25. Tätigkeitsbericht 2017/18

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Tätigkeitsbericht 2017/2018
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 2017 und 31. März 2018 ab.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Vorwort

Angesichts der ungebremsten Dynamik der digitalen Realität hat unsere Behörde auch in der aktuellen Berichtsperiode pragmatische Wege beschritten, um eine wirkungsvolle Aufsicht zu entfalten.

Beim Vollzug des Öffentlichkeitsgesetzes konnten wir mit dem Übergang zu einem vorwiegend mündlichen und summarischen Schlichtungsverfahren unter markanter Senkung der Verfahrensdauer und Abbau aller Pendenzen den Anteil an einvernehmlichen Lösungen auf 60 Prozent erhöhen. Wir deuten dies auch als weiteres Indiz dafür, dass sich der vom Gesetzgeber angestrebte Kulturwechsel hin zu einer offenen Verwaltungstätigkeit allmählich konsolidiert.

Um darauf hinzuwirken, dass Personendaten nicht mit der technisch machbaren, sondern rechtlich zulässigen Intensität bearbeitet werden, verlangten wir von den Verantwortlichen digitaler Applikationen, dass sie hohe datenschutzrechtliche Risiken frühzeitig dokumentieren und minimieren. Dank dieser zeitgemässen Arbeitsmethode, die der Entwurf des totalrevidierten Datenschutzgesetzes in Anlehnung an das revidierte europäische Recht konkretisiert, konnten wir den eigenen Arbeitsaufwand auch im Bereich der Datenschutzaufsicht senken.

Trotz dieser Effizienzsteigerungen ist der Anteil unserer Gesamtaufwendungen für die beratende Begleitung von digitalen Grossbaustellen im Berichtsjahr erstmals auf einen Rekordwert von über 50 Prozent angestiegen. Aufgrund der seit dem Jahre 2005 nahezu unveränderten Ressourcen zwang uns diese Entwicklung, bei der Eröffnung neuer Verfahren Zurückhaltung zu üben, sodass der schon in der letzten Berichtsperiode deutlich unter dem langjährigen Mittelwert von 20 Prozent liegende Anteil für Sachverhaltsabklärungen nunmehr auf 12 Prozent abgesunken ist. Damit liessen sich in der Bundesverwaltung und Privatwirtschaft noch 11 umfassendere Kontrollen durchführen, was angesichts der Anzahl von rund 12'000 mittleren und grossen Betrieben eine tiefe Kontrolldichte indiziert.

Ungeachtet dieser herausfordernden Entwicklungen wird das Team des EDÖB während der anspruchsvollen Übergangszeit bis zum Inkrafttreten eines totalrevidierten Datenschutzgesetzes alles daran setzen, um als Aufsichtsbehörde einerseits eine im In- und Ausland wahrnehmbare Präsenz zu entfalten und andrerseits betroffene Schweizer Unternehmen bei der Anwendung der im Mai in Kraft getretenen Datenschutzgrundverordnung der Europäischen Union mit Rat und Tat zu begleiten.

Adrian Lobsiger
Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter

Aktuelle Herausforderungen und Schwerpunkte

I Digitalisierung

Die Errungenschaften der Informations- und Telekommunikationstechnologie und die global vernetzte Wirtschaft haben eine digitale Realität geschaffen, die den Alltag der Menschen in der Schweiz bei Arbeit, Konsum und Freizeit prägt.

Technologie und Wirtschaft

Neben Computer und Smartphone kommen in rasch anwachsender Anzahl Sensoren zum Einsatz, die menschliche Bilder, Stimmen bis hin zu inneren Körperfunktionen aufzeichnen und dank erweiterten Bandbreiten des Internets der Dinge künstlichen Intelligenzen zuführen. Letztere sollen darauf hinwirken, dass mit einem Minimum an Ressourcen ein Maximum an kommerziellen, wissenschaftlichen, politischen oder wie auch immer gelagerten Bedürfnissen und Interessen bedient werden.

Der Datenschutz verlangt, dass bei der Messung, Analyse und Voraussage von Bedürfnissen stets Technologien zum Einsatz gebracht werden, welche die Menschen als Kunden, Konsumenten, Passagiere oder Patienten umfassend und benutzerfreundlich über die Zwecke und Wirkungsweisen der entsprechenden Applikationen informieren. Ebenso zentral ist, dass in Technologien investiert wird, die wirksam vor unberechtigten Zugriffen auf Personendaten schützen. Im Berichtsjahr war der EDÖB mit einer Vielzahl von Datenverlusten konfrontiert. Diese zeigten, dass die technische Sicherheit zurzeit nicht Schritt hält mit der beschleunigten Beschaffung, Verbreitung und Verwertung von Daten. Ähnlich wie nach der von Katastrophen geprägten Kommerzialisierung des Düsenantriebs in der Aviatik der 60er-Jahre muss die Sicherheitstechnik diesen Rückstand aufholen. Das kann nur gelingen, wenn die Bearbeitungsverantwortlichen die entsprechenden Risiken frühzeitig erheben und die nötigen Investitionen in deren Minimierung tätigen.

Gesellschaft, Politik und Recht

Die digitale Realität wird geprägt von Akteuren, die Daten von anderen unter Einsatz technischer Expertise kommerziell, wissenschaftlich oder politisch verwerten und mit ihren maschinell generierten Angeboten mehrheitlich Laien ansprechen. Das Recht auf Wahrung der informationellen Selbstbestimmung verlangt, dass auch jene sinnstiftend an der Digitalisierung mitgestalten können, deren Zugang zu technischem Know-how beschränkt ist. Mit dieser Zielsetzung schlagen der behördliche und betriebliche Datenschutz Brücken, über die Wissen von den Anbietern digitaler Leistungen zu den Bezügern fliessen kann. Leider wird die Notwendigkeit einer fairen und umfassenden Information nicht von allen Verantwortungsträgern erkannt. Solange die tatsächliche Verwendung von Kundendaten wie im Fall von Cambridge Analytica über Whistleblower statt aktive Kundeninformation offenbar wird, geht zwischen den Bezügern und Anbietern digitaler Leistungen Vertrauen verloren, was – wie im Falle von Facebook – Kontrollbehörden und Regulatoren auf den Platz ruft.

Besonders verletzlich ist die Privatsphäre mit Blick auf Browserdaten. Die angesurften Seiten ermöglichen Rückschlüsse auf die inneren Impulse, mit denen Menschen Inhalte auf dem Internet ansteuern. Sie erzeugen bereits nach kurzen Erfassungszeiträumen Persönlichkeitsprofile, die über Interessen, Vorlieben oder Kontakte und damit indirekt Gedanken- und Gesinnungsmuster bis hin zu sexuellen Orientierungen und intimen Fantasien mutmassen lassen. Obwohl technisch machbar, darf die Bearbeitung von Surfprofilen demzufolge – abgesehen von strafrichterlichen Anordnungen – nie zu einer Aussonderung und zwecküberschiessenden Auswertung oder gar Blossstellung eines Verhaltens bestimmbarer Einzelpersonen führen. Bis anhin fehlten dem EDÖB die Mittel, sich mittels aufwändiger technischer Kontrollen zu vergewissern, ob die Verantwortlichen von Applikationen, die gezielt Meldungen an aggregierte Gruppen von Benutzern absetzen, das Verbot der zweckü berschiessenden Identifizierung bestimmbarer Personen tatsächlich einhalten. Zudem stellen sich gerade bei sozialen Plattformen, deren Benützer dort über ein Konto verfügen, heikle Abgrenzungsfragen, wie die öffentliche Diskussion zum Fall Cambridge Analytica und Facebook zeigt.

In der Berichtsperiode konzentrierte unsere Behörde ihre Anstrengungen mit Blick auf das sog. «Mikro-Targeting» darauf, dass die Urheberschaft entsprechender Applikationen sowie die verfolgten kommerziellen, politischen und weiteren Zwecke benutzerfreundlich und umfassend transparent gemacht werden, ehe eine Einwilligung eingefordert wird. Mit Blick auf die bevorstehenden eidgenössischen Wahlen hat sich der EDÖB im Herbst 2017 denn auch diesbezüglich mit einem Merkblatt an die Veranstalter politischer Kampagnen gewandt (www.derbeauftragte.ch, Datenschutz – Dokumentation – Merkblätter – Einsatz digitaler Kampagnentools zu politischen Zwecken).

Damit der EDÖB als Aufsichtsbehörde sicher stellen kann, dass Personendaten nicht mit der technisch machbaren, sondern rechtlich zulässigen Intensität bearbeitet werden, verlangt er von den Verantwortlichen digitaler Applikationen, dass sie hohe datenschutzrechtliche Risiken frühzeitig minimieren und gegenüber der betrieblichen und behördlichen Datenschutzaufsicht dokumentieren. Zeitgemässe Arbeitsinstrumente wie die Datenschutz-Risikofolgenabschätzung haben sich in der Praxis der digitalen Realität herausgebildet. Sie wurden denn auch in den vom EDÖB begleiteten Grossprojekten angewendet (s. Kapitel 3.1 in diesem Bericht), lange bevor die EU-Datenschutz-Grundverordnung (DSGVO) in Kraft trat. Das Gleiche gilt für die Meldung von Datenschutzverletzungen: Allein im Monat Dezember 2017 wurden dem EDÖB von drei Unternehmen gravierende Ereignisse gemeldet.

Umso erstaunlicher ist es, dass die Behandlung der vom Bundesrat am 15. September 2017 vorgelegten Totalrevision des Datenschutzgesetzes von 1993, mit der eben diese Arbeitsinstrumente eingeführt und näher konkretisiert werden sollen, in der staatspolitischen Kommission des erstberatenden Nationalrats eine zeitliche Verzögerung erfahren hat. Nachdem sich die Kommission dafür aussprach, diese Neuerungen im Rahmen einer vorgezogenen Umsetzungen der «Schengen Direktive» zunächst auf die Datenbearbeitung von Strafverfolgungsbehörden zu beschränken, mussten die Totalrevision zurückgestellt und die Beratungen bis zur Erarbeitung eines entsprechenden Erlassentwurfs durch die Verwaltung unterbrochen werden. Dies mit der Konsequenz, dass der Datenschutz der Schweizer Bevölkerung nach wie vor auf einem 25-jährigen Gesetz beruht, das 12 Jahre vor der Vermarktung des ersten Smartphones in Kraft trat und die Digitalisierung nicht anspricht.

II Beratungs- und Kontrolltätigkeit

In der Berichtsperiode haben wir die Begleitung einer Vielzahl von Big-Data-Projekten von Bundesbehörden und Privatwirtschaft fortgesetzt, bei denen wir uns mit dem Risiko zweckwidriger Re-Identifikationen von Personen aus Sachdaten auseinandersetzen mussten. Angesichts der erwähnten Datenverluste mussten sich die interdisziplinären Teams des EDÖB zudem im Rahmen ihrer Projektbegleitungen zunehmend mit den technischen und organisatorischen Massnahmen zur Minderung entsprechender Verlustrisiken auseinandersetzen.

Obwohl der EDÖB mit Blick auf die Beurteilung hoher Sicherheitsrisiken auf dem erwähnten Einsatz moderner Arbeitsinstrumente beharrt und damit den eigenen Arbeitsaufwand senkt, ist der Anteil unserer Gesamtaufwendungen für die beratende Begleitung von privatwirtschaftlichen Projekten im Berichtsjahr auf einen neuen Rekordwert angestiegen (s. Kapitel 3.1 in diesem Bericht). Nebst der ansteigenden Komplexität von Big-Data-Projekten erklärt sich dieser Anstieg durch die gemeldeten Datenverluste, in deren Nachgang betroffene Unternehmen um Beratungsdienstleitungen ersuchten. Für Letztere musste der EDÖB kurzfristig erhebliche personelle Ressourcen bereitstellen, da die Schadensminderung und Information der Kunden keinen zeitlichen Aufschub erträgt. Angesichts unserer knappen Mittel führte diese Entwicklung zu Verzögerungen und Kürzungen bei den planbaren Kontrollen. Auch hinsichtlich der Bearbeitung von Personendaten durch Konsumenten-Apps und soziale Netzwerke ist der Beauftragte in der Berichtsperiode mit seinen knappen Ressourcen an Grenzen gestossen, sodass er die diesbezüglichen Erwartungen der Öffentlichkeit nicht mit der wünschbaren Proaktivität erfüllen konnte.

III Nationale und internationale Kooperation

Der EDÖB hat seine Zusammenarbeit mit den kantonalen und kommunalen Datenschutzstellen, die mit den gleichen Entwicklungen und Technologien zur Bearbeitung von Personendaten konfrontiert sind, weiter intensiviert. Seit dem 25. Oktober 2017 ist er assoziiertes, d. h. nicht stimmberechtigtes Mitglied bei der Vereinigung Privatim, in deren Gremien er mit beratender Stimme vertreten ist. Mit Blick auf die anstehende Totalrevision des DSG vertrat Privatim eine Haltung, die teilweise von jener des EDÖB abwich.

Neues Datenschutzrecht

Am 25. Mai 2018 ist die DSGVO in Kraft getreten, die unter gewissen Voraussetzungen auch für Bearbeitungen durch schweizerische Unternehmen Anwendung findet. Im Herbst 2017 hat der EDÖB ein Merkblatt veröffentlicht, welches insbesondere auf die extraterritoriale Geltung des neuen EU-Rechts eingeht (www.derbeauftragte.ch, EU-DSGVO). Zudem hat er an zahlreichen Informationsveranstaltungen zu diesem Thema mitgewirkt und im Rahmen seiner Beratungstätigkeit zahlreiche mündliche und schriftliche Anfragen von Bürgern und Medien beantwortet.

Die Übergangszeit bis zum Inkrafttreten der verzögerten Totalrevision des DSG (s. Kapitel 1.1.1 und 3.1 in diesem Bericht) gestaltet sich als besondere Herausforderung für unsere Behörde. Während die Datenschutzbehörden in den EU-Staaten mit Verfügungs- und Sanktionsbefugnissen und erheblichen zusätzlichen Ressourcen ausgestattet worden sind, verfügt der EDÖB bis auf Weiteres über die im DSG von 1993 vorgesehenen Empfehlungsbefugnisse und die gleichen Mittel wie 2005 (s. Kapitel 3.1 in diesem Bericht). Er wird weiterhin alles daran setzen, die betroffenen Schweizer Unternehmen bei der Anwendung der DSGVO mit Rat und Tat zu begleiten und als Aufsichtsbehörde eine auch im Ausland wahrnehmbare Präsenz zu entfalten. Letzteres ist bedeutsam mit Blick auf den Umstand, dass die Aufsichtsbehörden der EU-Mitgliedstaaten über neue und verstärkte Mechanismen zur Bündelung ihrer Aufsichtstätigkeit auch mit Blick auf die Datenbearbeitungen in Drittstaaten verfügen. Weiter ist zu beachten, dass die Institutionen der EU regelmässig evaluieren, inwiefern Drittstaaten wie die Schweiz einen mit dem EU-Niveau vergleichbaren Datenschutz aufweisen.

Die «Artikel 29»-Gruppe wird mit Inkrafttreten der DSGVO vom «Europäischen Datenschutzausschuss» abgelöst. Der EDÖB hat im ersten Semester 2018 mit dem Ausschuss Kontakt aufgenommen und einen Beobachterstatus verlangt. Kernaufgabe des Ausschusses wird sein, die einheitliche Anwendung der DSGVO sicherzustellen.

Swiss-US Privacy Shield

Im Berichtsjahr haben wir als Beobachter am ersten Review des EU-US Privacy Shields teilgenommen. Im Herbst 2018 werden wir das erste Review für das Swiss-US Privacy Shield durchführen, das im Anschluss an das zweite Review des EU-US Privacy Shields in Brüssel erfolgen wird. Dabei werden wir uns auch mit der EU koordinieren. Die Evaluation wird in enger zeitlicher und sachlicher Koordination mit der EU stattfinden (s. Kapitel 1.8 Swiss-US Privacy Shield in diesem Bericht).

IV Massnahmen zur Effizienzsteigerung

Aufgrund der erwähnten Herausforderungen bekräftigt der Beauftragte das strategische Ziel, seine gesetzlichen Aufgaben in der digitalen Realität fachkompetent, unabhängig und proaktiv wahrzunehmen.

Organisation und Geschäftskontrolle der Behörde

Die am 1. April 2017 in Kraft gesetzte Reorganisation der Behörde hat sich bewährt und wird konsolidiert. Besondere Beachtung verdient das Zusammenwirken der Mitarbeitenden in interdisziplinären Teams sowie deren fachliche Weiterbildung. Letztere kann aufgrund der hohen Geschäftslast nicht in jenem Umfang erfolgen, den der mit der Digitalisierung einhergehende technische Fortschritt nahe legt.

Der EDÖB nimmt seine gesetzlichen Aufgaben als Kontrollbehörde autonom wahr. Unterstützende logistische und administrative Leistungen bezieht er indessen von der Bundesverwaltung, welche diese nach Massgabe der allgemeinen Standards der Bundesverwaltung erbringt. In diesem Sinne wird der EDÖB von der Bundeskanzlei auch bei der Einführung des neuen Geschäftsverwaltungssystems Acta Nova betreut.

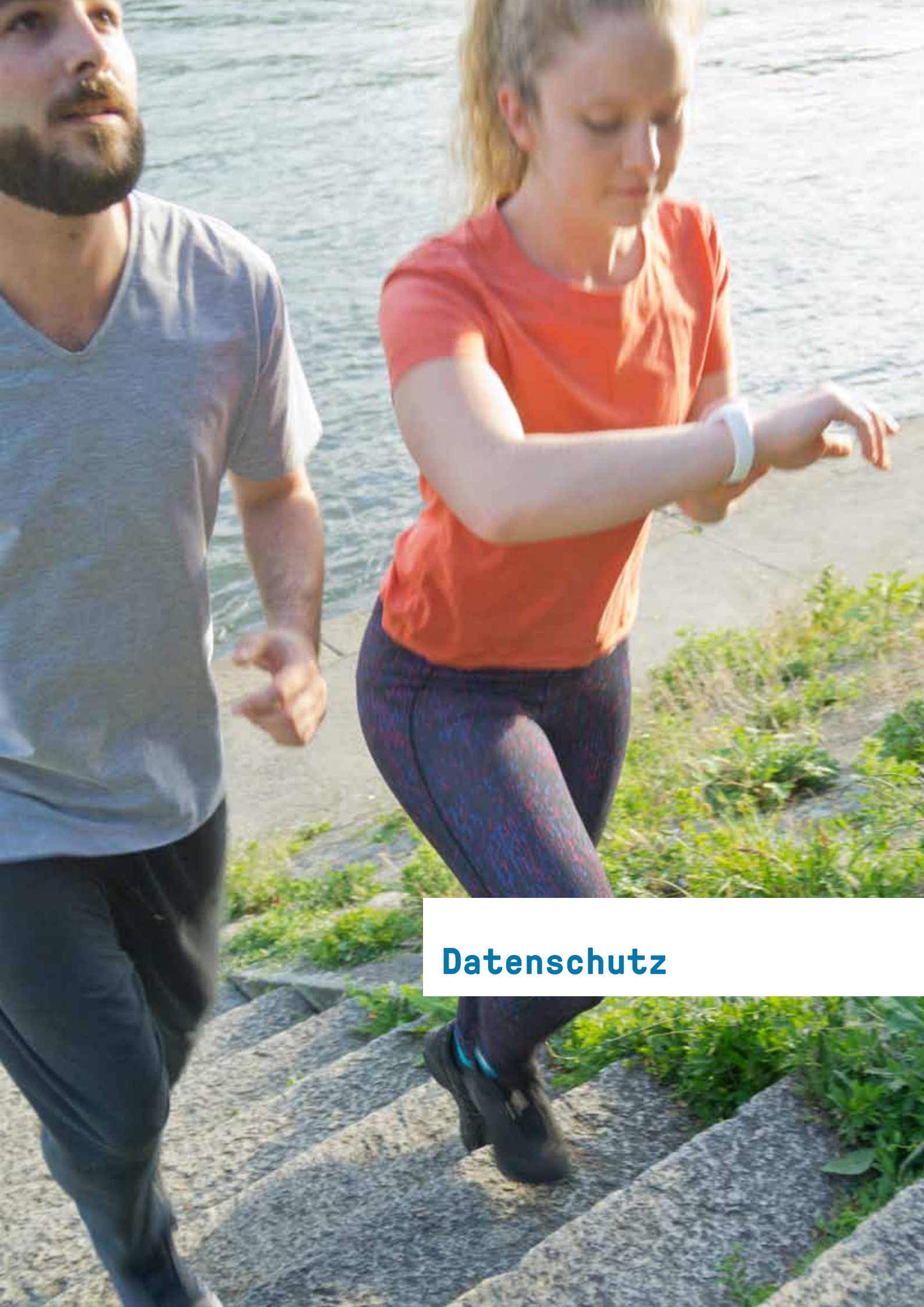
In der Berichtsperiode hat der EDÖB zudem mit «Cockpit» ein Instrument zur Priorisierung und Führung seiner Geschäfte in der Datenschutzaufsicht eingeführt, welches inskünftig auch über Acta Nova betrieben werden soll.

Informationsangebot

Das in der Berichtsperiode zusammen mit dem Geschäftsbericht erneuerte Informationsangebot soll weiter verbessert werden. Angesichts der hohen Geschäftslast haben sich diese Anpassungen verzögert.

Verfahren im Öffentlichkeitsgesetz (BGÖ)

Im Rahmen eines einjährigen Versuchs ist der EDÖB am 1. Januar 2017 zu einem beschleunigten und summarischen Verfahren übergegangen, das sich dadurch charakterisiert, dass in der Regel mündliche Schlichtungsverhandlungen durchgeführt werden. Nachdem sich dieser Versuch bewährt und zum angestrebten Abbau aller Pendenzen geführt hat, kann die neue Arbeitsmethode in den Dauerbetrieb überführt werden.



Datenschutz

1.1 Grundrechte und Datenschutzfragen allgemein

1.1.1 Revision des Bundesgesetzes über den Datenschutz

Am 15. September 2017 hat der Bundesrat die Botschaft zur Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz verabschiedet und an das Parlament überwiesen. Das Ziel der Revision besteht darin, den Datenschutz zu stärken, insbesondere indem die Transparenz der Datenbearbeitung erhöht wird und jede Person die sie betreffenden Daten besser kontrollieren kann.

Die Revision soll in unserem Recht die Grundlage schaffen, um:

- auf die Herausforderungen der Digitalisierung der Gesellschaft zu reagieren;
- die europäische «Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates» (Schengen-Besitzstand) zu übernehmen;
- sich den Anforderungen der «Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG» (Datenschutz-Grundverordnung) anzunähern;
- das überarbeitete Übereinkommen 108 zu ratifizieren.

Die Revision muss auch dazu beitragen, dass die Europäische Union die Angemessenheit des Schutzniveaus unseres Landes im Bereich Datenschutz weiterhin anerkennt.

Wie wir schon am Tag der Publikation der Botschaft (BBl 2017 6941) öffentlich mitgeteilt haben (s. dazu Mitteilung auf unserer Website), stimmen wir den Grundzügen der Revision zu.

Wir begrüssen die verbesserte Transparenz der Datenbearbeitung; die Informationspflicht zum Zeitpunkt der Beschaffung wird im privaten Bereich auf alle Bearbeitungen ausgedehnt, unabhängig von der Art der Daten. Wir begrüssen auch die Einführung der Pflicht zur Durchführung einer Datenschutzfolgenabschätzung für Projekte, die ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen darstellen. Positiv ist auch die Ausweitung der Pflicht, die betroffenen Personen über ihre Grundrechte wie bspw. das Auskunftsrecht zu informieren. Gleiches gilt für die Förderung der Selbstregulierung durch Verhaltenskodizes, die darauf abzielen, die Tätigkeit des Verantwortlichen zu erleichtern und zur Einhaltung der Vorschriften beizutragen. Zu erwähnen ist auch die explizite Einführung des Grundsatzes des Datenschutzes durch Technikgestaltung (Privacy by design) und datenschutzfreundliche Voreinstellungen (Privacy by default). Die Unabhängigkeit und Kompetenzen des EDÖB werden ebenfalls gestärkt. Der Gesetzesentwurf sieht vor, dass wir – wie unsere europäischen Amtskollegen – von Amtes wegen oder auf Anzeige hin gegenüber den Verantwortlichen und Auftragsbearbeitern eine Untersuchung eröffnen und beim Abschluss der Untersuchung eine Verfügung erlassen können. Es freut uns, dass der Bundesrat für die Umsetzung des neuen Gesetzes zusätzliche Mittel bereitstellen will, die dafür unbedingt nötig sind.

Während wir die Grundzüge der Revision befürworten, haben wir zum Entwurf des Bundesrats Vorbehalte geäussert betreffend die terminologischen und materiellen Abweichungen von der Datenschutz-Grundverordnung der EU und vom modernisierten Übereinkommen 108. Wir halten viele dieser Unterschiede für wenig sinnvoll, nicht zuletzt weil sie die Rechtslage der Schweizer Unternehmen und Behörden, die der Datenschutz-Grundverordnung direkt unterliegen, unnötig komplizieren und Rechtsunsicherheit schaffen.

Wir haben uns im Übrigen vergeblich für eine rasche Verabschiedung des Projekts eingesetzt. Die Staatspolitische Kommission des Nationalrats (SPK-N) hat beschlossen, die Revision aufzuteilen und zur Umsetzung der rechtlichen Änderungen des Schengen-Besitzstandes zunächst ein in seiner Geltung auf die Strafverfolgungsbehörden des Bundes beschränktes Datenschutzgesetz zu schaffen, was im April 2018 erfolgt ist. Aufgrund dieses Vorgehens wird dem Nationalrat als Erstrat in der Sommersession somit statt des totalrevidierten Gesetzes, diese vorgezogene Schengen-Vorlage unterbreitet werden.

Weiter hätten wir uns die Einführung des Rechts auf Portabilität von Personendaten gewünscht. Dieses Recht würde die Kontrolle der Nutzerinnen und Nutzer über ihre persönlichen Daten stärken. Wir befürworten die Einführung der Nachweispflicht, dass die Datenbearbeitung vorschriftsgemäss erfolgt ist, was eine Umkehr der Beweislast ermöglicht. Damit die Betroffenen ihre Rechte besser ausüben können, schlagen wir zudem vor, dass das neue Gesetz – wie die Datenschutz-Grundverordnung – ausdrücklich auch für Unternehmen gelten soll, die ihren Sitz nicht in der Schweiz haben, die aber Datenbearbeitungen mit Auswirkungen in der Schweiz vornehmen.

Dazu sollten solche Unternehmen in der Schweiz eine Ansprechperson haben. Das neue schweizerische Recht sollte für die Ernennung von Datenschutzverantwortlichen in Unternehmen die gleichen Voraussetzungen vorsehen wie die Datenschutz-Grundverordnung für Unternehmen, die direkt unter deren Bestimmungen fallen. Gleiches gilt für Verhaltenskodizes. Die schweizerischen Berufs- und Wirtschaftsverbände sollten uns diese nach den gleichen Regeln vorlegen, die sie nach der Datenschutz-Grundverordnung einzuhalten haben. Auch für Unternehmen mit einem Datenschutzverantwortlichen wäre es notwendig, sich an die Bestimmungen zur Durchführung von Datenschutz-Folgenabschätzungen zu halten. Bei besonders risikoreichen Datenbearbeitungen sollte ein Zertifizierungsverfahren durchgeführt werden.

Die vorgesehenen Bussen (bis höchstens 250'000 Franken) sind nicht sehr abschreckend im Vergleich mit denjenigen, die in der Datenschutz-Grundverordnung (bis 20 Millionen Euro oder 4 % des Jahresumsatzes) oder im Kartellgesetz vorgesehen sind. Gestützt auf Letzteres hat das Bundesgericht einen deutschen Automobilhersteller zur Bezahlung einer Busse von 157 Millionen Franken verurteilt. Wir empfehlen daher, das Sanktionssystem nochmals zu überdenken. Schliesslich sollte unser Budget nicht vom Bundesrat, sondern vom Parlament genehmigt werden, wie dies bei anderen unabhängigen Aufsichtsbehörden wie der Eidgenössischen Finanzkontrolle oder der neuen Aufsichtsbehörde über den Nachrichtendienst des Bundes der Fall ist.

