nicht allein gestützt auf Safe Harbor erfolgen können. Es brauchte zusätzliche Massnahmen vertraglicher Natur, damit Daten in die Vereinigten Staaten datenschutzkonform übermittelt werden können.

Der Bundesrat beauftragte in der Folge das Staatssekretariat für Wirtschaft (SECO), eine interdepartementale Arbeitsgruppe zu gründen mit dem Ziel, ein neues Abkommen zu verhandeln, das Safe Harbor ablösen sollte. Wir nahmen als Experten an den Sitzungen teil und haben die Verhandlungen eng begleitet. Im August 2016 trat der Privacy Shield zwischen der EU und den USA in Kraft; seither haben sich einige Hundert Unternehmen unter diesem Regulativ zertifizieren lassen. In Bezug auf den Swiss-US Privacy Shield forderten wir, dass dieser mindestens dieselben Garantien für betroffene Personen bieten muss wie jener der EU. Dieses Ziel konnte in den Verhandlungen mit den USA erreicht werden.

Im Vergleich zum Safe-Harbor-Framework wurden die Anwendung der Datenschutzprinzipien für die teilnehmenden Unternehmen sowie die Verwaltung und die Überwachung durch die US-Behörden verstärkt. Dies zeigt sich in folgenden getroffenen Massnahmen:

- Die Transparenz wird durch Bereitstellung entsprechender Instrumente für betroffene Personen auf den Websites der amerikanischen Behörden erhöht. So veröffentlichen die US-Behörden auf der Website des Swiss-US Privacy-Shield entsprechende Kontaktformulare, mit denen Privatpersonen ihre datenschutzrechtlichen Anfragen übermitteln können. Neben einer Liste mit den zertifizierten Unternehmen wird neu auch eine Liste mit denjenigen Unternehmen veröffentlicht werden, deren Zertifizierung abgelaufen ist oder entzogen wurde.
- Die Aufsicht über die zertifizierten Unternehmen durch die amerikanischen Behörden wird verstärkt.
- Betroffene Personen können sich nach Ausschöpfung eines unabhängigen Streitbeilegungsmechanismus an ein dem amerikanischen Recht unterworfenes Schiedsgericht wenden, um sich gegen persönlichkeitsverletzende Datenbearbeitungen zur Wehr zu setzen.
- Das Swiss-US Privacy Shield wird jährlich einem Überprüfungsprozess unterliegen. Das SECO, die amerikanischen Aufsichtsbehörden und wir werden daran teilnehmen. Das SECO wird dem Bundesrat Bericht erstatten, und unsere Behörde wird unabhängig davon ihre eigenen Feststellungen und Schlussfolgerungen vornehmen.

Auch sicherheitsbehördliche Zugriffe auf Personendaten sollen neu stärker beaufsichtigt werden, weshalb ein Ombudsmechanismus im Bereich der amerikanischen nationalen Sicherheitsdienste eingeführt wird. Auf Anfrage von betroffenen Bürgern überprüft die Ombudsperson, ob Datenbearbeitungen korrekt vorgenommen wurden. Personen, die ein Zugangsgesuch gestellt haben, erhalten die Auskunft dass ihre Daten entweder gesetzeskonform bearbeitet wurden oder falls dies nicht der Fall war, die Gesetzeskonformität wieder hergestellt wurde.

Unser Fokus wird nun auf der praktischen Umsetzung des Swiss-US Privacy Shield liegen.

1.8.2 Wirtschaftsauskunftei Moneyhouse – Klage vor Bundesverwaltungsgericht

Im Klageverfahren gegen die Wirtschaftsauskunftei Moneyhouse hat das Bundesverwaltungsgericht einen im aktuellen Umfeld der Digitalisierung wegweisenden Entscheid gefällt, indem es der profilbildenden Verknüpfung von Informationen und deren Publikation klare Grenzen setzt.

Die Auskunftei Moneyhouse macht im Rahmen ihres Web-Angebots für Bonitätsauskünfte systematisch verknüpfte Informationen zugänglich, die u.a. Angaben zu Alter, Beruf, Wohnliegenschaft und Mitbewohnern von Privatpersonen enthalten. Daran störten sich viele Menschen, weshalb unsere Behörde eine formelle Sachverhaltsabklärung durchführte und nach deren Abschluss beim Bundesverwaltungsgericht Klage zur Durchsetzung unserer Empfehlungen einreichte, soweit

diese von Moneyhouse bestritten wurden (vgl. unseren Tätigkeitsbericht 2015/2016, Ziffer 1.8.5).

In seinem Urteil vom 18. April (A-4232/2015), dem im Berichtsjahr mehrere Verhandlungen und ein umfangreiches Beweisverfahren mit Augenschein vorausgegangen sind, hält das Gericht fest, dass aus unterschiedlichen Quellen stammende Personendaten nicht in beliebigem Umfang gespeichert, verknüpft und reproduziert werden dürfen. Es macht klar, dass die Privatsphäre auch in der digitalisierten Gesellschaft Bestand hat, wenn es wie im beurteilten Fall um eine Bearbeitung von Informationen geht, die Rückschlüsse auf private Wohn- und Lebenssituationen zulässt und so zu Persönlichkeitsprofilen führt.

Unseren Anträgen folgend wird das beklagte Unternehmen verurteilt, diverse Daten und Links, die nicht bonitätsrelevant sind und von keiner Einwilligung der Betroffenen gedeckt sind, zu löschen. Zudem wird Moneyhouse verpflichtet, durch geeignete Massnahmen sicherzustellen, dass die Bonitätsauskünfte inhaltlich richtig und nur an Kunden erteilt werden, die über ein berechtigtes Interesse verfügen.

Bei Drucklegung war noch offen, ob die Beklagte das Urteil ans schweizerische Bundesgericht weiterzieht.

1.8.3 Verordnungen zur Energiestrategie 2050

Im Berichtsjahr nahmen wir Stellung zu den Verordnungen des ersten Massnahmenpakets zur Energiestrategie 2050. Die datenschutzrechtlichen Aspekte dieser Verordnungen betreffen die Publikation von Personendaten im Internet und die Datenbearbeitung durch intelligente Messsysteme (Smart Metering).

Im Rahmen der Ämterkonsultation zu den Verordnungen des ersten Massnahmenpakets zur Energiestrategie 2050 des Bundesrats äusserten wir uns zur Publikation von Personendaten und zur Datenbearbeitung durch intelligente Messsysteme. Dies sind auch die Themen, welche uns im Bereich der Energieversorgung schon über einen längeren Zeitraum hinweg beschäftigen (vgl. zum Thema Publikation von Personendaten, 23. Tätigkeitsbericht 2015/2016, Ziffer 1.2.6 sowie zum Thema Smart Metering, Ziffer 1.8.2).

Aus unserer Sicht nimmt das Verhältnismässigkeitsprinzip bei der Veröffentlichung von Personendaten im Internet eine zentrale Bedeutung ein. Gerade bei Gesetzesprojekten müssen die vorgesehenen Bestimmungen zur Publikation von Personendaten zielführend sein. Das Bundesamt für Energie (BFE) beabsichtigt erneut, die Personendaten sämtlicher Bezüger von Einmalvergütungen (EIV) und die kostendeckenden Einspeisevergütungen (KEV) im Internet zu publizieren. Ziel dieser Massnahme ist es, die Verwendung des bei den Endverbrauchern erhobenen Netzzuschlags transparent zu machen.

Es ist fraglich, ob durch die Publikation der Personendaten von Produzenten, welche eine Vergütung im Bereich von Kleinbeträgen erhalten, die Transparenz erhöht wird. Der Eingriff in das Recht auf informationelle Selbstbestimmung von zusätzlichen 5000 Personen, die nur rund acht Prozent der gesamten Vergütung ausmachen, ist nicht verhältnismässig. Daher forderten wir einen Verzicht auf die Ausweitung der Internetpublikation auf alle KEV- und EIV-Bezüger, zumal die Datenbekanntgabe im Rahmen von Zugangsgesuchen zu KEV- und EIV-Empfängern nach dem Öffentlichkeitsgesetz, unabhängig von der Anschlussleistung oder der Höhe der Vergütung, für jedermann offen bleibt.

Bei den Ausführungsbestimmungen zu den intelligenten Messsystemen (u.a. Smart Metering) äusserten wir uns zum Zugriff auf die eigenen Daten, zur Pseudonymisierung der Daten, zur Aufbewahrungsdauer der detaillierten Lastgangwerte sowie zur Auslesefrequenz. Diese Themen waren bereits im vorangegangenen Gesetzgebungsprozess zentrale Punkte aus der Sicht des Datenschutzes. Auf Grundlage des Auskunftsrechts forderten wir, den Betroffenen zu ermöglichen, auch über eine standardisierte Schnittstelle auf ihre Daten inklusive Lastgangwerte zuzugreifen und in eigene oder selbst gewählte Systeme zu exportieren.

Die Verordnung sieht weiter vor, dass Netzbetreiber die Daten aus intelligenten Mess-, Steuer- und Regelsystemen ohne Einwilligung der Betroffenen bearbeiten dürfen, wenn sie der Messung, Steuerung und Regelung dienen, oder für den Einsatz von Tarifsystemen sowie für den sicheren und effizienten Netzbetrieb und die Netzplanung in pseudonymisierter Form vorgesehen sind. Ohne Pseudonymisierung dürfen die Daten nur für die Abrechnung der Energielieferung, des Netznutzungsentgelts und der Vergütung für den Zugriff auf Steuer- und Regelsysteme bearbeitet werden. Hierzu gehören auch Lastgangwerte von fünfzehn Minuten und mehr.

Aus der Bestimmung und den Erläuterungen ging zu wenig klar hervor, wie die Netzbetreiber die Pseudonymisierung umzusetzen haben. Unserer Auffassung nach sollten sie mindestens die Massnahmen unseres Leitfadens zu den technischen und organisa-

torischen Massnahmen des Datenschutzes umsetzen (www.derbeauftragte.ch, Datenschutz – Dokumentation – Leitfäden). Insbesondere müssen sie sicherstellen, dass aus den dem Pseudonym zugeordneten Daten nicht auf eine bestimmte Person geschlossen werden kann. Hierzu gehört insbesondere, dass keine indirekt identifizierenden Informationen weitergegeben, sondern nicht sprechende Identifikatoren gewählt werden.

Zudem vertraten wir die Auffassung, dass nicht für alle in der Verordnung aufgeführten Bearbeitungszwecke die Lastgangwerte von fünfzehn Minuten notwendig sind und für zwölf Monate aufbewahrt werden müssen. Wir gehen davon aus, dass gewisse Zwecke mit aggregierten oder anonymisierten Daten ebenfalls erreicht werden können. Wir forderten daher, neben der maximalen Aufbewahrungsdauer von Lastprofilen auch deren frühestmögliche Anonymisierung oder Aggregierung vorzuschreiben.

Schliesslich verlangten wir, die Auslesefrequenz und die Bedingungen für eine Echtzeitauslesung der intelligenten Messsysteme zu regeln, wie dies das BFE ursprünglich vorgesehen hatte. Diese beiden Faktoren beeinflussen die Eingriffsintensität in die Privatsphäre in diesem Bereich nämlich entscheidend.

1.9 Finanzen

1.9.1 Bekanntgabe von Personendaten an ausländische Steuerbehörden

Die Umsetzung der neuen Standards in der weltweiten Bekämpfung von Steuerbetrug und Steuerhinterziehung ist bereits weit fortgeschritten. Im Bereich des neu eingeführten automatischen Informationsaustausches sammelt die Schweiz ab 2017 Daten, welche 2018 erstmals ausgetauscht werden sollen. Wir haben zu verschiedenen Vorlagen aus datenschutzrechtlicher Sicht Stellung genommen.

Die Schweiz hat sich 2013 mit Unterzeichnung des Übereinkommens der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) und des Europarats über die gegenseitige Amtshilfe in Steuersachen (Amtshilfeübereinkommen) zur Leistung von Amtshilfe in Steuersachen verpflichtet (vgl. unseren 23. Tätigkeitsbericht, Ziff. 1.9.2 a). Das Amtshilfeübereinkommen trat am 1. Januar 2017 in Kraft. Damit wurde eine multinationale Grundlage geschaffen, welche den automatischen und spontanen internationalen Austausch von Steuerdaten legitimiert, was aus datenschutzrechtlicher Sicht grundsätzlich kritisch betrachtet werden muss. Das Übereinkommen bedarf zu seiner Umsetzung der Ausarbeitung und Änderung diverser Rechtsgrundlagen. Unsere Aufgabe war und ist es, den Anforderungen des DSG dabei so gut wie möglich zur Umsetzung zu verhelfen.

