26. Tätigkeitsbericht 2018/19

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Tätigkeitsbericht 2018/2019
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 2018 und 31. März 2019 ab.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Vorwort

Die Schweiz belegt in den Rankings zur digitalen Wettbewerbsfähigkeit des World Economic Forum und des World Competitiveness Center vorderste Ränge. Damit unser Land seine Position behaupten kann, formuliert der Bundesrat Strategien und Aktionspläne, welche die Digitalisierung von Wirtschaft und Staat voranbringen sollen.

Aber auch der Datenschutz bietet Chancen für den Innovationsstandort Schweiz. Mit technischen Neuheiten, welche den Schutz der Privatsphäre und die digitale Selbstbestimmung der Menschen sicherstellen, lassen sich ebenfalls Punkte sammeln.

Im Wettlauf der Innovation sollten wir indessen nicht vergessen, die bestehenden Standortvorteile zu bewahren: Dank einer weitsichtigen Leistung des Gesetzgebers erhielt die Eidgenossenschaft 1992 – vor bald dreissig Jahren – ein international anerkanntes Datenschutzgesetz, das es der Schweizer Wirtschaft bis heute ermöglicht, mit den Unternehmen wichtiger Handelsnationen ohne weitere gesetzliche Auflagen und Restriktionen Daten auszutauschen.

Daten sind ein begehrtes Gut, und die Digitalisierung wirkt sich tiefgreifend auf die Privatsphäre der weltweit rund vier Milliarden Internetnutzer aus. Angesichts dieser Realität haben die Staaten des Europäischen Wirtschaftsraums den Datenschutz für ihre Bevölkerung erhöht und im Mai 2018 vereinheitlichte, zeitgemässe Regeln in Kraft gesetzt. Diese erlauben es ihren Unternehmen weiterhin, ungehindert den grenzüberschreitenden Datenaustausch zu pflegen, an dem inzwischen auch japanische und – im begrenzten Rahmen des Privacy Shield Übereinkommens – zertifizierte US-amerikanische Firmen teilnehmen.

Dass als ambitiöser Bildungs-, Technologie- und Wirtschaftsstandort auch die Schweiz weiterhin beim ungehinderten Datenaustausch dabei ist, wird allgemein erwartet. Im September 2017 hat der Bundesrat mit seiner Botschaft zur Totalrevision des Bundesgesetzes über den Datenschutz denn auch den parlamentarischen Gesetzgebungsprozess eingeleitet. Seither liegt der Ball bei den eidgenössischen Räten. Sie haben es in der Hand, das Schutzniveau der Daten unserer Bevölkerung nun jenem im umliegenden Europa anzupassen. Wenn diese Arbeit getan und unsere Bürgerinnen und Bürger angemessen geschützt sind, wird auch der Zugang der Wirtschaft zum freien Austausch von Daten gesichert und die Reputation der Schweiz als wettbewerbsfähige digitale Nation gewahrt sein.

Adrian Lobsiger
Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter

Aktuelle Herausforderungen 6

Datenschutz

1.1 **Digitalisierung und Grundrechte** 14

- Revision des Bundesgesetzes über den Datenschutz (DSG)
- Datenschutz-Leitfaden im Kontext von Wahlen und Abstimmungen
- Systematische Verwendung der AHV-Nummer durch die Behörden
- Eckwerte für eine Datenpolitik der Schweiz
- Datenverknüpfungen im Bereich Statistik

Schwerpunkt I 18

Elektronischer Identitätsnachweis (E-ID)

Die «SwissID»

1.2 **Justiz, Polizei, Sicherheit** 22

- Polizeimassnahmen gegen Terrorismus
- Beim Swiss-US Privacy Shield sind Verbesserungen angezeigt
- Bekanntgabe von Flugpassagierdaten in EU-Staaten
- Swiss-Buchungssystem – Massnahmen gegen Datenmissbrauch gefordert

Schwerpunkt II 26

Schengen-Datenschutzgesetz in Kraft

Schengen-Evaluation der Schweiz – ausreichende Mittel für Datenschutz gefordert

- Automatische Fahrzeugfahndung und Verkehrsüberwachung

1.3 **Steuer- und Finanzwesen** 31

- Bekanntgabe von Personendaten an ausländische Steuerbehörden
- Beschwerde gegen das EFD im ESTV-Fall noch hängig
- Empfehlung an Zentralstelle für Kreditinformation (ZEK) erlassen

1.4 **Handel und Wirtschaft** 35

- Datendiebstahl bei Swisscom ohne formelle Massnahmen abgeschlossen
- Datendiebstahl bei EOS – unnötig gespeicherte Patientendaten
- Verwendung der Daten von ricardo.ch in der Tamedia-Gruppe
- Sachverhaltsabklärung bei Smart-TV-Hersteller abgeschlossen
- Decathlon – verbesserte Information bei Datenbeschaffung nötig

1.5 **Gesundheit** 38

- Statistikprojekt mit Einzeldatensätzen der Versicherer (BAGSAN)
- Neue Aufgaben durch elektronisches Patientendossier
- Bonusprogramm «Helsana+» auf dem Prüfstand: Teilerfolg vor Bundesverwaltungsgericht
- Rasant wachsende Datenmengen in der «personalisierten Gesundheit» bergen Risiken

1.6 **Arbeit** 42

- Outsourcing: Bearbeitung von Personaldaten im Ausland
- Online-Bewerbungsverfahren und Bewerbungsgespräche: Was ist zu beachten?
- Bekämpfung der Schwarzarbeit im Kanton Wallis

1.7 **Versicherungen** 45

- Neuer Observationsartikel für Sozialversicherungen
- SUVA: Mehr Transparenz bei Forschung mit Versichertendaten

1.8 **Verkehr** 47

- Multimodale Mobilität – Wahrung der informationellen Selbstbestimmung ein Muss
- Datenschutzkonformität bei neuen Apps im öffentlichen Verkehr

1.9 **International** 49

- Aufsichtskoordinationsgruppen über die Informationssysteme SIS II, VIS und Eurodac
- Arbeitsgruppe «Border, Travel & Law Enforcement»
- Koordinationsgruppe der schweizerischen Datenschutzbehörden im Rahmen von Schengen
- Internationale Konferenz der Datenschutzbeauftragten
- Europäische Konferenz der Datenschutzbeauftragten
- Arbeitsgruppe der OECD über die Informationssicherheit und den Schutz der Privatsphäre
- Französischsprachige Vereinigung der Datenschutzbehörden (AFAPDP)

Schwerpunkt III 54

Die DSGVO – in gewissen Fällen auch in der Schweiz anwendbar

Europarat – Die Schweiz sollte das angepasste Übereinkommen so bald wie möglich unterzeichnen

Öffentlichkeitsprinzip

2.1 **Allgemein** 60

2.2 **Zugangsgesuche – stetige Zunahme** 61

2.3 **Schlichtungsverfahren – hoher Anteil einvernehmlicher Lösungen** 64
- Dauer der Schlichtungsverfahren
- Anteil einvernehmlicher Lösungen
- Anzahl hängiger Fälle

2.4 **Ämterkonsultation und weitere Stellungnahmen** 66
- Totalrevision des Bundesgesetzes über das öffentliche Beschaffungswesen
- Ämterkonsultation zur Genehmigung von Tarifstrukturen in der Krankenversicherung

Der EDÖB

3.1 **Aufgaben und Ressourcen** 70
- Leistungen und Ressourcen im Bereich Datenschutz
- Leistungen und Ressourcen im Bereich Öffentlichkeitsgesetz

3.2 **Kommunikation** 74
- Rege Sensibilisierungstätigkeit und grosse mediale Aufmerksamkeit
- Datenschutzbehörden von Bund und Kantonen traten am Internationalen Datenschutztag gemeinsam auf
- Diverse Leitfäden und Empfehlungen publiziert
- Website nach wie vor wichtigster Kanal unserer Kommunikation

3.3 **Statistiken** 76
- Statistiken über die Tätigkeiten des EDÖB vom 1. April 2018 bis 31. März 2019 (Datenschutz)
- Statistiken über eingereichte Zugangsgesuche nach Öffentlichkeitsgesetz vom 1. Januar 2018 bis am 31. Dezember 2018
- Übersicht der Zugangsgesuche der Departemente und der Bundeskanzlei
- Anzahl Schlichtungsgesuche nach Kategorien der Antragssteller
- Zugangsgesuche der gesamten Bundesverwaltung

3.4 **Organisation EDÖB** 83

Abkürzungsverzeichnis 84

Abbildungsverzeichnis 85

Impressum

In der Klappe

Die wichtigsten Zahlen und Fakten

Anliegen des Datenschutzes

Aktuelle Herausforderungen
I Digitalisierung

Die Bearbeitung von Personendaten wird weiterhin von der dynamischen Weiterentwicklung der Informations- und Telekommunikationstechnologie in der global vernetzten Wirtschaft geprägt, die den Alltag der Schweizer Bevölkerung bei Arbeit, Konsum und Freizeit in hohem Masse beeinflusst.

Technologie und Wirtschaft

Das technische und wirtschaftliche Potenzial für Eingriffe in die Privatsphäre und Selbstbestimmungsrechte der Bevölkerung bleibt hoch, was der Beauftragte schwergewichtig auf zwei Entwicklungen zurückführt:

- Das Internet ermöglicht Geschäftsmodelle, mit denen heute weltweit rund vier Milliarden Benutzer angesprochen werden. In den von amerikanischen Tech-Firmen wie Google, Amazon und Facebook geprägten Märkten hat sich für die Erbringung internetgestützter Kommunikations- und Informationsdienstleistungen eine Art «Gratis»-Modell durchgesetzt. Statt ihre Online-Dienste in Rechnung zu stellen, lassen sich die Anbieter von ihren Kunden Benutzerdaten abtreten. Diese Daten bearbeiten die Anbieter mithilfe von Algorithmen und entsprechenden Analyse-Methoden weiter, um den Kunden zielgerichtet Werbebotschaften zustellen zu können. Die Werbeplätze versteigert der Anbieter an die bestzahlenden Dritten. Einige wenige von ihnen verfolgen dieses Geschäftsmodell mit derart grossem Erfolg, dass Milliarden von Kunden ihre weltweiten «Gratis»-Dienste in Anspruch nehmen. Sie können ihre Algorithmen mit Strömen von Kundendaten versorgen, die sie in die Lage versetzen, die Analyse des Benutzerverhaltens laufend zu intensivieren und auf den Online-Werbemärkten astronomische Umsätze zu erzielen. Während mit der gezielten Zuspielung von kommerziellen und weltanschaulichen Botschaften die Datenschutzrisiken für die Nutzer steigen, gehen die Werbeeinnahmen der Zeitungen sowie von Radio und Fernsehen zurück.
- Nachdem in der Schweiz tätige Telekom-Gesellschaften angekündigt haben, die Netzinfrastruktur für Bandbreiten der fünften Generation (5G) auszurüsten, wird 5G-Technik bald Realität und damit Kapazität und Geschwindigkeit der mobilen Datenströme ein weiteres Mal gewaltig erhöhen. Der bereits in der Vorperiode thematisierte Trend rasch anwachsender Mengen von verknüpften Geräten mit Sensoren, die Bild, Ton oder Positions- und weitere Daten im privaten und öffentlichen Raum aufzeichnen und künstlichen Intelligenzen zuführen, wird sich somit noch beschleunigen.

Gesellschaft und Datenpolitik

Weiter akzentuiert hat sich im Berichtsjahr die öffentliche Kritik an den Betreibern sozialer Plattformen und Anbietern von Suchmaschinen, die das erwähnte Geschäftsmodell der Datenabschöpfung gegen «Gratis»-Dienstleistungen im globalen Umfang betreiben.

Angesichts der anwachsenden Mengen von erhobenen Kundendaten und der zunehmenden Komplexität und Autonomie der Analysetechnologien gestaltet sich die Gewährleistung eines hinreichenden Datenschutzes für die kritisierten Betreiber zunehmend anspruchsvoll: Zum einen müssen sie ihre Kunden leicht verständlich und vollständig über die Bearbeitung ihrer Daten informieren. Zum anderen müssen sie den Kunden hinreichende Gestaltungsmöglichkeiten einräumen, damit diese alle Aspekte der Bearbeitung freiwillig genehmigen oder ablehnen können. Um dieser Verantwortung gerecht zu werden, müssen die Anbieter Investitionen in datenschutzfreundliche Applikationen tätigen, die ihre Kunden mit wenigen Klicks zu den nötigen Informationen und Wahlmöglichkeiten führen. Der Schutz der Privatsphäre und Selbstbestimmung der Kunden muss also frühzeitig und benutzerfreundlich in die digitalen Produkte eingebaut werden.

Anbieter, die sich mit regulatorischen Lippenbekenntnissen und der mechanischen Abarbeitung von Schutzanliegen begnügen, spielen mit dem Vertrauen ihrer Kunden und werden früher oder später die Aufmerksamkeit unserer Behörde auf sich ziehen.

In den Mitgliedstaaten des EWR sind die Datenschutzbehörden im Berichtsjahr dazu übergegangen, Unternehmen für die vernachlässigte Gewährung von Transparenz und Selbstbestimmung mit empfindlichen Bussen zu belegen, welche die im Mai 2017 in Kraft getretene europäische Datenschutzgrundverordnung (DSGVO) vorsieht. Nach ersten Informationen des EDÖB sind inzwischen auch Schweizer Unternehmen, welche Daten von Einwohnern im EWR bearbeiten, von Verfahren der dortigen Datenschutzbehörden betroffen. Weiter befassen sich dort auch die Wettbewerbsbehörden zunehmend mit der Bearbeitung von Daten. In der Berichtsperiode forderte das deutsche Bundeskartellamt die Firma Facebook aufgrund ihrer als marktbeherrschend eingestuften Stellung auf, die Zustimmung zu ihren Nutzungsbedingungen von anderen Diensten des Konzerns zu entkoppeln.

Es wird sich zeigen, ob die marktmächtigen Plattformen angesichts des aufsichtsbehördlichen Drucks und der öffentlichen Kritik am System der «Gratisdienstleistungen» festhalten werden. Eine aus Sicht des Datenschutzes gangbare Alternative sind Geschäftsmodelle, die bezahlende Kunden von profilbildenden Datenauswertungen und personalisierten Zustellungen von Werbebotschaften ausnehmen. Solche Bezahlsysteme lassen sich sowohl über dezentral kontrollierte Crypto-Währungen als auch über das Bankensystem betreiben und sind etwa in China bereits verbreitet, weil dortige Plattformbetreiber auf Online-Vertragsabwicklungen Kommissionen erheben.

Gesetzgebung

In der Schweiz lässt der Abschluss der Beratung der vom Bundesrat im September 2017 vorgelegten Totalrevision des Datenschutzgesetzes (DSG) durch die staatspolitische Kommission des erstberatenden Nationalrats nach wie vor auf sich warten. Nachdem diese die Vorlage zur Totalrevision mit Entscheid vom 12. Januar 2018 in zwei Teile aufspaltete und in einem ersten Schritt die Änderungen behandelte, die für die Übernahme des sog. Schengen-Besitzstands erforderlich sind, haben die Eidgenössischen Räte ein neues Bundesgesetz über die Umsetzung der Richtlinie (EU) 2016/680 oder Schengen-Datenschutzgesetz (SDSG) verabschiedet. Dieses Sondergesetz, dessen Geltung sich auf die Datenbearbeitung der Strafverfolgungsbehörden des Bundes beschränkt, ist am 1. März 2019 in Kraft getreten. Es soll dereinst durch das totalrevidierte DSG wieder aufgehoben werden. Nachdem unsere Behörde durch dieses Gesetz bezüglich der besonders sensiblen Bearbeitung von Personendaten im Polizeibereich mit zusätzlichen Aufgaben und Befugnissen betraut wurde, wird sie namentlich bei der Kontrolle der Datenbearbeitung durch das Bundesamt für Polizei, fedpol, einen Schwerpunkt setzen müssen. Ob der Bundesrat unserer Behörde dafür die beantragten, zusätzlichen Mittel zusprechen wird, stand zur Zeit der Drucklegung dieses Berichts noch nicht fest.

Der Beauftragte hat sich in der staatspolitischen Kommission des Nationalrats, auf deren Einladung er bei den Beratungen des DSG teilnimmt, stets für eine baldige Anhebung des Datenschutzniveaus zu Gunsten der Schweizer Bevölkerung und demzufolge einen zügigen Abschluss der parlamentarischen Beratungen ausgesprochen. Wann dies der Fall sein wird, ist indessen schwer absehbar.