Im April 2018 verabschiedete die SPK-N das neue Schengener Datenschutzgesetz, das dem Nationalrat in der Sommersession vorgelegt wird. Wir hoffen, dass damit die aufgeschobenen parlamentarischen Beratungen der Totalrevision des Datenschutzgesetzes nun rasch eingeleitet werden können.

1.1.2 Verwendung der AHV-Nummer als Personenidentifikator und Evaluation der Risiken

Der Bundesrat hat das Eidgenössische Departement des Innern (EDI) mit der Erstellung eines Gesetzesentwurfs beauftragt, um die Verwendung der AHV-Nummer auch ausserhalb der Sozialversicherungen durch alle Behörden des Bundes, der Kantone und der Gemeinden zu vereinfachen. Aufgrund eines vom EDÖB mit dem Bundesamt für Justiz (BJ) erteilten Mandats hat ETH-Professor David Basin Ende September 2017 mit Blick auf die Verwendung von Personenidentifikatoren und die geplante Weiterausbreitung der AHVN eine Analyse der datenschutzrechtlichen Risiken vorgelegt.

Zur Verbesserung der Effizienz von Administrativverfahren hat der Bundesrat das Eidgenössische Departement des Innern (EDI) am 1. Februar 2017 mit der Abfassung eines Gesetzesentwurfs beauftragt, um die Verwendung der AHV-Nummer auch ausserhalb der Sozialversicherungen durch alle Behörden des Bundes, der Kantone und der Gemeinden zu vereinfachen. Bei den entsprechenden Vorbereitungsarbeiten war eine interne Arbeitsgruppe der Bundesverwaltung nach Prüfung zum Schluss gekommen, dass die Verwendung der AHV-Nummer als Personenidentifikator keine besonderen Risiken mit sich bringe. Der EDÖB war in dieser Gruppe nicht vertreten, obwohl sich die Datenschutzbehörden von Bund und Kantonen in den vergangenen Jahren stets für sektorenspezifische Identifikatoren und gegen die Ausbreitung der AHV-Nummer ausserhalb des Sozialversicherungsbereichs aussprachen.

Das Parlament musste sich schon mehrfach zur Verwendung der AHV-Nummer als Personenidentifikator ausserhalb der Sozialversicherungen äussern, etwa beim elektronischen Patientendossier, dem Handelsregister oder dem automatischen Informationsaustausch in Steuersachen sowie gerade vor Kurzem bei der geplanten Revision des Grundbuchrechts.

Um einen tieferen Einblick in die spezifisch mit Personenidentifikatoren verbundenen Risiken zu gewinnen, haben wir zusammen mit dem Bundesamt für Justiz eine externe Risikoanalyse in Auftrag gegeben. Nach einem Einladungsverfahren wurde das Mandat an David Basin, Professor für Informationssicherheit am Departement Informatik der ETH Zürich vergeben. Das Gutachten sollte insbesondere aufzeigen, ob bestimmte Risiken auftauchen, ob diese von bestimmten Arten von Identifikatoren und allenfalls dem Ausmass ihrer Nutzung abhängig sind. In seiner Analyse der Risikofolgen vom 27. September 2017 (s. www.derbeauftragte, Datenschutz – Statistik, Register, Forschung – AHV-Nummer) präzisierte Professor Basin das Ausmass der Risiken, indem er in der Zusammenfassung u.a. Folgendes festhielt:

«Persönliche, oftmals sensitive, Daten sind in über 14 000 administrativen und organisatorischen Registern gespeichert und mit einem einheitlichen Identifikator, der AHVN13, indexiert. Die entsprechenden Computersysteme und die darin gespeicherten Daten sind anfällig für Attacken durch interne und externe Angreifer […]. Diese Datenschutzrisiken werden in Zukunft weiter zunehmen, da einerseits immer mehr Organisationen die AHVN13 für die Datenverarbeitung nutzen und andererseits immer mehr Daten gesammelt, gespeichert und verarbeitet werden, insbesondere in relativ unsicheren IT-Systemen von Kantons- und Gemeindeverwaltungen sowie Nichtregierungsorganisationen.

Da die Registerdaten zusammen mit den zugehörigen Identitätsattributen gespeichert sind, würde das alleinige Ersetzen der AHVN13-Nummern in einem Register durch sektorspezifische Identifikatoren oder andere Pseudonyme die Datenschutzrisiken nicht wesentlich reduzieren. […] Allerdings gibt es Alternativen zum gegenwärtigen Ansatz, welche Datenschutzrisiken erheblich reduzieren. Diese beinhalten eine Umstrukturierung der Verarbeitung, Speicherung und Absicherung der Registerdaten.

Die nachfolgend aufgeführten Massnahmen würden die aktuellen Datenschutzrisiken erheblich reduzieren, insbesondere jene Risiken, welche die kontinuierliche Ausweitung der gegenwärtigen Verwendungsweise der AHVN13 mit sich bringen: Einführung von nichtsprechenden Pseudonymen (wie Steuer- oder Krankenkassen-identifikationsnummern) in einer angemessenen Art und Weise. Hierfür können sektorspezifische Identifikatoren in verschiedenen Varianten verwendet werden. Es ist wichtig zu beachten, dass die Speicherung dieser Identifikatoren direkt zusammen mit anderen Identitätsattributen im gleichen Register minimiert wird […]».

Nachdem die Kommission für Rechtsfragen des Nationalrats dieses Dokument zur Kenntnis genommen hatte, reichte sie am 20. Oktober 2017 ein Postulat ein, das den Bundesrat beauftragte, innerhalb der laufenden Legislatur in einem Konzept aufzuzeigen, wie den Risiken begegnet werden kann, die mit der Verwendung der dreizehnstelligen AHV-Nummer (AHVN13) als einziger Personenidentifikationsnummer verbunden sind. Zudem ist aufzuzeigen, wie der Datenschutz bei der Verwendung von Personenidentifikationsnummern durch Kantone, Gemeinden und Dritte verbessert werden kann. Dabei ist die Beurteilung des EDÖB zu berücksichtigen. Der Bundesrat hat das Postulat am 20. Dezember 2017 angenommen.

Es ist nun Aufgabe des Bundesrates und der Bundesverwaltung, auf Bundesebene die Konsequenzen aus dieser eingehenden Risikoanalyse zu ziehen. Zudem erwarten wir, dass das Bundesamt für Sozialversicherung (BSV) auf Grundlage der genannten Analyse darlegt, welche Schlussfolgerungen aus der beantragten generellen Verwendung der AHV-Versichertennummer im Rahmen seines Entwurfs zur Revision des Bundesgesetzes über die Alters- und Hinterlassenenversicherung (AHVG) zu ziehen sind.

Wir werden diese Entwicklungen weiterhin aufmerksam verfolgen und erwarten, dass die Bundesverwaltung mit Blick auf die Verwendung von Personenidentifikatoren Lösungen formulieren wird, welche sowohl dem berechtigten Anliegen nach Verwaltungseffizienz als auch den Anforderungen des Datenschutzes und der Datensicherheit angemessen Rechnung tragen. Angesichts der Tatsache, dass sich im Rahmen von bedeutenden digitalen Vorhaben im Zusammenhang mit der elektronischen Identität verwandte Problematiken stellen, sollten diese Lösungen möglichst bald erfolgen (s. Kapitel 1.3.3 des vorliegenden Berichts).

Der Bericht zur Risikofolgenabschätzung findet sich auf unserer Website unter folgender Adresse: www.derbeauftragte.ch, Datenschutz – Statistik, Register, Forschung – AHV-Nummer.

1.1.3 Einsatz von Online-Kampagnentools

Online-Kampagnentools erlauben es politischen Gruppierungen und Interessenverbänden, persönliche Kontakte digital zu organisieren und gezielt auf Interaktionen auszurichten. Da sich deren Einsatz zunehmender Beliebtheit erfreut, haben wir dazu ein datenschutzrechtliches Merkblatt publiziert.

Im Berichtsjahr haben wir aufgrund von Anfragen von Medienschaffenden und politischen Parteien datenschutzrechtliche Erläuterungen für den Einsatz von digitalen Kampagnentools erarbeitet. Bei diesen Tools handelt es sich um Applikationen, die es politischen Gruppierungen und Interessensverbänden erlauben, bestimmte Aktionen in ihre Webseitenumgebung zu integrieren. Das mit dem Ziel, die Kampagnen-Planung und -Durchführung gezielt auf Interaktionen mit bestimmten Personengruppen auszurichten. Grundlage dazu bilden Daten von interessierten Personen, welche sich zum Beispiel auf der Webseite einer Partei registriert haben.

Von datenschutzrechtlicher Relevanz sind beim Einsatz von digitalen Kampagnentools insbesondere die Grundsätze der Transparenz und der Zweckbindung. Wir haben zunächst darauf hingewiesen, dass die betroffenen Personen vor der Registrierung vollständig und verständlich über die Datenbearbeitung informiert werden müssen. Diese darf erst erfolgen, wenn die Nutzer auf Basis dieser Informationen ausdrücklich und selbstbestimmt zugestimmt haben. Das bedeutet auch, dass die Betroffenen jederzeit die Möglichkeit haben müssen, ihre einmal erteilte Einwilligung zu widerrufen. Nach dem Zweckbindungsgrundsatz dürfen politische Gruppierungen und Interessensverbände Daten mit solchen Tools nur zu den Zwecken bearbeiten, für die eine Einwilligung vorliegt. Weiter ist zu beachten, dass eine allfällige Anreicherung der personenbezogenen Daten mit Informationen aus weiteren Quellen wie z. B. Social Media Plattformen eine separate Einwilligung der betroffenen Personen voraussetzt.

Unser Merkblatt findet sich unter www.derbeauftragte.ch, Datenschutz – Dokumentation – Merkblätter.

1.2 Verkehr

1.2.1 Projekte im Öffentlichen Verkehr

Die Transportbranche, insbesondere die SBB, haben uns im Berichtsjahr über mehrere datenschutzrelevante Projekte informiert. Bei diesen handelte es sich zum einen um den Einsatz von Körperkameras (Bodycams) und zum anderen um die Entwicklung neuer Apps. Die datenschutzrechtliche Analyse dieser Vorhaben erfolgte jeweils vorgängig durch den Datenschutzberater der SBB.

Wir haben auch im aktuellen Berichtsjahr einen Schwerpunkt unserer Beratungstätigkeit bei der Transportbranche gesetzt. Im Unterschied zur formellen Sachverhaltsabklärung beschränkt sich die beratende Projektbegleitung in der Regel auf summarische Einschätzungen, die es ermöglichen sollen, datenschutzrechtliche Anliegen frühzeitig einzubringen (vgl. dazu auch 24. Tätigkeitsbericht 2016/2017, Ziff. 1.2.3). Die Geschäftsleitung der SBB stellte uns verschiedene Projekte vor, die dann auf technischer Ebene weiter begleitet wurden. Um unsere knappen Ressourcen gezielt einzusetzen, wirkten wir darauf hin, dass uns die Projekte und die damit verbundenen datenschutzrechtlichen Fragestellungen erst nach einer Vorprüfung durch den Unternehmensdatenschutz der SBB unterbreitet wurden.

Unter den von uns begleiteten Vorhaben befand sich der Pilotversuch, bei welchem die SBB den Einsatz von Bodycams getestet haben. Dabei handelt es sich um Video- und Audioaufnahmegeräte, die direkt von Mitarbeitenden der Transportpolizei am Körper getragen werden. Dieses Projekt befindet sich noch in der Evaluationsphase. Die SBB informierten uns auch über ihren Umgang mit Kundendaten und die Entwicklung verschiedener Apps, insbesondere auch der «SwissPass Mobile»-App. Wir haben im Rahmen dieser Begleitung auf datenschutzrechtliche Probleme hingewiesen und gehen davon aus, dass unsere Anliegen bei der weiteren Projektarbeit umgesetzt werden. Wir werden die Transportbranche weiterhin begleiten und insbesondere darauf hinwirken, dass alle Personen, die dies wünschen, die Möglichkeit behalten, anonym zu reisen, ohne dafür besondere Tarifzuschläge in Kauf nehmen zu müssen.

1.2.2 Bearbeitung von Fahrzeugdaten

Die digitale Entwicklung führt zu umfangreichen Datenbearbeitungen in Fahrzeugen. Wir haben einen Autohersteller beraten, der unsere Hinweise umsetzen wird.

Die digitale Entwicklung bietet der Autobranche enormes Potenzial. Daten in Fahrzeugen werden in immer grösserem Umfang erhoben, verknüpft und an Dritte weitergeleitet. Verschiedene Datenschutzbehörden haben deshalb in letzter Zeit bewährte Verfahren (Best Practices) entwickelt, so zum Beispiel die Konferenz der unabhängigen Datenschutzbehörden Deutschlands und der Verband der Automobilindustrie.

Wir untersuchten im Berichtsjahr die Bearbeitung von Fahrzeugdaten eines Automobilherstellers. Dabei legten wir den Fokus auf transparente Information des Fahrzeughalters, die Datenübermittlung ins Ausland und ausdrückliche Einwilligungserklärungen. Der Automobilhersteller hat unsere Hinweise entgegengenommen und umgesetzt.

1.2.3 Strassenverkehr: Einführung eines intelligenten Fahrtenschreibers

Wir haben zu den rechtlichen Grundlagen, mit denen ein intelligenter Fahrtenschreiber eingeführt werden soll, Stellung genommen. Wir kritisierten die mangelhafte Information über Datenzugriffe und die fehlende Vorschrift über die Aufbewahrungsdauer von polizeilich erhobenen Daten.

Wir wurden in der Ämterkonsultation betreffend die Einführung eines neuen Fahrschreibers um eine Stellungnahme aus datenschutzrechtlicher Sicht gebeten. Mit der Vorlage soll das Schweizer Recht in verschiedenen Verordnungen an europäische Vorgaben angepasst werden. Mit dem intelligenten Fahrtenschreiber wird die Erhebung von Daten wesentlich vereinfacht. Er ist mit einem globalen Satellitensystem verbunden und erfasst deshalb u.a. den genauen Standort des Fahrzeuges. Verschiedene Stellen, wie der Arbeitgeber des Chauffeurs oder die Polizei, können auf erfasste Daten zugreifen. Wir wiesen in unserer Stellungnahme darauf hin, dass die Fahrzeugführenden besser über diese Datenzugriffe von Dritten informiert werden müssen, um dem Prinzip der Transparenz zu genügen. Weiter kritisierten wir die fehlende Regelung der Aufbewahrungsdauer von Daten, die von der Polizei durch Fahrtenschreiber erhoben werden. Die entsprechende EU-Verordnung sieht eine Speicherdauer von drei Stunden vor, falls ein Fahrzeug nicht kontrolliert wird oder keine Manipulation oder Missbrauch des Fahrtenschreibers festgestellt wird. Wir baten darum, entsprechende Vorgaben in die Strassenverkehrskontrollverordnung aufzunehmen.

1.3 Internet und Telekommunikation

1.3.1 Smart-TV

Wir haben bei einem Hersteller von Smart-TV-Geräten ein Verfahren eröffnet, um die bei ihm anfallenden Bearbeitungen von Nutzerdaten auf ihre Datenschutzkonformität hin zu überprüfen.

Fernsehgeräte mit Computer-Zusatzfunktionen (sogenannte Smart-TV) erfreuen sich immer grösserer Beliebtheit. Sie bieten dem Nutzer ein erweitertes Fernseherlebnis, indem Sie Zugriff auf Online-Inhalte von TV-Stationen, App-Anbietern und TV-Herstellern ermöglichen. Dabei sind sich die Nutzer oft zu wenig bewusst, dass hierzu ein Datenaustausch stattfindet und ihre Daten den Anbietern solcher Inhalte übermittelt werden.

Aufgrund von Bürgeranfragen haben wir eine Sachverhaltsabklärung bei einem Hersteller von Smart-TV-Geräten eröffnet. Unser Fokus liegt dabei bei den Fragen, welche Daten über die TV-Nutzer durch die Gerätehersteller bearbeitet werden, wie die Nutzer darüber informiert werden und ob diese Datenbearbeitungen für die Nutzer freiwillig erfolgen.

Wir sind zurzeit daran, die diesbezüglichen Ausführungen des Geräteherstellers zu analysieren.

1.3.2 Datendiebstahl bei Swisscom

Swisscom hat uns Ende Dezember 2017 über einen missbräuchlichen Datenzugriff informiert. Betroffen sind rund 800'000 Kundinnen und Kunden.

Swisscom hat uns Ende Dezember 2017 darüber in Kenntnis gesetzt, dass im vorangehenden Herbst unberechtigte Zugriffe auf die Kontaktdaten von rund 800'000 Kundinnen und Kunden erfolgt sind. Betroffen sind vorwiegend private Inhaber von Mobil-Nummern und einige Festnetzkunden bzw. deren Name, Vorname, Adresse, Geburtsdatum und Telefonnummer. Der missbräuchliche Zugriff auf die Kundenkontaktdaten der Swisscom war über die Zugriffsberechtigungen eines Vertriebspartners erfolgt. Wir haben die Swisscom in der Folge mit Blick auf die laufende Einschätzung und Minderung der Folgerisiken wie auch die Wahrung der Informationsrechte ihrer Kunden beraten. Nachdem die Swisscom die nötigen Sachverhaltsklärungen und Schutzmassnahmen getroffen sowie ihre Kunden Anfang Februar 2018 über das Datenleck informiert hatte, konnte der EDÖB den Fall ohne Einleitung formeller Schritte abschliessen.

Nachdem uns wenig später von dritter Seite ein angeblich unberechtigter Zugriff auf weitere Daten eines Kunden gemeldet worden ist, sahen wir uns veranlasst, die Swisscom formell dazu aufzufordern, zu diesem konkreten Ereignis Stellung zu nehmen und uns zudem über das Risiko allfälliger Folgeschäden des Datenlecks ausführlich zu dokumentieren. Unmittelbar nach Empfang dieser Aufforderung hat uns die Swisscom dargelegt, dass sich der befürchtete Kausalzusammenhang zwischen dem gemeldeten Ereignis und dem Datenleck nicht erhärtet hat. Die zusätzlich verlangte Dokumentation wird vom EDÖB ausgewertet.

1.3.3 Aufbau eines elektronischen Identitätsnachweises (E-ID)

Mit der Schaffung einer elektronischen Identität (E-ID) soll in erster Linie die Rechtssicherheit im digitalen Verkehr gestärkt werden. Wir verfolgten dieses Grossvorhaben einerseits im Rahmen der Vernehmlassung zur gesetzlichen Grundlage. Andererseits begleiten wir zwei private Initiativen.

Die aktuelle Konzeption für eine elektronische Identität geht von einer Aufgabenteilung zwischen Staat und Privaten aus, die im Rahmen der Vernehmlassung zum Entwurf des Bundesgesetzes über staatlich anerkannte elektronische Identifizierungsmittel (E-ID-Gesetz) intensiv diskutiert wurde. Wir haben zum Entwurf Stellung genommen, datenschutzrechtliche Hinweise formuliert und werden die Arbeiten an der Gesetzesvorlage weiterverfolgen.

Bereits vor Abschluss der gesetzlichen Grundlage für eine E-ID präsentierten uns im Berichtsjahr zwei Konglomerate privater Unternehmen umfangreiche Konzepte zum Identitätsprovider nach dem geplanten Gesetz, denen unsere Behörde grundsätzlich konstruktiv-kritisch gegenübersteht.

In den zahlreichen Sitzungen mit den Firmen haben wir auf die Arbeitsinstrumente hingewiesen, die dazu dienen, die Risiken von digitalen Grossapplikationen und deren mögliche Folgen für die Persönlichkeitsrechte der betroffenen Personen bereits in der Konzeptphase detailliert abzuklären. Die von uns beratenen Unternehmen sind sich des Weiteren im Klaren, dass sie auch konkrete Massnahmen zur Vermeidung von Eingriffen in die informationelle Selbstbestimmung der Betroffenen vorsehen müssen.

Neben der Risikofolgenabschätzung sind für die Konzepte zur Herausgabe einer E-ID weitere datenschutzrechtliche Anforderungen zu beachten. So darf weder ein direkter noch indirekter Zwang zum Erwerb und Gebrauch einer E-ID ausgeübt werden. Vielmehr sollen nebst Online-Registrierungen (sog. Sign-In-Prozessen) Lösungen offen stehen, die den Zugang zu Informationen und Dienstleistungen ohne administrative Schikanen oder ökonomische Nachteile auf analogem Weg ermöglichen. Beim Zugang über ein Online-Sign-In unter Verwendung der E-ID sollen nicht mehr personenbezogene Daten preisgegeben werden müssen, als beim analogen Zugang zu vergleichbaren Informationen und Dienstleistungen. Besteht für die Dienstleistung oder die Informationen keine Notwendigkeit zur Identifizierung der Person, wie z.B. für Bahnreisen, muss der Zugang dazu weiterhin anonym möglich bleiben. Weiter verlangen wir, dass alle Aspekte der mit dem E-ID-Konzept verbundenen Datenbearbeitungen und die aktuellen regulatorischen Vorgaben und Nutzungsbestimmungen, auf denen sie beruhen, in verständlicher Form publik gemacht werden müssen.

Die technischen und organisatorischen Massnahmen müssen darauf ausgerichtet werden, dass eine missbräuchliche Verwendung der Daten ausgeschlossen wird. Es ist insbesondere sicherzustellen, dass keiner der beteiligten Akteure über mehr Informationen verfügt, als er zur Erfüllung seiner Teilaufgabe im arbeitsteiligen Gesamtsystem benötigt.

Diese Massnahmen und deren Wirkung müssen von den Unternehmen ausführlich dokumentiert und beschrieben werden. Die Dokumentation ist Voraussetzung dafür, dass unsere Behörde die entsprechenden Projekte im Rahmen ihrer Beratungstätigkeit mit interdisziplinären Teams von Juristen und Informatikern begleiten kann. Alle Akteure, mit denen wir im Gespräch sind, haben dieses Vorgehen begrüsst.

1.3.4 Bundesgerichtsurteil zum Auskunftsrecht zu den Randdaten

Das Bundesgericht hat die Position des EDÖB bezüglich des Auskunftsrechts zu den Randdaten des Fernmeldeverkehrs bestätigt. Die Fernmeldedienstanbieter müssen bei Auskunftsgesuchen alle Angaben, die sich auf die gesuchstellende Person beziehen beziehungsweise ihr zugeordnet werden können, herausgeben.

Mit dem Urteil vom 2. März 2018 (1C_598/2016) hat das Bundesgericht eine Beschwerde von sechs Privatpersonen im Zusammenhang mit der Speicherung und Aufbewahrung von Randdaten der Telekommunikation abgewiesen. Im selben Urteil hat es das Auskunftsrecht als verfahrensrechtliche Garantie zum Schutz vor unsachgemässen Datenbearbeitungen bestätigt.

Das Auskunftsrecht zu den Randdaten, welche durch Fernmeldedienstanbieter gespeichert werden, beschäftigt den EDÖB bereits seit längerer Zeit. Wir haben festgestellt, dass die Fernmeldeanbieter die Auskunft über diejenigen Randdaten verweigern, welche nicht für die Rechnungsstellung verwendet werden. In diesem Zusammenhang haben wir den Fernmeldedienstanbietern mehrfach kundgetan, dass das Auskunftsrecht alle Randdaten umfasst und nicht auf die Daten für die Rechnungsstellung beschränkt ist. Mit dem Wissen um das laufende Verfahren, welches nun abgeschlossen werden konnte, haben wir damals auf eine separate gerichtliche Überprüfung verzichtet. Im Rahmen der Vernehmlassung konnten wir unsere Position darlegen. Diese wurde nun durch das vorliegende Urteil des Bundesgerichts bestätigt.

Das Auskunftsrecht unterstützt die in der Bundesverfassung niedergelegten Grundrechte und ist damit ein zentrales Element der informationellen Selbstbestimmung. In diesem Sinne dient es der Durchsetzung des Persönlichkeitsschutzes, indem es den betroffenen Personen ermöglichen soll, die über sie in einer Datensammlung bearbeiteten Daten zu kontrollieren mit dem Ziel, die Einhaltung der datenschutzrechtlichen Grundsätze und Bestimmungen zu überprüfen und gegebenenfalls durchzusetzen.

Die Fernmeldedienstanbieter befürchten, dass die Gesuchsteller durch das Auskunftsrecht sensible Informationen über andere Benutzer ihrer Fernmeldeanschlüsse erhalten könnten. Das Bundesgericht hält fest, dass Auskunftsbegehren rechtsmissbräuchlich sind, welche einzig zum Zweck gestellt werden, eine andere Person auszuforschen. Ein solches Gebaren verdiene von vornherein keinen Rechtsschutz, weil es eine zweckwidrige Verwendung des Auskunftsrechts darstelle. Der befürchteten Missbrauchsgefahr kann weitgehend mittels geeigneter, auf das jeweilige Kommunikationsmittel (Fixnet, Internet, Mobile) abgestimmter Authentifizierungsmassnahmen zur Eruierung des Benutzers eines Fernmeldeanschlusses begegnet werden.

1.4 Justiz, Polizei, Sicherheit

1.4.1 Überwachung des Post- und Fernmeldeverkehrs-Revision der Ausführungserlasse

Während des Ämterkonsultationsverfahrens haben wir zu den revidierten Verordnungen zum Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs Stellung genommen. Diese regeln die Datenbearbeitungen des Dienstes Überwachung Post- und Fernmeldeverkehr (ÜPF) und führen die von den Fernmeldedienstanbietern zu liefernden Daten detailliert auf.

Im März 2016 verabschiedete das Parlament das totalrevidierte Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF). Nachfolgend mussten auch die Ausführungserlasse totalrevidiert werden. Wir haben erstmals 2016 zu den Entwürfen Stellung genommen (vgl. 24. Tätigkeitsbericht 2016/2017, Ziffer 1.4.2). Nach dem Vernehmlassungsverfahren blieben unberücksichtigte Differenzen bestehen, so dass wir eine erneute Stellungnahme abgaben. Diese befasste sich mit der Speicherung der Ziel-IP-Adresse und Ziel-Portnummer bei Internetzugängen mit Network Address Translation (NAT), dem Antennensuchlauf und den Kopfschaltungen beim E-Mail.

Wir forderten eine klare Regelung, welche festlegt, dass die Identifizierung des Anschlussinhabers bei der Verwendung von Carrier-grade NAT (Netzwerkadressübersetzung auf Betreiber-Ebene; cgNAT) auf Ebene der Dienstanbieterin nicht über die Speicherung der Verbindungsziele erfolgt. Mittels cgNAT werden den Teilnehmenden im Netz der Zugangsanbieterin private, nur innerhalb dieses Netzes gültige IP-Adressen zugeteilt. Diese werden bei Internet-Zugriffen an den Netzgrenzen der Zugangsanbieterin zum Internet in eine gemeinsame öffentliche Quell-IP-Adresse übersetzt (viele Teilnehmende teilen sich gleichzeitig eine öffentliche IP-Adresse). Die Unterscheidung der vielen einzelnen Internetverbindungen erfolgt mittels Port-Nummern. Diese Adressübersetzung muss für jedes eingehende und ausgehende IP-Paket durchgeführt werden. Bei nichtdeterministischen Verfahren führt das Gerät (Router) Zuordnungstabellen und speichert für jede Internetverbindung (Kontext) den Zeitstempel, die Quelle und das Ziel der Verbindung (jeweils IP-Adresse und Portnummer), die zugehörige private IP-Adresse und Portnummer des Teilnehmenden sowie die Art des Transportprotokolls. Wir schlugen vor, dass die Verordnung die Verwendung von deterministischen NAT-Verfahren vorschreibt, welche Adressen und Portnummern mit einem Algorithmus übersetzen, so dass später wieder eine Zurückrechnung möglich ist. Damit würde die Notwendigkeit der Speicherung der IP-Adressen und Portnummern der einzelnen Verbindungsziele durch die Zugangsanbieterin für die Zwecke der Teilnehmeridentifikation entfallen. Unserer Forderung wurde nur soweit entsprochen, dass in den Erläuterungen ausgeführt wird, dass aus datenschutzrechtlicher Sicht Verfahren zu implementieren sind, bei denen die Speicherung der Verbindungsziele nicht erforderlich und daher zu unterlassen ist.