Die verschiedenen Formen der Amtshilfe werden in unterschiedlichen Gesetzen geregelt. Im Berichtsjahr waren insbesondere der automatische aber auch der spontane Informationsaustausch Thema unserer Stellungnahmen.

a) Automatischer Informationsaustausch über Finanzkonten

Im Rahmen des neu eingeführten automatischen Informationsaustausches über Finanzkonten (AIA) sammelt die Schweiz ab 2017 Daten sammeln, welche 2018 erstmals ausgetauscht werden sollen. Damit der automatische Informationsaustausch mit einem Staat eingeführt werden kann, muss er bilateral aktiviert werden. Dies erfolgt entweder durch Unterzeichnung eines bilateralen Staatsvertrages oder auf Grundlage des Multilateral Competent Authority Agreement (MCAA), welches basierend auf dem Amtshilfeübereinkommen die Aktivierung vorsieht (vgl. unseren Tätigkeitsbericht 2015/2016, Ziff. 1.9.2 c).

Mit der Aktivierung verpflichten sich die teilnehmenden Staaten, den «gemeinsamen Melde- und Sorgfaltsstandard für Informationen über Finanzkonten» der OECD (Gemeinsamer Meldestandard, GMS, oder Common Reporting Standard, CRS) im innerstaatlichen Recht umzusetzen und anzuwenden. Er regelt, wie die Steuerbehörden der teilnehmenden Länder untereinander Daten über Konten und Wertschriftendepots von Steuerpflichtigen austauschen.

Verordnung über den internationalen Informationsaustausch in Steuersachen

In unserem letzten Tätigkeitsbericht haben wir über den Erlass des Bundesgesetzes über den internationalen automatischen Informationsaustausch (AIAG) informiert (vgl. unseren Tätigkeitsbericht 2015/2016, Ziff. 1.9.2 b). Es dient der Umsetzung der internationalen Vereinbarungen und des AIA-Standards in der Schweiz. Die Verordnung über den internationalen automatischen Informationsaustausch in Steuersachen (AIAV) konkretisiert dieses Gesetz. Ende 2016 hatte der Bundesrat die Verordnung verabschiedet. Sie tritt am 1. Januar 2017 in Kraft.

Bei der Ämterkonsultation zum Erlass der AIAV haben wir einerseits erreicht, dass die Vernetzung der Informationssysteme der ESTV auf den Zweck der Stammdatenverwaltung beschränkt wird. Andererseits wurde unserem Anliegen gefolgt, eine Regelung der Authentifikationsstärke in der Verordnung zu belassen. Diese Regelung bezieht sich auf das Abrufverfahren der Kantone auf die vom Ausland eingegangenen Informationen.

Darüber hinaus sind wir der Ansicht, dass die zwanzigjährige Dauer der Archivierung bis zur Vernichtung der Daten unverhältnismässig ist. Unser Vorschlag, die Aufbewahrung auf zehn Jahre zu reduzieren, wurde jedoch abgelehnt, was in den Divergenzen an den Bundesrat ausgewiesen wurde. Schliesslich wurde auch unserem Anliegen, die automatische Informationsübermittlung ins Ausland ebenfalls auf Verordnungsstufe zu regeln, nicht entsprochen. Grund dafür ist gemäss ESTV, dass eine Regelung in der Verordnung zum jetzigen Zeitpunkt weder möglich noch sinnvoll ist. Auf Seiten der OECD sind die Spezifikationen für den Anschluss an das Common Transmission System der OECD noch nicht bekannt und die technische Spezifikation für die Schnittstelle mit den Kantonen ist noch nicht zu Ende ausgearbeitet. Wir werden jedoch die Gelegenheit erhalten, bei der Anmeldung der Datensammlung zum Sicherheitskonzept und zum Datenbearbeitungsreglement Stellung zu nehmen.

Wegleitung – gemeinsamer Meldestandard

Die Einführung und tägliche Umsetzung des automatischen Informationsaustausches dürfte den schweizerischen Finanzsektor vor knifflige Fragen bei der konkreten Anwendung stellen. Aus diesem Grund hat die ESTV

einen Standard für den automatischen Informationsaustausch über Finanzkonten erstellt. In Form einer Wegleitung beschreibt und konkretisiert der Standard die Pflichten, die sich bei den schweizerischen Finanzinstituten und anderen Beteiligten wie z. B. der ESTV aus den schweizerischen Rechtsgrundlagen zur Umsetzung des AIA-Standards ergeben.

Anlässlich unserer Stellungnahme zum Entwurf erinnerten wir bezüglich der zu bearbeitenden Daten an die Grundsätze der Verhältnismässigkeit (Identifikatoren zum Gebäude, dem Stockwerk oder der Wohnung sind für die Adressbestimmung in der Schweiz regelmässig nicht notwendig) sowie der Datenrichtigkeit (das Geburtsdatum ist für die sichere Identifikation einer Person notwendig). Weiter haben wir auf die Gefahr einer irrtümlichen Meldung einer nicht meldepflichtigen Person hingewiesen, wenn für die Identifikation öffentlich zugängliche Informationen unbekannter oder schlechter Qualität verwendet werden.

Schliesslich erachteten wir eine einmalige Information der Kunden als ungenügend und sprachen uns deshalb neben der konkreten Information des betroffenen Kunden auch für eine allgemeine Information, z. B. auf der Internetseite des Finanzinstitutes, aus. Grundsätzlich ist die Wegleitung jedoch datenschutzfreundlich ausgestaltet und bietet unserer Ansicht nach ein effektives Hilfsmittel für die Einschätzung der Meldepflicht einer Person unter Wahrung ihrer Persönlichkeitsrechte.

Zusätzliche Anforderungen der Schweiz bei Staaten mit ungenügendem Datenschutzniveau

Unsere mehrmaligen Hinweise auf das Erfordernis von zusätzlichen Garantien bezüglich Staaten, welche über kein adäquates Datenschutzniveau verfügen, fruchteten: Eine Mitteilung betreffend zusätzliche Anforderungen der Schweiz im Bereich Datenschutz soll den AIA mit Staaten, welche über kein adäquates Datenschutzniveau verfügen, ergänzen. Wir begrüssen die Einführung einer solchen Mitteilung sehr. Anlässlich der Ämterkonsultation nahmen wir zum Inhalt Stellung. Dieser geht aus unserer Sicht zu wenig weit.

Wir regten an, die Verwendung der Daten auf die Zwecke des AIA zu beschränken und eine Verwendung für sämtliche Angriffe auf die Grundrechte und die persönliche Freiheit auszuschliessen. Immerhin wurden schwere Menschenrechtsverletzungen inzwischen ausdrücklich ausgeschlossen. Daneben setzten wir uns für die Ausweitung des Rekursrechts, eine situative Informationspflicht sowie ein ausdrückliches Rückwirkungsverbot ein. Die Ergebnisse der Ämterkonsultation lagen zum Zeitpunkt des Verfassens dieses Berichtes noch nicht vor.

Bundesbeschlüsse zur Einführung des automatischen Informationsaustausches mit weiteren Staaten

Unabhängig von der Art der Aktivierung des AIA wird der Bundesbeschluss bzw. der bilaterale Vertrag dem Parlament zur Genehmigung unterbreitet. Dieses hatte im Berichtsjahr der Einführung des AIA mit folgenden Ländern zugestimmt: Australien, Guernsey, Insel Man, Island, Japan, Jersey, Kanada, Norwegen, Südkorea sowie der EU-Staaten inklusive Gibraltar (in Bezug auf Australien und die EU vgl. auch unseren 23. Tätigkeitsbericht 2015/2016, Ziff. 1.9.2). Ende 2016 hat das Parlament zudem den Bundesbeschluss über die Genehmigung des Steuerinformationsabkommens mit Brasilien genehmigt. Mit diesen Staaten werden somit ab dem 1. Januar 2017 Informationen gesammelt und ab 1. Januar 2018 Daten ausgetauscht.

Mit einer weiteren Serie von Staaten soll der AIA ein Jahr später in Kraft treten, so dass im Jahr 2019 ein erster Datenaustausch erfolgen kann. Darunter gehören unter anderem Argentinien, die Bermuda-Inseln, die Cayman Inseln, Indien, Israel und Mexico. Für diese Staaten lief die Vernehmlassung für die Einführung des AIA am 15. März 2017 ab. Aktuell läuft die Vernehmlassung für die Einführung des AIA mit einer zweiten Serie von Staaten, darunter China, Russland, Saudi-Arabien, Liechtenstein und die Vereinigten Arabischen Emirate. Die Vernehmlassung für diese Staaten dauert bis zum 13. April 2017. Danach sollen beide Vorlagen zu einem Geschäft zusammengeführt und dem Parlament unterbreitet werden, weshalb die Entscheidung des Parlaments zum Zeitpunkt der Publikation dieses Berichtes noch nicht vorliegt. Schliesslich soll am 1. Januar 2018 auch der AIA mit Singapur eingeführt werden.

Im Rahmen der Ämterkonsultationen im Berichtsjahr wiesen wir auf das Erfordernis der Gewährleistung eines angemessenen Datenschutzniveaus im jeweiligen Partnerstaat hin. Unsere Länderliste enthält hierzu Angaben für jeden einzelnen Staat. In allen Fällen hoben wir die Staaten hervor, für welche wir keine Kenntnisse über die Gewährleistung eines angemessenen Datenschutzniveaus haben. Wir stehen der Umsetzung selbst von völkerrechtlich vereinbarten Datenschutzbestimmungen kritisch gegenüber, wenn im Partnerstaat ein Bewusstsein für möglichen Persönlichkeitsverletzungen durch Datenschutzbearbeitungen und angemessene Bestimmungen zum Schutz vor selbigen fehlen. Das EFD ist jedoch der Ansicht, für die Zwecke des AIA existiere eine hinreichende Datenschutzgesetzgebung bzw. genügten die jeweils völkerrechtlich vereinbarten Datenschutzvorschriften.

Automatischer Austausch länderbezogener Berichte

In Ergänzung der Strategie des Bundesrates zum AIA ist beabsichtigt, durch den automatischen Austausch länderbezogener Berichte (ALBA) die Transparenz im Bereich der Unternehmensbesteuerung zu erhöhen und die Steueroptimierung multinationaler Konzerne zu bekämpfen. Dieses Vorhaben stützt sich auf das gemeinsame Projekt Base Erosion and Profit Shifting (BEPS) der OECD und der G20-Staaten, womit sie gegen doppelte Nichtbesteuerung durch Gewinnverkürzung und -verschiebung vorgehen.

Die Konzernobergesellschaften der multinationalen Konzerne werden verpflichtet, sogenannte länderbezogene Berichte über ihre Gewinne, Steuern und Aktivitäten zu erstellen. Diese werden automatisch den nationalen Steuerbehörden der Staaten und Hoheitsgebiete übermittelt, in denen der multinationale Konzern über Geschäftseinheiten verfügt. Zur länderbezogenen Berichterstattung verpflichtet sind international tätige Unternehmen ab einem bestimmten konsolidierten jährlichen Gruppeneinkommen. In der Schweiz dürften rund 200 Konzerne diesen Grenzwert überschreiten.

Die Schweiz hat Anfang 2016 das multinationale Abkommen über den Austausch länderbezogener Berichte (ALBA-Vereinbarung) unterzeichnet. Zur Umsetzung wurde das Bundesgesetz über den internationalen automatischen Austausch länderbezogener Berichte multinationaler Konzerne (ALBA-Gesetz) geschaffen. Im Rahmen der Ämterkonsultation haben wir zu den Vorlagen Stellung genommen und dabei insbesondere betont, dass im Sinne der Transparenz und des Bestimmtheitsgebotes die konkret bearbeiteten Personendaten im Gesetz aufzulisten sind sowie eine abschliessende Liste der Verwendungszwecke des Informationssystems einzufügen sei. Zudem haben wir uns zur Übermittlung und Verwendung der länderbezogenen Berichte sowie zur Geheimhaltung geäussert.

Aufhebung der Quellenbesteuerungsabkommen mit Österreich und dem Vereinigten Königreich

Durch das Inkrafttreten des Abkommen zwischen der Schweiz und der EU zur Einführung des automatischen Informationsaustauschs über Finanzkonten braucht es die Quellenbesteuerungsabkommen mit Österreich und dem Vereinigten Königreich nicht mehr. Zu diesem Zweck hat der Bundesrat mit beiden Staaten sogenannte Aufhebungsabkommen abgeschlossen, welche einen reibungslosen Übergang vom Quellensteuersystem zum AIA ermöglichen. Unsere Bedenken bezüglich einer ungenügenden Regelung der heiklen Gruppenersuchen konnten ausgeräumt werden.

b) Spontaner Informationsaustausch – Änderung des Steueramtshilfegesetzes und Totalrevision der Steueramtshilfe verordnung

Mit dem Beitritt zum Amtshilfeübereinkommen hat die Schweiz den spontanen Informationsaustausch in Steuersachen eingeführt. Beim spontanen Informationsaustausch werden die Informationen ohne vorgängiges Ersuchen übermittelt, wenn der übermittelnde Staat bei bereits vorhandenen Informationen ein mögliches Interesse eines anderen Staats vermutet. Die Umsetzungserlasse, das Steueramtshilfegesetz (StAhiG) und die Steueramtshilfeverordnung (StAhiV) sind gleichzeitig mit dem Amtshilfeübereinkommen am 1. Januar 2017 in Kraft getreten. Aus diesem Grunde war die Änderung des StAhiG und die Totalrevision der StAhiV Thema einer Ämterkonsultation. Zur Änderung des StAhiG haben wir uns bereits im Tätigkeitsbericht 2015/2016, Ziff. 1.9.2, und Tätigkeitsbericht 2013/2014, Ziff. 1.9.3, geäussert.