Wenngleich gewisse Kreise der Wirtschaft das aus dem Jahre 1992 stammende DSG und die Befugnisse unserer Behörde für ausreichend erachten mögen, trifft der EDÖB in seinen Kontakten mit grenzüberschreitend tätigen, grossen und kleinen Schweizer Unternehmen auf eine ausgeprägte Bereitschaft, in einen glaubwürdigen betrieblichen Datenschutz zu investieren. Diese, von der Totalrevision unmittelbar betroffenen Unternehmen wollen auch ihrer Schweizer Kundschaft einen den erneuerten europäischen Standards entsprechenden Schutz bieten. Sie wissen auch, dass sich Datenbearbeitungsprojekte in der digitalen Realität nur unter Anwendung zeitgemässer Instrumente wie der Datenschutz-Folgenabschätzung risikogerecht abwickeln und gegenüber der Kundschaft kommunizieren lassen.

Und entsprechend lange werden ihre kleinen, mittleren und grossen Konkurrenten in den Staaten der EU und des EWR ihren diesbezüglichen Wettbewerbsvorteil zu nutzen wissen.

II Beratungs- und Kontrolltätigkeit

Damit der EDÖB als Aufsichtsbehörde sicherstellen 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 bereits im Planungs- und Projektstadium minimieren und gegenüber der betrieblichen und behördlichen Datenschutzaufsicht dokumentieren. Vor diesem Hintergrund haben wir denn auch in der aktuellen Berichtsperiode die Begleitung einer Vielzahl von Big-Data-Projekten von Bundesbehörden und privaten Unternehmen fortgesetzt.

Nicht zuletzt um den eigenen Arbeitsaufwand zu senken, wirkt der Beauftragte mit Blick auf Grossvorhaben, die mit hohen Datenschutzrisiken verbunden sind, weiterhin auf den selbstverantwortlichen Einsatz moderner Arbeitsinstrumente wie der Datenschutzfolgenabschätzung und gegebenenfalls auch die Einsetzung betrieblicher Datenschutzorgane hin. Dennoch ist der Anteil unserer Gesamtaufwendungen für die beratende Begleitung von privatwirtschaftlichen Projekten im Berichtsjahr weiter angestiegen.

Nachdem die Aufwendungen für die Kontrollaufgaben in der Vorperiode deutlich absanken, konnten diese wieder auf den Stand der Periode von 2016/17 angehoben werden. Sie liegen jedoch immer noch unter dem langjährigen Durchschnittswert der Vorperioden. Angesichts der anhaltend knappen Mittelausstattung unserer Behörde war dieser Anstieg nur unter Kürzung anderer Leistungen zu bewerkstelligen. Auch in der aktuellen Berichtsperiode vermochte der EDÖB die berechtigten Erwartungen der Öffentlichkeit nach aufsichtsrechtlichen Massnahmen hinsichtlich der Bearbeitung von Personendaten durch Konsumenten-Apps und soziale Netzwerke nicht im gewünschten Mass zu erfüllen (vgl. «Aufgaben und Ressourcen», Ziff. 3.1).

Einen besonderen Beratungsschwerpunkt hat der EDÖB mit Blick auf die eidgenössischen Erneuerungswahlen im Herbst 2019 gesetzt, indem er im Dezember 2018 zusammen mit den kantonalen Datenschutzbehörden einen Leitfaden zur Anwendung des Datenschutzrechts auf die digitale Personendatenbearbeitung im Kontext von Wahlen und Abstimmungen publizierte (www.edoeb.admin.ch/wahlen). Der Leitfaden ruft darin allen Akteuren ins Bewusstsein, dass personenbezogene Daten zu politischen und weltanschaulichen Ansichten einem höheren Schutzniveau unterliegen, als solche, die im kommerziellen Kontext bearbeitet werden. Die politischen Parteien sind in Anbetracht ihrer zentralen Rolle bei der Durchführung der eidgenössischen Erneuerungswahlen vom Herbst 2019 aufgerufen, mit Blick auf den Datenschutz eine Vorbildfunktion wahrzunehmen.

Je länger die Schweiz die Arbeitsinstrumente des modernen Datenschutzes nicht explizit in ihrer Datenschutzgesetzgebung verankert, desto öfter werden sich hiesige Unternehmen – unbesehen ihrer tatsächlichen Investitionen in den Datenschutz – mit kritischen Fragen nach dem regulatorischen Schutzniveau ihres Sitzstandorts konfrontiert sehen.

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. Als Beispiele sind hier zu nennen: die Schengen-Evaluation (vgl. Ziff. 1.2), der Leitfaden zu den Wahlen (Ziff. 1.1) oder die gemeinsame Durchführung des Internationalen Datenschutztages (Ziff. 3.2).

Neues Europäisches 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, das insbesondere auf die extraterritoriale Geltung des neuen EU-Rechts eingeht und laufend aktualisiert wird (www.edoeb.admin.ch/dsgvo). Wir werden weiterhin alles daransetzen, die betroffenen Schweizer Unternehmen bei der Anwendung der DSGVO mit Rat und Tat zu begleiten und als Aufsichtsbehörde eine auch im Ausland sichtbare Wirkung zu entfalten.

Die andauernde Übergangszeit bis zum Inkrafttreten der immer noch hängigen Totalrevision des DSG (vgl. Ziff 1.1 und 3.1) gestaltet sich nach wie vor als herausfordernd für den EDÖB. Während die personell verstärkten Datenschutzbehörden in den Staaten des EWR inzwischen ihre neuen Verfügungs- und Sanktionsbefugnisse zum Tragen bringen (vgl. Ziff. II), verfügt der EDÖB gegenüber der Wirtschaft und dem Gros der Bundesbehörden bis auf Weiteres nur über die im DSG von 1992 vorgesehenen Empfehlungsbefugnisse. Auch seine Mittel sind seit dem Jahre 2005 im Wesentlichen unverändert geblieben (vgl. Ziff. 3.1). Erschwerend kommt hinzu, dass die Europäische Kommission mit der Evaluation des schweizerischen Datenschutzniveaus eingesetzt hat (s. rechts).

Mit Inkrafttreten der DSGVO hat sich die vormalige «Artikel 29»-Gruppe der EU-Datenschutzbehörden neu als Europäischer Datenschutzausschuss (EDSA) konstituiert. Kernaufgabe des EDSA ist es, die einheitliche Anwendung der DSGVO sicherzustellen. Der Wunsch des EDÖB, bei den Sitzungen generell als Beobachter zugelassen zu werden, wurde abgelehnt. Unsere Teilnahme wird sich somit auf Plenarsitzungen und nur für Punkte, die für den Schengen-Besitzstand relevant sind, beschränken.

Evaluation des Datenschutzniveaus

Die Europäische Kommission überprüft das Datenschutzniveau von Drittländern und hat der Schweiz letztmals im Jahre 2000 attestiert, dass ihr Datenschutzniveau angemessen ist. Unternehmen in der EU können deshalb Personendaten ohne weitere Massnahmen mit Firmen in der Schweiz austauschen. Zurzeit ist die Kommission daran, die Angemessenheit des Schweizer Datenschutzniveaus gestützt auf die in der DSGVO aufgelisteten Kriterien erneut zu evaluieren. Sie hat angekündigt, den Angemessenheitsentscheid im Mai 2020 in Berichtsform zu veröffentlichen. Die Mitwirkung der Schweiz an der Evaluation wird vom Bundesamt für Justiz koordiniert und vom EDÖB unterstützt, indem er erbetene Informationen bereit stellt (vgl. Ziff. 1.9).

Vor dem Hintergrund der laufenden Evaluation wäre es für die Schweiz von Vorteil, wenn diese nicht mehr auf der Grundlage des aus dem Jahre 1992 stammenden, sondern des totalrevidierten DSG vorgenommen werden könnte, dessen Behandlung durch die Kommission des erstberatenden Nationalrats aber noch aussteht (vgl. Ziff. I). Weiter wäre es von Vorteil, wenn der Bundesrat davon Gebrauch machen würde, dass das modernisierte Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen 108) des Europarates seit Oktober 2018 zur Unterzeichnung aufliegt, hat doch die Europäische Kommission wiederholt darauf hingewiesen, dass die Ratifizierung dieses modernisierten Übereinkommens ein entscheidendes Kriterium für den Angemessenheitsentscheid darstellt (s. Ziff. 1.9).

Swiss-US Privacy Shield

Im Herbst 2018 haben wir im Rahmen einer vom Seco angeführten Delegation das aufsichtsbehörliche Review für das Swiss-US Privacy Shield durchgeführt, das im Anschluss an das zweite Review des EU-US Privacy Shields in Brüssel erfolgt ist. Obschon im Review Schwachstellen aufgezeigt wurden, konnte die Funktionsweise des Privacy Shields seit dessen Inkraftsetzung verbessert werden (vgl. Text «Beim Swiss-US Privacy Shield sind gewisse Verbesserungen angezeigt», Ziff. 1.2).

Die Stimmberechtigten haben Anspruch darauf, nachvollziehen zu können, aufgrund welcher Datenbestände und welcher digitaler Bearbeitungsmethoden und Technologien sie von den Parteien oder diesen nahe stehenden Dritten angesprochen werden.

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. Durch das an die Reorganisation und die Befragung des Personals anschliessende Konsolidierungsprogramm EFFET, das im Berichtsjahr gestartet wurde, soll nun die interne Zusammenarbeit optimiert und dadurch die Wirkung unserer Behörde zusätzlich verstärkt werden.

Im Berichtsjahr haben auch mehrere personelle Wechsel auf Ebene der Geschäftsleitung stattgefunden: Nach 38 Jahren als Datenschutzexperte beim Bund, wovon 25 Jahre als Stellvertreter des Beauftragten, verliess Jean-Philippe Walter unsere Behörde pensionshalber per Ende Januar 2019. Der ebenfalls frankofone Marc Buntschu übernahm Walters Nachfolge als stellvertretender Behördenleiter und Chef des Ressorts für nationale und internationale Zusammenarbeit. Bis am 1. Februar 2019 leitete Buntschu den Direktionsbereich Datenschutz, der ab diesem Datum von Daniel Dzamko geführt wird, der vorher in der Geschäftsleitung der Steuerverwaltung des Kantons Bern tätig war. Im Frühjahr 2018 wurde Hugo Wyler mit der Leitung des dem Beauftragten neu direkt unterstellten Bereichs Kommunikation betraut.

Der EDÖB nimmt seine gesetzlichen Aufgaben als Aufsichtsbehörde autonom wahr. Unterstützende logistische und administrative Leistungen bezieht er indessen von der Bundeskanzlei, welche diese nach Massgabe der allgemeinen Standards der Bundesverwaltung erbringt. In diesem Sinne wurde der EDÖB von der Bundeskanzlei auch bei der Einführung des neuen Geschäftsverwaltungssystems Acta Nova betreut, die im September 2018 erfolgreich abgeschlossen werden konnte.

Informationsangebot

Das in der Berichtsperiode erbrachte Informationsangebot wurde punktuell verbessert. Dies betrifft namentlich den vorliegenden 26. Tätigkeitsbericht. Die Weiterentwicklung der Inhaltsaufbereitung und der Kanäle ist hingegen eine Daueraufgabe, die der EDÖB angesichts des grossen Medieninteresses mit vergleichbar wenig Mitteln bewerkstelligen muss (vgl. Ziff. 3.2).

Verfahren im Bereich des Öffentlichkeitsgesetzes (BGÖ)

Der EDÖB ist nach Durchführung eines einjährigen Versuchs zu einem beschleunigten und summarischen Verfahren übergegangen, das sich dadurch charakterisiert, dass in der Regel mündliche Schlichtungsverhandlungen durchgeführt werden. Dieses Verfahren bewährt sich weiterhin, indem der Anteil der einvernehmlich abgeschlossenen Schlichtungen nach wie vor hoch und die Überschreitung der gesetzlichen Fristen im Wesentlichen auf prozessual und inhaltlich komplexe Fälle beschränkt werden konnten. Dies war bspw. der Fall bei Verfahren mit besonders schwierigen juristischen, technischen oder politischen Fragen, aufgrund des grossen Umfangs der verlangten Dokumente oder wenn Drittparteien ins Verfahren miteinzubeziehen sind.

Datenschutz

1.1 Digitalisierung und Grundrechte

Revision des Bundesgesetzes über den Datenschutz (DSG)

Der Abschluss der Beratungen der Totalrevision des Datenschutzgesetzes von 1992 durch die eidgenössischen Räte ist noch nicht absehbar.

Am 15. September 2017 hatte der Bundesrat seine Botschaft (17.059) zur Totalrevision des Bundesgesetzes über den Datenschutz (DSG) an die eidgenössischen Räte überwiesen. Im Rahmen ihrer Beratungen zur DSG-Revision beschloss die staatspolitische Kommission des erstberatenden Nationalrats, in einem ersten Schritt nur die Änderungen zu behandeln, die für die Übernahme des Schengen-Besitzstands erforderlich sind. Diese, auf die Strafverfolgungsbehörden des Bundes beschränkten Bestimmungen, wurden inzwischen vom Parlament genehmigt und vom Bundesrat per 1. März 2019 in Kraft gesetzt (vgl. Schengen-DSG Ziff. 1.2).

Dem gegenüber hat die erwähnte Kommission ihre Beratungen der Totalrevision des auf alle übrigen Bundesbehörden und -betriebe sowie die gesamte Privatwirtschaft anwendbaren DSG noch nicht abgeschlossen. Im Zeitpunkt der Drucklegung des vorliegenden Berichts war somit noch nicht absehbar, wann sich das Plenum des erstberatenden Nationalrats mit der Vorlage befassen wird (vgl. Ziff. I und Ziff. 1.9).

Datenschutz-Leitfaden im Kontext von Wahlen und Abstimmungen

Im Berichtsjahr hat der EDÖB zusammen mit den kantonalen Datenschutzbehörden und Experten einen Leitfaden für die Bearbeitung von Personendaten im Zusammenhang mit Wahlen und Abstimmungen verfasst.

Der EDÖB hat zusammen mit der Konferenz der kantonalen Datenschutzbeauftragten (Privatim) und in enger Absprache mit der Bundeskanzlei eine Arbeitsgruppe eingesetzt mit dem Ziel, die Öffentlichkeit für systemische Risiken der Personendatenbearbeitung im Zusammenhang mit Wahlen und Abstimmungen zu sensibilisieren. Im Rahmen dieser Arbeitsgruppe, in der neben Fachleuten für den Datenschutz auch ein Politologe vertreten ist, wurden im Berichtsjahr verschiedene Experten angehört. Die Erkenntnisse wurden in einem Leitfaden festgehalten, der den verschiedenen Akteuren im politischen Meinungsbildungsprozess als Auslegungshilfe dienen soll, um das aus dem Jahre 1992 stammende DSG im dynamischen Umfeld der Digitalisierung auf die Datenbearbeitung im Kontext von Wahlen und Abstimmungen anzuwenden.

Unrechtmässige Datenbeschaffung im Vorfeld einer Abstimmung

Im Vorfeld zur Abstimmung der sog. Selbstbestimmungsinitiative im November 2018 hat eine beauftragte Agentur über über eine Website unrechtmässig Personendaten beschafft. Auf unsere Intervention hin änderte diese ihre Praxis.

Auf der Website 25november.ch konnten einzelne Personen bis zu zehn Handynummern mit Name und Vorname ihrer Familienmitglieder, Freunde und Verwandten eintragen. Diese Personen wurden dann am Abstimmungswochenende zur Selbstbestimmungsinitiative mit per SMS mit einer Erinnerung bedient – vermeintlich versandt durch die Person, welche die Handynummern auf der Website erfasst und somit einem Dritten weitergegeben hatte. Der EDÖB gelangte darauf mit einem Schreiben an den Betreiber der Website. Darin hat er die Agentur aufgefordert sicherzustellen, dass alle, deren Handynummer angegeben werden, über die Datenbearbeitung, deren Zweck und die für sie Verantwortlichen informiert werden und dass nur Personendaten bearbeitet werden dürfen, für deren Beschaffung, Weitergabe und jede weitere Bearbeitung eine rechtsgültige Einwilligung vorliegt. Ausserdem musste der Betreiber gewährleisten, dass die Personendaten nur zum Zweck der SMS-Erinnerung verwendet und danach gelöscht – und nicht etwa für künftige Kampagnen aufbewahrt wurden. Unter anderem fehlte auf der Website eine gut sichtbare und vollständige Datenschutzerklärung, was die Betreiberin jedoch innert kurzer Frist nachgebessert hat.

Die Akteure werden im Leitfaden dazu aufgerufen, den Stimmbürgerinnen und Stimmbürgern ein Höchstmass an Transparenz und Selbstbestimmung einzuräumen und dafür entsprechend datenschutzfreundliche Anwendungen einzusetzen. Wer Daten im Kontext von Wahlen und Abstimmungen bearbeitet, soll sich bewusst sein, dass das Datenschutzrecht Angaben zu politischen und weltanschaulichen Ansichten einem höheren Schutzniveau unterstellt als Daten im gewerblich-kommerziellen Umfeld. Der Leitfaden richtet sich an alle Akteure der politischen Meinungsbildung wie z. B. Parteien und Interessengruppen, Datenhändler und Datenplattformen und will sie dazu anhalten, die digitalen Bearbeitungsmethoden für die Stimmbürger erkenn- und nachvollziehbar zu machen.