Gemäss der Verordnung können für eine bestimmte Mobilzelle bzw. einen WLAN-Zugangspunkt Antennensuchläufe über einen Zeitraum von bis zu zwei Stunden beantragt werden. Eines unserer Anliegen war die Limitierung der Antennensuchläufe auf Mobilfunkzellen. Ein anderes war, dass bei Antennensuchläufen nur die von den Strafverfolgern beantragte Schnittmenge an Verdächtigen übermittelt werden soll. Dies hatten wir bereits in der Ämterkonsultation zum Bundesgesetz ausgeführt. 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, im Extremfall sogar zur gesetzlich nicht vorgesehenen Rasterfahndung. Unsere Forderungen wurden nicht berücksichtigt, so dass die Zwangsmassnahmengerichte bei der Prüfung der Verhältnismässigkeit von Antennensuchläufen nur Einfluss auf die Dauer und die Anzahl der Zellen nehmen können, nicht jedoch auf den Umfang der anfallenden Daten mittels der Festlegung einer Schnittmenge.

Bei den Ausführungsbestimmungen zu den Kopfschaltungen wurde der Geltungsbereich auch auf die E-Mail-Kommunikation ausgedehnt. Hierbei handelt es sich um die Überwachung des E-Mail-Verkehrs zwischen dem Kunden einer E-Mail-Anbieterin und einer nicht durch diese verwaltete «fremde» E-Mail-Adresse. Je nach technischer Umsetzung kann dieses Instrument anstelle der gesetzlich vorgesehen Auskünfte zu den Randdaten zu einer gesetzeswidrigen Inhaltsüberwachung führen. Wir forderten, dass klar bestimmt wird, wie dieser Überwachungstyp ausgeführt werden muss. Dies erfolgte in den Erläuterungen und nicht direkt in der Verordnung. So wurde bei der E-Mail-»Kopfschaltung» festgehalten, dass nur Mail-Server-Operationen wie die Sende- und Empfangsvorgänge von E-Mails erlaubt sind, nicht aber Zugriffe auf die «fremde» Mailbox. Zudem darf die Auswertung nur über die Adressierungselemente im SMTP-Envelop (technische Daten bei der E-Mail-Übermittlung) erfolgen.

Da die Verordnungen inhaltlich sehr technisch sind und wie bereits ausgeführt nicht alles spezifizieren, wurden auch die Erläuterungen zu den einzelnen Ausführungserlassen publiziert. Dies entspricht dem von uns gewünschten Vorgehen zur Verbesserung des Verständnisses der einzelnen Bestimmungen.

1.4.2 Gesichtserkennung am Flughafen

Das Grenzwachtkorps plant, am Flughafen Genf die automatische Passkontrolle samt Gesichtserkennung einzuführen und die dazu erforderlichen Geräte zu betreiben.

Am Flughafen Zürich wurde im Berichtsjahr der Betrieb der automatischen Passkontrolle samt Gesichtserkennung getestet. Dieser von der Flughafenpolizei Zürich durchgeführte Testbetrieb fiel in die Zuständigkeit des Datenschutzbeauftragten des Kantons Zürich. Das Grenzwachtkorps plant, die gleichen Geräte ab Mitte 2018 am Flughafen Genf zu betreiben. Wir haben mit dem Grenzwachtkorps Kontakt aufgenommen, um über das Projekt informiert zu werden. Wir werden das Projekt weiterverfolgen und sicherstellen, dass dabei das Datenschutzrecht eingehalten wird.

1.4.3 Bundesgesetz über Vorläuferstoffe für explosionsfähige Stoffe und Bundesgesetz über polizeiliche Massnahmen zur Bekämpfung von Terrorismus

Im Rahmen der Ämterkonsultation sowie anlässlich einer Sitzung mit der Direktion des Bundesamts für Polizei fedpol hatten wir viele kritische Bemerkungen zu den beiden im Titel genannten Gesetzesentwürfen. Fedpol hat einen Teil unserer Kommentare berücksichtigt.

Unsere Anmerkungen zum Entwurf für ein Bundesgesetz über Vorläuferstoffe für explosionsfähige Stoffe wurden von fedpol mit einer einzigen Ausnahme berücksichtigt. Die Ausnahme bezieht sich auf die Verwendung der AHV-Nummer (AHVN13). Daher haben wir fedpol ersucht, im Vorschlag zuhanden des Bundesrates folgende Divergenz zu dokumentieren: «Solange der Bundesrat nicht in einem Konzept aufzeigt, wie den Risiken begegnet werden kann, die mit der Verwendung der dreizehnstelligen AHV-Nummer (AHVN13) als einziger Personenidentifikationsnummer verbunden sind, und wie der Datenschutz bei der Verwendung von Personenidentifikationsnummern verbessert werden kann (vgl. Postulat 17.3968 der Kommission für Rechtsfragen des Nationalrats), spricht sich der EDÖB gegen jegliche Nutzung der AHVN13 ausserhalb des Sozialversicherungsbereichs aus. Er ist der Ansicht, dass im vorliegenden Gesetzesentwurf auf eine Behandlung der AHVN13 verzichtet werden sollte.»

Die Divergenzen mit fedpol sind im Falle des Bundesgesetzes über polizeiliche Massnahmen zur Bekämpfung von Terrorismus deutlich ausgeprägter:

Das Polizeirecht des Bundes wird in verschiedenen Gesetzen geregelt, was eine Gesamtsicht der verschiedenen Bearbeitungen von Personendaten erschwert. Der vorliegende Entwurf verschärft die Komplexität der Lage. Daher fordern wir die Ausarbeitung eines Gesetzes über die Tätigkeit der Polizeiorgane des Bundes analog zu den bestehenden kantonalen Gesetzen. Ferner ist nicht klar, in welchem Informationssystem oder -subsystem die Daten im Zusammenhang mit den polizeilichen Massnahmen zur Bekämpfung von Terrorismus verarbeitet werden sollen.

Der Entwurf sieht neue Online-Zugangsmöglichkeiten für das Staatssekretariat für Migration (SEM) und die Grenzwachtkorps innerhalb von bestimmten Informationssystemen von fedpol vor. Diese Zugangsmöglichkeiten beziehen sich auf Daten der Kriminalpolizei oder Daten im Zusammenhang mit der Analyse von Delikten. Diese Daten sind äusserst sensibel und teilweise auch noch nicht erhärtet. Der Zugang zu solchen Daten durch die Migrations- und Grenzkontrollbehörden sollte im Rahmen der Amtshilfe erfolgen, nicht online. So könnte fedpol die Verbreitung dieser Daten auf das notwendige Mass beschränken.

Abschliessend haben wir auf die Notwendigkeit hingewiesen, die Zuständigkeitsbereiche der SBB Transportpolizei festzulegen, bevor ihr Zugang zum Fahndungssystem der Polizei (RIPOL) gewährt wird.

1.4.4 Arbeitsgruppe Revision DNA-Profil-Gesetz

Wir haben uns an der Arbeitsgruppe Revision DNA-Profil-Gesetz beteiligt. In diesem Zusammenhang haben wir darauf hingewiesen, dass unseres Erachtens der Nutzen einer Anpassung des DNA-Profil-Gesetzes nicht gegeben ist.

Die Arbeitsgruppe befasste sich mit drei Hauptthemen: Beim ersten Thema geht es um die Schaffung der gesetzlichen Grundlagen für eine gezielte behördliche Verfolgung der Täter bei schweren Gewalttaten wie Mord oder Vergewaltigung mittels DNA-Sequenzanalyse, um persönliche Merkmale zu identifizieren. Wir haben darauf hingewiesen, dass Sequenzanalysen grundsätzlich in einem strikten rechtlichen Rahmen zu erfolgen haben (Beschränkung auf Sonderfälle und Anordnung durch ein Gericht).

Das zweite Thema betrifft die Beurteilung der unterschiedlichen Speicherungsfristen von DNA-Profilen. Wir sind der Ansicht, dass die bestehenden Rechtsvorschriften verhältnismässig sind und den Anforderungen der Strafverfolgung mit ihren differenzierten und ausgewogenen Löschungsfristen ausreichend Rechnung tragen. Der Gedanke einer einheitlichen Aufbewahrungsfrist für DNA-Profile verstösst gegen den Grundsatz der Verhältnismässigkeit und trägt den besonderen Anforderungen des Jugendstrafrechts nicht Rechnung. Ein System mit zwei verschiedenen Fristen, d.h. einer langen und einer kurzen Frist, könnte allenfalls eine Lösung des Problems darstellen.

Das dritte Thema betrifft andere Fragen, bei denen eine Gesetzesrevision erforderlich ist, etwa die Aufbewahrungsdauer von biologischem Material in Laboratorien oder die Verwandtenrecherche. Mit letzterer werden mit dem mutmasslichen Täter verwandte Personen einzig aufgrund ihrer Verwandtschaft in ein Verfahren verwickelt. Das Gesetz erlaubt es den Strafbehörden nicht ausdrücklich, DNA-Profile in einer DNA-Profil-Datenbank zu vergleichen, um Profile nahe bei demjenigen eines mutmasslichen Straftäters zu finden. Die Verwandtenrecherche steht zudem in einem Spannungsverhältnis zum Recht auf Aussageverweigerung im Sinne von Artikel 168 ff. der Schweizerischen Strafprozessordnung. Falls der Gesetzgeber derartige Recherchen zulassen will, sind Vorschriften mit klar definierten Eingriffskriterien nötig. Im Rahmen der Revision des DNA-Profil-Gesetzes sind in diesem Fall auch die Verwandtenrecherchen einzubeziehen. Wir werden darauf hinwirken, dass eine allfällige Regulierung den allgemeinen Datenschutzgrundsätzen und insbesondere dem Grundsatz der Verhältnismässigkeit Rechnung trägt. Verwandtenrecherchen dürfen nur bei besonders schweren Straftaten und ausschliesslich als letztes Mittel (ergebnislose Recherchen in den schweizerischen und ausländischen Datenbanken) eingesetzt werden.

1.4.5 Schengenzusammenarbeit

Im Jahr 2017 nahmen wir an den Sitzungen der Aufsichtskoordinationsgruppen SIS II, VIS und Eurdoac teil. Auch an den Sitzungen der Arbeitsgruppe «Border, Travel & Law Enforcement Subgroup» (BTLE), die von der Datenschutzgruppe der Europäischen Union («Artikel 29») eingesetzt wurde, waren wir vertreten. Schliesslich fand im Februar/März 2018 die Schengen-Evaluation der Schweiz statt.

Aufsichtskoordinationsgruppen über die Informationssysteme SIS II, VIS und Eurodac

Auch in diesem Jahr nahmen wir an den Sitzungen der drei Aufsichtsgruppen teil. Diese fanden jeweils nacheinander im Juni sowie im November 2017 in Brüssel statt. Zusammenfassungen der Sitzungen, Tätigkeitsberichte und weitere Informationen zu diesen Gruppen können unter www.sis2scg.eu; www.visscg.eu; www.eurodacscg.eu auf Englisch, Französisch und Deutsch abgerufen werden. Seit November 2017 haben wir den Vorsitz der Aufsichtskoordinationsgruppe VIS inne. Das Sekretariat wird durch den Europäischen Datenschutzbeauftragten geführt.

Arbeitsgruppe «Border, Travel & Law Enforcement»

Im Berichtsjahr haben wir an fünf Sitzungen der Arbeitsgruppe teilgenommen, bei denen u.a. die Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten durch Polizei und Strafverfolgungsbehörden (EU-Richtlinie 216/680) und das Review des EU-US Privacy Shield besprochen wurden. Die erwähnte Richtlinie birgt für die Umsetzung in innerstaatliches Recht einige Herausforderungen aus datenschutzrechtlicher Sicht. Ausführlich diskutiert wurde insbesondere, welche Behörden in deren Anwendungsbereich fallen und wie die Abgrenzung zur Datenschutzgrundverordnung zu erfolgen hat. Die Arbeitsgruppe «Artikel 29» hat, gestützt auf diese Vorarbeiten, zum Jahresende eine Empfehlung (Opinion) unter http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610178 veröffentlicht. Auch die Vorbereitung und Auswertung des ersten Reviews des EU-US Privacy Shields wurde ausführlich diskutiert. Wir haben diese Arbeiten eng verfolgt und nahmen am Review als Beobachter teil (siehe Ziffer 1.8.1 des vorliegenden Berichts). Sowohl die EU-Kommission (siehe http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=605619) als auch die Gruppe «Artikel 29» (siehe http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610114) haben je einen Bericht dazu veröffentlicht. Beide Gremien begrüssen darin die verstärkte Zusammenarbeit mit den amerikanischen Behörden. Im kommerziellen Bereich wurde u.a. die noch mangelnde

eigenständige Kontrolltätigkeit der amerikanischen Partner kritisiert. Im Bereich der nationalen Sicherheit wurden die Nichtbesetzung von vakanten Stellen, die schwer nachvollziehbaren gesetzlichen Grundlagen und die teils ungenügende Zusammenarbeit der verschiedenen Kontrollbehörden angesprochen.

Schengen-Evaluation der Schweiz im Bereich Datenschutz

Im Jahr 2018 wurde die Umsetzung und Anwendung des Schengen-Besitzstands durch die Schweiz als assoziiertes Mitglied zum dritten Mal überprüft. Die Evaluierung, die spätestens alle fünf Jahre durchgeführt wird, betrifft sämtliche Bereiche der Schengener Zusammenarbeit: Management der Aussengrenze (Flughäfen), Rückkehr/Rückführung, Schengener Informationssystem SIS II/SIRENE, gemeinsame Visapolitik, polizeiliche Zusammenarbeit und Bearbeitung personenbezogener Daten. Zwischen dem 26. Februar und dem 23. März 2018 führten Sachverständige der Schengen-Staaten und der Europäischen Kommission mehrere Ortsbesichtigungen durch, darunter bei unserer Behörde und beim Kanton Luzern. Die Teams waren zusammengesetzt aus Sachverständigen der Schengen-Staaten und der Europäischen Kommission. Die Erkenntnisse aus der Evaluierung können in allfällige, an die Schweiz gerichtete Empfehlungen münden. Die Arbeiten zur Vorbereitung und Durchführung der Evaluierung wurden vom Bundesamt für Justiz (BJ) in Zusammenarbeit mit der Direktion für Europäische Angelegenheiten (DEA) koordiniert. Dabei wirkten wir aktiv an den Arbeiten für die Schengen-Evaluation in Sachen Datenschutz mit.

Die Schengener Zusammenarbeit basiert auf gegenseitigem Vertrauen und gegenseitiger Unterstützung. Ein gut funktionierender, effizienter Evaluierungsmechanismus, der Verbesserungsmöglichkeiten in der Umsetzung und Anwendung des Schengen-Besitzstandes aufzeigt, ist daher im Interesse aller Schengen-Staaten.

1.4.6 Schengenvisa-Kontrolle im Staatssekretariat für Migration

Im Jahr 2017 haben wir die Datenbearbeitungen beim Staatssekretariat für Migration (SEM) in Zusammenhang mit Schengenvisa überprüft sowie eine Kontrolle vor Ort durchgeführt.

Die Datenschutzbehörden der Schengen-Mitgliedstaaten sind gemäss EU-Recht verpflichtet, mindestens alle vier Jahre die Datenbearbeitungen ihrer nationalen Behörden betreffend Schengenvisa zu überprüfen. 2017 haben wir das SEM kontrolliert. Dabei überprüften wir die Datenbearbeitungen im Schweizer Visainformationssystem (ORBIS) und die Datenübermittlung über die nationale Schnittstelle N-VIS vom und ans zentrale Visa-Informationssystem der EU (C-VIS). Unsere Sachverhaltsabklärung beschränkte sich auf Schengenvisa. Nicht geprüft wurde der Zugriff durch die Strafverfolgungsbehörden. Wir befragten das SEM vorgängig zur Zugriffserteilung, der Ausbildung der zugriffsberechtigten Personen, den Datenbearbeitungen, den Rechten der betroffenen Personen sowie zur Sicherheit und der Datenaufbewahrung. Zudem führten wir im Herbst 2017 eine Kontrolle vor Ort durch. Zum Zeitpunkt der Redaktion dieses Berichtes war unsere Sachverhaltsabklärung noch nicht abgeschlossen.

1.4.7 Umsetzung Schengen: Kontrolle der Ausschreibungen beim SEM

Im Rahmen der Schengen-Assoziierungsabkommen haben wir beim SEM als Endbenutzer des Schengener Informationssystems (SIS) eine Kontrolle der Ausschreibungen zwecks Einreise- oder Aufenthaltsverweigerung durchgeführt.

Diese Kontrolle sollte insbesondere überprüfen, ob das SEM die geltenden datenschutzrechtlichen Anforderungen betreffend die Einführung der Ausschreibungen gemäss Artikel 24 der Verordnung SIS II (Voraussetzungen für Ausschreibungen zur Einreise- oder Aufenthaltsverweigerung), die Anwendung von Artikel 25 des Schengener Durchführungsübereinkommens (SDÜ) (Aufenthaltstitel und Ausschreibung zur Einreiseverweigerung) sowie der schweizerischen Umsetzungsvorschriften (insbesondere das Bundesgesetz über die polizeilichen Informationssysteme des Bundes [BPI]) und die Verordnung über den nationalen Teil des Schengener Informationssystems (N-SIS) und das SIRENE-Büro (N-SIS-Verordnung) einhält.

Wegen der Bedeutung und des Umfangs der Verarbeitungen von personenbezogenen Daten im Schweizer SIS haben wir uns bei der Kontrolle auf die im SIS durchgeführten Datenverarbeitungen konzentriert, spezifisch auf die Ausschreibungen auf der Basis des Ausländergesetz (AuG) (Aufenthaltstitel und Ausschreibung zur Einreiseverweigerung) und die Nutzung des SIS durch das SEM. Die Kontrolle betraf hingegen nicht die Zugriffe und die Datenverarbeitungen durch das Bundesamt für Polizei (fedpol) sowie das SIRENE-Büro oder die kantonalen Behörden, die der Aufsicht der kantonalen Datenschutzbeauftragten unterstehen.

Wir haben dem SEM zuerst einen Fragebogen zukommen lassen und die erhaltenen Unterlagen anschliessend analysiert. Ausserdem haben wir eine Kontrolle vor Ort durchgeführt, die verschiedene Punkte umfasste. Dies erlaubte uns zu sehen, wie die Mitarbeitenden des SEM auf die SIS-Daten zugreifen, welches Vorgehen bei den Ausschreibungen zwecks Einreise- oder Aufenthaltsverweigerung angewandt wird und welche Prozesse eingeführt wurden für Fälle, bei denen eine rechtswidrige Verarbeitung vorliegt oder in denen die Daten im SIS offensichtlich unrichtig sind. Wir haben auch die Profile der SEM-Mitarbeitenden überprüft, die eine SIS-Zugangsberechtigung haben. Die Protokolldateien wurden bei dieser Kontrolle nicht überprüft. In einer nächsten Kontrolle beim SEM sowie bei anderen Benutzern auf Bundesebene soll der Fokus aber darauf gelegt werden. Wir haben fedpol gebeten, uns weitere Angaben zu den SIS-Datenverarbeitungen zu liefern.

Wir sind zum Schluss gelangt, dass die in der Schweiz durchgeführten Datenverarbeitungen die Bestimmungen der Verordnung SIS II, des SDÜ3 sowie der schweizerischen Umsetzungsvorschriften erfüllen. Wir mussten folglich auch keine Empfehlung aussprechen.

1.5 Gesundheit und Forschung

1.5.1 Elektronisches Patientendossier

Die Umsetzung des elektronischen Patientendossiers schreitet voran. Der Bedarf an datenschutzrechtlicher Beratung und Information ist hoch und beansprucht erhebliche Ressourcen bei unserer Behörde.

Im Berichtsjahr nahmen der Beauftragte und seine Mitarbeiter an Podiumsdiskussionen zum elektronischen Patientendossier teil, hielten Präsentationen bei Verbänden und Unternehmen, wurden von politischen Gremien angehört, berieten Betreiber von Stammgemeinschaften, führten Gespräche mit kantonalen Datenschutzbehörden und beantworteten zahlreiche Bürgeranfragen zum Thema. Diese Tätigkeiten haben unsere Behörde stark in Anspruch genommen. Das Spektrum der Beratung geht von einfachen Auskünften zur freien Einwilligung bis zu anspruchsvollen Erläuterungen z.B. im Bereich der Labormedizin. Letztere setzen vertiefte Kenntnisse des Gesundheitswesens voraus, über die nur einzelne spezialisierte Mitarbeitende verfügen. Auch in den weiteren Projektphasen sind diese gefordert und werden mit dem Start der Produktivphase mit den Kontrollaktivitäten beginnen (voraussichtlich ab 2020).

1.5.2 Statistikprojekt BAGSAN

Die Anonymität der Versicherten hat im Projekt BAGSAN des Bundesamtes für Gesundheit (BAG) höchste Priorität. Im Rahmen der Begleitung des Projekts haben wir konkrete Vorschläge zur Minimierung der Risiken von Re-Identifizierungen und des internen Datenmissbrauchs eingebracht.

Das auf Individualdatensätzen der Krankenversicherer basierende Statistikprojekt BAGSAN wird vom BAG betrieben. Aufgrund der Erkenntnisse aus den ersten Datenerhebungen haben wir weitere Massnahmen zur Verringerung des Risikos von Re-Identifizierungen angeregt. Damit die Daten von unserer Behörde als anonymisiert betrachtet werden und nicht mehr als Personendaten gemäss Datenschutzgesetz gelten, darf eine Re-Identifizierung nur noch mit unverhältnismässig hohem Aufwand möglich sein. Weiter haben wir Massnahmen vorgeschlagen, die das Risiko senken, dass Personen mit umfassenden Zugriffs- und Bearbeitungsrechten Daten missbrauchen könnten. Man spricht in der Praxis auch vom «Administratorenproblem». Wir haben vorgeschlagen, die Rechte auf mehrere Personen zu verteilen, die zeitgleich handeln müssen, damit das System die Zugriffsberechtigung erteilt. Unsere Vorschläge wurden durch das BAG positiv aufgenommen. Für die geplanten weiteren Projektphasen mit umfassenderen Datensätzen zu jeder versicherten Person wurde aufgrund der politischen Diskussion ein Marschhalt beschlossen. Gemäss einer angenommenen parlamentarischen Initiative sollen die Krankenversicherer keine Individualdatensätze für den Zweck von BAGSAN liefern. Die vom BAG konsultierten Versicherer liefern deshalb bis auf Weiteres keine erweiterten Datensätze. Im Rahmen der politischen Beurteilung des Projekts BAGSAN beraten wir auch die zuständigen parlamentarischen Kommissionen, was erhebliche juristische und technische Ressourcen bindet.

1.5.3 Mehr Transparenz für Patienten beim Outsourcing von Arztrechnungen

Die Dienstleister Swisscom Health und die Ärztekasse wurden von uns dazu aufgefordert, die Patientinnen und Patienten auf ihren Internetseiten transparenter zu informieren.

Die Dienstleister Ärztekasse und Swisscom Health bearbeiten im Rahmen der Rechnungsstellung und des Forderungsmanagements grosse Mengen an Patientendaten. Es handelt sich um administrative Daten der medizinischen Leistungserbringer und der Patienten, sowie um Gesundheitsdaten, die für das Erstellen der Rechnung benötigt werden. Damit sich die betroffenen Patientinnen und Patienten informieren können, wie ihre Daten bearbeitet werden, forderten wir beide Unternehmen dazu auf, auf ihren Internetseiten die Musterverträge, die Produkteverträge, die Allgemeinen Geschäftsbedingungen und die Bearbeitungsreglemente in den aktuellen Versionen aufzuschalten. Beide Unternehmen reagierten positiv auf die Aufforderung: Die Ärztekasse hat die geforderten Informationen in einer neuen Rubrik «Patienteninfo» publiziert. Swisscom Health legte uns ein Umsetzungskonzept vor und hat erste Informationen auf ihrer Website aufgeschaltet. Die Transparenz bei beauftragten Dienstleistern ist wichtig, da sie zunehmend in der Position der bestimmenden Partei stehen. Wie auch andere Beispiele belegen, verlieren die Auftraggeber zunehmend die Möglichkeit zur Mitgestaltung der vertraglichen Beziehung und damit die Herrschaft über die Datenbearbeitung. Wie der Fall EOS zeigt (vgl. Kap. 1.8.2 des vorliegenden Berichts), ist gerade im medizinischen Bereich zu betonen, dass den Leistungserbringern als Auftraggebern die volle Verantwortung für Datenschutz- und Datensicherheit beim Dienstleister zukommt.

1.5.4 Neue einheitliche Tarifstruktur TARPSY: Ausweitung des Anwendungsbereichs der Datenannahmestellen

Seit dem 1. Januar 2018 kommt bei Behandlungen in der stationären Psychiatrie die Tarifstruktur TARPSY zur Anwendung. Es ist neu vorgesehen, dass die nach TARPSY ausgestellten Rechnungen analog den SwissDRG-Rechnungen die Datenannahmestelle der Krankenversicherung durchlaufen.

Mit der neuen Tarifstruktur TARPSY sollen sämtliche stationär vollzogenen psychiatrischen Behandlungen mittels leistungsbezogenen Fallpauschalen abgegolten werden, so wie dies bereits seit längerem bei stationären akutsomatischen Spitalleistungen gemäss dem Rechnungsformat SwissDRG der Fall ist. Es ist vorgesehen, dass die Leistungserbringer im Bereich der stationären Psychiatrie die TARPSY-Rechnungen analog den SwissDRG-Rechnungen neu ebenfalls an die zertifizierte Datenannahmestelle der jeweiligen Krankenversicherung übermitteln müssen, was eine Ausweitung des Anwendungsbereichs der Datenannahmestellen auf diesen neuen Rechnungstypus bedeutet. Wir werden die diesbezügliche Umsetzung bei den Versicherungen auf ihre Korrektheit hin kontrollieren.

1.5.5 Die SUVA gibt Versichertendaten zu Forschungszwecken weiter

Die Schweizerische Unfallversicherung SUVA verwendet Versichertendaten für Forschungsprojekte und gibt sie zu Forschungszwecken mitunter auch an Dritte weiter. Die durchgeführte Vorabklärung hat gezeigt, dass die SUVA im Zusammenhang mit der Information der Versicherten und deren Ausübung des Widerspruchsrechts Verbesserungen vornehmen muss.

Im März 2017 wies uns ein Arzt darauf hin, dass die SUVA offenbar Daten ihrer Versicherten Dritten für Forschungsprojekte zur Verfügung stellt. Die Betroffenen haben die Möglichkeit, der Verwendung ihrer Daten zu widersprechen und werden über dieses Widerspruchsrecht (in der Terminologie der SUVA «Vetorecht») durch den jeweiligen behandelnden Arzt informiert. Eine Broschüre mit Informationen zum Vetorecht liegt auch in Rehabilitationskliniken und den Agenturen der SUVA auf, dürfte aber nur von einer Minderheit der Versicherten zur Kenntnis genommen werden. Auf der Website ist das Dokument ebenfalls zu finden, allerdings unter der Rubrik «Arztinformationen», die sich an ärztliches Fachpersonal richtet.

Die SUVA legte uns anlässlich eines Treffens detailliert dar, wie sie Unterstützungsgesuche für interne und externe Forschungsprojekte prüft und wie die Versicherten ihr Widerspruchsrecht ausüben können. In der Regel unterstützt die SUVA die Projekte finanziell; zur Verwendung oder Herausgabe von Versichertendaten komme es bei den unterstützten Forschungsprojekten relativ selten. In aller Regel würden die Daten vor einer Herausgabe zudem anonymisiert. Genetische Daten seien bislang nicht betroffen gewesen.

Nach unserer Auffassung besteht bei der SUVA im Bereich der Versicherteninformation Verbesserungsbedarf. Dies sowohl in Bezug auf den Inhalt der Information als auch auf die Art, wie die Informationen über das Widerspruchsrecht verbreitet werden. Der Mehrheit der Versicherten ist der Umstand, dass mit ihren Daten Forschung betrieben werden kann, nicht bekannt, obwohl der behandelnde Arzt darüber informieren sollte. Entsprechend wird ihnen auch nicht bewusst sein, dass sie ein Widerspruchsrecht geltend machen können.