Im Rahmen der letzten Ämterkonsultation haben wir bei der Formulierung der StAhiV auf diverse Anpassungen hingewirkt: In einem ersten Schritt haben wir darauf hingewiesen, dass die Rechtsform der für den spontanen Informationsaustausch zuständigen Organisationseinheit genauer bestimmt werden soll. Dies ist wichtig, damit bestimmt ist, ob das DSG oder ein kantonales Datenschutzgesetz Anwendung findet und welches die zuständige Aufsichtsstelle ist.

In einem zweiten Schritt betonten wir im Sinne der datenschutzrechtlichen Prinzipien der Verhältnismässigkeit und der Zweckmässigkeit, dass einerseits jeweils für jeden Empfängerstaat von Informationen zu prüfen ist, ob er überhaupt für die Steuerveranlagung zuständig ist. Andererseits haben wir in Bezug auf die optional zu übermittelnden Informationen angeregt, jeweils zu prüfen, ob deren Übermittlung für die Steuerveranlagung notwendig ist. Diese Punkte haben zu einzelnen Anpassungen der Erläuterungen geführt.

Nicht einverstanden waren wir mit der der ESTV eingeräumten Möglichkeit zur Einschränkung der Übermittlung auf Staaten, welche sich zum Standard der OECD betreffend den spontanen Informationsaustausch über Steuervorbescheide bekennen, da die Formulierung dem Bestimmtheitsgebot widerspricht. Die ESTV bezweckt primär den Austausch mit sämtlichen Staaten. Damit geht die Formulierung der StAhiV in die falsche Richtung. Der Datenaustausch sollte nicht bloss daran anknüpfen, ob der andere Staat ebenfalls austauschbereit ist, sondern auch, ob dieser ein angemessenes Datenschutzniveau aufweist (vgl. «Bundesbeschlüsse zur Einführung des automatischen Informationsaustausches mit weiteren Staaten»).

1.10 International

1.10.1 Internationale Zusammenarbeit

Das vergangene Jahr war geprägt durch die Annahme der Reform des Rechtsrahmens für den Datenschutz in der Europäischen Union. Auch die Modernisierung des Übereinkommens des Europarates konnte auf Ebene der Regierungsexperten zum Abschluss gebracht werden. Diese Texte stehen im Mittelpunkt der Reformen des europäischen und nationalen Datenschutzrechts. Im Rahmen seiner Tätigkeiten für die internationale Zusammenarbeit beteiligt sich der EDÖB besonders an den Arbeiten des Europarates, der Europäischen Union im Rahmen der Schengen-Abkommen, der europäischen und internationalen Konferenz der Datenschutzbeauftragten und der französischsprachigen Vereinigung der Datenschutzbehörden (AFAPDP).

Europarat

Die Arbeiten zur Modernisierung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen 108) sind auf Ebene der Regierungsexperten abgeschlossen, die im Juni 2016 einen Revisionsentwurf verabschiedet haben (siehe unsere früheren Tätigkeitsberichte). Das Ministerkomitee des Rates sollte im Laufe des ersten Halbjahres 2017 ein Änderungsprotokoll zu dem Übereinkommen annehmen. Mit der Ratifizierung des Übereinkommens durch die Türkei sind nunmehr sämtliche Mitgliedstaaten des Europarates Parteien dieses Rechtsinstruments. Zudem sind nach Uruguay im Jahr 2013 auch Mauritius und der Senegal dem Übereinkommen beigetreten. Andere Staaten sollten ihnen in diesem Jahr folgen.

Der Beratende Ausschuss für das Übereinkommen 108 (T-PD) hat seine Arbeiten im Hinblick auf die Überarbeitung der Empfehlung R (97) 5 über den Schutz der medizinischen Daten, sowie die Ausarbeitung eines praktischen Leitfadens zum Datenschutz im Polizeisektor fortgesetzt. Ausserdem hat er ein Gutachten zu den datenschutzrechtlichen Auswirkungen der Bearbeitung der Passagierdaten (PNR-Daten) angenommen. In diesem Gutachten kommt der Ausschuss zu dem Schluss, dass in Anbetracht des Risikos einer besonderen Beeinträchtigung des Datenschutzrechts und des Rechts auf die Privatsphäre ein PNR-System sich streng nach den Grundsätzen der Rechtmässigkeit, Verhältnismässigkeit und Notwendigkeit richten muss. Dafür müssen insbesondere folgende Voraussetzungen gegeben sein:

- ein transparenter und messbarer Nachweis der Notwendigkeit und der Verhältnismässigkeit des Systems in Bezug auf die legitime Zielsetzung;
- präzise und strenge Definitionen des verfolgten legitimen Zwecks sind erforderlich; die Bearbeitung der PNR-Daten darf nur aus eingeschränkten und klar umschriebenen Gründen erlaubt sein (Verhütung, Aufdeckung, Ermittlung und Verfolgung terroristischer und anderer schwerer Straftaten, oder, in Ausnahmefällen, Abwehr schwerer Bedrohungen für die Öffentlichkeit);
- eine öffentliche Liste der zuständigen staatlichen Behörden (im Idealfall für die Koordinierung zuständige Spezialeinheiten);
- die Verwendung des «Push-Modus» für die Weitergabe von Daten sowie eine klare Bestimmung der anfänglichen Aufbewahrungsdauer und der geeigneten Sicherheitsmassnahmen;
- ein Verbot der systematischen Verwendung von besonders schützenswerten Daten;
- eine durch vorgegebene Risikoindikatoren begrenzte Datengewinnung mit nicht automatischer Einzelfallprüfung der Relevanz der Ergebnisse;
- ausschliesslich notwendige und gesetzlich vorgesehene Einschränkungen des Rechts des Einzelnen auf Information, Auskunft, Berichtigung und Löschung;
- die Kompetenz der mit dem Datenschutz betrauten Behörden (die konsultiert werden können und befugt sind, das PNR-System zu beurteilen und Einzelbeschwerden zu behandeln);
- die Verfügbarkeit effektiver Rechtsmittel vor Verwaltungs- und Gerichtsbehörden für die betroffenen Personen; eine unabhängige externe Kontrolle des PNR-Systems;
- eine regelmässige Prüfung des PNR-Systems durch die zuständigen Behörden.

Der Ausschuss hat schliesslich die Untersuchung eines Leitlinienentwurfs für den Schutz des Menschen bei der Verarbeitung personenbezogener Daten im Zeitalter von Big Data fortgesetzt. Diese Leitlinien, die der Ausschuss demnächst verabschieden sollte, legen einen allgemeinen Rahmen fest, damit die Parteien des Übereinkommens Strategien und Massnahmen planen können, die geeignet sind, den Grundsätzen und Bestimmungen des Übereinkommens 108 im Kontext von Big Data Wirkung zu verleihen. Dieser Text ist als dynamisches Instrument gedacht und stellt allgemeine Richtlinien auf, die in spezifischen Anwendungsbereichen von Big Data ergänzt werden können.

Europäische Konferenz der Datenschutzbeauftragten

Die europäische Konferenz der Datenschutzbeauftragten fand 2016 auf Einladung der ungarischen Datenschutzbehörde in Budapest statt. Rund einhundert Experten und Vertreter der Datenschutzbehörden aus ganz Europa nahmen daran teil. Die Konferenz setzte den Schwerpunkt auf die Reformen des rechtlichen Rahmens der Europäischen Union und des Übereinkommens 108 sowie auf Fragen im Zusammenhang mit der Beaufsichtigung der nationalen Sicherheitsbehörden. Die Konferenz verabschiedete zwei Resolutionen:

- Die erste betrifft den Rahmen für die Zusammenarbeit der Datenschutzbehörden. Sie fordert die Datenschutzbehörden in Europa auf, eine engere, effektive und proaktive Zusammenarbeit einzurichten. Diese Behörden müssen völlig unabhängig handeln können und über die für die Erfüllung ihrer Aufgaben notwendigen Ressourcen verfügen.
- Eine zweite Resolution betrifft den grenzüberschreitenden Datenverkehr. Ihr Schwerpunkt liegt besonders auf der Verantwortung der Datenschutzbehörden bei der Information der betroffenen Personen über deren Rechte bezüglich des Auslandstransfers von Personendaten.

Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre

Die 38. Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre fand 2016 in Marrakesch statt. Zu diesem Treffen kamen etwa 500 Teilnehmer aus 70 Ländern für eine Aussprache über die heutigen Fragestellungen rund um die Privatsphäre und namentlich über die Auswirkung der Technologien und die Bedeutung der digitalen Bildung zusammen. Während der geschlossenen Konferenz behandelten die Beauftragten das Thema künstliche Intelligenz und Robotertechnik sowie Kryptografie. Wie alle neuen Informations- und Kommunikationstechnologien schaffen auch die künstliche Intelligenz und die Robotertechnik neue Herausforderungen für das Datenschutzrecht. Dank künstlicher Intelligenz und Roboter lassen sich menschliche Eigenschaften simulieren, indem sie den Nutzern Hilfsfunktionen bieten oder bisher vom Menschen ausgeführte Aufgaben übernehmen. Diese Maschinen werden in zunehmendem Masse humanoide Formen annehmen und mit den Menschen interagieren. Sie sind mit zahlreichen Sensoren ausgestattete und vernetzte Instrumente, die in der Lage sind, massenweise Informationen zu sammeln und alle in ihrer Umgebung eingetretenen Ereignisse zu speichern und abzurufen. Bei den Ergebnissen ihrer Datenbearbeitung besteht jedoch immer noch eine gewisse Unvorhersehbarkeit. Aufgrund dessen stellt sich die Frage nach der Verantwortlichkeit bei den automatischen Entscheidungsprozessen, insbesondere wenn die verwendeten Algorithmen für den Entwickler oder Nutzer unbekannte Schlüsse ergeben. Es besteht auch das Risiko, dass einzelne Personen manipuliert werden, um ihr Verhalten oder ihre Entscheidung zu beeinflussen. An sich haben die Roboter kein selektives Gedächtnis, und sie sind unter Umständen fähig, sich an alles zu erinnern. Es stellt sich daher die Frage, ob und welche Regeln es braucht, um die Speicherkapazität zu begrenzen und die Transparenz und Kontrolle der Bearbeitungsprozesse zu gewährleisten, damit Fehlentwicklungen vermieden werden. Der Mensch muss die Verantwortung für die vom Roboter gespeicherten Daten tragen. Ein zentrales Anliegen der Gesellschaft ist es, Klarheit darüber zu schaffen, wie weit wir akzeptieren wollen und können, dass die künstliche Intelligenz unsere Entscheidungen und Handlungen bestimmt.

Die Frage der Chiffrierung oder Verschlüsselung war ebenfalls Thema der Konferenzdebatten. Diese Technologie ist ein wichtiger Mechanismus für die Geschäfts- und Wirtschaftswelt, aber auch für die Verbraucher und für die von der Bearbeitung von Personendaten betroffenen Menschen. Mit der Verschlüsselung können Informationen namentlich im Zusammenhang mit Transaktionen, der Bekanntgabe und der Speicherung von Daten gesichert werden. Sie kann für die Strafverfolgungsbehörden besonders bei der Kommunikationsüberwachung Schwierigkeiten verursachen. Angesichts widersprüchlicher Interessen ist noch keine befriedigende Lösung gefunden worden. Die Mehrheit der Experten spricht sich gegen die Ausrüstung der Chiffrierprogramme mit selektiven Schwachstellen aus, da dies zu einer Verminderung der Datensicherheit führen würde.

Die Konferenz erörterte sodann den Stand verschiedener laufender Initiativen. So nahm sie Kenntnis vom Zwischenbericht des Sonderberichterstatters der Vereinten Nationen für das Recht auf Privatsphäre. Wir informierten die Konferenz auch über die Aktivitäten der Arbeitsgruppe für humanitäre Hilfsaktionen. Schliesslich verabschiedete die Konferenz die folgenden vier Resolutionen:

- Eine Resolution für die Annahme eines internationalen Bildungsstandards im Bereich Personendaten. Ergänzt wird diese Resolution durch einen ersten Ausbildungsstandard für den Schutz von Personendaten.
- Eine Resolution zur Entwicklung neuer Datenschutz-Indikatoren, mit denen weltweit vergleichbare Informationen über die verschiedenen Strategien für den Schutz der Privatsphäre erlangt werden können.
- Eine Resolution betreffend die Menschenrechtsaktivisten, in der die Beauftragten deren wichtige

Arbeit für die Schaffung einer starken, nachhaltigen und demokratischen Gesellschaft und ihre Schlüsselrolle bei der vollständigen Verwirklichung des Rechtsstaates und der Stärkung der Demokratie anerkennen.
- Eine Resolution über die internationale Zusammenarbeit.