Systematische Verwendung der AHV-Nummer durch die Behörden

Der Bundesrat möchte eine weiterreichende Verwendung der AHV-Nummer erleichtern und hat am 7. November 2018 eine Vernehmlassung zur Änderung des Gesetzes über die AHV eröffnet. Die Vernehmlassung endete am 22. Februar 2019. Wir haben unsere Bemerkungen dazu angebracht, die in den Gesetzesentwurf übernommen wurden.

Der vom Bundesrat in die Vernehmlassung gegebene Entwurf sieht vor, dass die eidgenössischen, kantonalen und kommunalen Verwaltungen die AHV-Nummer ausserhalb des Sozialversicherungsbereichs systematisch als eindeutige Identifikationsnummer verwenden dürfen.

Wir begrüssen es, dass der Gesetzesentwurf des Bundesrats Einrichtungen, die über Datenbanken verfügen, in denen die AHV-Nummer systematisch verwendet wird, gestützt auf unsere Bemerkungen ausdrücklich dazu verpflichtet, periodische Risikoanalysen durchzuführen. Dies namentlich unter Beachtung der Gefahr von unerlaubten Datenverknüpfungen. Aufgrund dieser Risikoanalyse sind Massnahmen für die Sicherheit und den Schutz der Daten festzulegen und umzusetzen, die der Risikosituation angepasst sind und dem Stand der Technik entsprechen. Auch erachten wir als positiv, dass die in der Gesetzesvorlage bezeichneten Einrichtungen, die systematisch die AHV-Nummer verwenden, zur Führung eines Registers der relevanten Datenbanken verpflichtet werden, das insbesondere als Grundlage für die Risikoanalysen dienen soll. Schliesslich betonten wir die Notwendigkeit einer Verstärkung der technischen und organisatorischen Massnahmen.

Wie das Bundesamt für Sozialversicherungen (BSV) gegenüber dem EDÖB festhielt, wird das von der Kommission für Rechtsfragen NR mit dem Postulat 17.3968 bis Ende 2019 verlangte «Sicherheitskonzept für Personenidentifikatoren» im Rahmen der Gesetzgebungsarbeiten zur AHV in die Botschaft integriert werden. Dieses Sicherheitskonzept soll aufzeigen, wie den Risiken einer systematischen Verwendung der AHV-Nummer als eindeutiger Personenidentifikator entgegenzutreten ist und der Datenschutz gestärkt werden kann.

Der EDÖB befürwortet weiterhin die Verwendung von sektorspezifischen Personenidentifikatoren. Die mit der Verwendung von Einheitsidentifikatoren verbundenen Risiken lassen sich so erheblich verringern, insbesondere unzulässige Verknüpfungen unterschiedlicher Datenbanken bzw. Informationssysteme. In diesem Sinne ist aus der in die Vernehmlassung gegebenen Vorlage auch abzuleiten, dass es weiterhin möglich sein wird, in Spezialgesetzen für gewisse Zwecke sektoreigene Personenidentifikationsnummern anstelle der AHV-Nummer vorzuschreiben – wie beispielsweise für das elektronische Patientendossier.

Eckwerte für eine Datenpolitik der Schweiz

Der EDÖB konnte anlässlich der Ämterkonsultation zu den Eckwerten für eine Datenpolitik der Schweiz Stellung nehmen. Er befasst sich weiterhin mit datenpolitischen Teilbereichen.

Im Rahmen der Ämterkonsultation wies der EDÖB darauf hin, dass die Datenschutzbestimmungen nicht nur bei Open Government Data (OGD), sondern auch in anderen aufgeführten Bereichen zu beachten seien. Zu nennen sind: Stammdatenverwaltung des Bundes, Daten von bundesnahen Betrieben und Forschungsanstalten, Dateninnovation im Statistikbereich sowie Innovation durch Daten im Bereich der Mobilität und der Gesundheit. Bei anonymisierten Daten bestehe ausserdem immer das Risiko, dass je nach Menge der vorhandenen Daten Rückschlüsse auf die betroffenen Personen nicht ausgeschlossen werden könnten, weshalb der Datenschutz auch hier zu berücksichtigen sei. Weiter hielt der EDÖB fest, dass er sich seit der Ämterkonsultation zum DSG für die Einführung eines Rechts auf Datenübertragbarkeit (Portabilität) einsetzt. Die Bemerkungen des EDÖB wurden aufgenommen.

Zum Thema Digitalisierung und Datenpolitik laufen auf Bundesebene derzeit verschiedene Projekte, die vom BAKOM koordiniert werden. Der EDÖB nimmt an einzelnen aktiv teil, so beispielsweise bei einem Projekt betreffend Nutzung von Daten oder an der Unterarbeitsgruppe zum Thema Datenverfügbarkeit.

Beirat WBF und UVEK zur Digitalen Transformation

Der EDÖB nahm im März 2019 an der sechsten Sitzung des Beirats «Digitale Transformation» der Departemente WBF und UVEK teil. Ziel der Beiratssitzungen ist es, konkrete Transformationsprojekte und deren Nutzen für Wirtschaft und Bevölkerung aufzuzeigen. Beim Projekt «Swiss Data Custodian» handelt es sich um ein Datentreuhandsystem für Informationen, die nicht öffentlich zugänglich gemacht werden können. Der Betreiber des «Custodian» soll von verschiedenen Unternehmen – gegebenenfalls auch Behörden – personenbezogene und andere Rohdaten entgegennehmen, diese einer Analyse durch künstliche Intelligenz unterziehen und schliesslich die daraus gewonnenen, anonymisierten Erkenntnisse einer wertschöpfenden Verwertung zugänglich machen. Diskutiert wird derzeit eine Anwendung in den Bereichen Mobilität, Medizin und Humanitäres. Sowohl an den Vorbereitungssitzungen als auch an der Beiratssitzung nahm der EDÖB die Gelegenheit wahr, die datenschutzrechtlichen Rahmenbedingungen und Vorgaben, die dabei zu berücksichtigen sind, darzulegen. Der EDÖB wird das Projekt weiterhin begleiten.

Datenverknüpfungen im Bereich Statistik

Mittels Verknüpfungen lassen sich aus statistischen Datenbeständen neue Erkenntnisse gewinnen. Verknüpfungen können das Risiko von Re-Identifikationen massgeblich erhöhen. Um diesem zu begegnen, hat das BFS ein Verknüpfungsreglement erlassen.

Das Bundesamt für Statistik (BFS) verfügt über die gesetzlichen Grundlagen für das Durchführen von sog. Verknüpfungen. Solche Datenverknüpfungen aus verschiedenen Erhebungen sind ein valables Mittel im Bereich der Statistik, um aus Datenbeständen neue Erkenntnisse zu gewinnen, Entwicklungen über mehrere Jahre hinweg zu beobachten oder um Prognosen machen zu können. Dafür werden die einzelnen Datensätze in den verschiedenen Datenbeständen mit Identifikationsnummern versehen und anschliessend ein Verknüpfungsidentifikator generiert.

Verknüpfungen bergen das datenschutzrechtliche Risiko von unerwünschten Rückschlüssen auf bestimmbare Personen, also Re-Identifikationen. Die Identifikationsnummern und Indentifikatoren müssen deshalb intern so verwaltet werden, dass solche Rückschlüsse ausgeschlossen bleiben und es zu keinem Missbrauch kommen kann. Der EDÖB liess sich vom BFS über die laufenden und geplanten Verknüpfungsprojekte und die Massnahmen zur Wahrung der Persönlichkeitsrechte informieren. Der Austausch hat gezeigt, dass es sich um ein hochkomplexes Thema handelt, das der EDÖB weiter beobachten wird. Wir begrüssen, dass das BFS ein spezifisches Verknüpfungsreglement erlassen und publiziert hat.

Elektronischer Identitätsnachweis (E-ID)

Mit einer staatlich anerkannten elektronischen Identität soll bei elektronischen Anwendungen die Identität einer Person sichergestellt werden. Der EDÖB begleitet das digitale Grossprojekt auf allen Stufen. Er fordert, dass ein hinreichender Datenschutz mit hoher Priorität gewährleistet werden muss.

Rechtssicherheit und Vertrauen sind wesentliche Voraussetzungen für die Abwicklung von Geschäften. Für verschiedene Prozesse ist es dabei wesentlich, dass die Identität des Gegenübers sichergestellt ist. Für die analoge Welt stellt der Bund dazu konventionelle Identifizierungsmittel zur Verfügung – nämlich Schweizerpass, Identitätskarte und Ausländerausweis. Mit der Verlagerung von Geschäftsprozessen in die digitale Welt ändern sich die Anforderungen an die Identifikationsmöglichkeiten. Ergänzend soll die Identität einer natürlichen Person mittels einer staatlich anerkannten elektronischen Identität (E-ID) nachgewiesen werden können.

Die E-ID wird für den Online-Zugang zu privaten Dienstleistungen (wie z. B. die Eröffnung eines Bankkontos) und E-Government-Anwendungen (z. B. die Bestellung eines Strafregisterauszuges) ein zentrales Instrument darstellen. Aus diesem Grund hat der EDÖB sowohl das Gesetzgebungsprojekt für eine staatlich anerkannte E-ID wie auch die konkrete Umsetzung des Projektes bei der SwissSign Group AG (vgl. Die «SwissID») konstruktiv kritisch begleitet und gefordert, dass wesentliche datenschutzrechtliche Anforderungen bereits in der Konzeptphase der Projekte einfliessen.

Der Bundesrat hat am 1. Juni 2018 die Botschaft zum Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz, BGEID) verabschiedet, welche die staatlich anerkannte Identität gesetzlich regelt. Die Gesetzesvorlage wurde Ende März vom erstberatenden Nationalrat mit 128 zu 48 Stimmen genehmigt

Staatlich anerkannte private Unternehmen als Identity Provider

Der Nationalrat hat sich nach einer Anhörung der interessierten Kreise durch seine Kommission für Rechtfragen gegen eine ausschliesslich staatliche Lösung ausgesprochen und stattdessen eine Aufgabenteilung befürwortet: Staatlich anerkannte private Unternehmen, sogenannte Identity Provider (IdP), werden zur Ausstellung von elektronischen Identitäten ermächtigt. Die Anerkennung der IdP erfolgt durch das Informatiksteuerungsorgan des Bundes (ISB), welches darüber hinaus die Einhaltung der vorgegebenen Prozesse und technischen Standards durch die IdP überprüfen und auf Basis dieser Prüfung die Anerkennung erteilen bzw. verlängern oder entziehen. Eine vom Bundesamt für Polizei (fedpol) geführte elektronische Schnittstelle wird Personenidentifizierungsdaten, die in staatlich geführten Registern hinterlegt sind, den IdP zum ausschliesslichen Zweck der Identifikation zur Verfügung stellen. Durch die Aufgabenteilung sollen einerseits verlässliche und Sicherheit gewährende Rahmenbedingungen garantiert werden, die die staatlichen Institutionen im Rahmen von Anerkennungs- und Aufsichtsverfahren durchsetzen können. Andererseits kann die technische Umsetzung und Vermarktung der konkret ausgestalteten E-ID privaten Unternehmen überlassen werden.

Anhörung des EDÖB als Bedingung für die Anerkennung

Anlässlich der Anhörung in der Kommission sah der EDÖB seine Aufgabe darin, sich unabhängig vom politischen Entscheid zugunsten einer rein staatlichen oder nur teilstaatlichen Lösung, für ein höchstmögliches Niveau an Datenschutz einzusetzen. Der EDÖB hat darauf hingewiesen, dass die Datenbearbeitung der staatlichen Akteure auf einer genügenden gesetzlichen Grundlage beruhen muss und hat diesbezüglich punktuell Verbesserungen des E-ID-Gesetzes verlangt. So hat der Nationalrat als Anerkennungsvoraussetzung der IdP die vorgängige Anhörung des EDÖB durch das ISB in das Gesetz aufgenommen. Der EDÖB wird in diesem Rahmen die datenschutzrechtlichen Standards, die er anlässlich der Begleitung des Projektes von SwissSign erarbeitet hat, als Massstab für die Beurteilung fordern (vgl. folgenden Text «SwissID».

Des Weitern hat der EDÖB darauf bestanden, dass die Botschaft dahingehend präzisiert wird, dass die E-ID nur dort Anwendung finden soll, wo eine sichere Identifikation im Geschäftsverkehr unbedingt nötig ist. Für die zahlreichen Online-Konsumgeschäfte oder Bezüge von einfachen Dienstleistungen, wo dies nicht nötig ist, dürfen durch das E-ID-Gesetz weder im analogen noch im elektronischen Geschäftsverkehr neue Identifizierungspflichten geschaffen werden. Der Nationalrat hat den Zweckartikel des Gesetzes entsprechend angepasst.

Die «SwissID»

Mit einer «SwissID» stellt ein privater Anbieter dem Markt eine elektronische Identität zur Verfügung. In regelmässigen Sitzungen mit den Projektverantwortlichen begleitet der EDÖB das Vorhaben. Diese haben die Hinweise des EDÖB aufgenommen.

Die SwissSign Group AG ist ein Joint Venture aus staatsnahen Betrieben, Finanzunternehmen, Versicherungsgesellschaften und Krankenkassen. Mit ihrem Produkt «SwissID» ist sie daran, eine elektronische Identität für den Online-Geschäftsverkehr auf privater Basis auf verschiedenen Online-Plattformen einzuführen. Zu den Vertragspartnern zum Onlinedienst der SwissSign zählen bedeutende Unternehmen wie z. B. die schweizerische Post, Swisscom, Coop, Ringier – weitere wie bspw. die SBB kommen laufend hinzu. Verschiedene Kantone planen für ihre E-Government-Anwendungen die «SwissID» einzusetzen oder haben diese bereits eingeführt.

Derzeit basiert die «SwissID» noch auf einem Log-in-Passwort-Verfahren. Sie soll jedoch mit Blick auf die Inkraftsetzung des BGEID (vgl. dazu Artikel zur E-ID) zu einer elektronischen Identität auf privater Basis aufgewertet werden, damit die Nutzer identitätspflichtige Rechtsgeschäfte online abschliessen und staatliche Dienstleistungen online beziehen können.

Analysen datenschutzrechtlicher Risiken müssen ausgebaut werden

Dieses Vorhaben stellt auch aus datenschutzrechtlicher Sicht ein bedeutendes digitales Grossprojekt dar. Der EDÖB steht in regelmässigem Austausch mit den Projektverantwortlichen, berät diese punktuell und gibt Rückmeldung zu den ihm vorgelegten Dokumentationen und Informationen. Es hat sich gezeigt, dass sich die SwissSign über die Bedeutung des Datenschutzes für ihre Datenbearbeitung bewusst ist und wesentliche technische und organisatorische Massnahmen zum Schutz der Daten getroffen hat. Der EDÖB hat darauf hingewiesen, dass die Analysen der datenschutzrechtlichen Risiken, welche typischerweise mit dem Vorhaben verbunden sind, weiter ausgebaut werden müssen und entsprechende Massnahmen zur Vermeidung dieser Gefahren getroffen werden sollten. Zudem erachten wir es als unablässig, dass eine Person speziell für den betrieblichen Datenschutz eingesetzt wird, welche die Risiken und die entsprechenden Massnahmen laufend prüft und zu den unternehmerischen Entscheidungen aus der Perspektive des Datenschutzes Stellung nimmt.

Die Projektverantwortlichen von SwissSign sind mit den Hinweisen des EDÖB einig und werden ihre Analysen und Dokumente hinsichtlich der Personendatenbearbeitung ausbauen. Eine betrieblich datenschutzverantwortliche Person wurde in der Folge vom Unternehmen bestimmt.

1.2 Justiz, Polizei, Sicherheit

Polizeimassnahmen gegen Terrorismus

Im Rahmen der zweiten Ämterkonsultation zum Entwurf eines Bundesgesetzes über polizeiliche Massnahmen zur Bekämpfung von Terrorismus (PMT) hat der EDÖB erneut zahlreiche Bemerkungen angebracht. Er erneuerte seine Forderung nach Ausarbeitung einer einheitlichen Polizeigesetzgebung auf Bundesebene. Überdies verlangt er für die Migrationsbehörden eine Einschränkung des Zugangs zu den Datenbanken der Polizei.

Der EDÖB hat die grosse Anzahl an spezialgesetzlichen Erlassen und Normen zur Regelung der Polizeitätigkeiten des Bundes erneut kritisiert. Hinzu kommt, dass die polizeilichen Daten auf unübersichtliche Weise in mehreren Datenbanken und einer wachsenden Zahl von Anwendungen bearbeitet werden. Der vorliegende Entwurf für ein Bundesgesetz über polizeiliche Massnahmen zur Bekämpfung von Terrorismus (PMT) erschwert diese Situation noch zusätzlich. Aus diesen Gründen forderte der EDÖB erneut die Ausarbeitung einer einheitlichen Polizeigesetzgebung auf Bundesebene, so wie sie auch auf Kantonsebene existiert. Er erinnerte auch an die Wichtigkeit einer klaren Trennung der Zuständigkeiten zwischen dem Nachrichtendienst des Bundes (NDB) und fedpol.