Es muss klar kommuniziert werden, dass Versichertendaten für Forschungszwecke verwendet werden können. Die Informationen müssen derart bereitgestellt werden, dass sie leicht auffindbar sind. Daneben sollte nach unserer Einschätzung auch der interne Prozess zur Anonymisierung der Daten verbessert werden.

Die SUVA hat uns zugesagt, die notwendigen Anpassungen im ersten Quartal 2018 umzusetzen und hat uns ein entsprechendes Konzept zur Prüfung vorgelegt.

1.6 Versicherungen

1.6.1 Vollmachten im Bereich der Krankentaggeldversicherungen

Die von den Krankentaggeldversicherern verwendeten Vollmachten verärgern oder verunsichern oftmals die erkrankten Personen. Zahlreiche Personen wollen deshalb von uns wissen, ob diese Vollmachten zulässig sind.
Krankentaggeldversicherungen dienen den Arbeitgebern zur Absicherung des Risikos der Lohnzahlungspflicht gegenüber Mitarbeitenden, die längerfristig wegen Krankheit ausfallen. Tritt der Krankheitsfall ein, muss der Versicherer seine Leistungspflicht und deren Umfang abklären. Da zahlreiche Stellen und Personen, die über die notwendigen Informationen verfügen, durch gesetzliche oder vertragliche Geheimhaltungspflichten zur Verschwiegenheit verpflichtet sind, holt sich der Versicherer mit einer Vollmacht das Recht ein, die notwendigen Informationen zu erhalten. Das Ausmass der Vollmacht ist für die betroffenen Personen oft nicht nachvollziehbar, da sich ihnen nicht erschliesst, wieso sie alle behandelnden Ärzte, Spitäler, alle übrigen Versicherer, den Arbeitgeber, die Sozialdienste oder die Steuerverwaltung zur Auskunftserteilung ermächtigen sollen. Zudem ist ihnen auch nicht immer bewusst, dass sie aufgrund der gesetzlichen Schadenminderungspflicht zur Erteilung der Vollmacht verpflichtet sind. Aus datenschutzrechtlicher Sicht ist entscheidend, dass sich die Vollmacht auf ein konkretes Ereignis und auf Informationen, die für dieses Ereignis relevant sind, beschränkt. Es darf sich nicht um eine Blankovollmacht handeln. Zudem müssen auch die vom Versicherer angefragten Stellen bei einer Datenbekanntgabe den Grundsatz der Verhältnismässigkeit beachten. Sie dürfen nur Informationen an den Versicherer übermitteln, die im konkreten Fall relevant sind. Unsere Erläuterungen zum Thema befinden sich auf unserer Webseite unter: www.derbeauftragte.ch, Datenschutz – Versicherungen – Kranken- und Unfallversicherungen – Vollmachten.

1.6.2 Informationssystem zur Bekämpfung von Versicherungsbetrug

Wir beraten den Schweizerischen Versicherungsverband beim Aufbau eines zentralen Informationssystems zur Bekämpfung von Versicherungsbetrug.
Für den Aufbau dieses Systems werden Experten aus Deutschland beigezogen, die dort das Hinweis- und Informationssystem der deutschen Versicherungswirtschaft aufgebaut haben und betreiben. Wir beraten sowohl den Verband als auch die Experten in Fragen des Datenschutzes und der Datensicherheit.

1.6.3 Auslagerung von Aufgaben der Krankenversicherungen an branchenfremde Dienstleister

Im Krankenversicherungsbereich findet zunehmend eine Auslagerung von Aufgaben an branchenfremde Dienstleister statt, die zuvor von den Krankenversicherungen selber ausgeführt wurden. Wir haben einen Fall untersucht, bei dem der Auftragnehmer die Korrespondenz zwischen Versicherten und ihrer Krankenversicherung geöffnet und weiterverarbeitet hat.
Im Krankenversicherungsbereich herrscht zusehends ein Trend hin zum Outsourcing von klassischen Tätigkeiten der Krankenversicherungen an Dritte, deren Kerngeschäft nicht unbedingt im Gesundheitsbereich liegt. Die Krankenversicherungen versprechen sich davon offenbar Effizienzsteigerungen im Sinne einer Kostensenkung und Zeitersparnis.

Wir wurden auf einen Fall aufmerksam, bei dem die EGK Gesundheitskasse das Öffnen, Scannen und Digitalisieren von Briefen an die Schweizerische Post bzw. deren Tochtergesellschaft Swiss Post Solutions auslagerte. Die Verarbeitung von Versicherten-Korrespondenz durch eine zwischengeschaltete Firma, die in der Öffentlichkeit noch nicht als Dienstleisterin im Gesundheitsbereich wahrgenommen wird, sorgte bei etlichen Versicherten für Irritation. Sie warf auch Fragen betreffend die Einhaltung der datenschutzrechtlichen Vorgaben auf. Deshalb führten wir im Berichtsjahr bei der EGK Gesundheitskasse eine Vorabklärung durch. Unsere Untersuchung hat gezeigt, dass die delegierte Bearbeitung der Briefpost der Versicherten sorgfältig erfolgt und das Post- bzw. Schriftgeheimnis wie auch die zeitgemässen Standards der Datensicherheit eingehalten werden. Ferner informierte die EGK Gesundheitskasse ihre Versicherten offen und transparent über die Umstellungen in der Postverarbeitung. Somit konnten wir aus datenschutzrechtlicher Sicht keine Unregelmässigkeiten feststellen.

1.6.4 Gesundheitsapps und Bonusprogramme der Krankenversicherungen

Während des Berichtsjahres wurden wir auf mehrere Gesundheitsapps und Bonusprogramme von Krankenversicherungen aufmerksam. Wir prüften, ob die Versicherten ihre Gesundheitsdaten den Versicherungen freiwillig zur Verfügung stellen und die Vorgaben des Datenschutzes und der Datensicherheit eingehalten werden. Gegenüber der Helsana Krankenkasse haben wir eine formelle Sachverhaltsabklärung des Bonusprogramms «Helsana+» durchgeführt.

Während des Berichtsjahres statteten wir bei mehreren Versicherungen Besuche ab, um uns über neu entwickelte Bonusprogramme und Gesundheitsapps mit ihren dazugehörigen Plattformen aus erster Hand zu informieren sowie uns diese vorführen und erklären zu lassen.

Zu den geprüften Angeboten gehörten die von der CSS Versicherung angebotene Gesundheitsapp «myStep» und das Bonusprogramm «Benevita» der SWICA. Gemeinsam ist diesen Produkten, dass die Krankenkassen ihre Versicherten für eine gesunde und aktive Lebensweise mit Prämiennachlässen bei den Zusatzversicherungen belohnen. Bei «myStep» werden die Versicherten durch einen elektronischen Schrittzähler zu mehr Bewegung im Alltag ermutigt, wobei die gemachten Schritte in ihrem myStep-Konto gespeichert und auf dem myCSS-Portal eingesehen werden können. Die Versicherten erhalten eine «Schrittentschädigung», die über das Gesundheitskonto ausbezahlt werden kann. Die so erhobenen Schrittdaten dürfen jedoch nicht an Dritte weitergegeben werden. Das Bonusprogramm «Benevita» der SWICA belohnt ebenfalls Bewegung, wobei den Versicherten über die «Benevita Gesundheitsplattform» eine Vielzahl von Gesundheitsdienstleistungen wie individuelle Gesundheitstipps und Coaching durch Experten angeboten werden. Die Versicherten können Bonuspunkte sammeln und so ihre Prämien in den Zusatzversicherungen senken. Auch hier werden die Gesundheitsdaten nicht an Dritte, etwa für Werbezwecke, weitergegeben.

Im Oktober 2017 haben wir gegenüber der Helsana Krankenkasse eine formelle Sachverhaltsabklärung eröffnet. Dabei ging es u.a. darum festzustellen, ob im Rahmen des Bonusprogramms «Helsana+» Personendaten aus der Grundversicherung der Versicherten bearbeitet werden, da es sich um das erste Bonusprogramm handelt, das auch Versicherten zugänglich ist, die nur über eine Grundversicherung verfügen. Nach Abschluss der Sachverhaltsabklärung haben wir der Helsana Zusatzversicherungen AG infolge Fehlens der vom DSG verlangten gesetzlichen Grundlage empfohlen, die Bearbeitung von Grundversicherungsdaten zu unterlassen sowie die Bearbeitung von Daten von Kunden, die bei der Helsana ausschliesslich grundversichert sind, zur Bemessung und Ausrichtung geldwerter Rückerstattungen einzustellen (siehe dazu unsere Medienmitteilung und Empfehlung).

1.7 Arbeitsbereich

1.7.1 Sachverhaltsabklärung eRecruiting abgeschlossen

Im Rahmen der Sachverhaltsabklärung eRecruiting konnte mit dem Nachrichtendienst des Bundes eine Lösung für die Aufbewahrung und Löschung von Informationen aus elektronischen Bewerbungsdossiers gefunden werden.

Auch beim Nachrichtendienst des Bundes (NDB) kann man sich auf offene Stellen elektronisch bewerben. Im Rahmen einer Sachverhaltsabklärung stellten wir fest, dass die Praxis des NDB in Bezug auf die Aufbewahrung und Löschung von Bewerbungsdossiers teilweise nicht den gesetzlichen Vorgaben entsprach. Unter Einbezug des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport (VBS) konnte eine einvernehmliche Lösung gefunden werden, die sowohl die speziellen Bedürfnisse des Nachrichtendienstes als auch den Persönlichkeitsschutz der Bewerbenden berücksichtigt.

1.7.2 Der «saubere Abgang» bei Kündigung der Arbeitsstelle

Arbeitgeber sollten im Sinne der Transparenz den Umgang des Personals mit Informatikmitteln in einem Reglement festlegen und darin aufzeigen, wer welche Rechte und Pflichten hat. Dies verhindert Konflikte während und nach Beendigung des Arbeitsverhältnisses und erleichtert ein geordnetes Verlassen des Arbeitsplatzes.

Wir erhielten zahlreiche schriftliche und mündliche Anfragen von Arbeitnehmern und Arbeitgebern zur Frage, wie bei Verlassen der Arbeitsstelle in Bezug auf die Sperrung von Informatikmitteln wie personalisiertem E-Mail-Account oder Serverzugang rechtlich korrekt vorzugehen ist: Was muss bei der Sperrung des E-Mail-Kontos beachtet werden? Bis wann muss eine Sperrung des Serverzugangs und der Passwörter erfolgen? Was gilt für private Daten des Arbeitnehmers wie privaten E-Mails, Fotos und Texten etc.?

Wir empfahlen den Rechtssuchenden, die anwendbaren Grundsätze in einem betriebsinternen Reglement über die Nutzung von Informatikmitteln festzuhalten und der Belegschaft so zugänglich zu machen und durch Schulungen zu vertiefen. Zusammenfassend empfehlen wir folgendes Vorgehen:

- Vor dem Austritt soll der Arbeitnehmer die noch laufenden Geschäfte und E-Mails an die vom Arbeitgeber bezeichnete Person übergeben und quittieren.
- Der austretende Mitarbeiter erhält die Möglichkeit, seine privaten E-Mails und andere Dokumente auf privaten Datenträgern wie zum Beispiel USB-Sticks zu speichern und von den Servern des Arbeitgebers zu löschen.
- Spätestens am letzten Arbeitstag werden das E-Mail-Konto des austretenden Mitarbeiters sowie alle anderen EDV-Konten gesperrt und nach einer gewissen Zeit gelöscht.
- Im einem Todesfall wird das E-Mail-Konto des Verstorbenen sofort gesperrt und die Daten werden gesichert. Anschliessend sollten die privaten E-Mails und sonstigen privaten Daten des Verstorbenen unter Beizug von dessen Angehörigen nach dem Vier-Augen-Prinzip ausgesondert werden.
- Absender, die E-Mails an die gesperrte Adresse senden, werden automatisch informiert, dass die Empfängeradresse hinfällig geworden ist. In der automatischen Antwort wird eine geeignete Ersatz-E-Mail-Adresse der Firma angegeben. Es erfolgt keine automatische Weiterleitung an eine andere E-Mail-Adresse des Unternehmens.

Die Beachtung dieser Grundsätze trägt wesentlich dazu bei, dass die Privatsphäre und Geschäftsgeheimnisse der Vertragspartner gewahrt bleiben.

1.7.3 Tracking von Mitarbeitenden

Navigationsgeräte in Geschäftsfahrzeugen und andere Geräte mit GPS-Funktion scheinen immer häufiger zur Überwachung von Mitarbeitenden eingesetzt zu werden. Wir erhielten im Berichtsjahr mehrere Anfragen von Betroffenen. Diese Art der Überwachung ist nur zulässig, wenn sowohl die Rahmenbedingungen des Datenschutzrechts als auch des Arbeitsrechts berücksichtigt werden.

Über unsere Hotline wandten sich mehrere Personen an uns, die sich bei der Arbeit mit einer Überwachung durch Navigationsgeräte und sonstige Ortungssysteme konfrontiert sahen. Zumeist waren es Aussendienstmitarbeitende, deren Geschäftsfahrzeuge mit Navigationsgeräten ausgerüstet werden sollten oder bereits entsprechend bestückt waren. Auch Smartphones können zur Ortung eingesetzt werden.

Ein Arbeitgeber kann ein berechtigtes Interesse daran haben, seine Mitarbeitenden, beziehungsweise deren Fahrzeuge zu lokalisieren, beispielsweise um Einsätze der Aussendienstmitarbeitenden effizienter zu planen oder um den tatsächliche Zeitaufwand eines Einsatzes bei einem Kunden zu erfassen. Wichtig ist, dass er die betroffenen Mitarbeiter umfassend über die eingesetzten Technologien sowie seine Interessen und die Zwecke informiert, die er mit der Bearbeitung der gesammelten Daten erreichen will. Die Bearbeitung ist zulässig, sofern die Grundsätze der Rechtmässigkeit, Zweckgebundenheit, Verhältnismässigkeit, Transparenz und von Treu und Glauben eingehalten werden. Dabei muss der Arbeitgeber vor allem darauf achten, dass sich die Bearbeitung auf Daten beschränkt, die für die Abwicklung des Arbeitsverhältnisses oder für den Geschäftszweck tatsächlich relevant sind. Vor diesem Hintergrund dürfen die technischen Möglichkeiten, weitere Informationen, wie die gewählte Route oder die Geschwindigkeit der Firmenfahrzeuge zu erheben, nicht unbesehen ausgeschöpft werden.

Einer besonderen Rechtfertigung bedarf auch die Überwachung in Echtzeit und nach Arbeitsende: Eine Echtzeitlokalisierung kann auf eine profilbildende Verhaltensüberwachung hinauslaufen, welche eine Persönlichkeitsverletzung darstellt. Diese Art der Überwachung ist auch durch das Arbeitsrecht untersagt, wenn die Interessen des Arbeitgebers ebenso durch weniger einschneidende Massnahmen erreicht werden können.

Für eine Überwachung von Geschäftsautos und geschäftlichen Mobiltelefonen, die auch privat benutzt werden dürfen, besteht nach Arbeitsende in aller Regel keine gesetzliche Grundlage. Deshalb muss sichergestellt werden, dass der Arbeitgeber nach Arbeitsende keinen Zugriff mehr auf die Ortungsdaten hat.

1.7.4 Arbeitszeiterfassung per Fingerabdruck in der Gastronomie

Biometrische Zeiterfassungs- und Zutrittssysteme werden immer häufiger auch in der Gastronomie eingesetzt. Weil Daten wie Fingerabdrücke als besonders schützenswert einzustufen sind, sollte ihr Einsatz sorgfältig und restriktiv erfolgen.

Biometrische Zeiterfassungs-, Zutritts- oder Kassensysteme, bei denen die Mitarbeitenden sich mit ihrem Fingerabdruck identifizieren müssen, sind weit verbreitet – so auch in der Gastronomie. Teilweise wird sogar der Abschluss oder die Weiterführung eines Arbeitsvertrags davon abhängig gemacht, dass die Arbeitnehmerin oder der Arbeitnehmer mit der Erfassung ihres Fingerabdrucks einverstanden ist. Mehrere Betroffene haben sich deshalb im Berichtsjahr über die Hotline an uns gewandt.

Biometrische Daten wie Fingerabdrücke sind untrennbar mit einer Person verbunden und können bei Verlust nicht einfach ersetzt werden. Im Umgang mit solch sensiblen Daten gelten deshalb erhöhte Sicherheitsanforderungen. Insbesondere dürfen sie nur bearbeitet werden, soweit dies für den vorgesehenen Zweck erforderlich ist. Um zu verhindern, dass biometrische Daten der Mitarbeitenden an unberechtigte Dritte gelangen, sollten die Daten nicht zentral auf einem Server, sondern ausschliesslich lokal gespeichert werden, zum Beispiel auf einem Badge, der gleichzeitig mit dem Fingerabdruck eingelesen werden muss. Mit Blick auf die Einhaltung des Verhältnismässigkeitsprinzips kann es sich empfehlen, statt eines kompletten Fingerabdrucks lediglich einen Extrakt davon zu bearbeiten.

Um den Mitarbeitenden das Recht auf Selbstbestimmung zu gewähren, erscheint es wünschenswert, ihnen Alternativen zur biometrischen Zeiterfassung zur Verfügung zu stellen. Ob ein Arbeitgeber eine Anstellung an die Bedingung knüpfen darf, dass eine Arbeitnehmerin oder ein Arbeitnehmer der Erfassung des Fingerabdrucks zustimmt, ist vorab eine Frage des Arbeitsrechts. Angestellte, die sich im Einzelfall gegen die Einführung biometrischer Zeiterfassungssysteme wehren wollen, können sich an ein Arbeitsgericht wenden.

1.8 Handel und Wirtschaft

1.8.1 Swiss-U.S. Privacy Shield

Im laufenden Jahr haben wir die Umsetzung des Swiss-US Privacy Shield begleitet und einen Ratgeber für Bürgerinnen und Bürger veröffentlicht.

In unserem 24. Tätigkeitsbericht 2016/2017 (Ziffer 1.8.1) berichteten wir über den Swiss-US Privacy Shield. Seither haben sich über 1000 Unternehmen zertifizieren lassen. Im Berichtsjahr nahmen wir als Beobachter am Review des EU-US Privacy Shields teil und haben einen praktischen Ratgeber für Bürgerinnen und Bürger publiziert (www.derbeauftragte.ch, Datenschutz, Handel und Wirtschaft – Übermittlung ins Ausland – USA). Im kommenden Jahr wird erstmals auch die Umsetzung des Swiss-US Privacy Shield geprüft. Die Prüfung soll im Herbst 2018 gleichzeitig mit jener des EU-Privacy Shields stattfinden. Zum Zwecke des koordinierten Ablaufs und der Vorbereitung der Prüfungen spricht sich unsere Behörde mit den Datenschutzbehörden der EU und deren Mitgliedstaaten ab. Erste Gespräche fanden im Januar 2018 anlässlich eines Besuches des Beauftragten in Brüssel statt.

Des weiteren werden für das im Swiss-US Privacy Shield vorgesehene Schiedsgericht fünf bei Bedarf aufzubietende Schiedsrichter gesucht. Das Department of Commerce hat die Stellen im ersten Quartal 2018 ausgeschrieben. Auch der Zugang zum Ombudsverfahren wird in diesem Jahr umgesetzt.

1.8.2 Datenleck bei EOS Schweiz AG

Der Inkassofirma EOS Schweiz AG sollen Daten grösseren Umfangs gestohlen worden sein. Wir haben in dem Fall eine Sachverhaltsabklärung eröffnet.

Gemäss einem Bericht der Süddeutschen Zeitung vom 27. Dezember 2017 wurde das Inkasso-Unternehmen EOS im vergangenen Jahr Opfer eines Datenlecks, in dessen Zusammenhang mehrere Gigabyte an sensiblen Patientendaten übermittelt wurden. Zu den Betroffenen sollen insbesondere Patienten von Schweizer Ärzten und Zahnärzten zählen. EOS informierte uns kurz vor Erscheinen des Artikels über das mutmassliche Datenleck. Um die datenschutzrechtlichen Aspekte des Vorfalls abzuklären, haben wir am 28. Dezember 2017 eine Sachverhaltsabklärung gegenüber EOS Schweiz eröffnet.

Im Rahmen unserer veröffentlichten Stellungnahmen zur Berichterstattung der Süddeutschen Zeitung haben wir daran erinnert, dass Medizinalpersonen nur diejenigen Daten von Patienten an Dritte weitergeben dürfen, die für die Rechnungsstellung bzw. das Inkasso tatsächlich erforderlich sind. Geben sie deren Gesundheitsdaten ungerechtfertigt an Dritte weiter, machen sie sich strafbar.

1.8.3 Revision des Urheberrechtsgesetzes

In der Revision des Urheberrechtsgesetzes (URG) wurde unseren wichtigsten Anliegen Rechnung getragen: Sie betreffen die Verfolgung von Urheberrechtsverletzungen im Internet und dabei insbesondere die Streichung des Informationsanspruchs im Zivilverfahren.

Im Nachgang an das Urteil in Sachen Logistep (vgl. 18. Tätigkeitsbericht 2010/2011, Ziffer 1.3.5 und BGer 1C_285/2009 vom 8.9.2010) entbrannte eine Diskussion darüber, wie Personendaten zur Verfolgung von Urheberrechtsverletzungen im Internet bearbeitet werden dürfen. Wir haben diesbezüglich bereits vor einiger Zeit Best Practices veröffentlicht (vgl. 19. Tätigkeitsbericht 2011/2022, Ziffer 1.3.7 und 20. Tätigkeitsbericht 2012/2013, Ziffer 1.3.3). Unbestritten war indessen, dass der Gesetzgeber gefordert war, die nötige Rechtssicherheit zu schaffen.

Auf Basis der von Bundesrätin Sommaruga eingesetzten Arbeitsgruppe AGUR12 gemachten Vorschläge wurde inzwischen ein Entwurf für ein revidiertes Gesetz erarbeitet. Wir stellten erfreut fest, dass unsere Best Practices in einer Bestimmung dieser Vorlage ausdrücklich festgehalten sind.

Beanstanden mussten wir hingegen den neu vorgesehenen Informationsanspruch im Zivilverfahren. Gemäss diesem könnten die Rechteinhaber zur zivilrechtlichen Geltendmachung ihrer Ansprüche (also z.B. von Schadenersatz wegen Urheberrechtsverletzungen) auf Daten zugreifen, die eine Identifikation von Anschlussinhabern erlauben. Solche Daten aber werden gestützt auf das Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) erhoben und gespeichert, das lediglich die Verfolgung und Ahndung schwerer Straftaten ermöglichen soll. Eine Verwendung dieser Daten in Zivilverfahren würde nach unserer Auffassung eine systemwidrige Zweckänderung darstellen, die mit den engen Zulässigkeitsgrenzen von Vorratsdatenspeicherungen nicht mehr zu vereinbaren wäre (vgl. 23. Tätigkeitsbericht 2015/2016, Ziffer 1.3.5).

Dieser Kritik ist der Bundesrat gefolgt, indem er den Informationsanspruch aus der Vorlage gestrichen hat. Damit steht die Vorlage zur notwendigen Modernisierung des Urheberrechts in Einklang mit dem Persönlichkeitsschutz.

1.8.4 Personalisierte Werbung in Apps aufgrund von Standortdaten

Das Werbeunternehmen APG/SGA hat uns um eine datenschutzrechtliche Einschätzung zu einer Plattform für personalisierte Werbung in Apps gebeten. Wir haben dazu Stellung genommen und entsprechende Massnahmen vorgeschlagen.

Im Berichtsjahr haben wir das Werbeunternehmen APG/SGA beraten, welches eine Plattform zur situativen und personalisierten Ansprache von Nutzern mobiler Endgeräte (Smartphones) mit Onlinewerbung aufbauen will. Dazu wertet das Unternehmen Positionsdaten aus und analysiert zudem das Verhalten der Nutzer in bestimmten Apps. Diese Daten dienen dazu, den Nutzern standort- und verhaltensspezifische Werbung in Apps von Drittanbietern (z.B. News-Apps) einzublenden. Die Nutzerzuordnung der gesammelten Daten erfolgt jeweils über eine Werbe-ID, welche von den Herstellern der Endgeräte vergeben wird, sobald sich der Nutzer mit seinem Smartphone anmeldet.

Es hat sich gezeigt, dass mittels der Plattform umfangreiche Bewegungsprofile und Ortungsdaten grundsätzlich unbefristet bearbeitet werden sollen. Nach unserer Einschätzung ist die Identifizierung der betroffenen Personen in vielen Fällen relativ leicht möglich, auch wenn dem Nutzer mittels der Werbe-ID kein Name zugeordnet wird. Schliesslich zielt das Geschäftsmodell darauf ab, einer konkreten Person in einem bestimmten Kontext personenbezogene Werbung anzuzeigen. Aus diesen Gründen gehen wir davon aus, dass bei dem uns präsentierten Vorhaben personenbezogene Daten bearbeitet werden. Die Nutzer müssen deshalb bei der Installation der Applikationen der Drittanbieter umfassend und transparent über die Datenbearbeitung informiert werden. Auch ist ihre ausdrückliche Zustimmung erforderlich. Die Nutzer sollen zudem jederzeit die Möglichkeit haben, ihre einmal erteilte Einwilligung in die Datenbearbeitung der Werbeplattform zu widerrufen.

Die APG/SGA hat unsere Hinweise zur Kenntnis genommen und prüft deren Umsetzung.

1.8.5 Datenbearbeitung bei Admeira

Im Berichtsjahr fand ein erster Informationsaustausch mit dem Werbevermarktungsunternehmen Admeira statt, bei dem auch die Zusammenarbeit im Rahmen unserer Beratungstätigkeit definiert wurde.

Im vergangenen Berichtsjahr haben wir die Swisscom hinsichtlich ihrer datenschutzrechtlichen Informationspflichten gegenüber der Kundschaft in Zusammenhang mit ihren neuen Datenschutzbestimmungen beraten. Diese regeln unter anderem eine nicht-personenbezogene Weitergabe von Daten der Festnetzkunden an das Werbeunternehmen Admeira, welches in Besitz von Ringier, SRG und Swisscom ist. Die betroffenen Personen können dieser Weitergabe zu Werbezwecken widersprechen.

Admeira bearbeitet diese Daten, um zielgruppenspezifische Werbung bei Ringier, SRG und Swisscom anzubieten. In diesem Jahr haben wir einen ersten Informationsaustausch mit der Firma geführt, um das Projekt zu begleiten und datenschutzrechtliche Hinweise zu geben. Zudem stehen wir in Kontakt mit allen involvierten Unternehmen und begleiten diese im Rahmen unserer Beratungsfunktion. Dabei gilt es auch sicherzustellen, dass die Datenflüsse und Auswertungen für die betroffenen Personen durchgehend erkennbar sind.

1.8.6 Informationsschreiben im Zusammenhang mit der Kundenkarte von Coop

Im Berichtsjahr hat das Detailhandelsunternehmen Coop einzelne Kunden wegen neuer Teilnahmebestimmungen für ihre Kundenkarte angeschrieben. Aufgrund von Anfragen von Betroffenen klärten wir den Sachverhalt bei Coop ab.

Die allgemeinen Geschäftsbedingungen (AGB) für die Kundenkarte von Coop (Supercard) sehen seit dem Jahr 2012 die Bearbeitung von Warenkorbdaten zwecks Kundenprofilbildung vor. Die Warenkorbanalyse wurde nur vorgenommen, wenn die Kunden ausdrücklich durch aktives Setzen eines Häkchens einwilligten. Trotz diverser Massnahmen und Kommunikation auf verschiedenen Kanälen haben einzelne Kunden gemäss Coop noch nicht auf die damaligen AGB-Änderungen reagiert. Die Betroffenen wurden im Berichtsjahr erneut persönlich angeschrieben und über die neuen AGB in Kenntnis gesetzt. Einige haben sich daraufhin bei uns gemeldet und ihre Bedenken wegen der Warenkorbanalyse geäussert.

Unsere Nachfrage bei Coop ergab, dass in diesem Kundenschreiben transparent aufgezeigt wurde, wie die Betroffenen die Warenkorbanalyse verweigern können. Für die Kunden ist es weiterhin möglich, die Supercard auch ohne Analyse ihres Einkaufsverhaltens zu nutzen. Damit wird den gesetzlichen Anforderungen an die Transparenz und die Einwilligung genüge getan. Coop hat ihre Kunden daher richtig informiert.