Französischsprachige Vereinigung der Datenschutzbehörden (AFAPDP)

Die AFAPDP trat 2016 in Ouagadougou in Burkina Faso zu ihrer Konferenz zusammen. Die Teilnehmer dieser Veranstaltung erörterten die Datensicherheit, die Risikoanalysen im Datenschutz, den Datenschutz auf dem Gebiet der Forschung und den Zugriff auf die Datenbanken der Telekommunikationsbetreiber durch die Sicherheitsdienste. Dies ermöglichte einen regen Austausch über die Gesetzgebungen und die verschiedenen Praktiken in den französischsprachigen Ländern. Die AFAPDP verabschiedete eine Resolution über das Recht auf Vergessen, mit der die Vereinigung auf die Diskussionen aufmerksam macht, die auf nationaler und internationaler Ebene zur Anwendung des Rechts auf Löschung und Auslistung für Suchmaschinen und zu den Massnahmen für den Schutz der Online-Reputation stattgefunden haben. Sie fordert die Staaten und Regierungen des französischen Sprachraums auf, ein universell gültiges Recht auf Löschung und Auslistung anzuerkennen. Die AFAPDP wählte ausserdem ihren Vorstand und bestimmte den stellvertretenden Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten zu ihrem Vorsitzenden.

1.10.2 Aufsichtskoordinationsgruppen SIS II, VIS und Eurodac

Die Sitzungen der Aufsichtskoordinationsgruppen über das Schengener Informationssystem SIS II, über das Visa-Informationssystem (VIS) und über Eurodac fanden, jeweils nacheinander, vom April 2016 sowie vom November 2016 in Brüssel statt. Informationen zu den drei Koordinierungsgruppen werden auf der Internetseite des Europäischen Datenschutzbeauftragten unter eigenen Domainnamen aufgeschaltet (www.sis2scg.eu; www.visscg.eu; www.eurodacscg.eu; oder über www.edps.europa.eu -> de -> Kooperation -> Koordination der Aufsicht). Dort werden die durchgeführten Sitzungen zusammengefasst und die verabschiedeten Dokumente, Tätigkeitsberichte oder gemeinsamen Stellungnahmen veröffentlicht.

1.10.3 Arbeitsgruppe «Border, Travel & Law Enforcement»

Die «Border, Travel & Law Enforcement subgroup» (BTLE) ist eine von der Datenschutzgruppe der Europäischen Union («Artikel 29») eingesetzte Arbeitsgruppe. Sie hat den Auftrag, die gesetzgeberischen Entwicklungen im Bereich der Polizei, des Grenzschutzes und der Strafjustiz namentlich mit Bezug zum Schengen-Besitzstand zu beobachten. In diesem Kontext arbeitet sie Gutachten und Stellungnahmen aus, die danach von «Artikel 29» angenommen werden. Wir haben an den verschiedenen Treffen im Laufe des Berichtsjahres teilgenommen.

Die Arbeitsgruppe befasste sich unter anderem mit dem Privacy Shield zwischen der EU und den USA, der den vereinfachten Transfer von Personendaten aus der EU an Unternehmen in den Vereinigten Staaten ermöglicht (vgl. auch Ziff. 1.8.1 des vorliegenden Berichts). Mit besonderer Aufmerksamkeit verfolgt die Untergruppe das Projekt «intelligente Grenzen», in dessen Zusammenhang die Kommission einen Verordnungsvorschlag betreffend die Schaffung eines Ein- und Ausreisesystems für die Registrierung der Angehörigen von Drittstaaten beim Überschreiten der Aussengrenzen der Mitgliedstaaten der Europäischen Union angenommen hat. Die Arbeitsgruppe hat dazu ein Schreiben an den Vorsitzenden des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres gerichtet. Sie beschäftigt sich zudem mit dem Rahmenabkommen für den Austausch von Personendaten im Bereich Polizei und Justiz zur Beschränkung der Rechte der amerikanischen Verwaltungen bei der Bearbeitung europäischer Daten. Weitere Themen waren das Übereinkommen über Cyberkriminalität des Europarates sowie die Schaffung eines europäischen Rahmens für

die Bekanntgabe der PNR-Daten an Drittländer und für die Verwendung dieser Daten zu Strafverfolgungszwecken. Schliesslich hat die Arbeitsgruppe auch mit ihren Arbeiten zur Umsetzung der EU-Richtlinie 2016/680 begonnen.

1.10.4 Arbeitsgruppe für Datenschutz und internationale humanitäre Hilfe

Die 37. Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre hat eine Resolution über den Datenschutz und die internationale humanitäre Hilfe verabschiedet. Für die Analyse der datenschutzrechtlichen Anforderungen in der internationalen humanitären Hilfe und die Zusammenarbeit mit den betroffenen Akteuren wurde eine von unserer Behörde geleitete Arbeitsgruppe gebildet.

Die 37. Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre (IKBDSP) verabschiedete im Oktober 2015 eine Resolution über den Datenschutz und die internationale humanitäre Hilfe. In dieser Resolution verpflichtete sich die IKBDSP zur Schaffung einer Arbeitsgruppe, welche die datenschutzrechtlichen Anforderungen in der internationalen humanitären Hilfe analysieren und mit den betroffenen Akteuren auf diesem Gebiet zusammenarbeiten soll. Die Arbeitsgruppe wird von einem Vertreter unserer Behörde geleitet. Sie hat sich folgende Ziele gesetzt: Feststellung der von den humanitären Akteuren angewendeten Bearbeitungen und Technologien, Analyse des geltenden Rechts und Benennung der problematischen Punkte, um Leitlinien zur Verbesserung der bereits bestehenden Praktiken vorschlagen zu können.

Die Arbeitsgruppe verfolgte über das ganze Jahr 2016 vor allem zwei Arbeitsansätze. Einerseits förderte sie die Sachkenntnis der Datenschutzbehörden auf humanitärem Gebiet mittels Forschungsarbeiten und Tagungen. Andererseits arbeitete sie mit den internationalen humanitären Akteuren zusammen, hauptsächlich im Rahmen des Projekts «Datenschutz in der humanitären Hilfe» des Brussels Privacy Hub (BPH) und des Internationalen Komitees vom Roten Kreuz (IKRK). Ziel ist es, eine Verbindung zwischen humanitärer Hilfe und Datenschutzgesetzen herzustellen, die Auswirkungen des Einsatzes von Technologien auf den Datenschutz im humanitären Sektor zu verstehen und Leitlinien vorzuschlagen, die diesen Auswirkungen Rechnung tragen. Dieses Projekt entspricht ganz dem Sinn der im Oktober 2015 von der IKBDSP in Amsterdam angenommenen Resolution. Der BPH und das IKRK, auf die diese Initiative zurückgeht, haben die Arbeitsgruppe sowie zwei weitere Mitglieder der IKBDSP in ihr Vorhaben einbezogen: den europäischen Datenschutzbeauftragten und den Europarat. Das Projekt umfasst eine Serie von sechs über das Jahr 2016 veranstalteten thematischen Workshops, bei denen die Teilnehmer ihre Empfehlungen verfassten. Ein Handbuch mit allen diesen Empfehlungen ist derzeit in Ausarbeitung. Seine Veröffentlichung soll die Möglichkeit schaffen, zum Schutz von Personendaten Leitlinien aufzustellen, die sich an die humanitären Akteure richten. Die Veröffentlichung ist für Mitte 2017 geplant.

Die Arbeitsgruppe wird ihre Tätigkeiten mit dem IKRK und dem BPH fortsetzen, namentlich indem sie sich weiter in die Vorbereitung der Schlussfassung des Handbuchs einbringt.

Öffentlichkeitsprinzip

2.1 Zugangsgesuche

Gemäss den uns mitgeteilten Zahlen sind im Jahr 2016 bei den Bundesbehörden 551 Zugangsgesuche eingereicht worden (inklusive Bundesanwaltschaft und Parlamentsdienste sind es 558 Zugangsgesuche, siehe dazu Ziffer 2.1.2 f.). Dies sind rund 50 Gesuche weniger als im Jahr 2015. In 303 Fällen (55 %) gewährten die Behörden einen vollständigen, in 105 (19 %) einen teilweisen Zugang. Bei 87 Gesuchen (16 %) wurde die Einsichtnahme vollständig verweigert. Laut den Behörden wurden 26 Zugangsgesuche zurückgezogen und 33 Fälle meldeten sie Ende 2016 als noch hängig. Der Beauftragte hält fest, dass die Anzahl Gesuche sich nach einem starken Anstieg in den Jahren 2013 (469 Gesuche) und 2014 (575 Gesuche) bei einem Wert zwischen 550 und 600 pro Jahr einzupendeln scheint.

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, in einem Fünftel der Fälle wird er teilweise und in den restlichen Fällen vollständig verweigert.

2.1.1 Departemente und Bundesämter

Am meisten Zugangsgesuche für das Jahr 2016 auf Stufe Amt meldete das BAFU mit 27 Gesuchen. Danach folgen das SEM (26) und das BLW (23). Bei den Departementen liegen das EDA (118 Gesuche), das UVEK (89) und das WBF (85) an der Spitze. Besonders transparenzfreundlich fallen die Quoten beim EDA aus, das von insgesamt 118 Gesuchen 86 vollständig positiv beantwortete, in 11 Fällen den Zugang teilweise gewährte oder aufschob und bei 16 Gesuchen den Zugang vollständig verweigerte. 13 von 71 Behörden meldeten dem Beauftragten für 2016, dass bei ihnen kein einziges Zugangsgesuch eingegangen sei. Er selbst sah sich im Berichtsjahr mit zehn Zugangsgesuchen konfrontiert, wobei er den Zugang in acht Fällen vollständig und in einem weiteren Fall teilweise gewährte.

Der im Berichtsjahr für den Zugang zu amtlichen Dokumenten erhobene Gebührenbetrag fällt mit 22 770 Franken deutlich höher aus als in den letzten Jahren (2015: Fr. 13 663; 2014: Fr. 2600; 2013: Fr. 6502). Der Beauftragte merkt in diesem Zusammenhang an, dass der deutliche Anstieg der Gebührenbeiträge im Widerspruch zur parlamentarischen Initiative von Nationalrätin Edith Graf-Litscher steht, die den kostenlosen Zugang zu offiziellen Dokumenten fordert. Der Gesamtbetrag von 22 770 Franken entfällt auf lediglich 13 von insgesamt 550 im Jahr 2016 gemeldeten Zugangsgesuchen. Wie bereits in den Vorjahren werden damit weiterhin in den meisten Fällen (fast 98 % aller Gesuche) keine Gebühren in Rechnung gestellt. Auffällig sind dabei die relativ konstanten Unterschiede in der Gebührenhandhabung zwischen den verschiedenen Behörden. Während die Bundeskanzlei und das EDA überhaupt keine Gebühren erhoben, verrechneten die anderen sechs Departemente ihren Zeitaufwand den jeweiligen Gesuchstellern zumindest teilweise. Der Hauptteil der erhobenen Gebühren entfiel dabei auf das WBF (Fr. 12 730 für 2 Gesuche), das EJPD (Fr. 4000 für ein Gesuch) und das VBS (Fr. 2660 für 2 Gesuche).

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 und widerspiegeln die für die Bearbeitung der Gesuche aufgewendete Arbeitszeit nur teilweise. Gemäss diesen Angaben hat der gemeldete Zeitaufwand gegenüber den Vorjahren erneut zugenommen (2016: 3301 Stunden; 2015: 2912 Stunden; 2014: 1707 Stunden). Der Zeitaufwand für die Mitwirkung in Schlichtungsverfahren hat hingegen von 1148 Stunden im Jahr 2015 auf 857 Stunden im Jahr 2016 deutlich abgenommen. Nicht bzw. nicht gesondert erfasst wird dagegen der Zeitaufwand für den Erlass einer Verfügung sowie für ein allfälliges Beschwerdeverfahren.

2.1.2 Parlamentsdienste

Die Parlamentsdienste meldeten uns für das Jahr 2016 drei Zugangsgesuche, wobei der Zugang zweimal vollständig gewährt und einmal vollständig verweigert wurde.

2.1.3 Bundesanwaltschaft

Die Bundesanwaltschaft meldete uns für das Jahr 2016 vier Zugangsgesuche. Der Zugang wurde dabei dreimal vollständig und einmal teilweise gewährt.

2.2 Schlichtungsanträge

Im Jahr 2016 wurden beim Beauftragten insgesamt 149 Schlichtungsanträge eingereicht, was einer Zunahme um 52 Prozent gegenüber dem Vorjahr entspricht (2015: 98). Anders als im Vorjahr sind 2016 nicht die Medienschaffenden (23 Anträge) die häufigsten Antragsteller, sondern Privatpersonen (99 Anträge).

In 192 Fällen verweigerte die Bundesverwaltung den Zugang vollständig (87) respektive teilweise (105). Dem stehen 149 bei uns eingereichte Schlichtungsanträge gegenüber. Im Berichtsjahr wurde somit in über 77 Prozent aller Fälle von ganz oder teilweise abgelehnten Zugangsgesuchen ein Schlichtungsantrag eingereicht (2015: 43 %).