Der EDÖB äusserte auch Zweifel am Nutzen von Bestimmungen, denen zufolge das Staatssekretariat für Migration (SEM) auf die in Artikel 10, 11, 12 und 14 des Bundesgesetzes über die polizeilichen Informationssysteme des Bundes (BPI) erwähnten Informationssysteme zugreifen kann. Die im Ausländer- und im Asylgesetz vorgegebenen Rechtsgrundlagen betreffen ausschliesslich die Zusammenarbeit und die Koordination zwischen dem SEM und fedpol. Diese Bestimmungen bilden keine rechtlichen Grundlagen für einen ausdrücklichen Gesetzesauftrag an das SEM bei der Aufklärung von terroristischen Handlungen oder bei der Terrorismusbekämpfung. Zudem betreffen diese Zugangsrechte gerichtspolizeiliche Daten und kriminalpolizeiliche Analysen. Diese Daten sind äusserst sensibel und teilweise auch ungesichert. Der Zugriff auf solche Daten durch die Migrationsbehörden muss über die Amtshilfe und nicht über einen Online-Zugang erfolgen. Auf diese Weise könnte fedpol die Verbreitung dieser Daten auf das nötige Mass reduzieren.

Schliesslich wies der EDÖB auch darauf hin, dass die Einsicht in das automatisierte Fahndungssystem des Bundes (RIPOL) nicht dem gesetzlichen Auftrag der Tranzportpolizei entspricht, die Identität einer Person zu überprüfen oder eine Person zu identifizieren. RIPOL gibt nämlich an, ob eine Person zur Fahndung ausgeschrieben ist oder nicht. Ein Zugriff auf RIPOL erfordert sowohl die Änderung des Gesetzes über die polizeilichen Informationssysteme des Bundes als auch eine Anpassung des Bundesgesetzes über die Sicherheitsorgane der Transportunternehmen im öffentlichen Verkehr.

Beim Swiss-US Privacy Shield sind Verbesserungen angezeigt

Im Herbst 2018 fand in Brüssel die Überprüfung des Privacy Shield Übereinkommens zwischen der EU und den USA und erstmals auch der Schweiz und den USA statt. Die US-Behörden haben in diversen Belangen Verbesserungen vorgenommen, die auch der Schweiz zugutekommen. Hingegen besteht beispielsweise noch Abstimmungsbedarf bei HR-Daten.

Dem EDÖB sind im Berichtsjahr zwei Fälle betreffend Unternehmen gemeldet worden, die sich fälschlicherweise als Swiss-US Privacy Shield zertifiziert ausgaben («false claims»). Beide konnten in Zusammenarbeit mit dem U.S. Department of Commerce (DoC) gelöst werden. (vgl. auch Ziff. 1.4 im Bericht des EDÖB zum 1. Swiss-US Privacy Shield Review, Seite 4). Zudem sind rund zehn berechtigte Beschwerden von Betroffenen aus der Schweiz bei unabhängigen Beschwerdestellen (Independent Recourse Mechanism, IRM) eingereicht worden. Betreffend den Ombudspersonmechanismus, der bei behördlichen Zugriffen auf Personendaten Abhilfe schaffen soll, ist bisher noch kein Fall beim EDÖB eingegangen.

Der Schluss liegt nahe, dass die vom Swiss-US Privacy Shield zur Verfügung gestellten Rechtsinstrumente bislang noch wenig genutzt worden sind. Zu beachten ist allerdings, dass das Schweizer Übereinkommen erst seit April 2017 in Kraft ist, und dass vor einer offiziellen Beschwerde in der Regel zuerst das zertifizierte Unternehmen selbst angegangen wird. Es ist davon auszugehen, dass eine quantitativ schwer abschätzbare Anzahl von Datenschutzverletzungen bereits auf diesem Weg beseitigt werden konnte.

Erstmalige Überprüfung durch den EDÖB

Die Überprüfung des Privacy Shield betraf sowohl die gewerblichen Aspekte (z. B. Überwachung und Durchsetzung der Pflichten von zertifizierten Unternehmen) wie auch den behördlichen Zugriff zum Zwecke der nationalen Sicherheit auf Personendaten. Die Schweiz konnte am vorangehenden europäischen Review des EU-US Privacy Shield mit Beobachterstatus teilnehmen. Themen, die sowohl den Swiss-US als auch den EU-US Privacy Shield betrafen, wurden ausschliesslich am EU-US Review diskutiert. Die gewonnenen Erkenntnisse konnten auch für die schweizerisch-amerikanische Absprache verwendet werden.

Seit Inkraftsetzung des Swiss-US Privacy Shield konnten verschiedene Verbesserungen vorgenommen werden. Im Hinblick auf die gewerblichen Aspekte sucht das US-Handelsministerium beispielsweise verstärkt nach «false claims». Ausserdem überprüfen die US Behörden korrekt zertifizierte Unternehmen regelmässiger auf allfällige Schwachstellen und überwachen bei der Zertifizierung strenger, dass keine Diskrepanzen zwischen den Angaben in deren Privacy Policies und dem tatsächlichen Stand des Registrierungsprozesses bestehen.

Für das Schiedsverfahren, welches den betroffenen Personen nach Ausschöpfung der anderen Rechtsbehelfe (IRM) an einem dem amerikanischen Recht unterworfenen Schiedsgericht zur Verfügung steht (vgl. 24. Tätigkeitsbericht 2016/17, Ziff. 1.8.1), konnten bereits vor dem Review fünf zusätzliche Schiedsrichter für die Schweiz ernannt werden. Diese ergänzen die Liste der EU.

Im Hinblick auf den behördlichen Zugriff konnten im Vorfeld des Reviews Fortschritte erzielt werden. Der US-Senat bestätigte die Nominierungen des Vorsitzes sowie zweier Mitglieder der Stelle zur Überwachung des Schutzes der Privatsphäre und der bürgerlichen Freiheiten (Privacy and Civil Liberties Oversight Board, PCLOB), womit das nötige Quorum erreicht ist. Der PCLOB bestand im ersten Swiss-US-Privacy-Shield-Jahr aus nur einem Mitglied und war somit nicht beschlussfähig.

Verbesserungspotenzial vorhanden
In verschiedenen Bereichen teilt der EDÖB die Auffassung des Europäischen Datenschutzausschusses (EDSA), wonach weitere Verbesserungen angezeigt sind. Unter anderem wären substanziellere Überprüfungen der Compliance von zertifizierten Unternehmen durch die US-Behörden sinnvoll, so etwa der Zweck- und Verhältnismässigkeit bei Datentransfers an Dritte. Ferner muss eine Lösung betreffend die Auslegung des Begriffs «HR-Daten» durch die US-Behörden auf der einen Seite und dem EDÖB und Vertretern des EDSA auf der anderen Seite gefunden werden. HR-Daten geniessen einen erweiterten Schutz durch das Privacy-Shield-Übereinkommen. Nach Ansicht des EDÖB muss die Auslegung dieses Begriffs umfassender sein, als dies das DoC vorsieht.

Hinsichtlich des behördlichen Zugriffs auf Personendaten soll unter anderem sichergestellt werden, dass eine Ombudsperson ernannt wird, die gegenüber US-Behörden, die im Rahmen der nationalen Sicherheit Zugriffe tätigen, über die nötige Kompetenz und Unabhängigkeit verfügt.

Obschon im Review Schwachstellen aufgezeigt wurden, konnte die Funktionsweise des Privacy Shields seit dessen Inkraftsetzung insgesamt verbessert werden.

Rund 2900 US-Unternehmen zertifiziert

Das Swiss-US Privacy Shield ist seit 2017 in Kraft. Der Privacy Shield erlaubt es US-Unternehmen, Personendaten aus der Schweiz ohne weitere Datenschutzklauseln zu bearbeiten. Die Firmen können sich beim US-Handelsministerium für das Programm zertifizieren lassen und verpflichten sich damit, einem nach Schweizer Recht angemessenen Datenschutzniveau zu entsprechen. Betroffenen stehen Mechanismen zur Verfügung, mithilfe derer sie sich gegen Datenschutzverletzungen wehren können.

Bis im Februar 2019 haben sich 2883 US-Unternehmen unter dem Swiss-US Privacy Shield zertifiziert, darunter Facebook, Microsoft (mit 27 Tochtergesellschaften) und Google.

Zertifizierte Unternehmen können weitgehend wählen, ob sie sich zur Einhaltung des Independent Recourse Mechanism (IRM) den ADR (Alternative Dispute Resolution body) oder aber dem EDÖB unterstellen (vgl. Leitfaden zum Privacy Shield).

Eine alljährliche Überprüfung der Funktionsweise dieses Übereinkommens findet durch das SECO (Federführung) und den EDÖB, zusammen mit den US-Aufsichtsbehörden statt.

Bekanntgabe von Flugpassagierdaten in EU-Staaten

Verschiedene EU-Staaten planen, von Flügen aus der Schweiz Flugpassagierdaten zu verlangen. Eine gesetzliche Grundlage fehlt jedoch. Diese soll nun auf Verordnungsstufe geschaffen werden.

Im Frühjahr 2018 fand zwischen dem Bundesamt für Zivilluftfahrt (BAZL), dem Bundesamt für Justiz (BJ), dem Bundesamt für Polizei (fedpol) und dem EDÖB eine Sitzung zur Bekanntgabe von Flugpassagierdaten (PNR-Daten) in Mitgliedstaaten der EU statt. Diese Sitzung fand auf Initiative des BAZL statt, da die Fluggesellschaften von verschiedenen EU-Staaten informiert worden waren, dass diese planten, von Flügen aus der Schweiz die Lieferung von PNR-Daten zu verlangen – gestützt auf die EU-PNR-Richtlinie vom 27. April 2016 (Richtlinie (EU) 2016/681; EU-PNR-Richtlinie) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität. Die EU-PNR-Richtlinie wurde jedoch von der EU als nicht Schengen-relevant erklärt und muss somit von der Schweiz nicht automatisch übernommen werden.

Der EDÖB wies darauf hin, dass die Bekanntgabe von PNR-Daten durch Fluggesellschaften in Form eines Abkommens auf einer gesetzlichen Grundlage beruhen müsse. Während sich die anderen beteiligten Bundesämter klar zugunsten einer voraussetzungslosen Datenbekanntgabe geäussert hatten, hielt der EDÖB daran fest, dass eine Datenbekanntgabe durch Fluggesellschaften an Mitgliedstaaten in Umsetzung der EU-PNR-Richtlinie nur erfolgen dürfe, wenn bestimmte Punkte erfüllt sind. Die Schweiz müsse so rasch als möglich versuchen, eine Assoziierung an die EU-PNR-Richtlinie zu verhandeln und zu erhalten. In diesem Sinn plante das fedpol ursprünglich, dem Bundesrat noch im Herbst 2018 eine entsprechende Vorlage inklusive Verhandlungsmandat mit der EU vorzulegen. Allerdings wurde dieses Projekt bis auf Weiteres aufgeschoben. Als der EDÖB von diesem Aufschub erfuhr, wies er die betroffenen Bundesämter darauf hin, dass so rasch als möglich eine alternative Rechtsgrundlage geschaffen werden müsse. Dem EDÖB wurde in Aussicht gestellt, die gesetzliche Grundlage für die Lieferung von PNR-Daten an Staaten, welche diese gestützt auf die EU-PNR-Richtlinie verlangen würden, mit einer Revision der Luftfahrtverordnung (LFV) zu schaffen und vorzusehen, so dass eine Datenlieferung nur an Staaten erfolgen darf, die ein angemessenes Datenschutzniveau aufweisen. Der EDÖB wird die Gesetzgebungsarbeiten beratend begleiten.

Swiss-Buchungssystem – Massnahmen gegen Datenmissbrauch gefordert

Die Swiss International Air Lines trifft verschiedene zusätzliche Massnahmen zur Verhinderung allfälliger Missbräuche bei der Abrufung der Buchung über ihre Internetseite.

Der EDÖB wurde darauf hingewiesen, dass es auf der Internetseite der Swiss möglich sei, mit der Eingabe von Nachname, Vorname und Buchungsnummer beim Log-in verschiedene persönliche Daten (Vorname, Nachname, Geburtsdatum, Geschlecht, Nationalität, Wohnsitz, Nummer und Gültigkeitsdauer von Pass resp. Identitätskarte) abzurufen. Dabei sei es sehr einfach, Nachname, Vorname und Buchungsnummer von anderen Passagieren auf Bordkarten herauszufinden, die von diesen nach einem Flug liegen gelassen, weggeworfen oder in sozialen Medien publiziert wurden. Diese Informationen könnten auch aus dem Strichcode auf der Bordkarte mit einer einfachen Barcode-Lese-App herausgelesen werden. Mit diesem Log-in können auch sämtliche Buchungen der betroffenen Passagiere eingesehen und teilweise Daten geändert werden.

Weil der Inhalt des Boarding Passes inkl. QR-Code bestimmten internationalen Standards entsprechen muss, kann dieser von einzelnen Fluggesellschaften nicht ohne Weiteres geändert werden. Dennoch müssen und können die Fluggesellschaften die notwendigen Massnahmen treffen um sicherzustellen, dass die Passagierdaten im Buchungssystem vor allfälligen missbräuchlichen Bearbeitungen angemessen geschützt sind.

Im Austausch zwischen der Swiss und dem EDÖB wurde festgelegt, welche zusätzlichen Massnahmen zur Verhinderung allfälliger Missbräuche getroffen werden müssen. Die Swiss hat ihre allgemeinen Beförderungsbestimmungen (ABB) angepasst, um ihre Kunden besser auf die Schutzwürdigkeit der auf dem Boarding Pass ersichtlichen bzw. gespeicherten Personendaten hinzuweisen. Weiter erhalten die Kunden nach dem automatischen Check-in per E-Mail einen entsprechenden Warnhinweis. Erfolgt das Check-in online wird zudem angezeigt, an welche Adresse (Mail, Mobiltelefonnummer) die Nachricht geschickt wird. Dies um kontrollieren zu können, dass die Bordkarte an die richtige resp. gewünschte Adresse geschickt wird. Weiter soll die Passnummer, die in bestimmten Fällen beim Buchungsaufruf ersichtlich ist, teilweise unkenntlich gemacht werden. Der EDÖB hatte weiter vorgeschlagen, für die Aufrufung von Buchungen, die nicht über ein Reisebüro oder einen anderen Dritten, sondern direkt über die Internetseite der Fluggesellschaft erfolgen, nebst Name und Buchungsreferenz die Eingabe eines Zusatzelements, wie beispielsweise Handynummer oder E-Mail-Adresse, vorzusehen. Dieser Punkt war zum Ende des Berichtsjahres noch offen.

Schengen-Datenschutzgesetz in Kraft

Das Schengen-Datenschutzgesetz (SDSG) ist am 1. März 2019 in Kraft getreten. Es enthält verschiedene Neuerungen gegenüber den heutigen Kompetenzen des EDÖB. Unter anderem erhält dieser zur Anwendung des Schengen-Besitzstands in Strafsachen Untersuchungs- und Verfügungskompetenzen.

Im Rahmen seiner Beratungen zur Revision des Datenschutzgesetzes (DSG) beschloss das Parlament, in einem ersten Schritt die Änderungen zu behandeln, die für die Übernahme des Schengen-Besitzstands erforderlich sind. Gestützt darauf wurde das Bundesgesetz über die Umsetzung der Richtlinie (EU) 2016/680 verabschiedet und per 1. März 2019 in Kraft gesetzt. Mit diesem Bundesgesetz wird einerseits das Schengen-Datenschutzgesetz (SDSG) eingeführt, andererseits werden verschiedene Gesetze, welche im Bereich der Schengener Zusammenarbeit in Strafsachen anwendbar sind, angepasst.

Das SDSG gilt insbesondere für die Bearbeitung von Personendaten durch Bundesorgane in Strafsachen im Rahmen der Anwendung des Schengen-Besitzstands. Zu den betreffenden Bundesorganen gehören also nicht nur das Bundesamt für Polizei (fedpol), das BJ im Bereich der internationalen Rechtshilfe in Strafsachen und die Bundesanwaltschaft, sondern auch das Bundesstrafgericht, das Bundesgericht und die kantonalen Zwangsmassnahmengerichte, wenn sie für den Bund tätig werden. Auf kantonale Behörden ist das SDSG nicht anwendbar. Vielmehr obliegt es den Kantonen, ihre Gesetzgebungen soweit nötig an die neuen Anforderungen der EU anzupassen.