1.8.7 Auskunfts- und Widerspruchsrecht bei einem Adresshändler – Ergebnis des Verfahrens vor dem Bundesverwaltungsgericht

Ein Adresshändler liess die bei ihm eingegangen Auskunfts- bzw. Widerspruchsbegehren unbeantwortet und verletzte somit seine datenschutzrechtlichen Pflichten. Betroffene Personen haben sich bei unserer Behörde darüber beschwert. Unsere Klage vor dem Bundesverwaltungsgericht wurde gutgeheissen.

Aufgrund der vielen bei uns eingegangen Meldungen, wonach der Adresshändler Lucency AG Auskunfts- und Widerspruchsbegehren unbeantwortet liess, haben wir im September 2014 eine Empfehlung erlassen. Da unsere Empfehlung nicht befolgt wurde, legten wir sie dem Bundesverwaltungsgericht (BVGer) im Rahmen eines Klageverfahrens zum Entscheid vor (siehe dazu unseren 23. Tätigkeitsbericht 2015/2016, Ziffer 1.8.6).

Mit Urteil vom 12. April 2017 (A-5225/2015) hat das Bundesverwaltungsgericht unsere Klage gutgeheissen und die Beklagte unter anderem verpflichtet, Auskunftsgesuche nach Artikel 8 des Datenschutzgesetzes innert der gesetzlichen Frist von 30 Tagen zu beantworten, inklusive die pendenten Auskunftsbegehren. Zudem hat das Gericht die Lucency AG dazu verpflichtet, Personendaten auf Antrag zu sperren oder zu löschen bzw. das Vorliegen eines Rechtfertigungsgrundes für eine Weiterbearbeitung darzulegen und die betroffenen Personen entsprechend zu informieren. Für den Fall der Nichterfüllung dieser Verpflichtungen wurde den Mitgliedern des Verwaltungsrats der Beklagten eine Ungehorsamstrafe nach Artikel 292 des Schweizerischen Strafgesetzbuches (StGB) angedroht.

Das Urteil ist unterdessen rechtskräftig. Sollte die verlangte Auskunft bzw. Bestätigung der Datensperrung nach diesem Gerichtsentscheid immer noch nicht erteilt werden, kann eine Strafanzeige (gestützt auf Art. 292 StGB) gegen die Mitglieder des Verwaltungsrats der Lucency AG erstattet werden.

1.8.8 Datenweitergabe an Dritte durch das Internetauktionshaus ricardo.ch

Die Online-Auktionsplattform ricardo.ch hat ihre Datenschutzerklärung geändert, um den Datenaustausch innerhalb der Tamedia-Gruppe zu ermöglichen, insbesondere zum Zwecke personalisierter Werbung. Wir haben ein Verfahren eingeleitet, um zu prüfen, ob eine solche Weitergabe von Daten auf der Grundlage einer gültigen Einwilligung der Nutzer erfolgt.

Das Schweizer Internetauktionshaus ricardo.ch nahm im Juli 2017 Anpassungen seiner Datenschutzerklärung vor, um die Weitergabe von Daten an Dritte, d.h. an Unternehmen der Tamedia-Gruppe sowie verbundene Unternehmen, zu ermöglichen. Mit dem Datenaustausch innerhalb der Gruppe soll einerseits Missbrauch vorgebeugt und andererseits personalisierte Werbung ermöglicht werden. ricardo.ch informierte seine Nutzer in einem E-Mail über diese Anpassung der Nutzungsbedingungen und wies darauf hin, dass eine Ablehnung die automatische Schliessung des Benutzerkontos zur Folge habe. Bei Personen, die nicht auf dieses E-Mail reagierten, werde davon ausgegangen, dass sie die neuen Nutzungsbedingungen akzeptierten.

Die Weitergabe von Daten an Dritte zum Zwecke der personalisierten Werbung bedarf der freien und informierten Einwilligung der Betroffenen; bei besonders schützenswerten Personendaten oder Persönlichkeitsprofilen muss die Einwilligung zudem ausdrücklich erfolgen. Wir haben eine Sachverhaltsabklärung eröffnet, um insbesondere zu prüfen, ob sich das Unternehmen auf die Einwilligung seiner Nutzer (oder einen anderen Rechtfertigungsgrund) berufen kann. Es hat unseren Fragekatalog unterdessen beantwortet, und wir haben uns die Datenbearbeitungen präsentieren lassen. Zurzeit werten wir diese Informationen aus, um zu einer rechtlichen Beurteilung des Sachverhalts zu gelangen.

1.8.9 Zulässige Fragen in Anmeldeformularen für Mietobjekte

Die Frage nach der Konfession ist auf Anmeldeformularen für eine Mietwohnung unzulässig, da sie eine ungerechtfertigte Verletzung der Privatsphäre darstellt. Wir ersuchten die betreffenden Liegenschaftsverwaltungen um entsprechende Anpassungen ihrer Formulare.

Einer Zeitungsmeldung zufolge verlangen bestimmte Liegenschaftsverwaltungen anscheinend von den Bewerbern für Mietwohnungen Angaben zu ihrer Konfession. Die systematische Sammlung von Daten zur religiösen Gesinnung – die von Gesetzes wegen als besonders schützenswerte Daten gelten – stellt eine Verletzung der Privatsphäre dar, die sich grundsätzlich nicht mit dem überwiegenden privaten Interesse des Vermieters oder einem anderen Rechtfertigungsgrund begründen lässt.

Wir haben die Bewerbungsformulare der grössten Schweizer Liegenschaftsverwaltungen analysiert, um zu prüfen, ob es sich um eine verbreitete Praxis handelt. Es zeigte sich, dass der Hauseigentümerverband Schweiz in seinen Musterformularen keine solche Frage vorsieht. Eine Analyse von rund dreissig verschiedenen Fragebogen ermittelte drei Liegenschaftsverwaltungen, die die Frage nach der Religion in ihre Standardformulare aufgenommen hatten. Dies legt für uns den Schluss nahe,

dass es sich nicht um eine weitverbreitete Praxis handelt. Wir haben die betreffenden Liegenschaftsverwaltungen kontaktiert, um sie auf die Rechtslage aufmerksam zu machen und sie gebeten, ihre Formulare entsprechend anzupassen.

Zudem haben wir unsere Erläuterungen zur Datenerhebung durch Liegenschaftsverwaltungen überarbeitet. (Siehe www.derbeauftragte.ch, Datenschutz – Wohnen und Verkehr – Anmeldeformulare für Mietwohnungen).

1.8.10 Verordnungen zur Umsetzung des ersten Massnahmenpakets zur Energiestrategie 2050

Während des Ämterkonsultationsverfahrens nahmen wir Stellung zu den Verordnungen des ersten Massnahmenpakets zur Energiestrategie 2050. Die datenschutzrechtlichen Fragen betreffen die Publikation von Personendaten im Internet und die Datenbearbeitung durch intelligente Messsysteme (Smart Meter).

Im Rahmen der Ämterkonsultation zu den Verordnungen des ersten Massnahmenpakets zur Energiestrategie 2050 haben wir uns zur Publikation von Personendaten und zur Datenbearbeitung durch intelligente Messsysteme geäussert. Dies sind auch die Themen, welche uns im Bereich der Energieversorgung schon über einen längeren Zeitraum hinweg beschäftigen (vgl. auch 24. Tätigkeitsbericht 2016/2017, Ziffer 1.8.3 mit weiteren Verweisen).

Das Bundesamt für Energie (BFE) beabsichtigte die Personendaten sämtlicher Bezüger von Einmalvergütungen (EIV) und die kostendeckenden Einspeisevergütungen (KEV) im Internet zu publizieren. Ziel dieser Massnahme wäre es, die Verwendung des bei den Endverbrauchern erhobenen Netzzuschlags transparent zu machen. Wir beurteilen bei Gesetzesprojekten jeweils auch, ob die angestrebte Publikation von Personendaten zielführend ist. Die Ausweitung der Internetpublikation auf alle KEV-/EIV-Bezüge hätte das Recht auf informationelle Selbstbestimmung von zusätzlichen 5000 Personen, die nur rund acht Prozent der gesamten Vergütung ausmachen, eingeschränkt, was unseres Erachtens unverhältnismässig gewesen wäre. Das BFE hat unseren Bedenken Rechnung getragen, indem es die bisherige Veröffentlichungspraxis fortführt und Personendaten zu Betreibern von neuen Kraftwerken für die Produktion von Strom aus erneuerbaren Energien erst ab einer Anlagengrösse von über 30kVA publiziert.

Für weitere geplante Publikationsbestimmungen auf Verordnungsstufe fehlten formelle gesetzliche Bestimmungen, welche dem Bundesrat die Kompetenz für den Erlass von Ausführungsbestimmungen zur Publikation von Personendaten zuweisen. Das BFE beabsichtigt eine entsprechende Gesetzesbestimmung zu schaffen und wird erst mit Inkrafttreten einer solchen die Anpassungen in den Verordnungen vornehmen.

Bei den Ausführungsbestimmungen zu den intelligenten Messsystemen (u.a. Smart Meter) blieb schliesslich eine Differenz bezüglich der Auslesefrequenz von Energiebezügen bestehen. Auslesungen sind datenschutzrechtlich u.a. deshalb heikel, weil sie bei den Betroffenen das Gefühl der ständigen Beobachtung hervorrufen können. Das BFE hat zwar, wie vom EDÖB gefordert, eine Verordnungsbestimmung zur Auslesefrequenz geschaffen, die Intervalle dann aber bei sehr kurzen 15 Minuten festgelegt, sofern der sichere und effiziente Netzbetrieb nicht gar eine noch häufigere Auslesung erfordert. Nach unserer Intervention hat das BFE die Intervalle dann auf 24 Stunden erhöht, was aber immer noch zu einer unnötig häufigen Auslesung führt. Obwohl die von uns verlangte Auslesung im Zwei-Wochen-Rhythmus mit der Erfüllung der Bearbeitungszwecke problemlos vereinbar gewesen wäre, sind wir mit dieser Forderung auch beim Gesamtbundesrat nicht durchgedrungen.

1.8.11 Urteil Moneyhouse

Wie wir in unserem 24. Tätigkeitsbericht 2016/2017 in Ziffer 1.8.2 berichteten, ist das Bundesverwaltungsgericht in seinem Urteil vom 18.04.2017 (A-4232/2015) unseren Anträgen grösstenteils gefolgt. Da das Urteil nicht an das Bundesgericht weitergezogen wurde, ist es zwischenzeitlich in Rechtskraft erwachsen.

1.8.12 Zentralstelle für Kreditinformation (ZEK)

Im Berichtsjahr haben wir bei der Zentralstelle für Kreditinformation eine Sachverhaltsabklärung eingeleitet, nachdem uns datenschutzrechtliche Probleme gemeldet worden sind. Aktuell ist unsere Untersuchung noch im Gang.

Die Zentralstelle für Kreditinformation (ZEK) sammelt Bonitätsinformationen aus Kreditgeschäften natürlicher und juristischer Personen und stellt diese ihren Mitgliedern, insbesondere Banken, gegen Entgelt zur Verfügung. Durch Bürgeranfragen und Medienberichte wurden wir auf verschiedene datenschutzrechtliche Probleme bei der ZEK aufmerksam gemacht; beanstandet wurde etwa, dass Personen, welche in der Datenbank verzeichnet sind, nur eingeschränkt Auskunft über die gesammelten Daten erhielten, Einträge in der Datenbank fehlerbehaftet seien oder das Berichtigungsverfahren nicht effizient ablaufe. Um diesen Vorhaltungen nachzugehen, haben wir im Mai 2017 eine Sachverhaltsabklärung eingeleitet, die derzeit noch im Gang ist.

1.9 Finanzen

1.9.1 Automatischer Informationsaustausch

Die Umsetzung der neuen Standards zur weltweiten Verhinderung von Steuerbetrug und Steuerhinterziehung schreitet weiter fort. Im Berichtsjahr haben wir zu verschiedenen Vorlagen aus der Sicht des Datenschutzes Stellung genommen.

a) Automatischer Informationsaustausch über Finanzkonten (AIA)

Im Rahmen des neu eingeführten automatischen Informationsaustauschs über Finanzkonten (AIA) hat die Schweiz ab 2017 Daten gesammelt, 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 Staatsvertrags oder auf der Grundlage des Multilateral Competent Authority Agreement (MCAA). Mit der Aktivierung verpflichten sich die Teilnehmerstaaten, den «gemeinsamen Melde- und Sorgfaltsstandard für Informationen über Finanzkonten» (Gemeinsamer Meldestandard, GMS) der OECD im innerstaatlichen Recht umzusetzen und anzuwenden (vgl. unseren 24. Tätigkeitsbericht 2016/2017, Ziff. 1.9.1 a).

Einführung des automatischen Informationsaustauschs mit weiteren Staaten

Unabhängig von der Art der Aktivierung des AIA wird der betreffende Bundesbeschluss bzw. bilaterale Staatsvertrag der Bundesversammlung zur Genehmigung unterbreitet. Diese hatte 2016 der Einführung des AIA mit einer ersten Serie Länder zugestimmt, darunter mit den EU-Staaten (vgl. unseren 24. Tätigkeitsbericht 2016/2017, Ziff. 1.9.1 a). Als vorläufiges Ergebnis setzt die Schweiz ab dem 1. Januar 2017 den AIA mit insgesamt 38 Staaten und Territorien um; ein erster Austausch der kontorelevanten Informationen erfolgt im 2018.

Im Juni 2017 verabschiedete der Bundesrat die Botschaft über die Einführung des AIA mit weiteren 41 Partnerstaaten, mit denen der AIA ab dem Jahr 2018 mit einem ersten Austausch von Kontendaten im 2019 eingeführt werden soll. Wir wiesen darauf hin, dass von den 41 Staaten und Territorien mehr als 30 über kein angemessenes Datenschutzniveau nach Art. 6 Abs. 1 DSG verfügen (darunter etwa China, Russland oder Saudi-Arabien); für diese Staaten seien daher zusätzliche Datenschutzgarantien nach Art. 6 Abs. 2 DSG nötig. Bereits im letzten Berichtsjahr hatten wir deutlich gemacht, dass die von der Schweiz am 4. Mai 2017 übermittelte, auf dem Multilateral Competent Authority Agreement (MCAA) beruhende Mitteilung datenschutzrechtlicher Garantien nicht genügt, um in solchen Staaten ein adäquates Datenschutzniveau sicherzustellen (vgl. 24. Tätigkeitsbericht 2016/2017, Ziff. 1.9.1 a).

Mit der Botschaft über die Einführung des AIA mit 41 Partnerstaaten legte der Bundesrat dem Parlament auch den Entwurf eines Bundesbeschlusses über einen Prüfmechanismus zur Sicherstellung der standardkonformen Umsetzung des automatischen Informationsaustauschs vor. Gemäss diesem Mechanismus prüft der Bundesrat im Hinblick auf den ersten Informationsaustausch mit Partnerstaaten, welcher im September 2019 stattfindet, den Stand der Umsetzung des AIA, insbesondere ob die Partnerstaaten die massgebenden Voraussetzungen für die Einführung des AIA in diesem Zeitpunkt erfüllen. Auch wenn das Problem fehlender Datenschutzgarantien nach Art. 6 Abs. 2 DSG mit diesem Instrument nicht gelöst ist, sprachen wir uns anlässlich von Anhörungen vor der Kommission für Wirtschaft und Abgaben des Nationalrats (WAK-N) im August und September 2017 für einen solchen Mechanismus aus. Dabei unterstützten wir die Forderung, dass der Bundesrat die parlamentarischen Kommissionen betreffend der Ergebnisse seiner Prüfung nicht nur informieren, sondern konsultieren sollte. Ein Konsultationsrecht wurde in den parlamentarischen Beratungen in den Bundesbeschluss aufgenommen.

Stärkung des Rechtsschutzes beim automatischen Informationsaustausch

Gemäss einer Motion der Kommission für Wirtschaft und Abgaben des Ständerats vom 2. November 2017 (Nr. 17.3973) soll im Gesetz über den internationalen automatischen Informationsaustausch in Steuersachen (AIA-Gesetz) explizit verankert werden, dass kein Informationsaustausch erfolgt, wenn jemand glaubhaft macht, dass wesentliche Rechtsgüter verletzt werden. Im Rahmen der Ämterkonsultation hierzu haben wir uns zu Gunsten der Motion ausgesprochen. Der Ständerat als erstbehandelnder Rat hat die Motion am 5. Dezember 2017 gegen den Antrag des Bundesrats angenommen.

b) Austausch länderbezogener Berichte (ALBA)

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 einzudämmen. Demzufolge unterzeichnete die Schweiz Anfang 2016 das multinationale Abkommen über den Austausch länderbezogener Berichte (ALBA-Vereinbarung) und wurde per 1. Dezember 2017 das ALBA-Gesetz in Kraft gesetzt (betreffend unserer Stellungnahmen zu diesem Gesetz vgl. den 24. Tätigkeitsbericht 2016/2017, Ziff. 1.9.1 a). Der Datenschutz spielt hier deshalb eine Rolle, weil nach geltendem Recht alle Angaben in den Länderberichten, die sich auf eine bestimmte juristische Person beziehen, als Personendaten im Sinne des Datenschutzgesetzes (DSG) gelten (mit Inkrafttreten des revidierten DSG wird sich dies ändern). Im Verlaufe des Jahres 2017 äusserten wir uns im Rahmen von Ämterkonsultationen mehrfach zur Länderliste für die Aktivierung des Austauschs der länderbezogenen Berichte. Wir wiesen darauf hin, dass auf der Liste Länder figurieren, welche auf der Staatenliste des EDÖB mit ungenügendem Datenschutzniveau aufgeführt sind; es müssten darum zusätzliche Datenschutzgarantien im Sinne von Art. 6 Abs. 2 DSG eingeholt werden, um bei der Übermittlung von Personendaten in solche Länder ein angemessenes Datenschutzniveau zu gewährleisten. Dies wurde indessen nicht berücksichtigt.

1.9.2 Sachverhaltsabklärung bei der Eidgenössischen Steuerverwaltung

Im Berichtsjahr haben wir bei der Eidgenössischen Steuerverwaltung (ESTV) aus Anlass einer Datenübermittlung im Rahmen der US-Steueramtshilfe eine Sachverhaltsabklärung eröffnet. Gestützt darauf erliessen wir eine Empfehlung, wonach die ESTV in der internationalen Steueramtshilfe die vom Amtshilfeersuchen nicht formell betroffenen Personen, deren Namen übermittelt werden sollen, vorgängig zu informieren hat.

Im November 2017 eröffneten wir eine Sachverhaltsabklärung betreffend die Übermittlung von Personendaten durch die ESTV im Rahmen der US-Steueramtshilfe. Es stellte sich insbesondere die Frage, ob und gestützt auf welche Grundlagen die ESTV Namen von Personen, welche von Amtshilfeersuchen formell nicht betroffen sind, offen, d. h. ungeschwärzt, an die ersuchende US-Behörde übermittelt und ob im Fall einer solchen Übermittlung das Recht auf vorgängige Information beachtet wird.

Aufgrund der Ergebnisse der Sachverhaltsabklärung kamen wir im Dezember 2017 zum Schluss, dass im Einzelfall durch die Gerichte zu beurteilen ist, ob die ESTV den Namen eines nicht formell betroffenen Dritten, insbesondere eines Bankmitarbeiters, offen übermitteln darf; es darf allerdings nicht unter dem Deckmantel der Steueramtshilfe eine verdeckte Amtshilfe in Strafsachen gegen Bankmitarbeiter erfolgen. Wir erliessen eine formelle Empfehlung, wonach die ESTV in der internationalen Steueramtshilfe die vom Amtshilfeersuchen nicht formell betroffenen Personen, deren Namen offen übermittelt werden sollen, gemäss Art. 14 Abs. 2 des Steueramtshilfegesetzes vorgängig zu informieren hat.

Die ESTV hat unsere Empfehlung zurückgewiesen, worauf wir die Angelegenheit dem EFD zum Entscheid vorgelegt haben. Sobald dessen Verfügung vorliegt, wird der EDÖB über eine allfällige Beschwerde an das Bundesverwaltungsgericht befinden.

1.10 International

Eine enge Vernetzung und Zusammenarbeit der Datenschutzbehörden ist heute unabdingbar, da sich die Datenschutzgesetze nach wie vor auf die nationalen Rechtsordnungen berufen, während der Austausch von Personendaten grenzüberschreitend stattfindet.

Für einen effizienten Datenschutz ist neben der internationalen Zusammenarbeit auch die Entwicklung internationaler Standards von Bedeutung. Um sicherzustellen, dass Privatpersonen unabhängig von ihrem Wohnort dieselben Rechte haben, sind aufeinander abgestimmte Lösungen für den grenzüberschreitenden Datenverkehr erforderlich. Mehr denn je müssen sich die Datenschutzbehörden heute untereinander abstimmen und gemeinsam festlegen, wie sie auf technischer und normativer Ebene auf die jüngsten Herausforderungen im Datenschutz reagieren – etwa auf Big Data, das Internet der Dinge, die künstliche Intelligenz und die Massenüberwachung.

Die Beiträge unserer Behörde spielen eine wichtige Rolle in der internationalen Diskussion zu Fragen des Datenschutzes und des Schutzes der Privatsphäre, namentlich im Europarat, der Europäischen und der Internationalen Konferenz der Datenschutzbeauftragten, den gemeinsamen Kontrollinstanzen von Schengen und Eurodac sowie der Französischsprachigen Vereinigung der Datenschutzbehörden (AFAPDP) und der OECD.

Europarat

Die Arbeiten zur Modernisierung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen 108) sind noch nicht abgeschlossen. Das Dossier liegt nach wie vor bei der Gruppe von Berichterstattern des Ministerkomitees. Der Abschluss der Arbeiten dürfte im Laufe des ersten Halbjahres 2018 in Form eines durch das Ministerkomitee verabschiedeten Änderungsprotokolls oder eines revidierten Übereinkommens erfolgen. In seiner derzeitigen Form zählt das Übereinkommen 51 beigetretene Staaten einschliesslich Tunesien (Beitritt am 1. November 2017). Argentinien, Burkina Faso, Marokko und Mexiko wurden zum Beitritt eingeladen.

Der Beratende Ausschuss des Übereinkommens 108 (T-PD) hat die Leitlinien für den Schutz von Personendaten bei deren Verarbeitung im Zeitalter von Big Data verabschiedet. Diese Leitlinien sind ein erster Schritt zu einer eingehenderen Regulierung der Nutzung von Big Data. Sie geben einen allgemeinen Rahmen für politische Konzepte und Massnahmen vor, welche die im Übereinkommen 108 festgelegten Grundsätze im Big-Data-Kontext konkretisieren sollen. Der T-PD setzt seine Revision der Empfehlung R (97) 5 über den Schutz medizinischer Daten fort und arbeitet ein Praxishandbuch zum Datenschutz bei der Polizei aus. Ferner entwirft er die Leitlinien zum Schutz von Daten, die bei der Zentralstelle für die Vergabe von Internet-Namen und -Adressen (ICANN) zum Tragen kommen sollen, sowie die Leitlinien zum Schutz der Privatsphäre und der Medien.

Europäische Konferenz der Datenschutzbeauftragten

Die Europäische Konferenz der Datenschutzbeauftragten fand vom 27. bis 28. April 2017 in Limassol (Zypern) statt; Gastgeber war der zypriotische Datenschutzbeauftragte. Diese Konferenz bot Gelegenheit, den Stand der europäischen Reformen und insbesondere der Datenschutz-Grundverordnung zu betrachten, die am 25. Mai 2018 in Kraft tritt. Sie sorgt für eine starke und einheitliche Rechtsnorm in den 28 EU-Mitgliedstaaten. Zu den zentralen Punkten dieser Reform zählen der Ausbau der Befugnisse der Datenschutzbehörden (DSB) und insbesondere die Verstärkung der Instrumente für die Koordination und Kooperation zwischen den einzelnen Datenschutzbehörden. In einer Resolution unterstrich die Konferenz ferner, dass das Übereinkommen 108 als zentrales Element zur Prüfung der Angemessenheit des Datenschutzes von Drittstaaten durch die Europäische Kommission dringend und raschestmöglich modernisiert und in dieser Form in Kraft gesetzt werden sollte. Mit einem modernisierten Übereinkommen dürfte sich auch die Zusammenarbeit der Parteien vereinfachen und der Europäischen Konferenz würde eine bedeutende Rolle in der Zusammenarbeit der DSB zukommen. Deshalb will die Konferenz eine Arbeitsgruppe einrichten, an der auch der EDÖB teilnehmen wird. Diese Arbeitsgruppe soll Vorschläge zur zukünftigen Arbeitsweise und Rolle der Konferenz erarbeiten.

Ferner war die Konferenz Anlass zum Austausch über die Aufklärungspolitik der einzelnen DSB, über Fragen der Verantwortlichkeit, der Erfüllung der Anforderungen und der Transparenz im Zusammenhang mit dem Cloud Computing. Die mit der Genforschung verbundenen Herausforderungen für den Schutz von freiheitlichen Grundrechten wurden ebenfalls erörtert. Genomische Daten werfen zahlreiche Fragen juristischer, ethischer, politischer, wirtschaftlicher und technischer Art auf, die eine vertiefte Analyse erfordern. Auch unsere Rechtsrahmen sind an diese bahnbrechenden Entwicklungen anzupassen. Daher haben wir einmal mehr darauf hingewiesen, dass die Einhaltung des Grundsatzes der Datenminimierung, des Transparenzgebots und der Meldepflicht bei Verstössen gegen den Datenschutz, die Folgenanalyse, die Grundsätze «Privacy by design» und

«Privacy by default» oder die Zertifizierung in diesem Zusammenhang eine conditio sine qua non darstellen. Die Technologie ist auch beizuziehen, um die Verarbeitung von genetischen Daten zu vereinfachen und zugleich sicherzustellen, dass die Rechte der betroffenen Personen gewahrt bleiben. Der Zugang zu diesen Daten muss kontrollierbar sein, zugleich aber sollen sie für medizinische Zwecke leicht zugänglich sein und weitergegeben werden können. Wir haben die aktuellen, vielversprechenden Forschungsarbeiten der EPFL zu einer sogenannt homomorphen Verschlüsselungstechnik erwähnt. Die betreffenden Forschenden arbeiten zudem an statistischen Instrumenten, die es verunmöglichen sollen, die Identität eines Patienten aus einer Reihe von grundsätzlich anonymisierten Gendaten zu erschliessen.

Europäische Arbeitsgruppe für die Behandlung datenschutzrelevanter Fälle

Das 29. Treffen der europäischen Arbeitsgruppe für die Behandlung datenschutzrelevanter Fälle («Case Handling Workshop») fand vom 20. bis 21. Juni 2017 in Manchester statt. Die Arbeitsgruppe, die sich aus Vertretern von 29 nationalen Datenschutzbehörden zusammensetzt, befasste sich mit verschiedenen sensiblen und aktuellen Themen. Im Berichtsjahr konzentrierte sich die Gruppe vor allem auf die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und die Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung. Sie befasste sich insbesondere mit Fragen zur Umsetzung der genannten Verordnung und ihrer Auswirkung auf die einzelnen Mitgliedstaaten. Diskutiert wurden ferner die neuen Rechte der betroffenen Personen, die Meldung von Verstössen gegen den Datenschutz, die Behandlung von Beschwerden und die Zusammenarbeitsmechanismen. Das letztere Thema illustrierten wir mit einer Präsentation zu den Zusammenarbeitsmechanismen von Drittstaaten. In einer zweiten Phase befassten sich die Teilnehmenden damit, wie die Datenschutzbehörden gemeinsam effiziente Lösungen für drohende Probleme beim Datenschutz entwickeln können.