Insgesamt konnten im Berichtsjahr 159 Schlichtungsanträge abgeschlossen werden. Davon stammen 119 Anträge aus dem Berichtsjahr selbst, 36 aus dem Jahr 2015, drei aus dem Jahr 2014 und einer noch aus dem Jahr 2013. In 19 Fällen konnte zwischen den Beteiligten eine Schlichtung erzielt werden, wovon es in elf Fällen zu einer Schlichtung im eigentlichen Sinne kam und in den übrigen acht Fällen zu einer gütlichen Erledigung des Verfahrens aufgrund einer Intervention des Beauftragten. In fünf Fällen wurde der Zugang nach Eröffnung des Schlichtungsverfahrens ohne Mitwirkung des Beauftragten gewährt. Insgesamt erliess der Beauftragte 32 Empfehlungen in Fällen, in denen eine einvernehmliche Lösung nicht ersichtlich war. Mit diesen 32 Empfehlungen konnten 122 Schlichtungsanträge erledigt werden. Diese Differenz ist in erster Linie auf die Tatsache zurückzuführen, dass mit einer einzigen Empfehlung 74 Anträge erledigt werden konnten. Vier Schlichtungsanträge wurden zurückgezogen und in fünf Fällen waren die Voraussetzungen für die Anwendung des Öffentlichkeitsgesetzes nicht gegeben. In vier weiteren Fällen wurde der Schlichtungsantrag nicht fristgerecht eingereicht. Zwei Schlichtungsverfahren wurden schliesslich sistiert.

Im Berichtsjahr konnten deutlich mehr Schlichtungsverfahren als bisher abgeschlossen werden (zusätzliche 25 Schlichtungsverfahren). Dies ist in erster Linie auf den Umstand zurückzuführen, dass von Mai bis Dezember 2016 zwei zusätzliche befristete Stellen zur Verfügung standen. Dennoch konnten die bestehenden Rückstände in der Bearbeitung der hängigen Schlichtungsverfahren nicht vollständig abgebaut werden. Der Beauftragte wird im Jahr 2017 einen neuen Ansatz verfolgen, um die grosse Anzahl hängiger Schlichtungsverfahren nach Möglichkeit abzubauen (vgl. dazu Ziffer 2.4.1 des vorliegenden Tätigkeitsberichts).

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

2.3 Ämterkonsultationen

2.3.1 Einschränkung des Öffentlichkeitsprinzips bei der Aufsicht über den öffentlichen Verkehr

Der Bundesrat will Audit- und Kontrollberichte des Bundesamtes für Verkehr über die Sicherheit von Bahn und Schiff vom Öffentlichkeitsgesetz ausklammern. Dies hat er an seiner Sitzung vom 16. November 2016 durch Genehmigung der Vorlage zur Organisation der Bahninfrastruktur (OBI) entschieden. Der Beauftragte hat sich gegen diese Einschränkung des Öffentlichkeitsprinzips ausgesprochen.

Vom Bundesamt für Verkehr (BAV) vorgesehen waren vier identische Spezialbestimmungen im Eisenbahngesetz, im Bundesgesetz über Seilbahnen zur Personenbeförderung, im Bundesgesetz über die Personenbeförderung und im Bundesgesetz über die Binnenschifffahrt. Gemäss diesen Bestimmungen soll das Öffentlichkeitsgesetz (BGÖ) nicht mehr anwendbar sein für Berichte betreffend Audits, Betriebskontrollen und Inspektionen des BAV. Auch gilt dies für alle anderen amtlichen Dokumente, welche die technische oder betriebliche Sicherheit betreffen, soweit sie Personendaten enthalten. Gemäss BAV lasse sich nur so verhindern, dass die kontrollierten Unternehmen die zur Aufrechterhaltung der Sicherheit nötigen Informationen ungeachtet gesetzlicher Auskunfts- und Meldepflichten zurückhalten würden.

Nach unserer Ansicht bietet das BGÖ mit seinen Ausnahmebestimmungen ausreichend Möglichkeiten, um Vertraulichkeitsinteressen auch im Zusammenhang mit behördlichen Kontrollmassnahmen gebührend Rechnung zu tragen. Insbesondere sieht das Gesetz vor, dass die Verwaltung Unternehmen, die freiwillig Meldungen erstatten wollen, Vertraulichkeitszusagen abgeben kann. In einem Rechtsstaat ist davon auszugehen, dass gesetzliche Pflichten beachtet und durchgesetzt werden. Dies hat auch das Bundesverwaltungsgericht in seinem inzwischen ans Bundesgericht weitergezogenen Urteil vom 10. August 2016 bekräftigt. Darin hält es zudem fest, dass ein überwiegendes öffentliches Interesse an der Offenlegung von Informationen über die Gefährdung und Störung des öffentlichen Verkehrs besteht. Würde die Aufsichtstätigkeit des BAV integral vom BGÖ ausgenommen, könnte letztlich ein der Kontrolle der Öffentlichkeit vollständig entzogener (Geheim-)Bereich staatlichen Handelns entstehen. In der Ämterkonsultation lehnten wir die vorgesehenen Einschränkungen deshalb ab.

Am 16. November 2016 hat der Bundesrat trotz unserer Einwände die Einführung dieser kontrovers beurteilten Einschränkungen über den Weg einer verkehrspolitischen Spezialvorlage in die Wege geleitet. Unseres Erachtens wäre es zielführender gewesen, diese im Zusammenhang mit der ohnehin offenen Frage nach der Notwendigkeit einer Revision des BGÖ zu thematisieren.

2.3.2 Zugang zu Dokumenten über das öffentliche Beschaffungswesen

Der Bezug von Gütern und Dienstleistungen durch die Bundesverwaltung ist von besonderem öffentlichem Interesse. Wir haben uns deshalb gegen das Vorhaben des Bundesamtes für Bauten und Logistik (BBL) ausgesprochen, Unterlagen zu Beschaffungen grundsätzlich vom Öffentlichkeitsprinzip auszunehmen. Das heutige Zugangsrecht der Bevölkerung und der Medien würde damit wegfallen.

Das Bundesgesetz über das öffentliche Beschaffungswesen (BöB) und die entsprechende Verordnung werden zurzeit einer Totalrevision unterzogen. Obwohl weder in der Vernehmlassung noch in der Ämterkonsultation vorgesehen, verabschiedete der Bundesrat letztlich einen Gesetzesentwurf mit Sonderregelungen gegenüber dem Öffentlichkeitsgesetz (BGÖ), die unter den Titeln «Aufbewahrung von Unterlagen» sowie «Einsichtsrecht» aufgeführt werden. So sollen gemäss Artikel 49 des BöB alle Unterlagen für die Dauer ihrer Aufbewahrung der Geheimhaltung unterliegen, soweit das BöB nicht eine Offenlegung vorsehe. Vorbehalten bliebe damit lediglich die Auskunftspflicht gegenüber Behörden, soweit hierfür eine gesetzliche Grundlage im Bundes- oder kantonalen Recht bestünde. Neu sollen gemäss Artikel 59 des BöB ebenfalls alle Unterlagen betreffend Preisüberprüfungen der Eidgenössischen Finanzkontrolle geheim bleiben – auch sie sollen damit nach Ansicht des Bundesrates vollständig vom BGÖ ausgenommen werden.

Wir sprachen uns bereits vor dem Beschluss des Bundesrats gegen beide Regelungen aus, zumal die Veröffentlichung der Vergaben auf der Beschaffungsplattform simap.ch der Öffentlichkeit keinen Zugang zu Beschaffungsunterlagen verschafft: Bliebe dieser Zugang im Beschaffungswesen inskünftig verwehrt, würde das deklarierte Transparenzziel des revidierten BöB ins Gegenteil verkehrt und das BGÖ ausgehöhlt. Gerade im besonders sensiblen Bereich des Beschaffungswesens ist es unumgänglich, die uneingeschränkte Geltung des BGÖ beizubehalten. Dank diesem Zugang der Bevölkerung und der Medien konnten in der Vergangenheit schwerwiegende, die Steuerpflichtigen teuer zu stehen kommende Beschaffungspannen aufgedeckt und die entsprechenden Lehren gezogen werden.

Soweit in Beschaffungsunterlagen Geschäftsgeheimnisse enthalten sind, werden diese vom BGÖ explizit geschützt. Es besteht somit kein Grund, solche oder andere amtliche Dokumente vom Geltungsbereich des BGÖ auszunehmen (siehe dazu auch unseren Tätigkeitsbericht 2014/15, Ziff. 2.2.3). Der Entscheid des Parlaments in der Sache ist noch ausstehend.

2.3.3 Verordnung über den Nachrichtendienst

Der Verordnungsentwurf zum neuen Nachrichtendienstgesetz enthält eine Bestimmung, mir der praktisch sämtliche Dokumente des Nachrichtendiensts des Bundes vom Öffentlichkeitsgesetz ausgenommen würden. Wir sprachen uns gegen eine solche Regelung aus.

Das am 1. September 2017 in Kraft tretende neue Nachrichtendienstgesetz (NDG) sieht vor, dass das Öffentlichkeitsgesetz (BGÖ) nicht für den Zugang zu amtlichen Dokumenten betreffend die Informationsbeschaffung gilt. Der Entwurf für die Ausführungsbestimmung in der Verordnung über den Nachrichtendienst (NDV) sah vor, dass diese Ausnahme vom BGÖ für alle amtlichen Dokumente gelten soll, die direkte oder indirekte Rückschlüsse über die Informationsbeschaffung gemäss dem 3. Kapitel des NDG zulassen. Die Bestimmung zählte sodann beispielhaft drei typische Anwendungsfälle auf: eingehende Informationen oder darauf basierende nachrichtendienstliche Produkte, Informationen über die nachrichtendienstlichen Mittel, Methoden und Kontakte sowie Informationen über zum Einsatz gelangendes Gerät, Systeme und Infrastruktur.

Diese vorgeschlagene Ausführungsbestimmung lehnten wir in der Ämterkonsultation ab und gaben zu bedenken, dass diese Formulierung es erlauben würde, praktisch jede Information, die der NDB erhält oder selbst erstellt, vom BGÖ auszuschliessen. Dies käme einer vollständigen Ausklammerung des NDB gleich, was aber nicht dem Willen des Gesetzgebers entspricht. Wir verwiesen diesbezüglich auf die übergeordnete Bestimmung im NDG, welche die Spezialnorm zum BGÖ unmissverständlich auf die nachrichtendienstliche Informationsbeschaffung begrenzt. Im Umkehrschluss müssten daher alle weiteren, von der Informationsbeschaffung als solche zu unterscheidenden Aufgaben des NDB, wie etwa Lagebeurteilungen, Analysen und Auswertungen weiterhin unter das BGÖ und seine Ausnahmebestimmungen fallen.

Wir betonten, dass eine Verordnung aufgrund des Legalitätsprinzips nur eine bereits im Gesetz vorhandene Regelung durch Detailvorschriften näher ausführen könne. Die nun vorgesehene Verordnungsbestimmung weitete die im Gesetz angelegte Ausnahme aber in unzulässiger Weise auf praktisch sämtliche Dokumente des NDB aus.

Schliesslich hielten wir ausdrücklich fest, dass Informationen, die nicht die Beschaffung betreffen, nicht in jedem Fall öffentlich zugänglich sind. Vielmehr können je nach Einzelfall die im Öffentlichkeitsgesetz vorgesehenen Ausnahmen zur Anwendung kommen.

Unsere Vorschläge zur Anpassung der Bestimmung wurden nicht berücksichtigt. Der Verordnungsentwurf war bei Redaktionsschluss noch in der Vernehmlassung.

2.4 Varia

2.4.1 Neue Arbeitsmethode bei der Durchführung von Schlichtungsverfahren

Seit dem 1. Januar 2017 werden die neu eingehenden Schlichtungsanträge vorwiegend in einem beschleunigten, mündlichen Verfahren behandelt. Damit soll die Bearbeitungsdauer der Schlichtungsverfahren gesenkt werden.

Das Öffentlichkeitsgesetz (BGÖ) ist geprägt vom Beschleunigungsgebot, das sich in den Ordnungsfristen der einzelnen Verfahrensstadien (Beurteilung Zugangsgesuch durch Behörden, Schlichtungsverfahren, Verfügungsverfahren) niederschlägt. Der Beauftragte möchte Schlichtungsanträge künftig innert der gesetzlichen Frist von 30 Tagen behandeln. Dies erfordert eine Beschleunigung der Schlichtungsverfahren. Nach Ansicht des Beauftragten ist dies am ehesten zu erreichen, wenn die Schlichtungsverhandlungen vorwiegend mündlich, statt wie bis anhin schriftlich, durchgeführt werden.

Im Rahmen eines einjährigen Versuchs werden daher ab dem 1. Januar 2017 die neuen und, soweit sinnvoll, auch die bereits hängigen Schlichtungsanträge mehrheitlich in mündlichen Schlichtungen mit den beteiligten Personen und Ämtern behandelt werden. Vom vermehrten Gebrauch der mündlichen Arbeitsmethode verspricht sich der Beauftragte nicht nur eine kürzere Dauer der Schlichtungsverfahren, sondern auch einen höheren Anteil an einvernehmlichen Lösungen. In ausgewählten Fällen (z. B. mit neuen oder anspruchsvollen juristischen Fragestellungen sowie komplexen Zugangskonstellationen) behält sich der Beauftragte indessen vor, wie bis anhin schriftliche Verfahren durchzuführen.