Mit dem SDSG werden hauptsächlich folgende Neuerungen eingeführt:

- genetische und biometrische Daten, die eine Person eindeutig identifizieren, werden neu explizit als besonders schützenswerte Personendaten aufgeführt;
- der Begriff des Profilings tritt in Anlehnung an das europäische Recht neu an die Stelle des Persönlichkeitsprofils. Mit Profiling ist jede Art der automatisierten Bearbeitung von Personendaten zu verstehen, die darin besteht, dass diese Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten. Dies dient namentlich dazu, Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen;
- Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen («privacy by design and default») sind als Grundsätze verankert. Um die Einhaltung der Datenschutzvorschriften nachweisen zu können, muss das Bundesorgan die nötigen internen Vorkehrungen treffen und Massnahmen ergreifen, die diesen beiden Grundsätzen gerecht werden;
- die automatisierte Einzelentscheidung wird ausdrücklich geregelt. Eine solche Entscheidung liegt vor, wenn die inhaltliche Bewertung von Daten und die darauf gestützte Entscheidung nicht durch eine natürliche Person vorgenommen wird – wenn also die Maschine entscheidet und nicht der Mensch;
- wenn die vorgesehene Datenbearbeitung ein hohes Risiko für die Grundrechte der betroffenen Personen mit sich bringen kann, müssen Bundesorgane Datenschutz-Folgenabschätzungen durchführen und dazu unter Umständen den EDÖB konsultieren;

- hat das Bundesorgan eine Datenschutz-Folgenabschätzung vorgenommen, so müssen die Ergebnisse bei der Entwicklung der Massnahmen berücksichtigt werden;
- Bundesorgane müssen dem EDÖB Datenschutzverletzungen melden;
- der EDÖB kann neu als Verwaltungsmassnahme Verfügungen erlassen.

Schengen-Evaluation der Schweiz – ausreichende Mittel für Datenschutz gefordert

Im Jahr 2018 wurden die Umsetzung und die Anwendung des Schengen-Besitzstands durch die Schweiz als assoziiertes Mitglied zum dritten Mal kontrolliert. Die Experten der übrigen Schengen-Staaten und der Europäischen Kommission prüften hauptsächlich die Anwendung der Schengen-Regelung im Bereich Datenschutz. Auf Basis der Ergebnisse hat der Rat der EU der Schweiz seine Empfehlungen abgegeben.

Die Evaluierung, die in Abständen von maximal fünf Jahren erfolgt, bezieht sich auf sämtliche Bereiche der Schengenzusammenarbeit: Sicherung der Aussengrenzen (Flughäfen), Rückkehr/Rückschaffung, Schengener Informationssystem SIS II/SIRENE, gemeinsame Visumspolitik, polizeiliche Zusammenarbeit und Datenschutz. Das Bundesamt für Justiz (BJ) ist für die Koordination sämtlicher Evaluierungen verantwortlich. Die Vorbereitungsarbeiten wurden vom BJ in Zusammenarbeit mit der Direktion für europäische Angelegenheiten (DEA) koordiniert. Der EDÖB beteiligte sich aktiv an den Arbeiten der Schengen-Evaluierung im Datenschutzbereich, in Kooperation insbesondere mit dem BJ, dem Bundesamt für Polizei (fedpol), dem Staatssekretariat für Migration (SEM), dem Eidgenössischen Departement für auswärtige Angelegenheiten (EDA) und den kantonalen Datenschutzbehörden (vgl. Koordinationsgruppe der schweizerischen Datenschutzbehörden im Rahmen von Schengen in Ziff. 1.9).

Die Evaluation des Datenschutzbereichs lief in drei Etappen ab. In einem ersten Schritt musste die Schweiz rund 200 Fragen zur Umsetzung und Anwendung der Schengenregelung beantworten und die seit der ersten Evaluierung erfolgten wichtigsten gesetzgeberischen und operativen Änderungen aufzeigen. In der zweiten Phase erfolgten Inspektionen in der Schweiz. Die Experten der EU und anderer Schengen-Staaten vergewisserten sich vor Ort, dass die Schweiz die Schengen-Datenschutzbestimmungen korrekt umsetzt und anwendet. Die Besuche fanden vom 26. Februar bis 2. März 2018 statt und konzentrierten sich auf die Gesetzgebung im Datenschutzbereich sowie auf die Kompetenzen des EDÖB, der luzernischen Datenschutzbehörde und anderer Bundesorgane (s. oben). Im Besonderen wurden die Aufsichts-, Untersuchungs- und Interventionsbefugnisse der Kontrollbehörden sowie deren Unabhängigkeit geprüft. Analysiert wurden die gesetzlichen Grundlagen und speziell die Befugnisse zur Überwachung des SIS II und des VIS sowie der an ihrer Verwaltung beteiligten Dienste. Die Rechte der betroffenen Personen, die Datensicherheit, die Zusammenarbeit mit den ausländischen Behörden und die Information der Öffentlichkeit wurden ebenfalls geprüft.

Gestützt auf die Ergebnisse der Evaluierung hat der Rat der EU am 7. März 2019 eine Empfehlung an die Schweiz zur Beseitigung der festgestellten Mängel beschlossen. Betreffend den EDÖB empfiehlt der Rat insbesondere, er solle die Rechtmässigkeit der Bearbeitung von personenbezogenen Daten in Zusammenhang mit den schengen-relevanten Informationssystemen häufiger kontrollieren. Damit er alle seine Aufgaben im Rahmen des SIS-II- und des VIS-Besitzstands erfüllen kann, seien dem EDÖB ausreichende finanzielle und personelle Ressourcen zuzuweisen. Zudem solle dem EDÖB ein konkreter Einfluss auf seinen Haushaltsvorschlag zukommen, wobei das Parlament im Rahmen der Behandlung des Gesamthaushaltsvorschlags über den Haushaltsvorschlag des EDÖB zu informieren sei. Der Rat würdigt in seinen Erwägungen auch Positives, wie etwa den von der Schengen-Koordinationsgruppe der Schweizerischen Datenschutzbehörden ausgearbeiteten Leitfaden «Beaufsichtigung der Nutzung des Schengener Informationssystems (SIS)», oder die umfangreichen spezifischen Musterbriefe für die Ausübung der Rechte Betroffener und zielführenden Informationen, welche sich auf der Website des EDÖB finden. Die Schweiz solle nun innerhalb von drei Monaten nach Annahme des Beschlusses einen Aktionsplan erstellen und diesen der Kommission und dem Rat vorlegen. Die nächste Evaluierung ist für 2023 vorgesehen.

Automatische Fahrzeugfahndung und Verkehrsüberwachung

Die Polizei- und Zollbehörden dürfen die neuen Module und Funktionen des Systems zur automatischen Fahrzeugfahndung und Verkehrsüberwachung nutzen, wenn eine ausreichende Rechtsgrundlage dies vorsieht.

Die Systeme zur automatischen Fahrzeugfahndung und Verkehrsüberwachung (AFV) werden von der Eidgenössischen Zollverwaltung (EZV) und den Kantonspolizeikorps seit über zehn Jahren genutzt. Die Schweizerische polizeitechnische Kommission sieht einen Ersatz der Software (AFV Redesign) sowie die Einführung neuer Module und neuer Funktionalitäten vor. Der EDÖB und Privatim haben die Anforderungen und rechtlichen Grundlagen in einer Ad-hoc-Arbeitsgruppe überprüft. Die AFV-Nutzer dürfen die neuen Module und Funktionalitäten nur verwenden, wenn dies in einer gesetzlichen Grundlage vorgesehen ist.

Auch ist das Verhältnismässigkeitsprinzip einzuhalten. Diese Analyse beruht auf der Anzahl Kameras, deren Standort, der Verwendung der Daten, der Nutzungsart der Fahndungsdaten, der Bekanntgabe der Daten, usw. In den Kantonen erfolgt die Überprüfung im Allgemeinen anlässlich einer vorherigen Konsultation der Datenschutzbehörde. Beim Bund wird die Einhaltung des Verhältnismässigkeitsprinzips im Rahmen der Ämterkonsultation zu einer Gesetzesvorlage überprüft.

1.3 Steuer- und Finanzwesen

Bekanntgabe von Personendaten an ausländische Steuerbehörden

Die Umsetzung der neuen Standards zur weltweiten Bekämpfung von Steuerbetrug und Steuerhinterziehung sind weit fortgeschritten. Als problematisch erweist sich dabei das ungenügende Datenschutzniveau einiger Staaten. Im Berichtsjahr haben wir zu verschiedenen Vorlagen aus der Sicht des Datenschutzes Stellung genommen.

a) Automatischer Informationsaustausch über Finanzkonten (AIA)

Der globale Standard über den automatischen Informationsaustausch über Finanzkonten (AIA) ist in der Schweiz seit dem 1. Januar 2017 in Kraft. Er zielt darauf ab, die Steuertransparenz zu erhöhen und damit die grenzüberschreitende Steuerhinterziehung zu vermeiden. Bisher haben sich mehr als 100 Länder zur Übernahme dieses Standards bekannt, darunter auch die Schweiz. Nun will der Bundesrat das Schweizer AIA-Netzwerk mit derzeit 18 zusätzlichen Partnerstaaten ausweiten, mit denen der AIA ab 2020/2021 umgesetzt werden soll. (Weitere Informationen dazu sind auf der Website des EFD verfügbar.)

Wie bei den vorausgegangenen Ämterkonsultationen wies der EDÖB auch im aktuellen Berichtsjahr im Zusammenhang mit der Einführung des AIA mit weiteren Staaten auf das Erfordernis der Gewährleistung eines angemessenen Datenschutzniveaus im jeweiligen Partnerstaat hin. Unsere Staatenliste enthält hierzu eine Beurteilung für jedes einzelne Land. Anlässlich einer Anfang November 2018 durchgeführten Ämterkonsultation betreffend die Einführung des AIA mit weiteren Partnerstaaten ab 2020/21 merkten wir an, dass sämtliche vorgeschlagenen Partnerstaaten, mit denen der AIA in reziproker Weise durchgeführt werden soll (darunter Albanien, Aserbaidschan, Brunei Darussalam etc.) über kein angemessenes Datenschutzniveau (vgl. Art. 6 Abs. 1 DSG) verfügen und ein genügender Datenschutz folglich durch zureichende Datenschutzgarantien (vgl. Art. 6 Abs. 2 DSG) sichergestellt sein muss. Der Bundesrat berief sich in diesem Zusammenhang auf die basierend auf dem Multilateral Competent Authority Agreement (MCAA) ergangene, von der Schweiz am 4. Mai 2017 übermittelte Mitteilung an das Koordinationsgremium, in der datenschutzrechtliche Garantien festgelegt sind, welche auch für die Steuerpflichtigen in den Partnerstaaten gelten müssen. Diese Mitteilung stellt nach Ansicht des EDÖB jedoch keine ausreichende Garantie nach Art. 6 Abs. 2 DSG dar (vgl. 24. und 25. Tätigkeitsbericht, jeweils Kapitel 1.9.1 a). Daher ist die geplante Erweiterung datenschutzrechtlich problematisch.

b) Austausch länderbezogener Berichte multinationaler Konzerne (ALBA)

Auch in diesem Berichtsjahr äusserte sich der EDÖB im Rahmen einer Ämterkonsultation zur Länderliste für die Aktivierung des Austauschs der länderbezogenen Berichte (vgl. 24. und 25. Tätigkeitsbericht, Kapitel 1.9.1). Dabei wies er darauf hin, dass die jüngst vorgesehene Erweiterung auf acht weitere Staaten und Territorien (darunter etwa die Vereinigten Arabischen Emirate, Serbien oder Sambia) solche betrifft, die auf der Staatenliste des EDÖB mit einem ungenügenden Datenschutzniveau aufgeführt sind. Der EDÖB hielt deshalb erneut fest, dass mit Blick auf solche Länder zusätzliche Garantien nach Art. 6 Abs. 2 DSG notwendig sind, um ein angemessenes Datenschutzniveau zu gewährleisten.

c) Lockerung der internationalen Amtshilfe in Steuersachen bei gestohlenen Daten

Im Berichtsjahr befasste sich der EDÖB im Rahmen einer Ämterkonsultation erneut mit Art. 7 lit. c des Steueramtshilfegesetzes (StAhiG), welcher den Informationsaustausch auf Ersuchen eines ausländischen Staats betrifft und regelt, in welchen Fällen auf ein solches Ersuchen nicht eingetreten wird. Nach geltendem Recht wird auf ein Ersuchen namentlich dann nicht eingetreten, «wenn es den Grundsatz von Treu und Glauben verletzt, insbesondere wenn es auf Informationen beruht, die durch Handlungen erlangt wurden, die nach schweizerischem Recht strafbar sind». In der Vergangenheit hatte der EDÖB dazu festgehalten, dass es seiner Meinung nach keine Rolle spielt, ob der ersuchende Staat solche Informationen passiv (etwa durch spontane Amtshilfe) oder aktiv erlangt hat; in beiden Fällen handelt der Staat, welcher die ihm angebotenen gestohlenen Daten annimmt, rechtswidrig (vgl. Kapitel 1.9.3 unseres 23. Tätigkeitsberichts 2015/16).

Diese Sichtweise deckt sich mit der bislang herrschenden Praxis, die vom «Global Forum on Transparency and Exchange of Information for Tax Purposes» jedoch als zu restriktiv kritisiert worden ist. Ein inzwischen ergangener Bundesgerichtsentscheid (Urteil 2C_648/2017 vom 17. Juli 2018) hält fest, dass grundsätzlich auch auf Ersuchen eingetreten werden darf, die sich auf Daten deliktischen Ursprungs stützen, solange der ersuchende Staat sie nicht mit der Absicht gekauft hat, sie danach für ein Amtshilfeersuchen zu verwenden. Art. 7 lit. c StAhiG soll neu deshalb nur noch statuieren, dass auf ein Ersuchen nicht eingetreten wird, wenn es den Grundsatz von Treu und Glauben verletzt. In Anbetracht des zu respektierenden Bundesgerichtsurteils hat der EDÖB darauf verzichtet, Einwände zu erheben.

Beschwerde gegen das EFD im ESTV-Fall noch hängig

Die vom EDÖB Ende 2017 erlassene Empfehlung betreffend Information der im Rahmen von internationalen Steueramtshilfeverfahren offen übermittelten Namen wurde vom Eidg. Finanzdepartement (EFD) nicht gestützt. Der EDÖB hat gegen die ablehnende Verfügung des EFD Beschwerde beim Bundesverwaltungsgericht eingereicht.

Ende Dezember 2017 erliessen wir eine formelle Empfehlung, wonach die Eidgenössische Steuerverwaltung (ESTV) in der internationalen Steueramtshilfe auch die vom Amtshilfeersuchen nicht formell betroffenen Personen, deren Namen offen, d.h. ungeschwärzt an die ersuchende ausländische Behörde übermittelt werden sollen, vorgängig zu informieren hat (vgl. Kapitel 1.9.2 des 25. Tätigkeitsberichts 2017/2018). Die ESTV lehnte diese Empfehlung ab, worauf der EDÖB von der gesetzlich vorgesehenen Möglichkeit Gebrauch machte, die Angelegenheit dem zuständigen Departement vorzulegen.

Das Eidg. Finanzdepartement (EFD) stützte in seinem Entscheid vom 20. September 2018 die Haltung der ESTV, wonach die vom EDÖB empfohlene Information von Drittpersonen, deren Namen im Amtshilfeverfahren offen übermittelt werden sollen, einen zu grossen Aufwand verursachen und damit eine wirksame Amtshilfe verunmöglichen würde. Den Rechten der Betroffenen würde bereits dadurch Rechnung getragen, dass nur das notwendige Minimum an Daten übermittelt werde. Es lehnte folglich den Antrag des EDÖB ab.

Information der Drittpersonen mit vertretbarem Aufwand möglich

Der EDÖB vertritt nach wie vor die Ansicht, dass Drittpersonen die Möglichkeit haben müssen, die Gerichte beurteilen zu lassen, ob im konkreten Einzelfall eine offene Übermittlung ihres Namens zulässig ist. Nur so kann sichergestellt werden, dass deren verfassungsmässigen Rechte gewahrt werden. Um die notwendigen rechtlichen Schritte einleiten zu können, müssen die betroffenen Personen von der geplanten Übermittlung in Kenntnis gesetzt werden. Zudem geht der EDÖB davon aus, dass der Aufwand für die Information durch geeignete technische und organisatorische Massnahmen in einem vertretbaren Rahmen gehalten werden kann und damit eine wirksame Amtshilfe nicht verhinderte würde. Er hat daher am 5. Oktober 2018 gegen die Verfügung des EFD Beschwerde bei Bundesverwaltungsgericht eingereicht. Der Fall war dort zum Ende des Berichtsjahrs noch hängig.