Internationale Konferenz der Datenschutzbeauftragten

Die 39. Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre (ICDPPC) fand vom 25. bis 29. September 2017 in Hongkong statt. Gastgeber war die Datenschutzbehörde Hongkongs. Die Konferenz zog über 800 Teilnehmende an, die sich mit den Herausforderungen beim Schutz der Privatsphäre befassten. Im Vordergrund standen die Folgen von Technologien und der Stellenwert der digitalen Kompetenz. Im Verlauf der Konferenz wurden fünf Vertreterinnen und Vertreter der nationalen Datenschutzbehörden von Japan, Montenegro, Südafrika, Türkei und der belgischen Aufsichtsbehörde für polizeiliche Informationssysteme als Neumitglieder aufgenommen. Sie vertreten die Länder. Hiermit zählt die Konferenz nun 119 Mitglieder. Am ersten Tag besprachen die Datenschutzbeauftragten den zwischenstaatlichen Informationsaustausch und insbesondere die besten Möglichkeiten zum Schutz von sensiblen Informationen, zur Vermeidung von Diskriminierung und zum Risikomanagement. Die Herausforderungen der gemeinsamen Nutzung von Informationen wurden unter verschiedenen Aspekten besprochen. Die Experten erläuterten auch den Risikomanagementprozess, die Analyse nach ethischen Gesichtspunkten zur Vermeidung von Diskriminierungen und die Komplexität der gemeinsamen Datennutzung in staatlichen Institutionen sowie mit anderen Akteuren. Am Ende des ersten Tages wurden die ersten «ICDPPC Global Privacy and Data Protection Awards» vergeben. Am zweiten Tag stellte Joseph Cannataci, der Sonderberichterstatter der Vereinten Nationen für Vertraulichkeit und Datenschutz, die Fortschritte im Rahmen seines Mandats und seine Ziele für das kommende Jahr vor. Danach informierten die Arbeitsgruppen Digitale Kompetenz, Entwicklung neuer Datenschutz-Identifikatoren, humanitäre Hilfe, Telekommunikation und Zusammenarbeit im Rechtsvollzug über den Stand ihrer Arbeit. Die Datenschutzbeauftragten wendeten viel Zeit für die Diskussion interner Angelegenheiten auf, etwa in Bezug auf die Zusammensetzung, den Umfang und die Ziele der Konferenz. Es wurden Wahlen abgehalten, um einen neuen Ausschuss und eine neuen Präsidentin zu ernennen: Isabelle Falque-Pierrotin (Präsidentin der französischen Datenschutzbehörde CNIL) wird die Nachfolgerin von John Edwards (Datenschutzbeauftragter von Neuseeland). Schliesslich verabschiedete die Konferenz drei Resolutionen: Die erste bezieht sich auf den Datenschutz in automatisierten und vernetzten Fahrzeugen, die zweite auf die Zusammenarbeit zwischen Datenschutz- und Konsumentenschutzbehörden zwecks eines besseren Schutzes der Bürger und Konsumenten in der digitalen Wirtschaft und die dritte auf Möglichkeiten einer zukünftigen grenzüberschreitenden Zusammenarbeit im Rechtsvollzug. Die 40. internationale Konferenz findet

in Brüssel statt; sie wird durch den EDSB zusammen mit Bulgarien organisiert; das Hauptthema ist die digitale Ethik. Im Jahr 2019 wird die internationale Konferenz in Albanien stattfinden.

Französischsprachige Vereinigung der Datenschutzbehörden (AFAPDP)

Die Französischsprachige Vereinigung der Datenschutzbehörden (AFAPDP) wird durch den Stellvertreter des Eidgenössischen Datenschutzbeauftragten präsidiert. Die Konferenz traf sich am 4. und 5. September 2017 in Gammarth (Tunesien). Die Teilnehmenden befassten sich mit dem Datenschutz und der internationalen humanitären Hilfe und diskutierten das zugehörige Handbuch (s. oben), zu dem auch die AFAPDP beigetragen hat. Diskussionsthemen waren der Schutz von biometrischen Daten, die Rolle der Datenschutzbeauftragten und die extraterritoriale Reichweite der Datenschutz-Grundverordnung der Europäischen Union.

Die Mitglieder der AFAPDP verabschiedeten eine Resolution zur Verfolgung der Entwicklungen auf dem Gebiet der Künstlichen Intelligenz (KI). Mit dieser Resolution weisen sie darauf hin, dass KI-Technologien in den Dienst der Menschen zu stellen sind und dass die Rechte und Freiheiten des Einzelnen dabei gewahrt werden müssen. Die AFAPDP unterstreicht, dass die Verfolgung der KI-Technologien und der Innovation von Anfang an von Austausch, demokratischer Wachsamkeit und Berücksichtigung der Bedürfnisse zur Sicherstellung der Rechte und Freiheiten des Einzelnen geprägt sein sollte. Dies gilt insbesondere für die Zuverlässigkeit, Nachvollziehbarkeit und Sicherheit der KI für jeden Einzelnen sowie für die Sicherstellung, dass die betroffenen Personen das Recht haben, über die sie betreffenden Daten zu verfügen. Abschliessend betont sie die Notwendigkeit der Einführung von Gesetzesnormen zum Schutz von Personendaten und Privatsphäre im französischsprachigen Raum als Grundbedingung für eine Entwicklung der genannten Technologien unter Wahrung der Rechte und Freiheiten des Einzelnen.

Die AFAPDP schlägt zudem eine Schulung der Mitarbeitenden in den Behörden ihrer Mitglieder zu Kontrolltechniken vor. Am 11. Dezember 2017 feierte die AFAPDP zudem ihr zehnjähriges Bestehen am Sitz der «Organisation internationale de la Francophonie» in Paris. Das Jubiläum war für die AFAPDP Anlass, französischsprachige Autoren einzuladen, ihre Auffassung von Privatsphäre darzulegen und damit den Begriff zu erläutern, der für die Datenschutzbehörden zentral ist. Zum Abschluss der Diskussionen unterzeichneten die AFAPDP und die parlamentarische Versammlung der Frankophonie eine Partnerschaftsvereinbarung.

Arbeitsgruppe für Datenschutz und internationale humanitäre Hilfe

Anlässlich der 37. Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre wurde eine Resolution zum Datenschutz und der internationalen humanitären Hilfe verabschiedet. Zur Analyse der Anforderungen an den Datenschutz in der internationalen humanitären Hilfe und zur Zusammenarbeit der betroffenen Akteure wurde eine Arbeitsgruppe unter Leitung unserer Behörde eingesetzt. Sie hat ein entsprechendes Handbuch erarbeitet und veröffentlicht.

Die 37. Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre (IKBDSP) verabschiedete im Oktober 2015 in Amsterdam eine Resolution zum Datenschutz und der internationalen humanitären 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 sowie Analyse des geltenden Rechts und Benennung der problematischen Punkte, um Leitlinien zur Verbesserung der bereits bestehenden Praktiken vorzuschlagen. Die Arbeitsgruppe verfolgte in den letzten beiden Jahren 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. In diesem Zusammenhang veranstalteten Behörden, humanitäre Organisationen und Fachpersonen eine Reihe von themenbezogenen Workshops, die sich mit den neuen Technologien im Dienst der humanitären Hilfe und dem entsprechenden, zwingend zu berücksichtigenden Schutz der hiermit verbundenen Personendaten befassten. Im Verlauf dieser Workshops zeigte sich, dass die gute Praxis zum Schutz von Personendaten für die humanitären Helfer identifiziert und zugänglich gemacht werden muss. Im Rahmen ihrer Aufgabe führte die Ad-hoc-Arbeitsgruppe Arbeitssitzungen mit dem IKRK und

dem BPH durch. Diese Sitzungen gaben den Anstoss zur Schaffung eines praxisbezogenen Instruments für humanitäre Helfer. Das im Juli 2017 in englischer Sprache auf der Website des IKRK veröffentlichte Handbuch nimmt die Grundprinzipien und gesetzlichen Grundlagen des Datenschutzes auf und widmet jeder der Technologien zur Nutzung von Personendaten in der humanitären Hilfe ein eigenes Kapitel.

Erster Workshop des Global Privacy Enforcement Network (GPEN)

In Manchester wurde im Juni 2017 die erste jährliche Koordinationssitzung des «Global Privacy Enforcement Network» (GPEN) abgehalten. Das GPEN wurde eingerichtet, um die grenzüberschreitende Vernetzung der Datenschutzbehörden zu fördern. Vertreten waren 34 Länder aus verschiedenen Kontinenten, die alle befugt sind, die vorschriftsgemässe Verarbeitung personenbezogener Daten zu prüfen und gegebenenfalls einzugreifen bzw. Sanktionen auszusprechen. Wir beteiligen uns an diesem informellen Kooperationsnetzwerk, das durch Erfahrungsaustausch und Abgleich von Methodologien zum Ausbau des Fachwissens und Verbesserung der Reaktionsfähigkeit in grenzüberschreitenden bzw. weltweit relevanten Datenschutzfragen beitragen kann.

Über 70 Vertreter von 34 Behörden auf der ganzen Welt beteiligten sich an dem Workshop, ebenso Fachleute aus den Bereichen Konsumentenschutz und Telekommunikation. Behandelt wurden sämtliche entscheidenden Phasen von Datenschutzfällen und Fällen, in denen der Schutz der Privatsphäre tangiert wird. Ein besonderer Schwerpunkt lag beim internationalen Wissensaustausch und der Diskussion praktischer Erfahrungen.

Arbeitsgruppe der OECD für die Informationssicherheit und den Schutz der Privatsphäre

Die Arbeitsgruppe der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) zur Informationssicherheit und den Schutz der Privatsphäre hat verschiedene Empfehlungen erarbeitet. Sie befasste sich mit dem revidierten Empfehlungsentwurf der OECD zur Governance von Gesundheitsdaten, der in enger Zusammenarbeit mit dem Gesundheitsausschuss und einer informellen Experten-Beratungsgruppe erstellt wurde. Der Entwurf umfasst insbesondere eine Liste der zwölf wichtigsten Massnahmenempfehlungen zur Bewältigung der grossen Herausforderungen bei der Governance von Gesundheitsdaten sowie den Zeitplan der bis anhin durchgeführten Beratungen und Arbeiten. Die Delegierten unterstrichen, dass die Beschreibung der «De-Identifikation» präzisiert werden müsse.

Die Delegierten befassten sich mit einem Vorschlag zur Ausarbeitung eines globalen Instruments zur Verbesserung der Kohärenz der Rechtsakte der OECD, die den Zugang zu Daten sowie ihre Verknüpfung und Wiederverwendung fördern. Die Delegierten prüften den Vorschlag und bestätigten, dass die zentralen Konzepte nachvollziehbarer gestaltet werden müssten. Ferner waren sie sich bewusst, dass die Governance von Daten derzeit einige Probleme aufwirft und dass diese auf internationaler Ebene erörtert werden müssen. Sie wiesen darauf hin, dass einerseits die wirtschaftlichen Vorteile eines verbesserten Zugangs zu den Daten unbedingt weiter zu analysieren seien und andererseits auch die Opportunitätskosten oder der Verlust potenzieller Vorteile, falls keine Verbesserungen vorgenommen würden, aufgezeigt werden müssten. Diese Diskussion erhellte auch die Risiken im Zusammenhang mit der Datenerhebung: Nebst Verletzungen der Privatsphäre besteht auch das Risiko einer sinkenden Datenqualität.

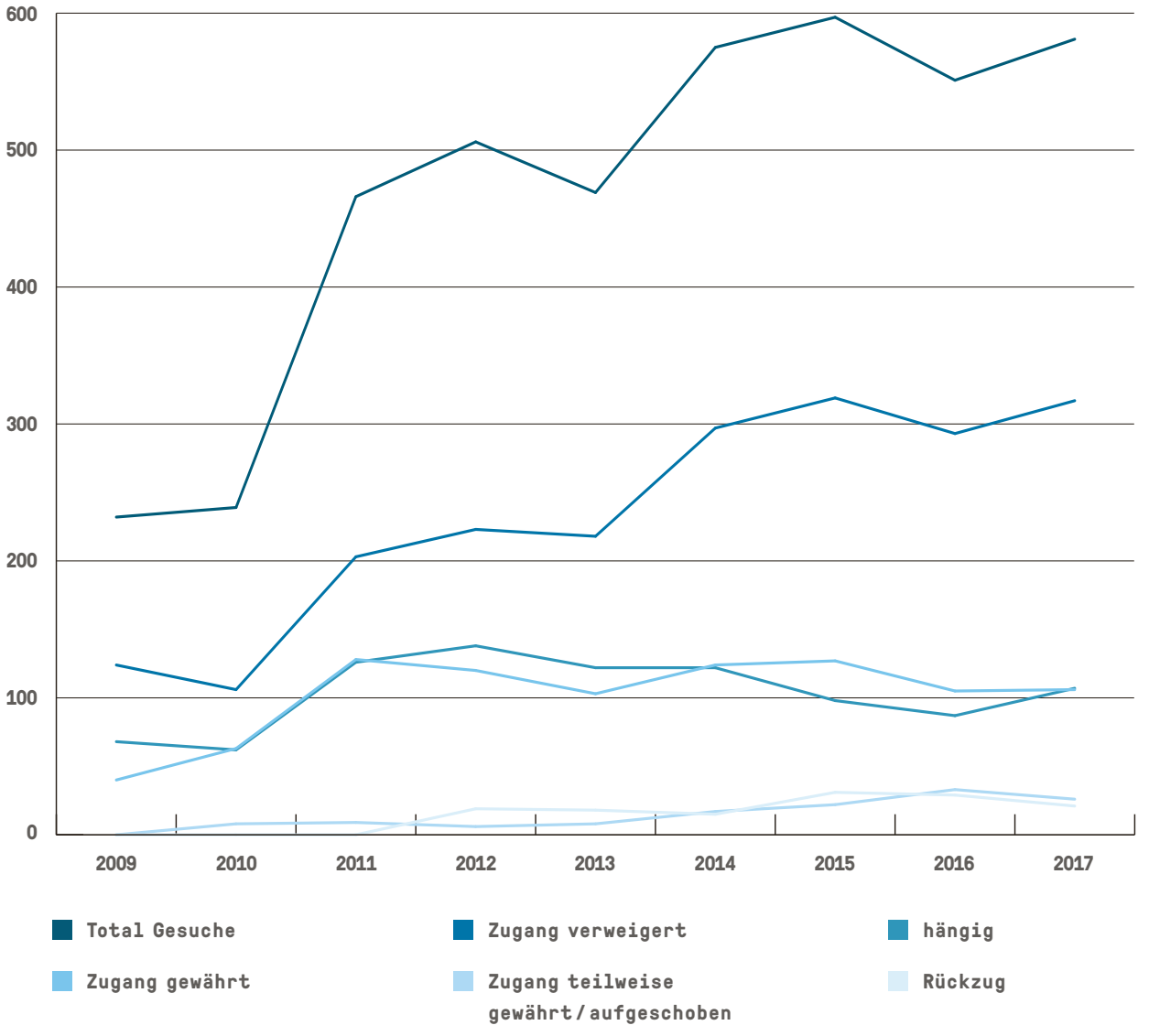
Schliesslich befassten sich die Delegierten mit der Empfehlung aus dem Jahr 2012 zum Kinderschutz im Internet. Sie sollte überarbeitet und auf den neusten Stand gebracht werden, da sich die Politik zum Schutz der Kinder im Cyberspace seit 2012 weiterentwickelt hat. Die Delegierten diskutierten insbesondere die Risiken, denen Kinder im Internet ausgesetzt sind. Ihrer Ansicht nach sind eingehendere Untersuchungen und verstärkte Aufklärung und Schulung notwendig – sowohl bei Kindern als auch bei Erwachsenen. Bei der Erhebung von Personendaten über Kinder mittels mobiler Anwendungen und der Rolle der elterlichen Zustimmung wurde ebenfalls Vertiefungsbedarf ermittelt. Zudem stellt sich die Frage, inwiefern die Anonymität ein Risiko darstellt und ob die digitale Identität daher auch Gegenstand der Arbeiten sein sollte. Das vorgeschlagene Verfahren zur ersten Überprüfung der Empfehlung wird verabschiedet.

Öffentlichkeitsprinzip

2.1 Zugangsgesuche

Gemäss den uns übermittelten Zahlen für das Jahr 2017 wurden bei den Bundesbehörden 581 Zugangsgesuche eingereicht (gegenüber 551 im Jahr 2016). 2017 waren es (einschliesslich Bundesanwaltschaft und Parlamentsdienste) insgesamt gar 590 Zugangsgesuche (siehe unten). In 317 Fällen (55 %) gewährten die Ämter einen vollständigen Zugang (gegenüber 293 im Jahr 2016, d.h. 53,17 %), während in 106 Fällen (18 %) nur ein teilweiser Zugang zu den Dokumenten gewährt wurde (gegenüber 105 Fällen im Jahr 2016 [19,05 %]). Bei 107 Gesuchen (18 %) wurde die Einsichtnahme vollständig verweigert (gegenüber 87 Fällen im Jahr 2016 [15,78 %]). 21 Zugangsgesuche (4 %) wurden zurückgezogen (gegenüber 29 im Jahr 2016 [5,26 %]) und 26 Fälle (5 %) waren Ende 2017 noch hängig (gegenüber 33 im Jahr 2016 [5,98 %]).

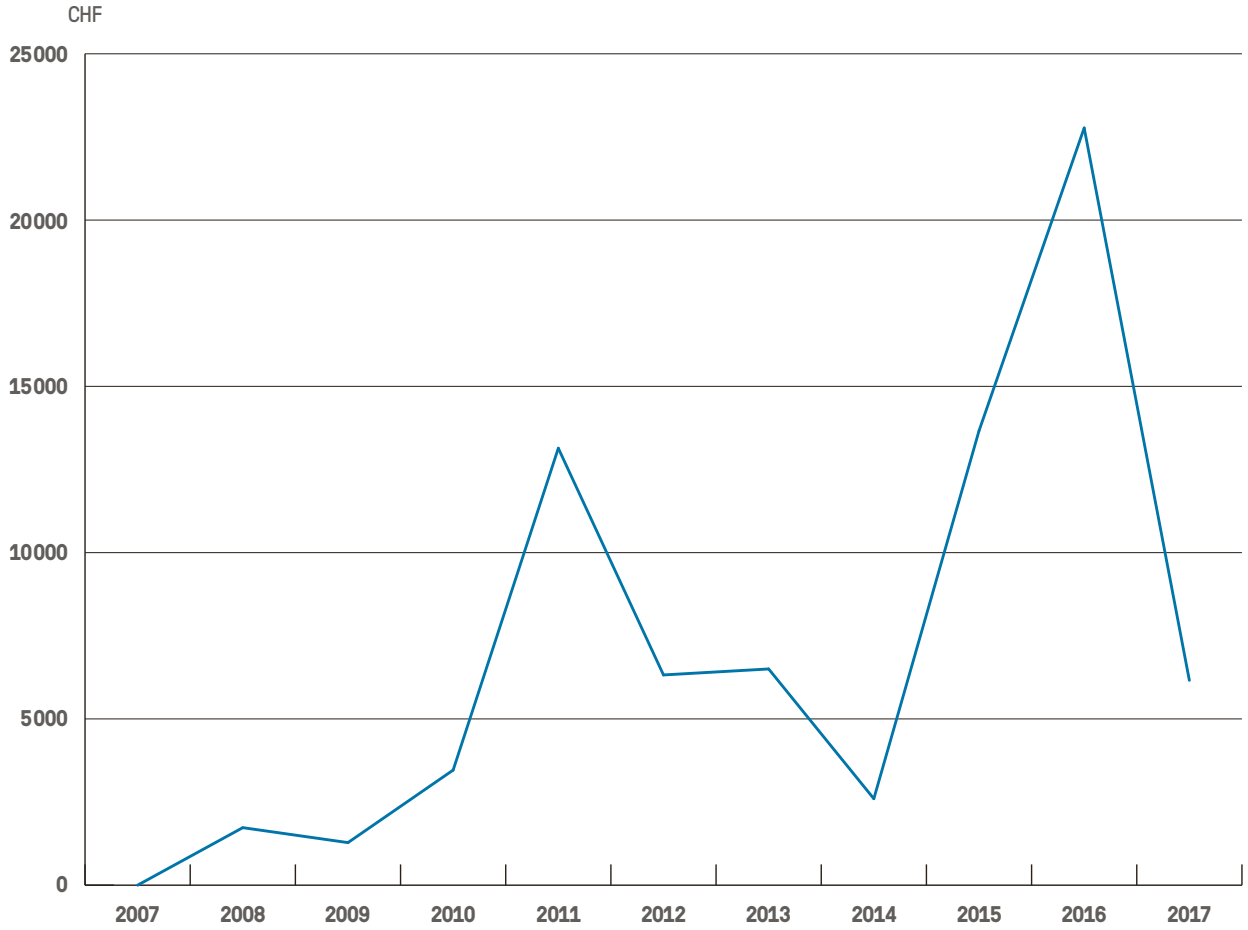
Der EDÖB hält generell fest, dass sich die Anzahl Gesuche nach einem starken Anstieg in den Jahren 2013 (469 Gesuche) und 2014 (575 Gesuche) nun bei einem Wert zwischen 550 und 600 Gesuchen pro Jahr eingependelt zu haben scheint. Was die Gesamtzahl der Zugangsgesuche und die Praxis der Ämter im Umgang mit Gesuchen anbelangt, zeigen die Zahlen mit Blick auf die vergangenen Jahre insgesamt ein stabiles Bild. Demnach wurde der Zugang durchschnittlich in etwas mehr als der Hälfte aller Fälle vollständig gewährt, in einem Fünftel der Fälle wurde er teilweise und in den restlichen Fällen vollständig verweigert. Seit 2015 stellt der EDÖB zudem eine Stabilisierung der Anzahl Gesuche auf vollständige Zugang bei knapp über 50 Prozent fest. Im Vergleich dazu ist die Zahl der vollständig abgelehnten Zugangsgesuche seit 2015 stark zurückgegangen und hat sich bei 16,5 Prozent eingependelt.



2.1.1 Departemente und Bundesämter

Die meisten Zugangsgesuche für das Jahr 2017 auf Stufe Amt wurden dem EDÖB vom BAG mit 28 Gesuchen mitgeteilt. Danach folgen das ENSI (23) und das SEM (21). Bei den Departementen liegt das EDA (159 Gesuche) an der Spitze, gefolgt vom WBF (81) und vom UVEK (75). Bei 20 Ämtern ist im Lauf des Jahres 2017 kein einziges Zugangsgesuch eingegangen. Im selben Zeitraum sind beim EDÖB 13 Zugangsgesuche eingegangen: In 5 Fällen wurde der Zugang vollständig gewährt, in 6 weiteren teilweise. In zwei Fällen waren die geforderten amtlichen Dokumente nicht vorhanden.

Seit dem Inkrafttreten des Öffentlichkeitsgesetzes wurden nur bei 130 Zugangsgesuchen Gebühren erhoben. Dies entspricht lediglich 2,7 Prozent der bei den Bundesämtern und der Bundeskanzlei gemeldeten Zugangsgesuche (4780). Im Vergleich dazu wurden 2017 nur bei 1,89 Prozent der Zugangsgesuche Gebühren erhoben (bei 11 von 581). Wie bereits in den Vorjahren stellt der EDÖB daher fest, dass die Erhebung einer Gebühr die Ausnahme bleibt. Der im Berichtsjahr 2017 für den Zugang zu amtlichen Dokumenten erhobene Gebührenbetrag beläuft sich insgesamt auf 6160 Franken und fällt damit deutlich geringer aus als in den letzten Jahren (2016: 22'770 Fr.; 2015: 13'663 Fr.). Auffällig sind dabei auch die relativ konstanten Unterschiede in der Gebührenhandhabung zwischen den verschiedenen Ämtern. Während die Bundeskanzlei und das EDA einmal mehr überhaupt keine Gebühren erhoben, verrechneten die anderen sechs Departemente ihren Zeitaufwand den jeweiligen Gesuchstellern zumindest teilweise. Die effektiv erhobenen Gebühren gestalten sich schliesslich einigermassen homogen (EDI: 1600 Fr.; EJPD: 200 Fr.; VBS: 1300 Fr.; EFD: 1600 Fr.; WBF: 1300 Fr.; UVEK: 160 Fr.).



2.1.2 Parlamentsdienste

Die Parlamentsdienste meldeten uns für das Jahr 2017 3 Zugangsgesuche. Der Zugang wurde in allen 3 Fällen gewährt.

2.1.3 Bundesanwaltschaft

Die Bundesanwaltschaft meldete uns 6 Zugangsgesuche. Die Einsichtnahme wurde dabei 5 Mal vollständig gewährt und einmal vollständig verweigert.

2.2 Schlichtungsanträge

Im Jahr 2017 wurden beim EDÖB insgesamt 79 Schlichtungsanträge eingereicht, was einer Abnahme um 4 Prozent gegenüber dem Vorjahr entspricht (2016: 149). Wie im Vorjahr wurden die meisten Anträge von Privatpersonen eingereicht (99 von insgesamt 149 Anträgen im Jahr 2016 und 35 von insgesamt 79 Anträgen im Jahr 2017).

Diese Zahlen lassen folgende Schlüsse und Bemerkungen zu: In 213 Fällen verweigerte die Bundesverwaltung den Zugang vollständig (107) respektive teilweise (106). Es wurden 79 Schlichtungsanträge eingereicht, was nur 37 Prozent der vollständig bzw. teilweise abgelehnten Zugangsgesuchen entspricht (77 % im Jahr 2016 und 43 % im Jahr 2015). Insgesamt konnten im Berichtsjahr 110 Schlichtungsanträge abgeschlossen werden. Davon stammen 76 Anträge aus dem Berichtsjahr selbst, 30 aus dem Jahr 2016, 3 aus dem Jahr 2015 und einer noch aus dem Jahr 2014. Für die lange Verfahrensdauer der 3 aus dem Jahr 2015 stammenden Fälle gibt es mehrere Gründe (mangelnde Kooperationsbereitschaft des Amtes, Verlängerung der Fristen durch die Betroffenen etc.), während im Fall aus dem Jahr 2014 das Verfahren bis zu einem Urteil des Bundesverwaltungsgerichts sistiert wurde.

2017 konnte in 47 Fällen zwischen den Beteiligten eine Schlichtung erzielt werden. In Fällen, in denen eine einvernehmliche Lösung nicht ersichtlich war, erliess der EDÖB 31 Empfehlungen, mit denen 40 Schlichtungsanträge erledigt werden konnten. 5 Schlichtungsanträge wurden ferner zurückgezogen und in zwei Fällen waren die Voraussetzungen für die Anwendung des Öffentlichkeitsgesetzes nicht gegeben. In 15 weiteren Fällen wurde der Schlichtungsantrag nicht fristgerecht eingereicht. Ein eingereichter Schlichtungsantrag wurde auf Wunsch der Beteiligten sistiert.

Sämtliche im Verlauf des Jahres ausgesprochenen Empfehlungen können auf der Website des EDÖB eingesehen werden (www.edoeb.admin.ch, Öffentlichkeitsprinzip – Empfehlungen).

2.3 Auswertung des Pilotversuchs 2017

Zur Beschleunigung des Schlichtungsverfahrens und zum Abbau von Pendenzen führte der EDÖB im Jahr 2017 einen Pilotversuch durch. Der Auswertungsbericht zeigt nun, dass mit den ergriffenen Massnahmen die gesetzten Ziele erreicht wurden und der Pilotversuch erfolgreich war. Angesichts der positiven Resultate wird er in den ordentlichen Betrieb überführt.

Wie in seinem letzten Tätigkeitsbericht angekündigt, hat der EDÖB auf Januar 2017 die Methode zur Durchführung von Schlichtungsverfahren angepasst und einen Pilotversuch gestartet, um die Dauer der Schlichtungsverfahren zu verkürzen und die Rückstände bei den hängigen Anträgen abzubauen (s. 24. Tätigkeitsbericht 2016/2017, Ziffer 2.4.1). Diese Anpassung rechtfertigte sich angesichts der seit Inkrafttreten des Öffentlichkeitsgesetzes ergangenen grossen Anzahl an Empfehlungen des EDÖB und Urteilen des Bundesverwaltungs- und des Bundesgerichts.