Angesichts der hohen Anzahl an Empfehlungen und bundesgerichtlichen Urteilen, die seit Inkrafttreten des BGÖ ergangenen sind, ist der Beauftragte zuversichtlich, dass die neue Methode die Schlichtungsverfahren beschleunigt und zur Senkung der Anzahl behördlicher Verfügungen führt. Die ersten Erfahrungen sind positiv.

2.4.2 Veranstaltung 10 Jahre Öffentlichkeitsgesetz

Anlässlich des 10-jährigen Bestehens des Öffentlichkeitsgesetzes hat der Beauftragte zusammen mit dem Bundesamts für Justiz am 2. September 2016 die zweite Schweizerische Tagung zum Öffentlichkeitsprinzip organisiert. An der Veranstaltung nahmen insbesondere Vertreter der Bundesverwaltung sowie der Kantone sowie Medienschaffende teil. Die Referenten setzten sich aus verschiedenen Blickwinkeln mit dem Motto der Veranstaltung «Wie transparent ist unsere Bundesverwaltung nach 10 Jahren Öffentlichkeitsgesetz?» auseinander. Der Beauftragte stellte an diesem Anlass das neue beschleunigte Schlichtungsverfahren vor, das seit Januar 2017 zur Anwendung gelangt (vgl. Ziffer 2.4.1 des vorliegenden Tätigkeitsberichts). Die Präsentationen der Referenten sind abrufbar auf www.derbeauftragte.ch, unter Aktuell – Veranstaltungen – 2016.

Der EDÖB

3.1 Aufgaben und Ressourcen

Leistungen und Ressourcen im Bereich Datenschutz

Personalbestände

Seit 2005 hat der Personalbestand für den Vollzug des Datenschutzgesetzes (DSG) zwischen 20 und 24 Mitarbeitenden fluktuiert. Die Schwankungen erklären sich zum einen damit, dass 2006 das Öffentlichkeitsgesetz (BGÖ) in Kraft trat. Da die dafür vorgesehenen Stellen vom Bundesrat nie bewilligt wurden, musste auf das bereits bestehende Personal des EDÖB und teilweise auch auf Mittel der Bundeskanzlei zurückgegriffen werden. Zum anderen konnten die mit dem Beitritt zum Abkommen von Schengen und Dublin sowie dem Erlass von Spezialgesetzen im Gesundheitsbereich bewilligten zusätzlichen Stellen infolge allgemeiner Sparvorgaben nicht im vollen Umfang rekrutiert werden.

Für DSG-Belange	2005	2010	2017
einsetzbare Stellen	22	23	24

Leistungen

Die Aufgaben des EDÖB als für die Bundesorgane und die Privatwirtschaft zuständige Datenschutzbehörde werden gemäss dem Neuen Führungsmodell Bund (NFB) den vier Leistungsgruppen Beratung, Aufsicht, Information und Gesetzgebung zugewiesen. 2016 wurden die beim EDÖB für den Datenschutz einsetzbaren Personalressourcen wie folgt auf diese Gruppen aufgeteilt:

Beratung Private	18.2 %	
Beratung Bund	15.7 %	
Zusammenarbeit mit Kantonen	4.0 %	
Zusammenarbeit mit ausl. Behörden	11.1 %	
Total Beratung		**49.0 %**
Aufsicht	14.6 %	
Zertifizierung	0.1 %	
Register Datensammlung	0.9 %	
Total Aufsicht		**15.6 %**
Information	12.2 %	
Ausbildung/Referate	5.9 %	
Total Information		**18.1 %**
Gesetzgebung	17.3 %	
Total Gesetzgebung		**17.3 %**
Total Datenschutz		**100.0 %**

Beratung

Wie im Kapitel «Aktuelle Herausforderungen und Schwerpunkte» dargelegt wurde, sieht sich der EDÖB im Leistungsbereich der Beratung aufgrund des ausgeweiteten Zuständigkeitsbereichs und des gesteigerten Bedürfnisses nach Projektbegleitungen mit einer wachsenden Nachfrage konfrontiert. 2016 wurden rund 50 Prozent der personellen Mittel für die Beratung aufgewendet. Gemäss dem Kontrollplan des EDÖB für das Jahr 2017 ist die beratende Begleitung von zehn grossen Projekten im Gang.

Beratungen in umfangreicheren Projekten für 2017	
Verkehr	3
Finanzen	1
Gesundheit und Arbeit	3
Sicherheit	1
Telekom / Internet of Things (IOT)	2

Da die Mittel des EDÖB bisher weder an die gestiegenen technologischen Re-Identifikationsrisiken noch an die übrigen Herausforderungen der Digitalisierung angepasst wurden, kann er die gestiegene Nachfrage nach beratender Projektbegleitung nicht in der gewünschten Tiefe und Zeit erfüllen. Vor allem aber muss er bei anderen Posten in der Leistungsgruppe Beratung, wie der internationalen Zusammenarbeit, Abstriche machen. Da sich Big Data und «künstliche Intelligenz» in immer mehr Branchen als Geschäftsmodell durchsetzen und die technologischen Datenschutzrisiken den Aufsichtsbereich des EDÖB weiter ausdehnen werden, ist mit einer weiter steigenden Anzahl von umfangreichen Datenbearbeitungsprojekten von Staat und Wirtschaft zu rechnen.

Aufsicht

Wie vorne dargelegt wurde, müssen Kontrollen aufgrund der Dynamik von Cloud-gestützten Applikationen heute rasch durchgeführt werden. Diese Beschleunigung sowie die immer wichtiger werdende Kombination von juristischem und technischem Fachwissen schliessen längere Unterbrüche bei den Sachverhaltsklärungen aus, sodass umfassendere Kontrollen von mehreren Mitarbeitenden betreut werden müssen.

Die aktuellen Personalbestände setzen der Dichte der Kontrollen enge Grenzen. Im Jahr 2016 wurden für die Aufsichtstätigkeit rund 16 Prozent der Personalressourcen aufgewendet, was unter dem langjährigen Mittelwert von rund 20 Prozent liegt. Gemäss Kontrollplan für das Jahr 2017 werden mit diesen Mitteln acht umfassendere Kontrollen bestritten.

Im Vergleich zu der Anzahl von rund 12 000 grossen und mittleren Unternehmen in der Schweiz erweist sich die aktuelle Kontrolldichte somit als tief.

Gesetzgebung

Die vom Bundesrat als «rasant» bezeichnete technologische Entwicklung findet auch bei der Datenbearbeitung durch die Bundesorgane ihren Niederschlag. Sie zieht eine Vielzahl von Bearbeitungsvorschriften in der Spezialgesetzgebung des Bundes nach sich, zu denen der EDÖB im Rahmen der diversen Konsultationsverfahren Stellung beziehen muss. Der diesbezügliche Aufwand ist in letzten zehn Jahren stark gestiegen. Diese Tendenz setzt sich fort.

Totalrevision des DSG

Zur Umsetzung der erwähnten Regulierungsziele, denen auch der aktuelle Entwurf zum totalrevidierten Bundesgesetz über den Datenschutz (E-DSG) verpflichtet ist, sind neue Instrumente wie z. B. Empfehlungen der guten Praxis oder Risikofolgenabschätzungen vorgesehen, die von den Regelwerken des Europarats und der EU übernommen werden sollen. Die Handhabung der meisten dieser Instrumente beruht auf einem Zusammenwirken zwischen den Applikationsverantwortlichen und der Datenschutzbehörde.

Gemäss Begleitbericht zum E-DSG rechnet der Bundesrat damit, dass der finanzielle Bedarf des EDÖB insgesamt «massgeblich steigt». Von der Quantifizierung dieser Verstärkung wird letztlich die Intensität abhängen, mit welcher die Datenschutzbehörde des Bundes ihre Aufgaben wahrnehmen kann. Da einige der neuen Instrumente im Gesetzestext generell beschrieben werden, wird offensichtlich, dass den politischen Behörden bei der Einschätzung künftiger Entwicklungen und deren Quantifizierung ein erheblicher Ermessensspielraum bleibt.

Dabei sollten die politischen Organe der Besonderheit der Aufgaben der Datenschutzbehörde die nötige Beachtung schenken: Hauptaufgabe des EDÖB ist der Schutz der Privatsphäre und die Gewährleistung des Rechts auf informationelle Selbstbestimmung in der digitalen Gesellschaft. Der EDÖB muss unabhängig handeln können. Dies erfordert angemessene und ausreichende personelle, materielle, technische und finanzielle Ressourcen, welche die Aufsichtsbehörde nicht darauf beschränken, reaktiv das Unabdingbare zu erledigen, sondern ihr die Initiative zum Handeln ermöglichen; und zwar mit einem Mass an Glaubwürdigkeit und Intensität, das die betroffene Öffentlichkeit zum Schutz ihrer Grundrechte vernünftigerweise erwarten darf.

Mit Blick auf die einzelnen Leistungsgruppen ergeben sich somit folgende, für die Bemessung der Mittel wegleitende Wirkungsziele:

Leistungsgruppe	Wirkungsziele
Beratung	Der EDÖB entfaltet eine erwartungsadäquate Präsenz für die Beratung von Privatpersonen sowie die Begleitung von datenschutzsensiblen Projekten der Wirtschaft und der Bundesbehörden.
Aufsicht	Der EDÖB entfaltet eine glaubwürdige Dichte an Kontrollen.
Information	Der EDÖB sensibilisiert die Öffentlichkeit proaktiv für technologie- und anwendungsbezogene Risiken der Digitalisierung.
Gesetzgebung	Der EDÖB nimmt rechtzeitig und aktiv Einfluss auf alle datenschutzrelevanten Spezialnormen und Regelwerke, die auf nationaler und internationaler Ebene geschaffen werden. Er unterstützt die interessierten Kreise bei der Formulierung von Regeln der guten Praxis

Leistungen und Ressourcen im Bereich Öffentlichkeitsgesetz

In der Einheit BGÖ, wo 3.6 Stellen eingesetzt werden, sind in den letzten Jahren erhebliche Arbeitsrückstände bei Schlichtungsverfahren entstanden. Um diese nicht weiter anwachsen zu lassen, sondern mittelfristig abzubauen, ist der EDÖB ab dem 1. Januar 2017 zu einem beschleunigten und summarischen Verfahren übergegangen, das sich dadurch charakterisiert, dass in der Regel mündliche Schlichtungsverhandlungen durchgeführt werden.

Die Erfahrungen der ersten Monate sind positiv: Die Bearbeitungsdauer der neu eingehenden Schlichtungsanträge konnte beträchtlich reduziert werden, und es zeichnet sich eine Erhöhung des Anteils an einvernehmlichen Lösungen zwischen den Antragstellenden und den Behörden ab. Zudem konnte der EDÖB den Aufwand senken, indem er anstelle von detailliert begründeten nur mehr summarische Empfehlungen abgibt. Allerdings erhöhte sich das zeitliche Engagement des Beauftragten und des Leiters des Direktionsbereichs BGÖ, welche die Schlichtungsverhandlungen stets persönlich leiten und bis zu vier Termine pro Woche wahrnehmen. Ob sich der geplante Pendenzenabbau mit dem gegenwärtig eingesetzten Personalbestand bewerkstelligen lässt, wird der im ersten Semester 2018 vorliegende Evaluationsbericht zeigen.

3.2 11. Datenschutztag – Grenzen der Videoüberwachung

Den diesjährigen Datenschutztag haben wir zum Anlass genommen, um auf die Risiken der Videoüberwachung hinzuweisen. Auch Privatpersonen setzen vermehrt Videoüberwachungsanlagen ein, um für Sicherheit und Ordnung auf ihrem Anwesen oder im eigenen Unternehmen zu sorgen. Für einen datenschutzkonformen Betrieb müssen bestimmte Grundsätze beachtet werden.

Weil Videokameras immer günstiger werden, finden sie vermehrt zur Überwachung des Privatbereichs Einsatz oder werden von Privatpersonen als kamerabestückte Drohnen oder Dashcams in Fahrzeugen verwendet, was die Privatsphäre Dritter beeinträchtigen kann. Videoüberwachung ist zu einem Thema geworden, das in seinen vielen Facetten weite Bevölkerungsteile interessiert und betroffen macht, was sich in unserer Beratungstätigkeit niederschlägt. Auch in der Medienberichterstattung ist Videoüberwachung ein Dauerthema.

Der Internationale Datenschutztag wird auf Initiative des Europarates seit 2007 jedes Jahr am 28. Januar europaweit und auch in Übersee ausgerichtet. Er soll Bürgerinnen und Bürger für den Schutz der Privatsphäre und das Recht auf informationelle Selbstbestimmung sensibilisieren und eine nachhaltige Verhaltensänderung im Umgang mit neuen Technologien bewirken.

Wir haben auf unserer Website die neue Seite «Videoüberwachung durch Private» publiziert, die einen Überblick über die verschiedenen Ausprägungen und Risiken der Videoüberwachung liefert und aufzeigt, worauf Betreiber einer Videoüberwachungsanlage achten müssen und über welche Rechte Betroffene verfügen.