Empfehlung an Zentralstelle für Kreditinformation (ZEK) erlassen

Kreditgesuche, die aus Gründen abgelehnt worden sind, die nichts mit der Kreditwürdigkeit oder Kreditfähigkeit des Gesuchstellers zu tun haben, sind unmittelbar nach der Ablehnung aus der Datenbank zu löschen. Der EDÖB hat gegenüber der Zentralstelle für Kreditinformation eine entsprechende Empfehlung erlassen.

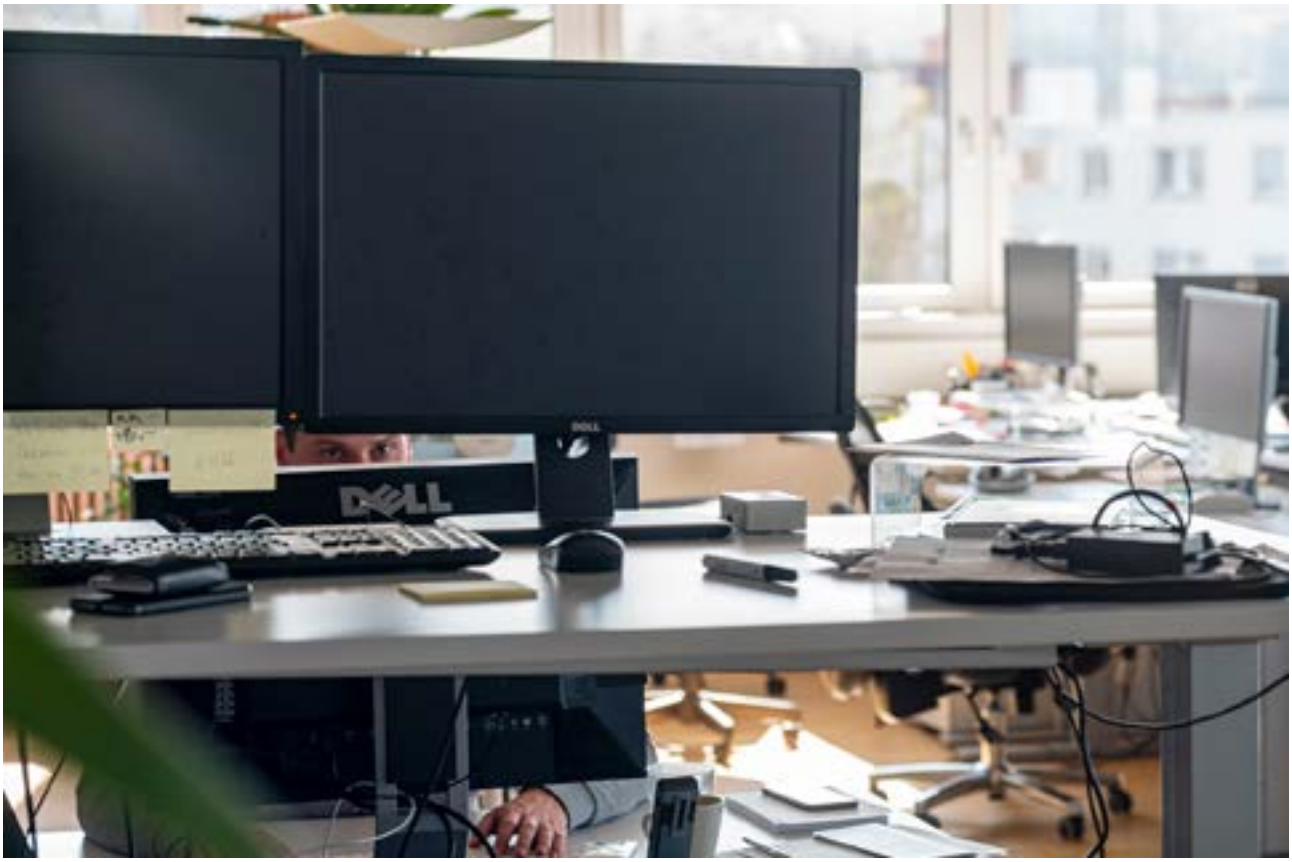
Die Zentralstelle für Kreditinformation (ZEK) sammelt Bonitätsinformationen aus Kreditgeschäften natürlicher und juristischer Personen und stellt diese ihren Mitgliedern, insbesondere Banken, gegen Entgelt zur Verfügung. Im vorigen Berichtsjahr haben wir bei der ZEK eine Sachverhaltsabklärung eingeleitet (vgl. Kapitel 1.8.12 des 25. Tätigkeitsberichts 2016/17). Aufgrund der eingegangenen Meldungen der Bürger und von Medienberichten verortete der EDÖB mögliche Mängel hinsichtlich der Datenschutzkonformität bei der Bearbeitung von Auskunftsgesuchen, bei der Berichtigung und Löschung von Daten, bei den Massnahmen zur Verhinderung zweckfremder Abfragen sowie bei der technischen und organisatorischen Trennung der Datenbestände der ZEK von denjenigen der Informationsstelle für Konsumkredit (IKO). Diese hat mit der ZEK einen Nutzungsvertrag für deren Informationssystem abgeschlossen.

Im Rahmen unserer Abklärungen hat sich jedoch gezeigt, dass die ZEK in den untersuchten Bereichen datenschutzkonform handelt. Auskunfts-, Berichtigungs- und Löschbegehren werden korrekt bearbeitet, die Massnahmen zur Verhinderung zweckfremder Anfragen entsprechen den gestellten Anforderungen und die Datenbestände von ZEK und IKO sind sowohl technisch als auch organisatorisch ausreichend getrennt.

Empfehlung betreffend nicht zweckgemässer Datenspeicherung

Einzig im Bereich der Ablehnung von Kreditgesuchen und Kartenanträgen hat der EDÖB eine Empfehlung erlassen. Er stellte fest, dass Kreditgesuche und Kartenanträge, welche aus Gründen abgelehnt worden sind, die nichts mit der Kreditwürdigkeit oder Kreditfähigkeit des Gesuchstellers zu tun haben (z. B. Ausschöpfung des Kreditkontingents für einen bestimmten Zeitraum), in der Datenbank der ZEK auch nach Ablehnung des Kreditgesuches gespeichert bleiben, obwohl diese Information für die Beurteilung der Kreditvergabe und damit für den mit der Datenbank verfolgten Zweck unerheblich ist. Der EDÖB hat daher empfohlen, dass solche Einträge unmittelbar nach der Ablehnung aus der ZEK-Datenbank zu löschen sind.

Die ZEK hat die Empfehlung des EDÖB akzeptiert und wird die entsprechenden Änderungen in ihrem Reglement und in der Datenbank vornehmen. Dementsprechend konnte der EDÖB das Verfahren ohne weitere Massnahmen abschliessen.


DELL

1.4 Handel und Wirtschaft

Datendiebstahl bei Swisscom ohne formelle Massnahmen abgeschlossen

Die Swisscom hatte den EDÖB Ende 2017 über einen Datendiebstahl in Kenntnis gesetzt. Betroffen waren vorwiegend private Inhaber von Mobilnummern. Der EDÖB konnte das bei der Swisscom durchgeführte Verfahren zur Prüfung möglicher Risiken von Folgeschäden aufgrund des gemeldeten Datendiebstahls ohne formelle Empfehlungen abschliessen.

Ende Dezember 2017 hatte die Swisscom den EDÖB darüber ins Bild gesetzt, dass im Herbst unberechtigte Zugriffe auf die Kontaktdaten von rund 800 000 Kundinnen und Kunden erfolgt sind. Betroffen waren vorwiegend private Inhaber von Mobilnummern und einige Festnetzkunden. Kurz darauf wurde dem EDÖB ein Ereignis eines angeblich unberechtigten Zugriffs auf Daten eines Kunden der Swisscom gemeldet. Ein Kausalzusammenhang mit dem gemeldeten Datendiebstahl bestand jedoch nicht (vgl. 25. Tätigkeitsbericht 2017/2018, Kapitel 1.3.1). Nach Meldung eines jedoch möglicherweise mit dem Anfang Februar 2018 publik gewordenen Datendiebstahls bei der Swisscom zusammenhängenden missbräuchlichen Zugriffs auf Kundendaten hat der EDÖB ein Verfahren eröffnet und bei der Swisscom Informationen im Zusammenhang mit dem Risiko allfälliger Folgeschäden einverlangt (vgl. Kapitel 1.3.2 im 25. Tätigkeitsbericht 2017/2018). Die Swisscom hat daraufhin eine Dokumentation über die bei ihr gemeldeten Verdachtsfälle sowie die jeweils getroffenen Massnahmen eingereicht. In den behandelten Fällen stand jeweils der Verdacht im Raum, dass mit Hilfe der gestohlenen Daten ein unrechtmässiger Zugriff auf weitere Kundendaten ermöglicht worden sei.

Der EDÖB hat gestützt auf diese Dokumentation untersucht, ob die durch die Swisscom in Zusammenhang mit dem Datendiebstahl getroffenen Massnahmen die betroffenen Personen genügend schützen oder ob sich durch die gemeldeten Verdachtsfälle zeigt, dass weitergehende Massnahmen notwendig sind.

Auch nach vertieften Abklärungen konnte bei keinem der untersuchten Fälle ein Zusammenhang mit dem fraglichen Datenleck festgestellt werden. Die Vorfälle konnten allesamt auf technische Fehler oder auf Fehlmanipulationen zurückgeführt werden. Nachdem die Swisscom Massnahmen zur Fehlerbehebung sowie zur Verhinderung künftiger vergleichbarer Vorfälle getroffen hat, konnte der EDÖB das Verfahren ohne formelle Massnahmen abschliessen.

Nach der Publikation des Datenlecks durch die Swisscom ist beim EDÖB – gestützt auf das Öffentlichkeitsgesetz – ein Zugangsgesuch zu den betreffenden Dokumenten eingegangen. Der EDÖB hat nach Anhörung der Swisscom entschieden, dass der Zugang, mit Ausnahme der in den Dokumenten enthaltenen Personendaten, gewährt werden soll und eine entsprechende Verfügung erlassen. Gegen diese Verfügung hat die Swisscom Beschwerde beim Bundesverwaltungsgericht eingereicht. Der Fall war zum Ende des Berichtjahres noch hängig.

Datendiebstahl bei EOS – unnötig gespeicherte Patientendaten

EOS hat das von einem Datendiebstahl betroffene System durch ein neues ersetzt. Der EDÖB konnte das Verfahren zur Sachverhaltsabklärung damit abschliessen.

Der EDÖB hat Ende Dezember 2017 bei der Inkassofirma EOS Schweiz eine Sachverhaltsabklärung eröffnet, um die datenschutzrechtlichen Aspekte des auch in den Medien publik gewordenen mutmasslichen Datendiebstahls zu klären, von dem insbesondere die Patienten von Schweizer Ärzten und Zahnärzten betroffen seien (vgl. Kap. 1.8.2 im 25. Tätigkeitsbericht 17/18).

Obschon die konkreten Umstände des mutmasslichen Datendiebstahls bisher nicht abschliessend geklärt werden konnten, haben die Abklärungen des EDÖB insbesondere ergeben, dass auf den Servern der EOS deutlich mehr Patientendaten gespeichert wurden, als für die Rechnungsstellung oder das Inkasso nötig gewesen wäre. Zudem wurden dabei Löschfristen missachtet. Dies führt zu einem unverhältnismässig grossen Datenbestand.

EOS ist im Rahmen eigener Abklärungen zu demselben Schluss gelangt, hat das betreffende System unterdessen durch ein neues ersetzt und dabei die festgestellten Mängel behoben. Der EDÖB konnte daher darauf verzichten, Massnahmen zu ergreifen und hat das Verfahren ohne formelle Empfehlungen abgeschlossen. Er erinnert daran, dass Medizinalpersonen für die Rechnungsstellung oder das Inkasso nur diejenigen Patientendaten weitergeben dürfen, die dazu auch tatsächlich erforderlich sind.

Verwendung der Daten von ricardo.ch in der Tamedia-Gruppe

Die Auktionsplattform ricardo.ch teilt die Daten ihrer Nutzer in der Tamedia-Gruppe zum Zwecke der Sicherheit und der gezielten Werbung. Nach der Eröffnung unseres formellen Verfahrens hat ricardo.ch seine Datenschutzerklärung im Mai 2018 angepasst. Wir beurteilen die Sachlage auf dieser Basis neu.

Im Juli 2017 informierte die Online-Auktionsplattform ricardo.ch ihre Nutzer über die Änderung ihrer Datenschutzerklärung, die derjenigen der anderen Tochtergesellschaften der Tamedia-Gruppe – der ricardo.ch angehört – angepasst wurde. Die neuen Nutzungsbedingungen sollen insbesondere einen Datenaustausch innerhalb der Gruppe ermöglichen, um gezielte Werbung zu betreiben, aber auch, um etwaige Missbräuche zu verhindern. Ohne Reaktion seitens der Nutzer von ricardo.ch galt die neue Datenschutzerklärung und damit auch die Bekanntgabe der Nutzerdaten an Tamedia und ihre Tochtergesellschaften als akzeptiert. Wenn jemand Einspruch erhob, wurde das Konto automatisch gesperrt oder suspendiert. Da wir bezüglich der Gültigkeit der Einwilligung der betroffenen Personen Zweifel hatten, eröffneten wir ein formelles Verfahren, um zu prüfen, ob die gesetzlichen Anforderungen in dieser Hinsicht erfüllt waren (vgl. Kapitel 1.8.8 unseres 25. Tätigkeitsberichts 2017/18).

Inzwischen hat Ricardo seine Datenschutzerklärung gleichzeitig mit der Inkraftsetzung der europäischen Datenschutz-Grundverordnung (DSGVO) ab dem 25. Mai 2018 geändert. Die Nutzer von Ricardo können sich nunmehr der gemeinsamen Datennutzung mit der Tamedia-Gruppe widersetzen, wenn sie dies ausdrücklich beantragen. Es wird also davon ausgegangen, dass die Nutzer der Datenbearbeitung zum Zweck der zielgruppenspezifischen Werbung zwar zustimmen, aber die Möglichkeit haben, ihre Zustimmung nachträglich zu widerrufen. Wir haben die neuen Bedingungen analysiert, wozu einige Abklärungen erforderlich waren. Wir bewerten nun die Sachlage auf dieser neuen Basis. Insbesondere prüfen wir, ob die Nutzer von ricardo.ch ausreichend informiert werden und ob die Möglichkeit, dem Profiling und der Datenanreicherung für gezielte Werbezwecke nachträglich zu widersprechen (Opt-out), ausreicht. Das DSG verlangt nämlich, dass die Einwilligung – wenn kein anderer Rechtfertigungsgrund vorliegt – bei der Bearbeitung besonders schützenswerter Daten oder Persönlichkeitsprofilen ausdrücklich erfolgen muss. Zum Zeitpunkt des Abschlusses dieses Tätigkeitsberichts war die rechtliche Prüfung noch im Gang.

Sachverhaltsabklärung bei Smart-TV-Hersteller abgeschlossen

Ein bei einem Hersteller von Smart-TV-Geräten durchgeführtes Verfahren zur Klärung der Datenschutzkonformität bei der Bearbeitung von Nutzerdaten konnte ohne formelle Massnahmen abgeschlossen werden.

Der EDÖB hat bei einem Hersteller von Smart-TV-Geräten eine Sachverhaltsabklärung durchgeführt um zu klären, welche Daten dort über die TV-Nutzer bearbeitet werden, wie die Nutzer darüber informiert werden und ob diese Datenbearbeitungen freiwillig erfolgen (vgl. Kapitel 1.3.1 des 25. Tätigkeitsberichts 2017/2017). Eine vertiefte Analyse der eingereichten Dokumentation ergab, dass der Hersteller die bei ihm anfallenden Nutzerdaten datenschutzkonform bearbeitet.

Der Gerätehersteller bearbeitet die Nutzerdaten nur dann personenbezogen, wenn dies technisch notwendig oder vom Nutzer aufgrund bestimmter Zusatzfunktionen gewünscht wird. Die übrigen Datenbearbeitungen erfolgen ohne Personenbezug, z. B. zu statistischen Zwecken.

Die Gerätenutzer werden über mögliche Datenübermittlungen an den Hersteller und deren Bearbeitung informiert. Sie können eine solche vollständig unterbinden und die Geräte als herkömmliche Fernseher, d.h. ohne Smart-TV-Funktionen, nutzen. Werden die Smart-TV-Funktionen genutzt, ist die Bearbeitung bestimmter Daten technisch notwendig und kann in dem Umfang vom Nutzer nicht eingeschränkt oder unterbunden werden. Diejenigen Datenbearbeitungen, die dem Komfort oder gewissen Zusatzfunktionen dienen, kann der Nutzer dagegen deaktivieren.

Nachdem der EDÖB keine datenschutzwidrigen Datenbearbeitungen durch den Gerätehersteller feststellen konnte, hat er das Verfahren ohne formelle Massnahmen abgeschlossen.