2.3.1 Pilotversuch

Im Rahmen des einjährigen Pilotversuchs wurden ab dem 1. Januar 2017 die neuen und, soweit sinnvoll, auch die bereits hängigen Schlichtungsanträge mehrheitlich in mündlichen Schlichtungsverhandlungen mit den beteiligten Personen und Behörden durchgeführt. Konnte im Pilotversuch an der Schlichtungsverhandlung keine Einigung erzielt werden, eröffnete der EDÖB seine Empfehlung mündlich. Die schriftliche Empfehlung mit einer kurzen, summarischen Begründung wurde den Beteiligten zeitnah zugestellt. Nur in Ausnahmefällen wurde direkt, d.h. ohne vorgängige Schlichtungsverhandlung, eine schriftliche Empfehlung abgegeben, so z.B. bei neuen, anspruchsvollen juristischen Fragestellungen, komplexen Zugangskonstellationen, bei Massenverfahren (mehrere Dritte oder Antragsteller) oder wenn die Aktenlage offensichtlich und der Entscheid eindeutig war (z.B. Nichteintreten).

Tabelle 1: Bearbeitungsdauer Schlichtungsverfahren

Bearbeitungsdauer in Tagen	Zeitraum 2014 – August 2016	Pilotphase 2017
innert 30 Tagen	11 %	59 %
zwischen 31 und 99 Tagen	45 %	37 %
mehr als 100 Tage	44 %	4 %

*Quelle: Präsentation Beauftragter, Veranstaltung 10 Jahre BGÖ, 2.9.2017

Mit dem Pilotversuch wurden folgende drei Ziele verfolgt:

- mindestens teilweise Einhaltung der Ordnungsfristen;
- Steigerung des Anteils an einvernehmlichen Lösungen;
- mittelfristiger Abbau von Pendenzen.

Anfang 2018 hat der EDÖB den Pilotversuch ausgewertet und einen Bericht erstellt. Auszugsweise werden nachfolgend die Ergebnisse präsentiert. Der vollständige Auswertungsbericht ist auf unserer Website veröffentlicht (www.derbeauftragte.ch, Öffentlichkeitsprinzip – Evaluationen).

2.3.2 Einhaltung der Ordnungsfrist

Die Tabelle 1 zeigt die Dauer der behandelten Schlichtungsverfahren, aufgeteilt in die gesetzliche Ordnungsfrist von 30 Tagen sowie in Zeitabschnitte von 31 und 99 Tagen und von mehr als 100 Tagen. Diesen zugeordnet wurde in Prozentwerten die durchschnittliche Bearbeitungsdauer der Schlichtungsanträge für den Zeitraum der Jahre 2014 bis Ende August 2016 sowie die Prozentwerte der in der Pilotphase im Jahr 2017 eingegangenen Schlichtungsanträge.

Im Zeitraum der Jahre 2014 bis 2016 konnte in 11 Prozent der Fälle die 30-tägige Ordnungsfrist eingehalten werden. In 45 Prozent der Fälle betrug die Bearbeitungsdauer zwischen 31 und 99 Tagen und in 44 Prozent der Fälle wurde ein Bearbeitungsaufwand von über 100 Tagen ausgewiesen.

Im Pilotjahr wurde die 30-tägige Ordnungsfrist in 45 von 76 Schlichtungsverfahren eingehalten.

Dies entspricht nahezu 60 Prozent der erledigten Schlichtungsanträge. In 28 Fällen (37 %) betrug die Bearbeitungsfrist zwischen 31 und 99 Tagen und in lediglich 3 Fällen (4 %) wurde für die Bearbeitung der Verfahren mehr als 100 Tage benötigt.

Werden die Prozentwerte des Jahres 2017 mit den durchschnittlichen Werten des Zeitraumes von 2014 bis 2016 verglichen, so zeigt sich, dass im Pilotversuch die Einhaltung der gesetzlichen Ordnungsfrist von 30 Tagen signifikant von 11 auf 59 Prozent gesteigert werden konnte. Ebenso deutlich konnte die Anzahl der Fälle, für welche die Bearbeitungszeit mehr als 100 Tage beträgt, von 44 auf 4 Prozent gesenkt werden.

Fazit: Mit dem Pilotversuch konnte nicht nur die Anzahl der innert Frist erledigten Schlichtungsanträge markant gesteigert, sondern auch die Bearbeitungszeit der gesamten erledigten Schlichtungsverfahren erheblich reduziert werden.

In den verbleibenden Fällen konnte die 30-tägige Ordnungsfrist aus folgenden, in erster Linie fallimmanenten Gründen nicht eingehalten werden:

- Verschiebung des Termins der Schlichtungsverhandlung auf Begehren der Parteien;
- Schlichtungsfälle mit besonders aufwändiger Bearbeitung;
- Abwarten der Frist zur Einreichung von Schlichtungsanträgen aufgrund mehrerer Gesuchsteller respektive Dritter in derselben Angelegenheit;
- Zusätzlicher Zeitaufwand für Einigungsbemühungen oder Sistierungen im Einvernehmen mit den Parteien;
- Eingehen von vielen Schlichtungsanträgen innerhalb eines kurzen Zeitraums.

Im Zusammenhang mit der Durchführung des Schlichtungsverfahrens gilt es darüber hinaus zu beachten, dass die knappe Ordnungsfrist von 30 Tagen in einem Spannungsverhältnis zum Mediationszweck des Schlichtungsverfahrens steht.

2.3.3 Anzahl der einvernehmlichen Lösungen

Für die Beantwortung der Frage, ob mit dem Pilotversuch eine Steigerung der einvernehmlichen Lösungen gegenüber der Praxis in den Jahren von 2006 bis 2016 erzielt werden konnte, wurde die Anzahl der erzielten Einigungen und Empfehlungen zueinander in Verhältnis gesetzt. Dabei wurden drei Zeitabschnitte analysiert: Der erste Zeitraum bildet gesamthaft die Ergebnisse der Schlichtungstätigkeit der Jahre 2006 bis 2016 ab. Der zweite Zeitraum der Jahre 2013 bis 2016 wurde gewählt, da ab 2013 vermehrt Schlichtungsverhandlungen durchgeführt wurden. Für den dritten Zeitraum, die Zeitspanne des Pilotversuches, wurden nicht nur die neu im Versuchsjahr eingegangenen Schlichtungsanträge, sondern zusätzlich alle noch hängigen 33 Schlichtungsverfahren berücksichtigt.

Tabelle 2: Verhältnis Empfehlungen und einvernehmliche Lösungen

Verhältnis Empfehlungen und einvernehmliche Lösungen	
2006–2016	25% einvernehmliche Lösungen
2013–2016	40% einvernehmliche Lösugen
2017	60% einvernehmliche Lösungen

Gesamthaft betrachtet wurden bis 2016 in 25 Prozent der Verfahren einvernehmliche Lösungen erzielt. Im Zeitraum 2013 bis 2016 kam es in 40 Prozent der Fälle zu einer einvernehmlichen Lösung. Im Jahr 2017 wurde in 60 Prozent der Schlichtungsverfahren eine einvernehmliche Lösung erzielt und in 40 Prozent eine Empfehlung erlassen.

Fazit: Mit dem Pilotversuch konnte der Anteil einvernehmlicher Lösungen erheblich gesteigert werden.

2.3.4 Auswertung Feedbackfragebogen

Seit mehreren Jahren werden die Teilnehmenden am Ende jeder Schlichtungsverhandlung eingeladen, einen Feedbackbogen auszufüllen. Für jede Aussage kann eine Punktzahl zwischen 5 (höchste) und 1 (niedrigste) vergeben werden.

Der Schlussbericht Evaluation 2014 enthält auch eine Auswertung dieser Feedbackbogen. Ebenso wurden die Feedbacks der Beteiligten für das Pilotjahr ausgewertet. Die Tabelle 3 vergleicht die Ergebnisse des Pilotversuches mit jenen der Evaluation 2014.

Im Jahr 2017 wurden 80 Feedbackbogen ausgefüllt (gegenüber 52 ausgewerteten in der Evaluation 2014). Davon lassen sich 37 Feedbackbogen den Antragstellenden (25 im Jahr 2014) und 43 den Vertretern der Bundesbehörden (27 im Jahr 2014) zuordnen. Die Auswertung aller eingereichten Feedbackbogen ergibt, dass die Ergebnisse nach wie vor ausgezeichnet sind. Nach Ansicht des Beauftragten zeigen die hohen Bewertungen durch die Teilnehmenden auch deutlich die Bedeutung und die positiven Auswirkungen von Schlichtungsverhandlungen bei der einvernehmlichen Erledigung von Zugangsgesuchen nach dem Öffentlichkeitsgesetz, was nicht zuletzt auch zu einer Verbesserung der Beziehungen zwischen Verwaltung und Bürgerinnen und Bürgern führt.

Tabelle 3: Auswertung der Feedbackfragebogen, arithmetischer Mittelwert

Aussagen	Pilotversuch 2017	Evaluation 2014
1. Ich bin mit dem Verlauf der Schlichtungsverhandlung zufrieden. (zufrieden – nicht zufrieden)	4.3*	4.4*
2. Ich bin der Meinung, dass die Schlichtungsverhandlung in einem Klima des Vertrauens stattgefunden hat. (trifft zu – trifft nicht zu)	4.7*	4.5*
3. Ich habe den Eindruck, dass die Schlichtung fair und gerecht geführt wurde. (trifft zu – trifft nicht zu)	4.7*	4.8*
4. Ich habe den Eindruck, dass die Schlichtungspersonen meine Anliegen gehört und ernst genommen haben sowie darauf eingegangen sind. (trifft zu – trifft nicht zu)	4.7*	4.8*
5. Ich hatte den Eindruck, dass die Gegenseite meine Anliegen gehört hat und darauf eingegangen ist. (trifft zu – trifft nicht zu)	3.5*	3.8*
6. Das Sitzungszimmer wirkte auf mich (angenehm – nicht angenehm)	4.1*	3.9*
7. Insgesamt beurteile ich die Schlichtungsverhandlung – unabhängig vom Resultat – als (positiv – negativ)	4.5*	4.6*
Anzahl ausgewertet Feedbackbogen	**80**	**52**

* Die höchste Punktzahl beträgt 5

2.3.5 Abbau Pendenzen

Ende des Jahres 2016 waren insgesamt 33 Schlichtungsverfahren pendent. Von den im Jahr 2017 eingereichten 79 Schlichtungsanträgen konnten 76 Verfahren bis Ende 2017 erledigt werden. Zwei Fälle waren zu diesem Zeitpunkt in Bearbeitung und ein Fall wurde im Einvernehmen mit den Beteiligten sistiert.

Die Tabelle 4 zeigt die Anzahl Pendenzen des Schlichtungsverfahrens Ende 2016 sowie jene am Ende des Pilotversuches.

Tabelle 4: Pendenzen Schlichtungsverfahren

Pendenzen Schlichtungsverfahren	
Ende 2016	33
Ende 2017	3 (2 in Bearbeitung; 1 Sistierung)

Fazit: Bis Ende 2017 konnte die Anzahl der pendenten Schlichtungsverfahren von 33 auf drei abgebaut werden.

2.3.6 Zusammenfassung

In seiner Gesamtheit beurteilt der Beauftragte den einjährigen Pilotversuch als erfolgreich. Alle drei vom Beauftragten gesetzten Ziele wurden erreicht:

- Die Ordnungsfrist von 30 Tagen konnte für die im Jahr 2017 eingegangenen Schlichtungsanträge in fast 60 Prozent der Fälle eingehalten werden. In den übrigen Schlichtungsverfahren war dies aufgrund fallimmanenter Gründe nichtt möglich. Die knappe Ordnungsfrist steht grundsätzlich in einem Spannungsverhältnis zum Mediationszweck des Schlichtungsverfahrens;
- Der Anteil einvernehmlicher Lösungen konnte im Vergleich zu früheren Zeiträumen erheblich gesteigert werden. Im Pilotjahr konnte in 60 Prozent aller Schlichtungsverfahren eine Einigung erzielt werden;
- Die Pendenzen aus den Vorjahren wurden abgebaut.

Angesichts der positiven Resultate überführt der Beauftragte den Pilotversuch in den ordentlichen Betrieb. Die erfolgreich eingesetzten Massnahmen (mehrheitlich mündliche Verfahren, summarische Begründungen der Empfehlungen, schriftliche Verfahren nur in Ausnahmefällen) werden für die Durchführung von Schlichtungsverfahren integral beibehalten. Anpassungen an neue Entwicklungen und Erkenntnisse bleiben selbstverständlich vorbehalten.

2.4 Ämterkonsultationen und Stellungnahmen

2.4.1 Verordnung über den Nachrichtendienst

Der Verordnungsentwurf zum neuen Nachrichtendienstgesetz enthielt anfangs eine Bestimmung, mit der praktisch sämtliche Dokumente des Nachrichtendiensts des Bundes (NDB) vom Öffentlichkeitsgesetz ausgenommen worden wären. Die von uns kritisierte Bestimmung wurde im Anschluss an die Vernehmlassung gestrichen.

Das am 1. September 2017 in Kraft getretene Nachrichtendienstgesetz (NDG) sieht vor, dass das Öffentlichkeitsgesetz (BGÖ) nicht für den Zugang zu amtlichen Dokumenten betreffend die Informationsbeschaffung gilt. Der Entwurf für die Verordnung über den Nachrichtendienst (NDV) sah zunächst eine Ausführungsbestimmung zu dieser im Gesetz vorgesehenen Ausnahme vor. Wir haben diese Bestimmung im Rahmen der ersten Ämterkonsultation abgelehnt, da sie die Ausnahme vom Öffentlichkeitsgesetz nicht auf die im übergeordneten Recht vorgesehene nachrichtendienstliche Informationsbeschaffung begrenzte, sondern in unzulässiger Weise auf praktisch sämtliche Dokumente und Informationen des NDB ausweitete. Die von uns beantragten Änderungen wurden vor dem Vernehmlassungsverfahren nicht übernommen (vgl. unseren 24. Tätigkeitsbericht 2016/2017, Ziffer 2.3.3).

Im Anschluss an die Vernehmlassung unterbreitete der NDB einen angepassten Entwurf der NDV zur erneuten Ämterkonsultation, welcher die oben erwähnte Bestimmung nicht mehr enthielt. Wir begrüssten diesen Schritt. Die Verordnung über den Nachrichtendienst ist am 1. September 2017 in Kraft getreten.

2.4.2 Bundesgerichtsurteil: Zugang zu Gefährdungs- und Störungsmeldungen im öffentlichen Verkehr

Das Bundesgericht hat entschieden, dass die in einer Datenbank des Bundesamts für Verkehr (BAV) verzeichneten Gefährdungen und Störungen im öffentlichen Verkehr bekannt gegeben werden müssen. Es hat die Beschwerde der Behörde abgewiesen, die einem Journalisten die Einsicht verweigern wollte.

Das zuständige Bundesamt für Verkehr (BAV) hatte den Zugang abgelehnt, da es bei einer Offenlegung dieser Informationen eine ernsthafte Beeinträchtigung seiner Aufsichtstätigkeit befürchtete. Es berief sich dabei auf eine im Öffentlichkeitsgesetz vorgesehene Ausnahmebestimmung, wonach der Zugang zu Dokumenten verweigert werden kann, wenn die zielkonforme Durchführung konkreter behördlicher Massnahmen beeinträchtigt wird. Das BAV rechnete bei einer Bekanntgabe insbesondere mit einem künftigen Rückgang der Meldungen von Zwischenfällen durch die Transportunternehmen und einem sich daraus ergebenden Sicherheitsrisiko im öffentlichen Verkehr.

Das Bundesgericht ist dieser Argumentation nicht gefolgt. Es stimmte den Erwägungen des vorinstanzlichen Urteils des Bundesverwaltungsgerichts zu, wonach die angerufene Ausnahmebestimmung höchstens bei einzelnen, konkreten behördlichen Massnahmen zur Anwendung gelangt, nicht jedoch bei der Aufgabenerfüllung und Aufsichtstätigkeit einer Behörde insgesamt. Es wies darauf hin, dass hinsichtlich sicherheitsrelevanter Vorfälle eine gesetzliche Meldepflicht für die beaufsichtigten Transportunternehmen besteht und davon ausgegangen werden kann, dass diese beachtet wird. Sollte dies nicht der Fall sein, so beeinträchtige bereits dieses rechtswidrige Verhalten der Beaufsichtigten das Ergreifen geeigneter aufsichtsrechtlicher Massnahmen und nicht erst die Bekanntgabe von vorhandenen Informationen nach dem Öffentlichkeitsgesetz. Gemäss Bundesgericht obliegt es dem BAV, im Rahmen seiner Aufsichtstätigkeit durch Kontrollen oder andere geeignete Massnahmen die Einhaltung der gesetzlichen Meldepflicht der Transportunternehmen zu überprüfen und entsprechende Verstösse zu sanktionieren. Das Bundesgericht betonte, dass das Öffentlichkeitsprinzip durch die Schaffung von Transparenz eine wirksame Kontrolle der staatlichen Behörden und deren (Aufsichts-) Tätigkeit bezweckt. Diese Kontrolle sei in diesem konkreten Fall nur möglich, wenn offen gelegt wird, bei welchen der wichtigsten Transportunternehmen es zu wie vielen und welchen

Zwischenfällen auf welchen Strecken gekommen ist, weshalb eine Anonymisierung der Namen der Transportunternehmen nicht möglich sei. Nach Auffassung des Gerichts besteht ein überwiegendes öffentliches Interesse an der Offenlegung von Zwischenfällen im öffentlichen Verkehr, zumal diese Unternehmen aufgrund des Konzessionsverhältnisses und der Mitfinanzierung durch die öffentliche Hand eine gewisse Staatsnähe aufweisen. (Urteil BGer 1C_428/2016 vom 27. September 2017)

Wie das Bundesgericht in diesem Urteil festhält, steht das Öffentlichkeitsprinzip der Aufsichtstätigkeit des BAV nicht entgegen. Gleichwohl ist der Nationalrat am 27. Februar 2018 dem Bundesrat gefolgt und hat sich im Rahmen der Detailberatung der Vorlage zur Organisation der Bahninfrastruktur (OBI) für die Ausnahme der Aufsichtstätigkeit des BAV im Sicherheitsbereich vom Öffentlichkeitsgesetz ausgesprochen. (vgl. unseren 24. Tätigkeitsbericht 2016/2017, Ziffer 2.3.1)

2.4.3 Vorentwurf zur Änderung der Verordnung über den Zugang zu Dokumenten des Kantons Freiburg

Im Rahmen seiner Zusammenarbeit mit den Kantonen wurde der EDÖB vom Kanton Freiburg um eine Stellungnahme zum Vorentwurf zur Änderung der Verordnung über den Zugang zu Dokumenten gebeten. Letztere ist an die Aarhus-Konvention anzupassen und beruht auf dem Gesetz vom 5. Oktober 2016 über die Änderung des Gesetzes über die Information und den Zugang zu Dokumenten (InfoG), bei dem der EDÖB bereits im Jahr 2015 zur Kommentierung aufgefordert wurde (siehe 23. Tätigkeitsbericht 2015/2016, Ziffer 2.3.5).

Der im Verlauf des Jahres 2017 vorgestellte Vorentwurf sollte in erster Linie dazu dienen, die notwendigen Änderungen einzuführen, um der Erweiterung des persönlichen und sachlichen Anwendungsbereichs des InfoG Rechnung zu tragen, neue Verfahrensvorschriften insbesondere hinsichtlich der in der Aarhus-Konvention geforderten Fristen vorzusehen, die Zuständigkeitsregelungen bei der Behandlung bestimmter Zugangsgesuche anzupassen sowie aufgrund der in den ersten sechs Jahren erworbenen Erfahrungen verschiedene verfahrenstechnische Schwerfälligkeiten zu beheben.

In seiner Stellungnahme hat der EDÖB sich für den vorgeschlagenen Vorentwurf ausgesprochen, aber auch darauf hingewiesen, dass die Ämter kein Recht haben sollten, den Zugang zu verweigern, wenn ein Gesuch ihnen von vornherein missbräuchlich erscheint. Tatsächlich ist es gemäss dem Öffentlichkeitsprinzip nicht erforderlich, dass der Gesuchsteller ein schutzwürdiges Interesse oder eine spezifische Verwendung geltend macht, um Zugang zu Dokumenten bzw. die Dokumente selber zu erhalten. Daher darf nicht ohne Weiteres von einem allfälligen missbräuchlichen Verhalten des Gesuchstellers ausgegangen werden. Infolgedessen hat das betroffene Amt in jedem konkreten Fall zu prüfen, ob das Zugangsgesuch tatsächlich missbräuchlich ist.

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. Im Rahmen seiner Botschaft zur Totalrevision des DSG hat der Bundesrat dem EDÖB die Schaffung zusätzlicher Mittel in der Grössenordnung von 10 Stellen in Aussicht gestellt (BBl 2017 7172). Aufgrund der Verzögerung der Totalrevision (s. Kapitel 1.2.1 des vorliegenden Berichts) ist zurzeit nicht absehbar, ob und wann diese Stellen rekrutiert werden können.

Für DSG-Belange einsetzbare Stellen	2005	2010	2017	2018
	22	23	24	24

Beratung

Wie im Kapitel «Aktuelle Herausforderungen und Schwerpunkte» dargelegt wurde, sieht sich der EDÖB im Leistungsbereich der Beratung, aufgrund der Notwendigkeit immer umfangreichere und komplexere Projekte zu begleiten, mit einer ungebremst wachsenden Nachfrage konfrontiert. In der Berichtsperiode wurden erstmals über 50 Prozent der personellen Mittel für die Beratung aufgewendet. Besonders akzentuiert hat sich der Anstieg des Beratungsaufwandes für Private von 18,2 auf 20,8 Prozent fortgesetzt. Gemäss dem Kontrollplan des EDÖB für das Jahr 2018 ist die beratende Begleitung von 13 grossen Projekten im Gang.

Da die Mittel des EDÖB bisher weder an die gestiegenen technologischen Risiken der Re-Identifikation und zweckwidrigen Datenabflüsse noch an die übrigen Herausforderungen der Digitalisierung angepasst wurden, kann er die gestiegene Nachfrage nach beratender Projektbegleitung nach wie vor 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, ist wie in den Vorjahren von einer weiter steigenden Anzahl von umfangreichen Datenbearbeitungsprojekten von Staat und Wirtschaft auszugehen.

Beratungen in umfangreicheren Projekten für 2018	
Verkehr	3
Finanzen	2
Gesundheit und Arbeit	3
Sicherheit	2
Telekom / Internet of Things (IOT)	3

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	20.8 %	
Beratung Bund	14.0 %	
Zusammenarbeit mit Kantonen	4.6 %	
Zusammenarbeit mit ausl. Behörden	11.9 %	
Total Beratung		**51.3 %**
Aufsicht	10.8 %	
Zertifizierung	0.1 %	
Register Datensammlung	1.3 %	
Total Aufsicht		**12.2 %**
Information	13.5 %	
Ausbildung/Referate	4.4 %	
Total Information		**17.9 %**
Gesetzgebung	18.6 %	
Total Gesetzgebung		**18.6 %**
Total Datenschutz		**100.0 %**

Aufsicht

Aufgrund der Dynamik von Cloud-gestützten Applikationen müssen Kontrollen 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 bereits deutlich unter dem langjährigen Mittelwert von rund 20 Prozent lag. In der aktuellen Berichtsperiode ist dieser Wert noch einmal deutlich auf 12 Prozent abgesunken. Gemäss Kontrollplan für das Jahr 2018 werden mit diesen Mitteln noch 11 umfassendere Kontrollen bestritten.

Im Vergleich zu der Anzahl von rund 12'000 grossen und mittleren Unternehmen in der Schweiz erweist sich die aktuelle Kontrolldichte als tief. Für den Beauftragten wird es zunehmend schwierig, seine ressourcenbedingte Zurückhaltung bei der Eröffnung formeller Sachverhaltsabklärungen gegenüber Medien und Konsumentenschutzorganisationen zu vermitteln.

Gesetzgebung

Die vom Bundesrat in der Einleitung seiner Botschaft zur Totalrevision des DSG als «rasant» bezeichnete technologische Entwicklung (BBl 2017 6943) findet auch bei der Personendatenbearbeitung durch die Bundesorgane ihren Niederschlag, die nur auf der Basis gesetzlicher Grundlage zulässig ist und demzufolge eine Vielzahl von neuen Bearbeitungsvorschriften im Bundesrecht nach sich zieht, zu denen der EDÖB in diversen Konsultationsverfahren Stellung beziehen muss. Der diesbezügliche Aufwand ist in den letzten zehn Jahren und auch in der aktuellen Berichtsperiode deutlich angestiegen, was ebenfalls zum weiteren Absinken der Kontrolldichte beigetragen hat.

Totalrevision des DSG

Wie vorne dargelegt wurde, haben sich zeitgemässe Arbeitsinstrumente – wie die Datenschutz-Risikofolgenabschätzung – in der Praxis der digitalen Realität herausgebildet. Sie sind denn auch bei der Betreuung von digitalen Grossprojekten (s. Tabelle oben) für unsere Behörde zum Alltag geworden. Zur rechtssicheren Konsolidierung dieser Arbeitsinstrumente und der damit einhergehenden Aufsichtstätigkeit des EDÖB ist es unabdingbar, dass diese nicht nur in der DSGVO, sondern auch im schweizerischen Datenschutzrecht verankert werden, wie dies der Bundesrat in seiner Vorlage zur Totalrevision des DSG denn auch vorsieht. Da infolge Verzögerung dieser Totalrevision nicht absehbar ist, wann der in der Botschaft in Aussicht gestellte Stellenausbau in der Grössenordnung von 10 Stellen erfolgen kann, muss unsere Behörde die neuen Arbeitsinstrumente mit den bestehenden Personalressourcen so pragmatisch wie möglich umsetzen.

Dienststellenbesuche und Anhörungen durch die Geschäftsprüfungskommissionen

Am 14. Februar 2018 hat die für den EDÖB zuständige Subkommission EJPD/BK der Geschäftsprüfungskommission des Ständerats bei unserer Behörde einen Dienststellenbesuch vorgenommen, bei welchem die Geschäftslast im Bereich der Datenschutzaufsicht sowie das damit einhergehende Absinken der Kontrolldichte aufgrund der Zahlen des Tätigkeitsberichts 2016/17 erörtert wurden. Das Gleiche gilt für die Anhörungen durch die Subkommission EDI/UVEK der Geschäftsprüfungskommission des Nationalrates vom 6. Oktober 2017 betreffend «Digitale Technologie, Big Data, e-Ticketing, Sensorik und digitaler Lebensstil», durch die Subkommission EDI/UVEK der Geschäftsprüfungskommission des Nationalrates vom 20. März 2018 betreffend «eHealth – elektronisches Patientendossier» sowie durch das Plenum der Geschäftsprüfungskommission des Ständerats vom 27.3.2018 betreffend «Präsentation und Diskussion: Nationale E-Government Studie».

Bemessungskriterien

Ob und wann dem EDÖB zusätzliche Ressourcen zugesprochen werden, liegt in der Verantwortung der politischen Behörden, denen bei der Einschätzung aktueller und künftiger Entwicklungen der Digitalisierung und deren Auswirkungen auf die Tätigkeit unserer Behörde ein erheblicher Ermessensspielraum bleibt.
Kernaufgabe 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.

Wie die in Kapitel 2.3 dargelegte Auswertung zeigt, konnte dieses Ziel erreicht werden, zumal die Anzahl neuer Schlichtungsanträge im langjährigen Vergleich stabil geblieben ist.

3.2 Publikationen im laufenden Geschäftsjahr

Die Website www.derbeauftragte.ch ist der wichtigste Informationskanal des EDÖB und wird laufend aktualisiert und ergänzt. Sämtliche Empfehlungen und Urteile aus dem Bereich des Öffentlichkeitsgesetzes werden dort veröffentlicht. Im Bereich Datenschutz haben wir im Berichtsjahr zwei ausführliche Leitfäden für Schweizer Unternehmen publiziert: der eine erläutert den Swiss-US Privacy Shield, der andere die Ende Mai in Kraft getretene EU-Datenschutzgrundverordnung. Ausserdem wurde das Lehrmittel für die Sekundarstufen I und II aktualisiert.

Die EU-Datenschutz-Grundverordnung (DSGVO) ist auch für Schweizer Unternehmen, die Daten von EU-Bürgern bearbeiten oder ihre Dienstleistungen in der EU anbieten, unmittelbar anwendbar. Wir haben einen Leitfaden dazu erstellt, der sowohl über die neuen Pflichten für Unternehmen informiert als auch über die Rechte für Privatpersonen zum Schutz ihrer Privatsphäre. Mit der DSGVO sollen Bürgerinnen und Bürger mehr Kontrolle über ihre Personendaten erhalten. (www.derbeauftragte.ch, Dokumentation – Rechtliche Grundlagen – Datenschutz International).