3.3 Publikationen und Veranstaltungsteilnahmen

Unsere Website www.derbeauftragte.ch enthält umfassende Informationen zu den verschiedenen Tätigkeitsbereichen des EDÖB. Im Berichtsjahr kamen insbesondere neue Erläuterungen zum Einsatz von Fitnesstrackern im Versicherungsbereich und zu den Datenschutzaspekten beim Internetprotokoll IPv6 hinzu. Darüber hinaus nahm der EDÖB an zahlreichen Veranstaltungen teil.

Die spielerische Messung der eigenen Körperfunktionen und Leistungen mittels Fitness-Apps oder Wearables kann motivierend sein und einen positiven Effekt auf die Gesundheit und das allgemeine Wohlbefinden haben. Bei der digitalen Selbstvermessung fallen jedoch gewaltige Datenmengen an, die sich kaum mehr überblicken lassen. Es droht ein Kontrollverlust, der das Grundrecht auf informationelle Selbstbestimmung infrage stellt (www.derbeauftragte.ch, Gesundheit – Kranken- und Unfallversicherungen).

Das Internet ist heute die wichtigste Technologie zur Übermittlung jeder Art von Kommunikation geworden. Weil die IP-Adressen des gegenwärtig genutzten Internet Protokoll Version 4 (IPv4) in absehbarer Zeit erschöpft sind, wurde ein neues Internetprotokoll (IPv6) entwickelt. Im Vergleich zu IPv4 bietet IPv6 eine Reihe praktischer Vorteile, birgt aber auch gewisse Risiken für den Datenschutz und die Privatsphäre. Diese Risiken können mit geeigneten technischen und organisatorischen Massnahmen minimiert werden (www.derbeauftragte.ch, Datenschutz – Internet und Computer).

Überarbeitet wurden zudem unsere Erläuterungen zur Videoüberwachung am Arbeitsplatz (www.derbeauftragte.ch, Datenschutz – Arbeitsbereich – Überwachung am Arbeitsplatz). Die Videoüberwachung wird häufig in Gastronomie-, Detailhandels- und Freizeitbetrieben eingesetzt, meistens mit dem Ziel, sich vor Diebstahl zu schützen oder die Beschädigung von Mobiliar und WC-Anlagen zu verhindern. Oft wird jedoch ausser Acht gelassen, dass nicht nur die Kunden betroffen sind, sondern auch das Personal mitgefilmt wird. Aus Datenschutzsicht kann beides problematisch sein.

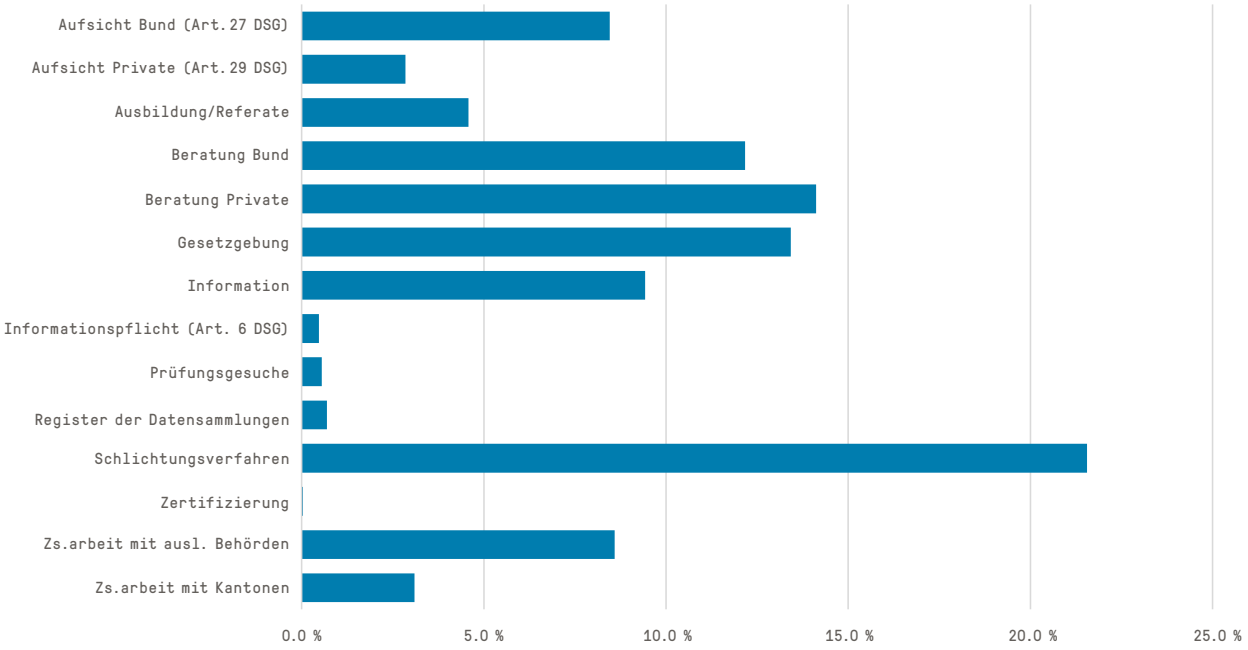
Der Bundesrat hat am 11. Januar 2017 Kenntnis von der Einrichtung eines neuen Rahmens für die Übermittlung von Personendaten aus der Schweiz in die USA genommen. Der sogenannte Privacy Shield ersetzt das vom EDÖB für ungenügend erklärte und nun auch vom Bundesrat formell aufgehobene Safe-Harbor-Abkommen. Wir haben weiterführende Informationen zum Privacy Shield und die einschlägigen Dokumente aufgeschaltet (www.derbeauftragte.ch, Datenschutz/Handel und Wirtschaft – Übermittlung ins Ausland – USA).

Im Berichtsjahr wurde der EDÖB von zahlreichen Unternehmen, Verbänden, Nicht-Regierungsorganisationen und Institutionen an ihre Veranstaltungen eingeladen. Aus Kapazitätsgründen konnte er nicht allen Anfragen nachkommen. Er hat aber insbesondere zu den Themen Verkehr, Medizin, Big Data, digitale Gesellschaft und zur anstehenden Revision des Datenschutzgesetzes an insgesamt 80 Podiumsgesprächen und Konferenzen teilgenommen. Darüber hinaus stand er in regelmässigem Kontakt mit Akteuren aus Wirtschaft und Politik.

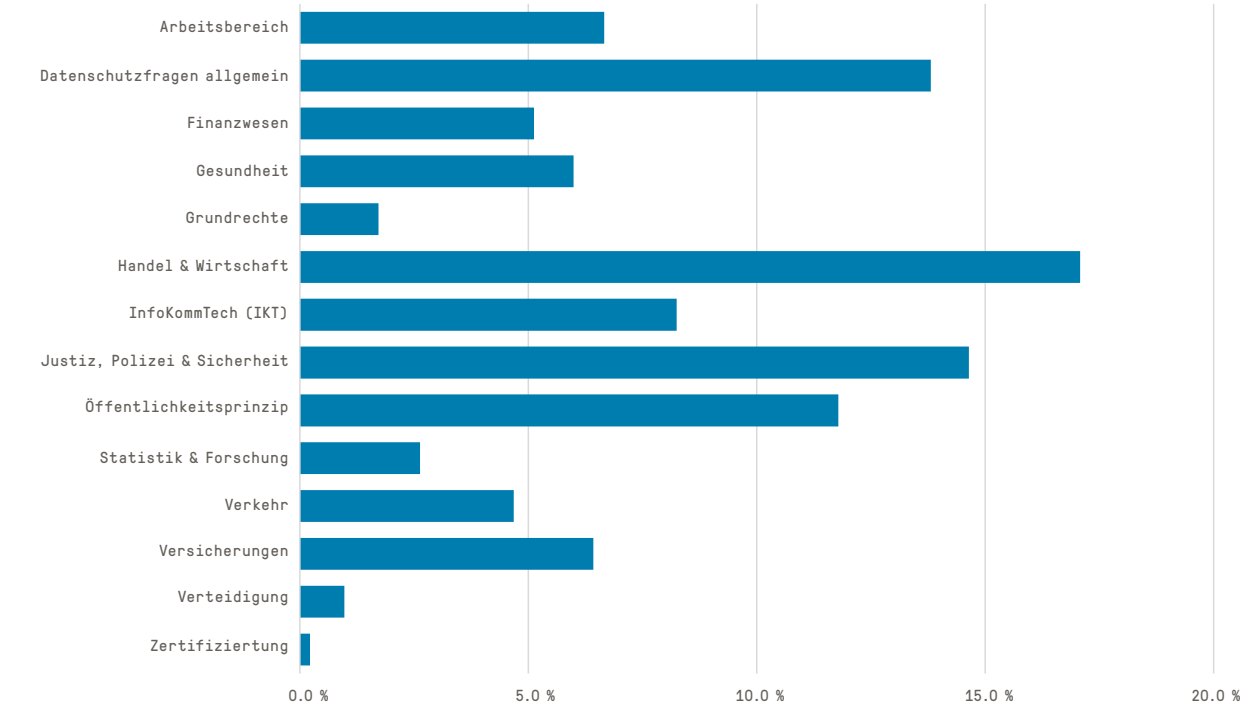
3.4 Statistiken

3.4.1 Statistiken über die Tätigkeiten des EDÖB vom 1. April 2016 bis 31. März 2017 (Datenschutz und Öffentlichkeitsprinzip)

Aufwand nach Aufgabengebiet



Aufwand nach Sachgebiet



3.4.2 Statistiken über eingereichte Zugangsgesuche nach Öffentlichkeitsgesetz vom 1. Januar 2016 bis am 31. Dezember 2016

Bundeskanzlei BK

Betroffener Bereich	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teil-weise gewährt / aufgeschoben	Zugangsgesuch hängig	Zugangsgesuch zurückgezogen
BK	19	9	2	3	4	1
EDÖB	10	8	0	1	0	0
TOTAL	29	17	2	4	4	1

Eidgenössisches Departement für auswärtige Angelegenheiten EDA

Betroffener Bereich	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teil-weise gewährt / aufgeschoben	Zugangsgesuch hängig	Zugangsgesuch zurückgezogen
EDA	118	86	16	11	2	3
TOTAL	118	86	16	11	2	3

Eidgenössisches Departement des Inneren EDI

Betroffener Bereich	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teil-weise gewährt /aufgeschoben	Zugangsgesuch hängig	Zugangsgesuch zurückgezogen
GS	6	2	2	2	0	0
EBG	2	1	0	1	0	0
BAK	1	1	0	0	0	0
BAR	3	3	0	0	0	0
METEO CH	0	0	0	0	0	0
NB	0	0	0	0	0	0
BAG	16	7	2	3	3	1
BFS	6	2	2	1	1	0
BSV	11	6	0	3	2	0
BLV	7	2	0	3	0	2
SNM	0	0	0	0	0	0
SWISS MEDIC	19	7	6	5	0	1
SUVA	1	1	0	0	0	0
TOTAL	71	31	12	18	6	4

Eidgenössisches Finanzdepartement EFD

Betroffener Bereich	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teil-weise gewährt /aufgeschoben	Zugangsgesuch hängig	Zugangsgesuch zurückgezogen
GS	8	2	3	3	0	0
ISB	2	0	0	1	1	0
EFV	4	1	0	3	0	0
EPA	3	2	1	0	0	0
ESTV	5	2	1	2	0	0
EZV	13	3	7	1	1	0
EAV	3	2	1	0	0	0
BBL	4	2	0	0	1	1
BIT	3	3	0	0	0	0
EFK	6	4	1	1	0	0
SIF	3	1	2	0	0	0
PUBLICA	0	0	0	0	0	0
ZAS	1	0	0	1	0	0
TOTAL	55	22	16	12	3	1

Eidgenössische Justiz- und Polizeidepartement

Betroffener Bereich	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teil-weise gewährt / aufgeschoben	Zugangsgesuch hängig	Zugangsgesuch zurückgezogen
GS	4	3	1	0	0	0
BJ	1	1	0	0	0	0
FEDPOL	16	4	4	4	3	1
METAS	4	4	0	0	0	0
SEM	26	16	3	5	0	2
SIR	6	5	0	1	0	0
IGE	1	1	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	0	0	0	0	0	0
NKVF	0	0	0	0	0	0
TOTAL	58	34	8	10	3	3

Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation

Betroffener Bereich	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teil-weise gewährt /aufgeschoben	Zugangsgesuch hängig	Zugangsgesuch zurückgezogen
GS	7	5	0	0	1	0
BAV	7	5	1	0	1	0
BAZL	10	6	2	2	0	0
BFE	12	8	0	3	1	0
ASTRA	8	8	0	0	0	0
BAKOM	3	1	1	1	0	0
BAFU	27	18	3	3	0	3
ARE	0	0	0	0	0	0
ComCom	0	0	0	0	0	0
ENSI	11	1	1	4	4	1
PostCom	1	1	0	0	0	0
UBI	3	3	0	0	0	0
TOTAL	89	56	8	13	7	4