Decathlon – verbesserte Information bei Datenbeschaffung nötig

Der Sportwarenhändler Decathlon machte in seinen Schweizer Filialen den Warenverkauf von der Angabe von Kundendaten abhängig. Der EDÖB eröffnete deshalb eine Sachverhaltsabklärung. Das umstrittene Vorgehen hat der Sportwarenhändler daraufhin geändert.

Im Berichtsjahr eröffneten wir beim Sportwarenhändler Decathlon eine Sachverhaltsabklärung, nachdem wir aufgrund von Zeitungsberichten sowie Meldungen von Bürgern und Konsumentenschutzorganisationen vernommen hatten, dass dieser in seinen Schweizer Filialen den Warenverkauf von der Angabe gewisser Kundendaten abhängig mache.

Nach der Eröffnung des Verfahrens teilte Decathlon dem EDÖB mit, dass die Kundinnen und Kunden ihre E-Mail-Adresse oder Telefonnummer angeben müssten, um Waren vor Ort kaufen zu können. Die Unternehmung werde fortan aber darauf verzichten, den Warenverkauf von der Angabe dieser Daten abhängig zu machen und diese Daten nur noch auf freiwilliger Basis erheben. Da der primäre Anlass für die Sachverhaltsabklärung damit dahingefallen war, konzentrierte der EDÖB seine weiteren Abklärungen auf die Frage, ob diese Freiwilligkeit für die Kunden auch tatsächlich erkennbar ist.

Die Abklärungen des EDÖB hatten ergeben, dass die Informationen von Decathlon dazu uneinheitlich und teilweise zu wenig klar formuliert sind, so dass der Eindruck entstehen kann, die ursprünglich obligatorischen Angaben seien noch immer zwingend für einen Warenkauf. Er unterbreitete dem Sportwarenhändler Decathlon daher Vorschläge für eine Verbesserung der Information.

1.5 Gesundheit

Statistikprojekt mit Einzeldatensätzen der Versicherer (BAGSAN)

Das Bundesamt für Gesundheit betreibt das Statistikprojekt BAGSAN mit anonymisierten Individualdatensätzen der Versicherer. Der EDÖB begleitet das Projekt, das auch die Politik bewegt.

Der EDÖB begleitet das Statistikprojekt BAGSAN des Bundesamtes für Gesundheit (BAG) seit dem Jahr 2016 (s. 23. Tätigkeitsbericht, Kapitel 1.6.4). Wir haben mit den Projektverantwortlichen die Massnahmen zur Verhinderung von unberechtigten internen Zugriffen diskutiert. Dass die Zugriffe mittels Logs dokumentiert werden, ist eine Selbstverständlichkeit; automatisierte Alerts wären wünschenswert, z. B. wenn eine auffällig hohe Anzahl von Zugriffen durch einen Mitarbeiter erfolgt. Aus Gründen des Persönlichkeitsschutzes der Mitarbeitenden wird nun eine Lösung mit pseudonymisierten Benutzerdaten implementiert werden. Bei einem konkreten Verdacht auf einen Missbrauch könnte sodann eine namentliche Auswertung durchgeführt werden.

Das Projekt BAGSAN wird auch auf politischer Ebene weiter diskutiert. Eine parlamentarische Initiative von Ständerat Joachim Eder hat zum Ziel, dass das BAG im Sinne des Datenschutzes nur noch gruppierte Daten von den Versicherern erhält, die keinen Rückschluss auf Einzelpersonen mehr zulassen. Das Bundesgesetz über die Aufsicht über die soziale Krankenversicherung (KVAG) soll entsprechend angepasst werden. Mittlerweile befasste sich die eigens gegründete parlamentarische Subkommission «Datenlieferung» mit dem Geschäft und hat einen Revisionsentwurf zu Handen der Kommission für Soziale Sicherheit und Gesundheit (SGK) erarbeitet. Die SGK hat den Vorentwurf mit dem erläuternden Bericht in die Vernehmlassung gegeben. Wenn das BAG von den Krankenversicherern nur noch gruppierte Daten erhielte, würde das Projekt BAGSAN zwar nicht hinfällig, jedoch müssten erhebliche Anpassungen vorgenommen werden. Der EDÖB wird das Projekt BAGSAN weiterhin aufmerksam verfolgen.

Neue Aufgaben durch elektronisches Patientendossier

Die Umsetzungsarbeiten für das Elektronische Patientendossier schreiten voran. Ab Frühjahr 2020 soll es in allen Regionen der Schweiz verfügbar sein. Damit ergeben sich für den EDÖB wichtige neue Aufsichtsaufgaben.

Das Elektronische Patientendossier (EPD) gemäss Bundesgesetz über das Elektronische Patientendossier (EPDG) wird durch Bund und Kantone mit Hockdruck vorangetrieben. Damit es ab Frühjahr 2020 in allen Regionen der Schweiz der Bevölkerung angeboten werden kann, braucht es gemäss EPDG zertifizierte privatrechtlich organisierte Anbieter, die sog. Gemeinschaften und Stammgemeinschaften. Die Datenbearbeitungen durch derartige Anbieter richten sich ergänzend zu den spezialgesetzlichen Bestimmungen nach dem DSG, dessen Anwendung der Aufsicht unserer Behörde unterliegt. Die Gemeinschaften gelten als private juristische Personen, deren Aufsicht in die Zuständigkeit des Bundes fällt (unabhängig davon, ob die einzelnen Mitglieder der Gemeinschaften Spitäler des öffentlichen kantonalen Rechts oder des Privatrechts sind). Zudem werden zentrale Komponenten, die für den Betrieb des EPD notwendig sind, durch den Bund betrieben.

Sowohl die Patientinnen und Patienten als auch die Behandelnden benötigen für den Zugang zum EPD Identifikationsmittel, die eine eindeutige Authentisierung ermöglichen. Dafür werden elektronische Identitäten verwendet, die bspw. auf einer Chipkarte oder einem Smartphone gespeichert werden können. Die Herausgeber von Identifikationsmitteln gemäss EPDG müssen sich zertifizieren lassen. Auch die Datenbearbeitungen im Rahmen des Erstellens und Verwaltens der elektronischen Identitäten unterstehen dem DSG. Mit Blick auf die rechtlichen und technischen Anforderungen des Datenschutzes müssen hohe Standards erfüllt werden, damit die Patientinnen und Patienten dem EPD vertrauen werden. Auf Wunsch von Parlamentarierinnen und Parlamentariern hat der EDÖB denn auch in verschiedenen Kommissionen der eidgenössischen Räte seine Aufgaben im Bereich des EPD dargelegt, die er aufgrund der Budgetvorgaben des Bundesrats ohne zusätzliche Personalressourcen wahrnehmen muss.

Bonusprogramm «Helsana+» auf dem Prüfstand: Teilerfolg vor Bundesverwaltungsgericht

Im laufenden Berichtsjahr nahm der EDÖB das Bonusprogramm «Helsana+» genauer unter die Lupe. Er erliess eine Empfehlung gegen die Helsana Zusatzversicherungen AG, welche diese ablehnte. Der EDÖB hat daraufhin beim Bundesverwaltungsgericht Klage eingereicht, die im März 2019 teilweise gutgeheissen wurde.

Bereits in der vorangehenden Berichtsperiode wurde der EDÖB auf mehrere Gesundheits-Apps und Bonusprogramme von Krankenversicherungen aufmerksam, darunter auch auf das Bonusprogramm «Helsana+» der Krankenkasse Helsana, das im September 2017 lanciert wurde. Dabei handelt es sich um ein Programm, das die daran teilnehmenden Versicherten zu einem gesundheitsbewussten Verhalten und aktiven Lebensstil anregen soll. Als Belohnung für ihre aufgezeichneten Aktivitäten erhalten die Teilnehmenden sog. «Pluspunkte» gutgeschrieben, die sie in Barauszahlungen umwandeln oder aber für Angebote und Rabatte bei Partnerfirmen der Helsana einlösen können. Anders als bei vergleichbaren Angeboten anderer Krankenkassen können bei «Helsana+» auch Personen teilnehmen, die bei der Helsana ausschliesslich eine Grundversicherung abgeschlossen haben.

Nachdem wir im letzten Berichtsjahr eine formelle Sachverhaltsabklärung bei der Helsana Krankenkasse durchgeführt und abgeschlossen hatten, erliess der EDÖB am 26. April 2018 eine Empfehlung gemäss Art. 29 DSG gegenüber der Helsana Zusatzversicherungen AG. Darin empfahl der EDÖB erstens, den Datenfluss von der Grund- in die Zusatzversicherung im Rahmen des Registrierungsprozesses zu beenden, d.h. bei der Registrierung für das Bonusprogramm die Bearbeitung von Personendaten der Grundversicherten zu unterlassen. Zweitens verlangte der EDÖB von der Helsana Zusatzversicherungen AG, Datenbearbeitungen betreffend Kunden, die bei der Helsana ausschliesslich grundversichert sind, zwecks Bemessung und Ausrichtung von geldwerten Rückerstattungen zu unterlassen. Der EDÖB ist der Ansicht, dass die beanstandeten Datenbearbeitungen wirtschaftlich gesehen auf eine nachträgliche Rückerstattung eines Teils der Grundversicherungsprämie hinauslaufen, welche so vom Gesetz nirgends vorgesehen ist.

Da die Helsana Zusatzversicherungen AG seine Empfehlung ablehnte, entschied sich der EDÖB, den Fall dem Bundesverwaltungsgericht vorzulegen. Er reichte deshalb am 18. Juni 2018 Klage ein.

Datenbeschaffung war mangels rechtsgültiger Einwilligung rechtswidrig

Mit Entscheid vom 19. März 2019 hat das Bundesverwaltungsgericht die Klage des EDÖB teilweise gutgeheissen. Die Datenbeschaffung beim Grundversicherer war mangels rechtsgültiger Einwilligung rechtswidrig. Hingegen erwiesen sich die weiteren Datenbearbeitungen im Rahmen von «Helsana+» als rechtmässig. Dabei äusserte sich das Bundesverwaltungsgericht erstmals grundsätzlich zur Frage, wann eine Datenbearbeitung zu einem rechtswidrigen Zweck gegen das Datenschutzgesetz (DSG) verstösst. Es kam zum Schluss, dass die Datenbearbeitung zu einem rechtswidrigen Zweck nur dann auch im Sinne des DSG unrechtmässig ist, wenn sie gegen eine Norm verstösst, die zumindest auch den Schutz der Persönlichkeit bezweckt.

Rechtsvergleichend weist das Gericht dabei zudem auf die gegenüber dem DSG sowie dem Entwurf für ein totalrevidiertes DSG weitergehende europäische Datenschutz-Grundverordnung (DSGVO) hin, nach welcher die Daten nur für «legitime Zwecke» erhoben werden dürfen.

Damit auferlegt das Bundesverwaltungsgericht dem EDÖB eine gewisse Zurückhaltung bei der dynamischen Auslegung des DSG von 1992 im Hinblick auf digitale Applikationen. Das Urteil offenbart damit die Grenzen des in die Jahre gekommenen Gesetzes. Weil die vorliegend in Frage stehenden Bestimmungen des Krankenversicherungsgesetzes (KVG) nicht auch dem Persönlichkeitsschutz dienen, konnte das Bundesverwaltungsgericht letztlich die KVG-Konformität der Datenbearbeitung offenlassen. Das Gericht hielt aber bei dieser Gelegenheit gleichwohl fest, dass eine Verletzung des KVG nicht ersichtlich sei und liess damit erkennen, dass es der wirtschaftlichen Betrachtungsweise des EDÖB nicht folgen würde.

Mit Blick auf die hängige Totalrevision des DSG von 1992 hat der EDÖB von einer Anfechtung des Urteils abgesehen. Der Gesetzgeber hat es in der Hand, die vom Bundesverwaltungsgericht aufgezeigte Diskrepanz zum europäischen Recht schliessen.

Rasant wachsende Datenmengen in der «personalisierten Gesundheit» bergen Risiken

Die fortschreitende Digitalisierung in Medizin und Forschung führt zu immer grösseren Mengen an Gesundheitsdaten. Insbesondere wenn die Daten Rückschlüsse auf Einzelpersonen zulassen, sind die Grundsätze des Datenschutzes zu beachten.

Im Gesundheitsbereich entstehen immer grössere Datenbestände. Es handelt sich beispielsweise um klinische Daten aus Spitälern, Arztpraxen oder Biobanken sowie von den betroffenen Personen selber gesammelte Daten. Letztere entstehen z. B. durch das Nutzen von Gesundheits-Apps, Fitnesstrackern oder medizinischen Geräten wie einem Blutzuckermessgerät. Ziel der «personalisierten Gesundheit» ist es, diese Daten zu nutzen, um übergeordnete Gesundheitsstrategien zu entwickeln, bestimmte Krankheitsrisiken früher zu erkennen oder medizinische Behandlungen speziell für einzelne Patienten oder Patientengruppen zu entwickeln. Die wachsende Datenmenge birgt für die medizinische Forschung und Behandlung Chancen, Herausforderungen und Datenschutzrisiken. Eine Herausforderung besteht darin, eine gleichbleibende Qualität und Verlässlichkeit solcher Daten zu garantieren oder deren Vergleichbarkeit sicherzustellen. Datenschutzrisiken sind etwa in Bezug auf die technische Sicherheit oder schwer vorhersehbare Zweckänderungen auszumachen. Zudem stellen sich ethische Fragen. Um all diese Aspekte mit einem einheitlichen Ansatz zu lösen, wurde unter der Leitung der Schweizerischen Akademie der Medizinischen Wissenschaften (SAMW) die Initiative «Swiss Personalized Health Network» (SPHN) lanciert. Das SPHN ist vom Bund beauftragt, die Grundlagen und Infrastrukturen zu schaffen, damit Forschungsinstitutionen gesundheitsbezogene Daten austauschen können. Der EDÖB war an diesen Arbeiten beteiligt. Es ist wichtig, dass bei der Bearbeitung von nicht-anonymisierten Gesundheitsdaten Transparenz herrscht – sowohl hinsichtlich des Bearbeitungszwecks wie der Verwendung der jeweiligen Daten – und die Einwilligung der Patienten vorgängig rechtsgültig eingeholt wird.

1.6 Arbeit

Outsourcing: Bearbeitung von Personaldaten im Ausland

Aus Kosten- oder Organisationsgründen entscheiden sich viele Arbeitgeber, die Personaldaten ihrer Mitarbeitenden ausserhalb der Landesgrenzen bearbeiten zu lassen. Dabei ist die transparente und umfassende Information der Arbeitnehmenden zentral – ihre Einwilligung ist jedoch in der Regel nicht nötig und wäre auch nicht gültig.

Der Trend der Wirtschaft, Personaldaten zum Zwecke der Rationalisierung und Zentralisierung im Ausland zu speichern und zu bearbeiten, hält an. Zahlreiche betroffene Mitarbeitende, aber auch Arbeitgeber oder Personalverantwortliche haben dem EDÖB im vergangenen Berichtsjahr Fragen zur Zulässigkeit und zu den Ausgestaltungsmöglichkeiten eines Outsourcings gestellt. Eine Datenübermittlung ins Ausland findet statt, sobald die Daten einem im Ausland ansässigen Unternehmen oder einer im Ausland ansässigen Einheit zugänglich gemacht werden oder die Daten in einer Cloud gespeichert werden, die sich im Ausland befindet. Im Vordergrund standen Fragen zur Informationspflicht und Einwilligung der Arbeitnehmenden, wenn Personaldaten über die Landesgrenze hinaus bearbeitet werden. Der EDÖB empfiehlt Arbeitgebern eine umfassende interne Kommunikation sowohl über die Datenübermittlung ins Ausland als auch über die konkret vorgenommenen Datenbearbeitungen im Ausland und deren Zwecke. Eine solche Information beinhaltet demnach bspw. in welches Land der Export und an welches Unternehmen dieser erfolgt und welche Auswertungen zu welchen Zwecken vorgenommen werden.

Diese Information ist nicht mit der Einwilligung zu verwechseln. Da es aufgrund des Subordinationsverhältnisses im Arbeitsverhältnis regelmässig an der von Art. 4 Abs. 4 DSG geforderten «Freiwilligkeit» mangelt, erweist sich eine Einwilligung des Arbeitnehmers in der Regel als rechtlich unbeachtlich resp. als Rechtfertigungsgrund nach Art. 13 Abs. 1 DSG ungeeignet. Insbesondere bei global tätigen Unternehmen scheint es jedoch üblich, im Rahmen von Datenschutzrichtlinien die Einwilligung der Mitarbeitenden einzuholen, die sich nach schweizerischem Recht in der Regel als unwirksam erweisen. Ob eine Datenübermittlung im konkreten Einzelfall rechtmässig erfolgt und die Information der betroffenen Personen angemessen war, ist vom zuständigen Zivilgericht zu entscheiden.

Online-Bewerbungsverfahren und Bewerbungsgespräche: Was ist zu beachten?