Seit dem 12. April 2017 können sich amerikanische Unternehmen für das Swiss-US Privacy Shield zertifizieren lassen und damit ein angemessenes Datenschutzniveau garantieren. Die Broschüre des EDÖB zum Swiss-US Privacy Shield informiert über die Pflichten der zertifizierten Unternehmen und die Rechte betroffener Personen und wie diese im Beschwerdefall vorgehen können (www.derbeauftragte.ch, Datenschutz – Handel und Wirtschaft – Übermittlung ins Ausland – USA).

Mieterinnen und Mieter, die sich für eine Wohnung bewerben, müssen im Anmeldeformular oft viel Persönliches preisgeben. Welche Auskünfte in einem solchen Formular zulässig sind und aus welchen datenschutzrechtlichen Überlegungen auf gewisse Fragen verzichtet werden sollte, wird in unseren Erläuterungen ausführlich dargelegt (www.derbeauftragte.ch, Datenschutz – Wohnen und Verkehr – Anmeldeformulare für Mietwohnungen).

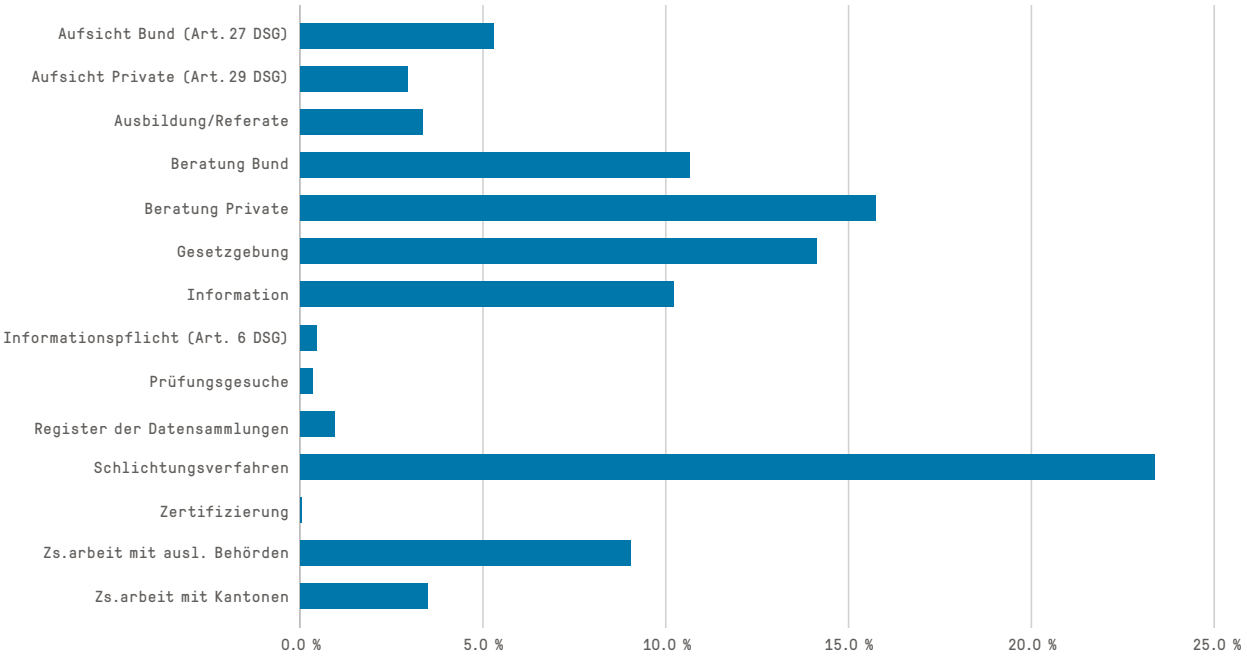
Damit ein Arbeitgeber der Krankentaggeldversicherung die nötigen Daten liefern darf, benötigt er eine Vollmacht des betroffenen Mitarbeiters. Die Versicherer verfügen bei der Formulierung dieser Vollmacht über einen grossen Spielraum. Sie sind jedoch dem Verhältnismässigkeitsprinzip verpflichtet und müssen sich auf die im konkreten Fall notwendigen Informationen beschränken (www.derbeauftragte.ch, Datenschutz – Versicherungen – Kranken-und Unfallversicherungen – Krankentaggeldversicherung).

Die Unterrichtseinheiten zum Datenschutz wurden letztes Jahr neu überarbeitet. Sämtliche Lektionen für die Sek-Stufen I und II liegen nun erstmals in allen drei Landessprachen vor (www.derbeauftragte.ch, Datenschutz – Internet und Computer – Kinder und Jugendliche).

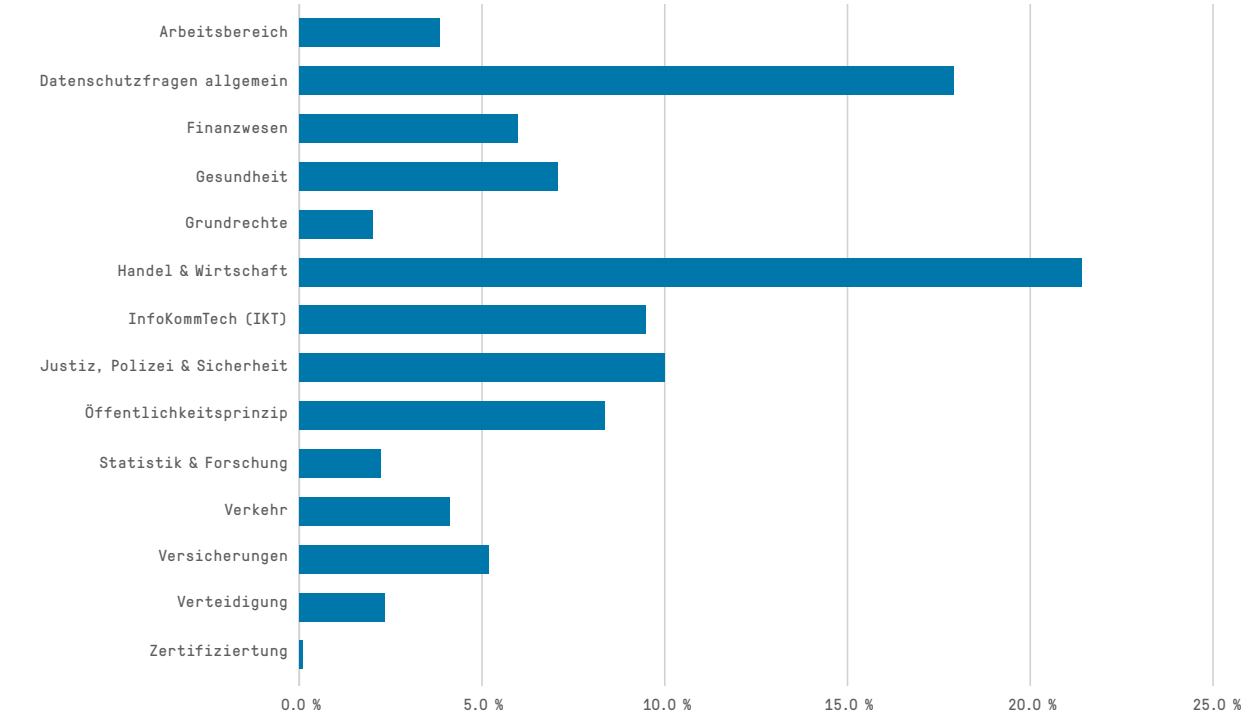
3.3 Statistiken

3.3.1 Statistiken über die Tätigkeiten des EDÖB vom 1. April 2017 bis 31. März 2018 (Datenschutz und Öffentlichkeitsprinzip)

Aufwand nach Aufgabengebiet

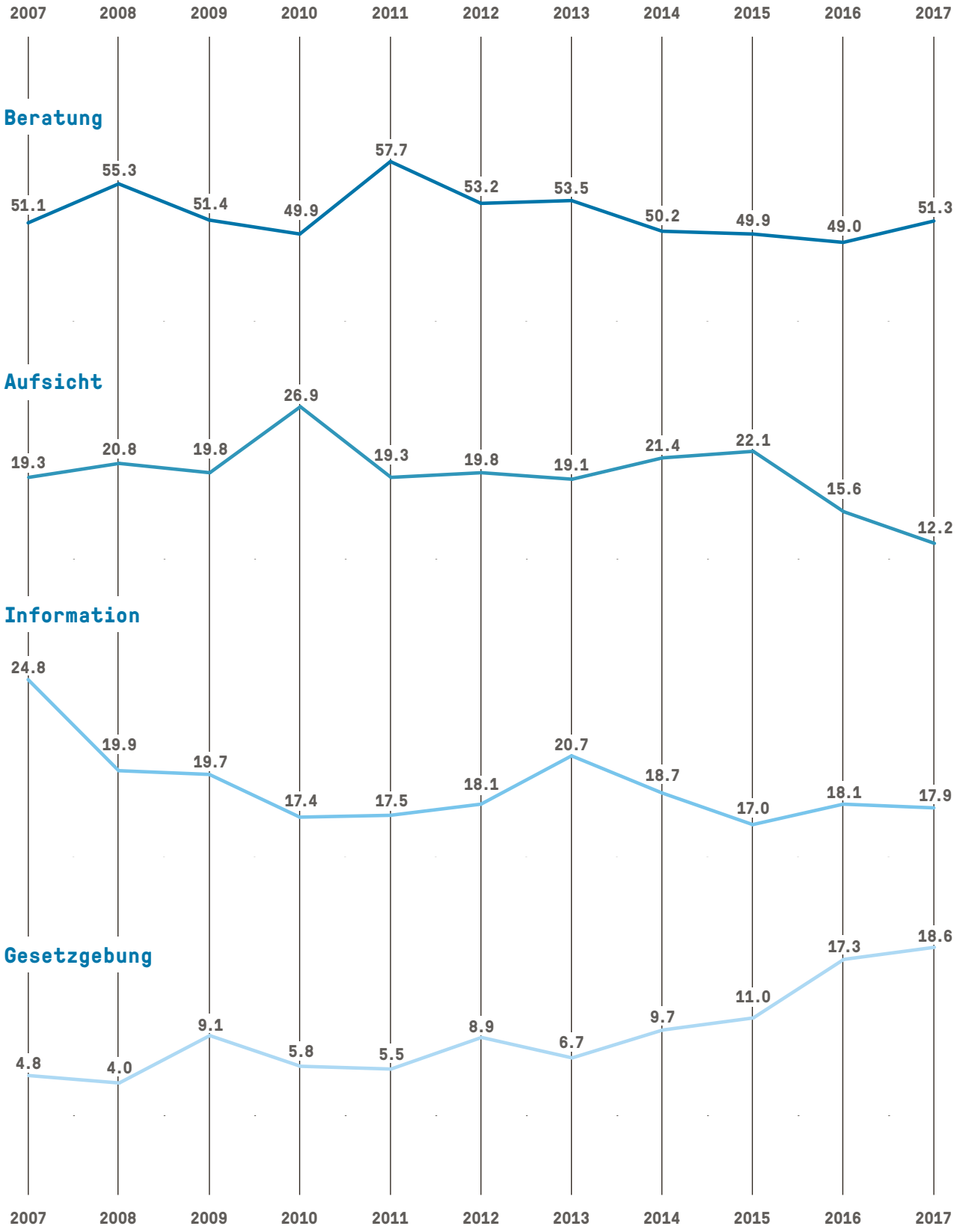


Aufwand nach Sachgebiet



Mehrjahresvergleich Aufwand

(alle Angaben in Prozent)



3.3.2 Statistiken über eingereichte Zugangsgesuche nach Öffentlichkeitsgesetz vom 1. Januar 2017 bis am 31. Dezember 2017

Bundeskanzlei BK

Betroffener Bereich	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teil-weise gewährt / aufgeschoben	Zugangsgesuch hängig	Zugangsgesuch zurückgezogen
BK	17	10	6	0	1	0
EDÖB	13	5	0	6	0	0
TOTAL	30	15	6	6	1	0

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	159	133	16	7	2	1
TOTAL	159	133	16	7	2	1

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	0	0	0	0	0	0
EBG	3	2	0	1	0	0
BAK	2	1	1	0	0	0
BAR	5	5	0	0	0	0
METEO CH	0	0	0	0	0	0
NB	0	0	0	0	0	0
BAG	28	9	3	8	5	3
BFS	1	0	0	1	0	0
BSV	8	4	3	0	0	0
BLV	10	6	1	2	1	0
SNM	0	0	0	0	0	0
SWISS MEDIC	11	2	2	4	0	3
SUVA	1	0	1	0	0	0
TOTAL	69	29	11	16	6	6

Eidgenössisches Finanzdepartement EFD

Betroffener Bereich	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teil-weise gewährt /aufgeschoben	Zugangsgesuch hängig	Zugangsgesuch zurückgezogen
GS	11	4	1	6	0	0
ISB	3	1	0	2	0	0
EFV	4	2	1	1	0	0
EPA	4	3	0	1	0	0
ESTV	6	1	3	1	1	0
EZV	12	4	6	2	0	0
EAV	1	1	0	0	0	0
BBL	9	5	0	3	0	1
BIT	0	0	0	0	0	0
EFK	12	4	5	3	0	0
SIF	3	1	1	0	0	1
PUBLICA	0	0	0	0	0	0
ZAS	4	1	1	2	0	0
TOTAL	69	27	18	21	1	2

Eidgenössische Justiz- und Polizeidepartement EJPD

Betroffener Bereich	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teil-weise gewährt / aufgeschoben	Zugangsgesuch hängig	Zugangsgesuch zurückgezogen
GS	2	2	0	0	0	0
BJ	4	2	1	0	1	0
FEDPOL	8	6	2	0	0	0
METAS	4	4	0	0	0	0
SEM	21	10	1	6	0	4
Dienst ÜPF	1	0	0	1	0	0
SIR	3	3	0	0	0	0
IGE	0	0	0	0	0	0
ESBK	0	0	0	0	0	0
ESchK	0	0	0	0	0	0
RAB	2	0	2	0	0	0
ISC	0	0	0	0	0	0
NKVF	0	0	0	0	0	0
TOTAL	45	27	6	7	1	4

Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK

Betroffener Bereich	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teil-weise gewährt /aufgeschoben	Zugangsgesuch hängig	Zugangsgesuch zurückgezogen
GS	0	0	0	0	0	0
BAV	5	3	0	0	0	2
BAZL	6	4	2	0	0	0
BFE	12	6	0	2	2	2
ASTRA	7	5	2	0	0	0
BAKOM	4	2	2	0	0	0
BAFU	14	9	2	2	1	0
ARE	0	0	0	0	0	0
ComCom	1	1	0	0	0	0
ENSI	23	5	3	4	9	1
PostCom	2	2	0	0	0	0
UBI	1	1	0	0	0	0
TOTAL	75	38	11	8	12	5

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	13	3	0	10	0	0
Verteidig./ Armee	6	3	1	1	1	0
NDB	10	3	7	0	0	0
armasuisse	16	1	11	4	0	0
BASPO	8	7	1	0	0	0
BABS	0	0	0	0	0	0
swisstopo	0	0	0	0	0	0
TOTAL	53	17	20	15	1	0

Eidgenössisches Departement für Wirtschaft, Bildung und Forschung WBF

Betroffener Bereich	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teil-weise gewährt /aufgeschoben	Zugangsgesuch hängig	Zugangsgesuch zurückgezogen
GS	17	6	1	10	0	0
SECO	20	10	5	4	0	1
SBFI	8	4	3	1	0	0
BLW	14	2	6	5	1	0
BWL	4	2	2	0	0	0
BWO	0	0	0	0	0	0
PUE	1	1	0	0	0	0
WEKO	9	4	2	2	0	1
ZIVI	0	0	0	0	0	0
BFK	2	2	0	0	0	0
SNF	0	0	0	0	0	0
EHB	0	0	0	0	0	0
KTI	0	0	0	0	0	0
ETH Rat	6	0	2	4	0	0
TOTAL	81	31	21	26	1	2

Bundesanwaltschaft

Betroffener Bereich	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teil-weise gewährt / aufgeschoben	Zugangsgesuch hängig	Zugangsgesuch zurückgezogen
BA	6	5	1	0	0	0
TOTAL	6	5	1	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	3	0	0	0	0
TOTAL	3	3	0	0	0	0

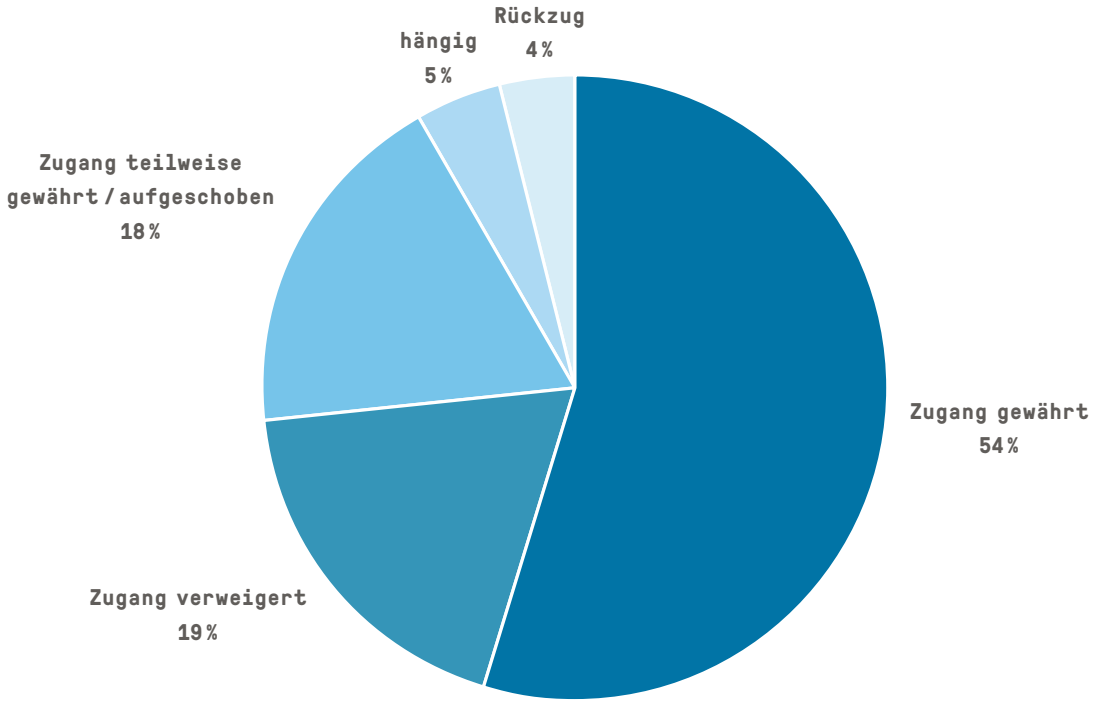
Übersicht der Zugangsgesuche der Departemente und der Bundeskanzlei

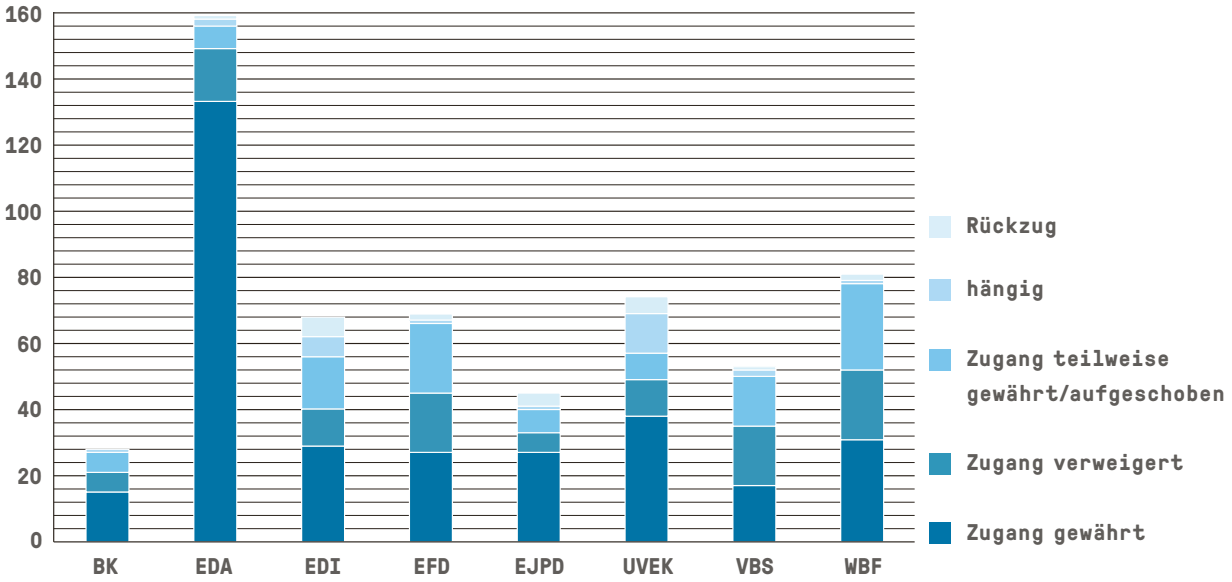
Depatement	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teil-weise gewährt / aufgeschoben	Zugangsgesuch hängig	Zugangsgesuch zurückgezogen
BK	30	15	6	6	1	0
EDA	159	133	16	7	2	1
EDI	69	29	11	16	6	6
EFD	69	27	18	21	1	2
EJPD	45	27	6	7	1	4
UVEK	75	38	11	8	12	5
VBS	53	17	18	15	2	1
WBF	81	31	21	26	1	2
TOTAL 2017 (%)	581 (100)	317 (55)	107 (18)	106 (18)	26 (5)	21 (4)
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	**2017**
Medien	**21**
Privatpersonen (bzw. keine genaue Zuordnung möglich)	**35**
Interessenvertreter (Verbände, Organisationen, Vereine usw.)	**14**
Rechtsanwälte	**2**
Unternehmen	**7**
Total	**79**

Zugangsgesuche der gesamten Bundesverwaltung





3.4 Das Sekretariat des EDÖB

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter

		Lobsiger Adrian
	Stellvertreter:	Walter Jean-Philippe

Direktionsbereich Datenschutz

	Leiter:	Buntschu Marc
	Stellvertreterin:	Haag Sophie
Team 1	Leiter:	Meier Thomas, Jurist
		Berger Cyrill, Jurist
		Frey Franziska, Juristin
		Weber Nathalie, 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
		Krüsi Melanie, Juristin
		Rossier Odile, Juristin

Direktionsbereich Öffentlichkeitsprinzip

Team	Leiter:	Ammann Reto
		Keller Annina, Juristin
		Bulliard Florian, 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
	Fasel Frédéric, Fachsp. I kaufm. Verwaltungsdienste
	von Gunten Fabien, Fachsp. I kaufm. Verwaltungsdienste

Fachbereich Kommunikation

	Meier Francis, Informationsbeauftragter
	Böhlen Silvia, Kommunikationsspezialistin

Kompetenzzentrum IT und Digitale Gesellschaft

Leiter:	Sidler Andreas, Informatiker/Jurist
	Aad Imad, Informatiker
	Däppen Daniel, Informatiker
	Gaukel Rahel, Informatikerin
	Scherrer Urs, Informatiker
	Stüssi Philipp, Informatiker

Direktionsbereich Internationale Angelegenheiten, Gesetzgebung und Kantone

Team	Leiter:	Walter Jean-Philippe
		Lennman Catherine, Juristin

Abkürzungsverzeichnis

AFAPDP	Französischsprachige Vereinigung der Datenschutzbehörden
AHV	Alters- und Hinterlassenenversicherung
AHVN13	13-stellige AHV-Nummer
AIA	Internationaler automatischer Informationsaustausch
ALBA	Automatischer Austausch länderbezogener Berichte
ARE	Bundesamt für Raumentwicklung
ASTRA	Bundesamt für Strassen
BA	Bundesanwaltschaft
BABS	Bundesamt für Bevölkerungsschutz
BAFU	Beratungsstelle für Unfallverhütung
BAG	Bundesamt für Gesundheit
BAK	Bundesamt für Kultur
BAKOM	Bundesamt für Kommunikation
BAR	Bundesarchiv
BASPO	Bundesamt für Sport
BAV	Bundesamt für Verkehr
BAZL	Bundesamt für Zivilluftfahrt
BBL	Bundesamt für Bauten und Logistik
BFE	Bundesamt für Energie
BFK	Eidgenössisches Büro für Konsumentenfragen
BFS	Bundesamt für Statistik
BIT	Bundesamt für Informatik
BJ	Bundesamt für Justiz
BK	Bundeskanzlei
BLV	Bundesamt für Lebensmittelsicherheit und Veterinärwesen
BLW	Bundesamt für Landwirtschaft
BPH	Brussels Privacy Hub
BSV	Bundesamt für Sozialversicherung
BÜPF	Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs
BWL	Bundesamt für wirtschaftliche Landesversorgung
BWO	Bundesamt für Wohnungswesen
ComCom	Eidgenössische Kommunikationskommission
EAV	Eidgenössische Alkoholverwaltung
EBG	Eidgenössisches Büro für die Gleichstellung von Frau und Mann
EDA	Eidgenössisches Departement des Äussern
EDI	Eidgenössisches Departement des Innern
EFD	Eidg. Finanzdepartement
EFK	Eidgenössische Finanzkontrolle
EFV	Eidgenössische Finanzverwaltung
EHB	Eidgenössisches Hochschulinstitut für Berufsbildung
E-ID-Gesetz	Bundesgesetz über staatlich anerkannte elektronische Identifizierungsmittel
EJPD	Eidgenössisches Justiz- und Polizeidepartement
ENSI	Eidgenössische Nuklearsicherheitsinspektorat
EPA	Eidgenössisches Personalamt
ESBK	Eidgenössische Spielbankenkommission

ESchK	Eidgenössische Schiedskommission
ESTV	Eidgenössische Steuerverwaltung
EZV	Eidgenössische Zollverwaltung
fedpol	Bundesamt für Polizei
GPEN	Global Privacy Enforcement Network
GS	Generalsekretariat
IGE	Institut für geistiges Eigentum
IKBDSP	Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre
IKRK	Internationales Komitee vom Roten Kreuz
ISB	Informatiksteuerorgan des Bundes
ISC	Informatik Service Center
KTI	Eidgenössische Kommission für Technologie und Innovation
METAS	Eidgenössisches Institut für Metrologie
NB	Schweizerische Nationalbibliothek
NDB	Nachrichtendienst des Bundes
NDG	Nachrichtendienstgesetz
NKVF	Nationale Kommission zur Verhütung von Folter
NVD	Nachrichtendienstverordnung
OBI	Organisation der Bahninfrastruktur
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
PostCom	Eidgenössische Postkommission
Publica	Pensionskasse des Bundes
PUE	Preisüberwacher
RAB	Eidgenössische Revisionsaufsichtsbehörde
RIPOL	Automatisiertes Fahndungssystem der Polizei
SBFI	Staatssekretariat für Bildung, Forschung und Innovation
SECO	Staatssekretariat für Wirtschaft
SEM	Staatssekretariat für Migration
SIF	Staatssekretariat für internationale Finanzfragen
SIR	Schweizerisches Institut für Rechtsgleichheit
SIS	Schengener Informationssystem
SIS II	Schengener Informationssystem der zweiten Generation
SNF	Schweizerischer Nationalfonds
SNM	Schweizerisches Nationalmuseum
SPK-N	Staatspolitische Kommission des Nationalrats
SUVA	Schweizerische Unfallversicherunsanstalt
UBI	Unabhängige Beschwerdeinstanz für Radio und Fernsehen
UVEK	Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation
VBS	Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport
VIS	Visa-Informationssystem
VöV	Verband öffentlicher Verkehr
WAK-N	Kommission für Wirtschaft und Abgaben des Nationalrats
WBF	Eidgenössisches Departement für Wirtschaft, Bildung und Forschung
WEKO	Wettbewerbskommission
ZAS	Zentrale Ausgleichskasse
ZIVI	Vollzugsstelle für den Zivildienst

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