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS

Betroffener Bereich	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teil-weise gewährt / aufgeschoben	Zugangsgesuch hängig	Zugangsgesuch zurückgezogen
GS	11	7	1	2	0	1
Verteidig./ Armee	5	1	2	2	0	0
NDB	8	0	1	1	3	3
armasuisse	17	0	5	3	2	7
BASPO	2	1	1	0	0	0
BABS	2	0	0	1	0	1
TOTAL	45	9	10	9	5	12

Eidgenössisches Departement für Wirtschaft, Bildung und Forschung

Betroffener Bereich	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teil-weise gewährt /aufgeschoben	Zugangsgesuch hängig	Zugangsgesuch zurückgezogen
GS	8	5	0	2	1	0
SECO	19	8	4	7	0	0
SBFI	6	2	4	0	0	0
BLW	23	4	5	12	2	0
BWL	0	0	0	0	0	0
BWO	1	0	0	0	0	0
PUE	5	2	0	3	0	0
WEKO	16	13	1	1	0	1
ZIVI	1	0	0	1	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	5	2	1	2	0	0
TOTAL	85	37	15	28	3	1

Bundesanwaltschaft

Betroffener Bereich	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teil-weise gewährt / aufgeschoben	Zugangsgesuch hängig	Zugangsgesuch zurückgezogen
BA	4	4	0	0	0	0
TOTAL	4	4	0	0	0	0

Parlamentsdienste

Betroffener Bereich	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teil-weise gewährt / aufgeschoben	Zugangsgesuch hängig	Zugangsgesuch zurückgezogen
PD	3	2	1	0	0	0
TOTAL	3	2	1	0	0	0

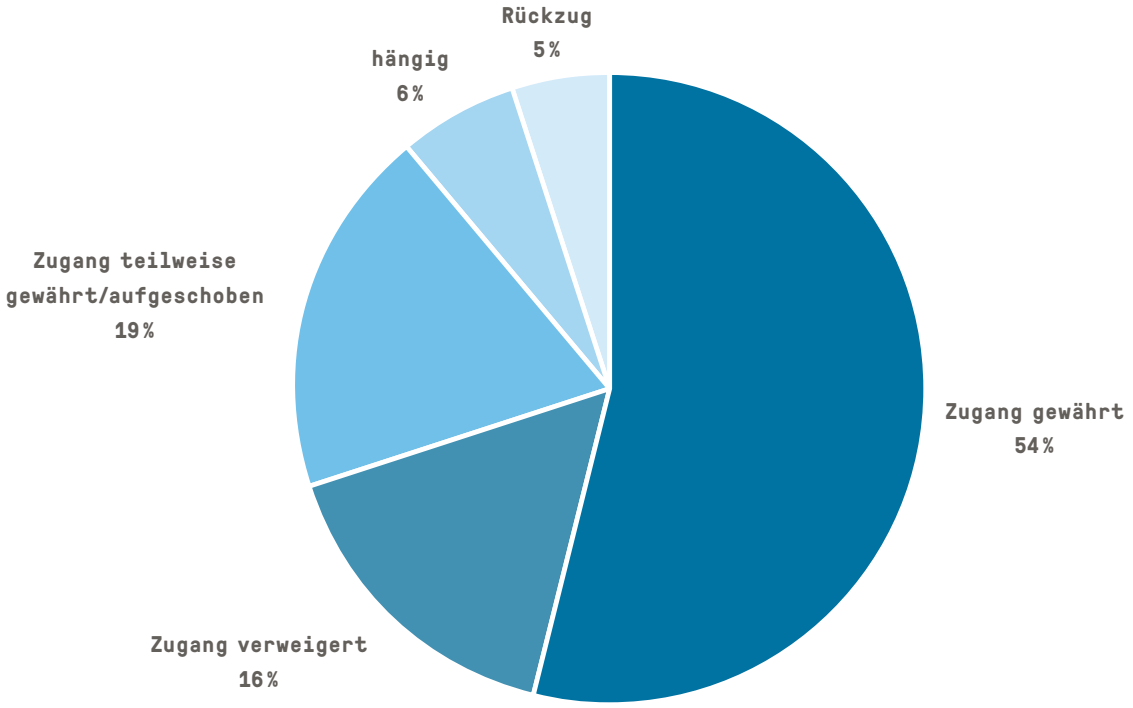
Übersicht der Zugangsgesuche der Departemente und der Bundeskanzlei

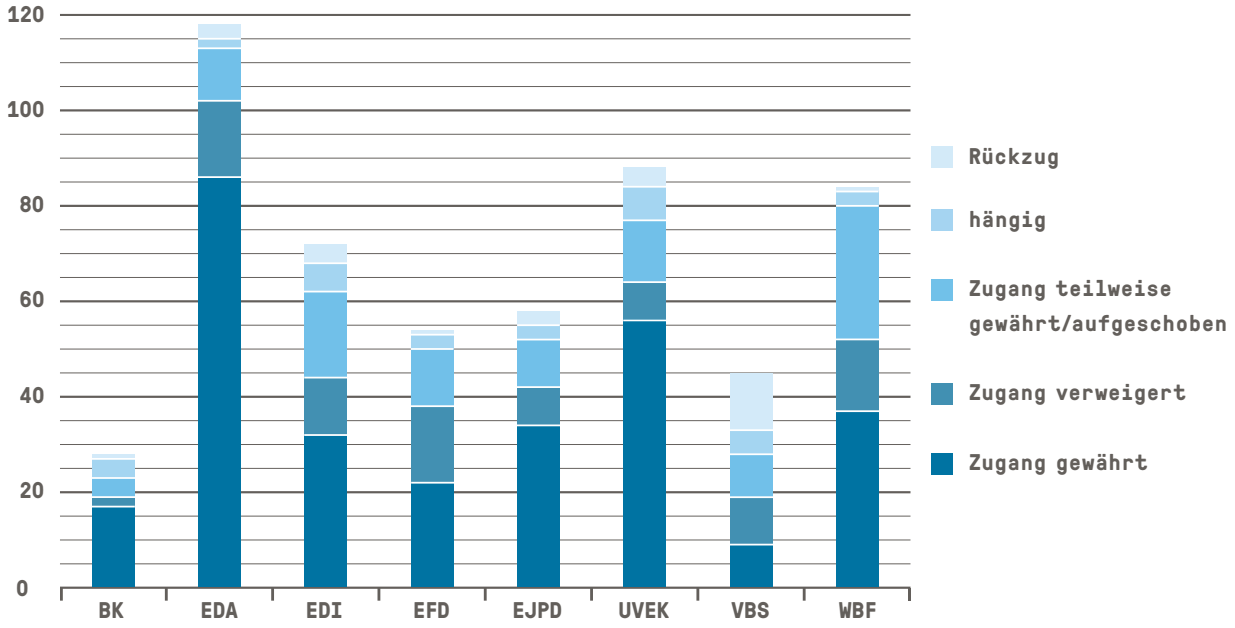
Depatement	Azahl Gesuche		Zugang vollständig gewährt		Zugang vollständig verweigert		Zugang teil-weise gewährt / aufgeschoben		Zugangsgesuch hängig		Zugangsgesuch zurückgezogen	
BK	29		17		2		4		4		1	
EDA	118		86		16		11		2		3	
EDI	72		32		12		18		6		4	
EFD	55		22		16		12		3		1	
EJPD	58		34		8		10		3		3	
UVEK	89		56		8		13		7		4	
VBS	45		9		10		9		5		12	
WBF	85		37		15		28		3		1	
TOTAL 2016 (%)	551	(100)	293	(55)	87	(16)	105	(19)	33	(6)	29	(4)
TOTAL 2015 (%)	597	(100)	319	(54)	98	(16)	127	(21)	22	(4)	31	(5)
TOTAL 2014 (%)	575	(100)	297	(51)	122	(21)	124	(22)	17	(3)	15	(3)
TOTAL 2013 (%)	469	(100)	218	(46)	122	(26)	103	(22)	8	(2)	18	(4)
TOTAL 2012 (%)	506	(100)	223	(44)	138	(27)	120	(24)	6	(1)	19	(4)
TOTAL 2011 (%)	466	(100)	203	(44)	126	(27)	128	(27)	9	(2)	–	
TOTAL 2010 (%)	239	(100)	106	(45)	62	(26)	63	(26)	8	(3)	–	
TOTAL 2009 (%)	232	(100)	124	(54)	68	(29)	40	(17)	–		–	

Anzahl der eingegangenen Schlichtungsgesuche

Kategorie Antragsteller	**2016**
Medien	23
Privatpersonen (bzw. keine genaue Zuordnung möglich)	99
Interessenvertreter (Verbände, Organisationen, Vereine usw.)	5
Rechtsanwälte	2
Unternehmen	20
Total	**149**

Zugangsgesuche der gesamten Bundesverwaltung





3.5 Das Sekretariat des EDÖB

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter

	Lobsiger Adrian (ab 1. Juni)
Stellvertreter:	Walter Jean-Philippe

Direktionsbereich Datenschutz

Leiter:	Buntschu Marc
Stellvertreterin:	Haag Sophie

Team 1

Leiter:	Meier Thomas, Jurist
	Berger Cyrill, Jurist
	Frey Franziska, Juristin

Team 2

Leiterin:	Gloor Scheidegger Caroline, Juristin
	Koç Karin, Juristin
	Schönbett Frédéric, Jurist
	Trolliet Sabine, Juristin

Team 3

Leiterin:	Haag Sophie, Juristin
	Gisin Philipp, Jurist
	Rossier Odile, Juristin

Direktionsbereich Öffentlichkeitsprinzip

Leiter:	Ammann Reto

Team

	Keller Annina, Juristin
	Moinat Marc, Jurist (Praktikant)
	Prinz Alessandra, Juristin
	Schwegler Astrid, Juristin

Direktionsbereich Kompetenzzentren

Leiter:	Tsiraktsopoulos Kosmas
Stellvertreter:	Sidler Andreas

Kompetenzzentrum Geschäftsverwaltung, Personelles, Finanzen und Kommunikation

Fachbereich Geschäfte

Verantwortlicher:	Jörg Paul
	Fuhrer Muriel, Fachsp. I kaufm. Verwaltungsdienste

Fachbereich Kommunikation

	Meier Francis, Informationsbeauftragter
	Böhlen Silvia, Kommunikationsspezialistin

Fachbereich Digitale Gesellschaft

Verantwortlicher:	Sidler Andreas
	Fasel Frédéric, Fachsp. I kaufm. Verwaltungsdienste

Kompetenzzentrum Informatik

Leiterin:	Gaukel Rahel, Informatikerin
	Aad Imad, Informatiker
	Scherrer Urs, Informatiker
	Stüssi Philipp, Informatiker

Direktionsbereich Internationale Angelegenheiten, Gesetzgebung und Kantone

Leiter:	Walter Jean-Philippe

Team

	Lennman Catherine, Juristin

Abkürzungsverzeichnis

AHV	Alters- und Hinterlassenenversicherung
AIA	Internationaler automatischer Informationsaustausch
AIAG	Bundesgesetzes über den internationalen automatischen Informationsaustausch
AIAV	Verordnung über den internationalen automatischen Informationsaustausch in Steuersachen
BAG	Bundesamt für Gesundheit
BBL	Bundesamt für Bauten und Logistik
BFE	Bundesamt für Energie
BFK	Eidgenössisches Büro für Konsumentenfragen
BFS	Bundesamt für Statistik
BWIS	Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit
DAS	Datenannahmestelle
E-ID-Gesetz	Bundesgesetz über staatlich anerkannte elektronische Identifizierungsmittel
EJPD	Eidgenössisches Justiz- und Polizeidepartement
EPA	Eidgenössisches Personalamt
ESTV	Eidgenössische Steuerverwaltung
IKBDSP	Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre
IKRK	Internationales Komitee vom Roten Kreuz
IV	Invalidenversicherung
IVG	Bundesgesetz über die Invalidenversicherung
IVV	Verordnung über die Invalidenversicherung
KVV	Verordnung über die Krankenversicherung
MEDAS	Medizinische Abklärungsstelle
NAD	Nationaler Adressdienst
NDB	Nachrichtendienst des Bundes
NDG	Nachrichtendienstgesetz
NVD	Nachrichtendienstverordnung
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
RAD	Regional ärztlicher Dienst
RHG	Registerharmonisierungsgesetz
RVOG	Regierungs- und Verwaltungsorganisationsgesetz
SAS	Schweizerische Akkreditierungsstelle
SBB	Schweizerische Bundesbahnen
SIS	Schengener Informationssystem
SIS II	Schengener Informationssystem der zweiten Generation
StAhiG	Steueramtshilfegesetz
StAhiV	Steueramtshilfeverordnung
StGB	Schweizerisches Strafgesetzbuch
VIS	Visa-Informationssystem
VöV	Verband öffentlicher Verkehr

Impressum

Dieser Bericht ist auch über das Internet (www.derbeauftragte.ch) abrufbar.
Vertrieb: BBL, Verkauf Bundespublikationen, CH-3003 Bern
www.bundespublikationen.admin.ch
Art.-Nr. 410.024.d

Layout: Duplex Design GmbH
Fotografie: Maya Valentin, Peter Mosimann (Vorwort)