Im Online-Bewerbungsverfahren der digitalisierten Arbeitswelt gelangen verbreitet automatisierte Verhaltens- und Stimmanalysen zur Anwendung. Da damit detaillierte Persönlichkeitsprofile erstellt werden könnten, ist ein erhöhtes Datenschutzniveau zu beachten.

Bewerbungsgespräche finden vermehrt online statt. Sowohl die Bewerber als auch Rekrutierenden stellen sich Fragen nach der Zulässigkeit und den rechtlichen Voraussetzungen von Verhaltens- oder Stimmanalysen. Nach Art. 328b OR ist es dem Arbeitgeber im Bewerbungsverfahren erlaubt, diejenigen Informationen über die Bewerber zu bearbeiten, die zur Klärung der Eignung für die Stelle oder zur Durchführung des Arbeitsvertrages erforderlich sind.

Der EDÖB hat im Rahmen seiner Beratungen darauf hingewiesen, dass es sich bei der Bearbeitung von Lebensläufen und weiteren Informationen durch die Personalverantwortlichen regelmässig um die Bearbeitung von wesentlichen Zügen der Persönlichkeit des Bewerbers resp. von Persönlichkeitsprofilen i.S.v. Art. 3 lit. d DSG handelt. Dies gilt umso mehr, wenn Aufnahmen von Bewerbungsgesprächen zudem Verhaltens- oder Stimmanalysen unterzogen werden. Die Auswertungen müssen verhältnismässig sein, und es müssen geeignete Massnahmen bezüglich Datensicherheit getroffen werden. Die Bewerbenden sind vorgängig nicht nur über die geplanten Auswertungen zu informie-

ren, sondern auch über Art und Zweck der Verwendung der Ergebnisse, über die Dauer der Aufbewahrung sowie über das ihnen zustehende Auskunftsrecht.

Bekämpfung der Schwarzarbeit im Kanton Wallis

Auf Intervention des EDÖB hat der Verband ARCC seine gleichnamige Smartphone-App für verstärkte Kontrollen auf Walliser Baustellen deaktiviert. Der EDÖB verlangt die Löschung der damit bereits beschafften Daten.

Für die Kontrolle von Baustellen haben mehrere paritätische Kommissionen des Kantons Wallis den Verband ARCC (franz. Association pour le Renforcement des Contrôles sur les Chantiers, ARCC) gegründet. Sein Haupteinsatzgebiet sind Kontrollen bezüglich Einhaltung des Schwarzarbeitsverbotes und des Entsendegesetzes. Wir haben aufgrund der eingegangenen Hinweise beim Verband eine Sachverhaltsabklärung gemäss Art. 29 DSG durchgeführt. In deren Rahmen hat sich der EDÖB auf die Smartphone-Applikation «ARCC» konzentriert, welche Meldungen direkt an den Verband ermöglicht. Übermittelt werden Fotos, auf welchen die Firma der betroffenen Bauunternehmung und allenfalls sogar Baustellen-Mitarbeiter ersichtlich sind, sowie Angaben zu Namen und Standort der Benutzer der Applikation.

Im Zuge unserer Abklärungen deaktivierte der Verband die Applikation wieder. Der EDÖB ist der Ansicht, dass für den Betrieb der Applikation und die aus deren Nutzung resultierenden Datenbearbeitungen derzeit keine ausreichende gesetzliche Grundlage vorhanden ist. Wir begrüssen deshalb die Deaktivierung und haben den Verband schriftlich ersucht, die bereits gesammelten Personendaten zu vernichten. Zudem haben wir den Verband darauf hingewiesen, dass er das Risiko von eventuellen zivilrechtlichen Klagen von betroffenen Personen trägt, falls er die gesammelten Daten weiterhin bearbeiten sollte.

1.7 Versicherungen

Neuer Observationsartikel für Sozialversicherungen

Verdeckte Beobachtungen sind ein wirksames Mittel zur Aufdeckung von Betrug und Missbräuchen im Sozialversicherungsbereich. Da sie einen massiven Eingriff in die Privatsphäre darstellen, sind sie aufs Notwendigste zu beschränken. Der EDÖB begrüsst die Bewilligungspflicht für den Einsatz von technischen Geräten zur Standortbestimmung.

Am 25. November 2018 hat das Stimmvolk den neuen Observationsartikel für verdeckte Überwachungen im Bereich der Sozialversicherung angenommen. Die neue Bestimmung wird voraussichtlich im Herbst 2019 in Kraft treten. Wir werden die Gelegenheit wahrnehmen, zu gegebener Zeit zu den noch ausstehenden Vollzugsbestimmungen auf Verordnungsstufe Stellung zu nehmen. Aus datenschutzrechtlicher Sicht bedeutsam sind insbesondere die Anforderungen an die externen Spezialistinnen und Spezialisten, die mit der Observation beauftragt werden. Das Auswahlverfahren und möglicherweise auch ein Zulassungsverfahren müssen dafür Gewähr bieten, dass die missbräuchliche Verwendung des Observationsmaterials mit höchster Wahrscheinlichkeit ausgeschlossen werden kann.

Der EDÖB erwartet ausserdem Konkretisierungen auf Verordnungsstufe oder mindestens Weisungen zur Observation von Versicherten, die sich an einem Ort befinden, der von einem allgemein zugänglichen Ort eingesehen werden kann. Im Sinne der Verhältnismässigkeit ist dafür zu sorgen, dass der Privatbereich, wie das Innere einer Wohnung, im Sinne der bisherigen Rechtsprechung des Bundesgerichts geschützt bleibt. Wir begrüssen, dass für den Einsatz von technischen Instrumenten zur Standortbestimmung eine gerichtliche Genehmigung eingeholt werden muss. Diese darf nur dann erteilt werden, wenn dem Gericht eine ausreichende Begründung für die Notwendigkeit des Einsatzes von derartigen Geräten im konkreten Einzelfall vorgebracht wurde. Ohne gerichtliche Genehmigung dürfen somit keine Trackinggeräte, zum Beispiel an Fahrzeugen, eingesetzt werden. Bild- und Tonaufnahmen dürfen allerdings weiterhin ohne richterliche Bewilligung gemacht werden.

Als wichtig erachtet der EDÖB auch die im neuen Observationsartikel festgehaltene Pflicht zur nachträglichen Information der versicherten Person, wenn sich der Verdacht eines Missbrauchs durch die Observation nicht bestätigt hat. In diesem Fall muss der Versicherer eine Verfügung erlassen, die über den Grund, die Art und die Dauer der Observation informiert. Die Versicherten können Einblick in das Observationsmaterial verlangen und dann entscheiden, ob es in den Akten bleibt oder vernichtet werden soll. Der Versicherer darf das Observationsmaterial jedoch erst dann vernichten, wenn die Verfügung rechtskräftig geworden ist und die versicherte Person nicht ausdrücklich erklärt hat, dass es in den Akten verbleiben soll.

SUVA: Mehr Transparenz bei Forschung mit Versichertendaten

Die SUVA hat die Information der Versicherten in Bezug auf die Verwendung ihrer Daten für Forschungszwecke in Zusammenarbeit mit dem EDÖB massgeblich verbessert. Auf der Website der SUVA finden Interessierte wichtige Informationen zur Verwendung der Versichertendaten für Forschungszwecke und zum Widerspruchsrecht.

Die SUVA verwendet Daten der Versicherten, meist in Zusammenarbeit mit Dritten, im Bereich der Arbeits-, Versicherungs- und Rehabilitationsmedizin für Forschungszwecke. Im Rahmen unserer Beratung haben wir darauf hingewirkt, dass die SUVA auf der Internetseite (Rubrik Unfall – Medizinische Forschung) ausführlich darüber informiert, wieso und in welchen Bereichen sie die Daten der Versicherten für Forschungszwecke verwendet. Die Forschungstätigkeit der SUVA findet schwerpunktmässig in den Bereichen Bewegungsapparat, Berufskrankheiten, traumatische Hirnverletzungen, chronische Schmerzen, psychische Unfallfolgen und Amputation statt. Sie dient aber auch der Verbesserung der Gutachtenmethodik und der Prävention. Die SUVA informiert jetzt auch klar darüber, dass jeder versicherten Person ein Widerspruchsrecht zusteht und wie dieses einfach ausgeübt werden kann.

Durch die Aufschaltung entsprechender Informationen auf ihrer Website kann die SUVA somit weiterhin einen wertvollen Beitrag zur medizinischen Forschung leisten. Gleichzeitig wahrt sie die Grundsätze der Erkennbarkeit und Transparenz der Datenbearbeitung. Die Teilnahme an Forschungsprojekten, respektive das Zurverfügungstellen der persönlichen Daten für Forschungszwecke, bleibt für die Versicherten freiwillig und darf keinen Einfluss auf die medizinische Betreuung oder die Beurteilung eines Leistungsfalles haben. Wichtig ist hier auch die Rolle der behandelnden Fachpersonen. Sie sollten die Patientinnen und Patienten darüber informieren, dass ihnen in Bezug auf die Nutzung ihrer Daten für Forschungszwecke ein Vetorecht zukommt. Teilt die Patientin oder der Patient der SUVA die Sperrung der eigenen Daten für Forschungszwecke mit, macht die SUVA einen Vermerk, der eine solche Nutzung verhindert.

Im Rahmen des gleichen Projekts hat unsere Beratung weiter dazu geführt, dass die SUVA die internen Richtlinien überarbeitet und wo nötig angepasst hat. Wir haben Wert darauf gelegt, dass die Anonymisierung der Personendaten so früh als möglich erfolgt. Zudem müssen die Forschenden, wenn sie mit nicht-anonymisierten oder nicht-pseudonymisierten Daten arbeiten, spezifische Vertraulichkeitsvereinbarungen mit der SUVA abschliessen. Bei der Verwendung von anonymisierten oder pseudonymisierten Daten ist es ihnen zudem untersagt, Datenbearbeitungen vorzunehmen, die zu einer Re-Identifikation von Personen führen könnten. Insbesondere dürfen die Forschungsdaten nicht mit Daten aus anderen Quellen verknüpft werden. Weiter müssen die Daten nach Abschluss des Forschungsprojekts und Publikation der Ergebnisse gelöscht werden. Die Forschenden haben die SUVA darüber schriftlich zu informieren. Entsprechende Informationen stehen für die Forschenden nun auf der Website der SUVA bereit. Unsere Beratung ist damit abgeschlossen, doch ist es an der SUVA sicherzustellen, dass die Informationen und die internen Richtlinien jederzeit auch bei Anwendung von neuen Behandlungs- und Forschungsmethoden den Anforderungen des Datenschutzgesetzes genügen. Insbesondere ist hier auch an den Umgang mit genetischem Material oder Resultaten von genetischen Untersuchungen (zum Beispiel aus dem Bereich der hochspezialisierten Medizin) zu denken.

1.8 Verkehr

Multimodale Mobilität – Wahrung der informationellen Selbstbestimmung ein Muss

Das UVEK prüft im Auftrag des Bundesrats, wie der Bund die multimodale Mobilität fördern und deren Potenziale nutzen kann. Den Reisenden soll die einfache, flexible Kombination von verschiedenen Mobilitätsangeboten auf allen Verkehrskanälen ermöglicht werden. Der EDÖB begleitete das Projekt im Berichtsjahr, beriet die Anbieter in datenschutzrechtlichen Belangen und nahm im Rahmen der Ämterkonsultation Stellung.

Mit neuen digitalen Technologien sollen sich Reisende einfacher über die Kombination von verschiedenen Mobilitätsangeboten informieren können. Dabei werden grosse Mengen an Personendaten bearbeitet. Der EDÖB verfolgte das Projekt, welches sich immer noch in der Anfangsphase befindet, und beriet die Anbieter der multimodalen Mobilitätsdienstleistungen unter anderem in verschiedenen Sitzungen. Die Anbieter sind sich bewusst, dass bei der Bearbeitung von Personendaten die Wahrung der informationellen Selbstbestimmung der Betroffenen gewahrt werden muss und dass konkrete Massnahmen zum Schutz der Persönlichkeitsrechte der Betroffenen getroffen werden müssen. Der EDÖB wies darauf hin, dass insbesondere kein direkter oder indirekter Zwang zur Preisgabe von Personendaten ausgeübt werden darf. Damit die Einwilligung durch die Betroffenen freiwillig erfolgen kann, müssen sie vorgängig transparent darüber informiert werden, welchen Datenbearbeitungen sie mit der Wahl einer bestimmten Mobilitätsdienstleistung zustimmen und welche alternative Wahl sie haben. Wenn durch die Verknüpfung von Sachdaten, die an sich nicht unter das Datenschutzgesetz fallen, Rückschlüsse auf Personen möglich werden, müssen die datenschutzrechtlichen Grundsätze erfüllt werden.

Ferner machte der EDÖB darauf aufmerksam, dass mit der Benutzung von multimodalen Mobilitätsdienstleistungen schnell Bewegungsprofile entstehen können, aus denen wiederum Persönlichkeitsprofile resultieren können. In diesem Fall muss das erhöhte Schutzniveau für besonders schützenswerte Personendaten und Persönlichkeitsprofile eingehalten werden.

Echte Wahlmöglichkeiten und anonymes Reisen für die Kunden

Der EDÖB nahm zudem im Rahmen der Ämterkonsultation zur multimodalen Mobilität Stellung. Dabei äusserte er sich auch zur geplanten Anpassung der Bestimmung im Personenbeförderungsgesetz (PBG) betreffend Datenbearbeitung durch die Unternehmen des öffentlichen Verkehrs (öV). Mit dieser Anpassung sollen die öV-Unternehmen bei der Bearbeitung von Daten nicht mehr den datenschutzrechtlichen Vorgaben für Bundesorgane, sondern neu grundsätzlich jenen für private Personen unterstehen und mit Einwilligung der Reisenden deren Daten für bestimmte Zwecke bearbeiten dürfen. Der EDÖB war mit der vorgeschlagenen Formulierung nicht einverstanden und wies darauf hin, dass in diesem Fall die Einwilligungen der Kunden nur beachtlich seien, wenn sie freiwillig, d.h. aufgrund echter Wahlmöglichkeiten erfolgen würden. Beim automatischen Ticketing hiesse dies, dass die Kunden alternativ zu den geplanten Modellen die Möglichkeit haben müssten, zu den gleichen Bedingungen, d.h. diskriminierungsfrei, ohne Preisgabe ihrer Personendaten anonym zu reisen. Zudem bedürfe die Bearbeitung von Personendaten zu Zwecken der Eingriffsverwaltung unverändert einer gesetzlichen Grundlage. Der EDÖB begrüsst, dass seine Bemerkungen im Vernehmlassungsentwurf Eingang fanden.

Der EDÖB wird das Projekt weiterhin begleiten. Zu gegebener Zeit werden die mit dem Projekt verbundenen Datenschutzrisiken zu evaluieren sein.

Datenschutzkonformität bei neuen Apps im öffentlichen Verkehr

Die Transportbranche hat uns über diverse Projekte informiert wie etwa die Weiterentwicklung verschiedener Apps (Applikationen). Dabei muss die Datenschutzkonformität laufend neu beurteilt werden. Insbesondere dürfen nicht mehr Daten gesammelt werden, als für die Erbringung eines Dienstes nötig sind.

Auch in diesem Jahr wurde der EDÖB von einzelnen Transportunternehmen über Datenschutzprojekte informiert. Darunter befanden sich unter anderem die Datenbearbeitungen in Zusammenhang mit der Weiterentwicklung verschiedener Apps von Transportunternehmen, insbesondere der SBB. Zuweilen war von anonymisierten Daten die Rede, obwohl betroffene Personen bestimmbar bleiben. In solchen Fällen darf in der Information an die betroffenen Personen nicht von anonymisierten Daten die Rede sein. Der EDÖB wies die SBB darauf hin, dass sie die Frage der Anonymisierung vor der Durchführung weiterer Datenbearbeitungen nochmals sorgfältig abklären müssen. Im gleichen Sinn wies der EDÖB die SBB darauf hin, dass bei der Datenbearbeitung auch die Grundsätze der Verhältnismässigkeit und Datensparsamkeit einzuhalten sind. Dies gilt auch dann, wenn für die Datenbearbeitung eine Einwilligung eingeholt wurde.

Es ist wichtig, dass die Transportunternehmen für jedes Projekt die Datenschutzkonformität sicherstellen. Dabei sind die durchgeführten oder geplanten Datenbearbeitungen entsprechend zu prüfen und gegebenenfalls an die datenschutzrechtlichen Voraussetzungen anzupassen. Bei Weiterentwicklungen von Apps ist die Datenschutzkonformität laufend neu zu analysieren.

1.9 International

Aufsichtskoordinationsgruppen über die Informationssysteme SIS II, VIS und Eurodac

Im Berichtsjahr trafen sich die Aufsichtsgruppen in Brüssel. Sie nahmen Stellung zu den Vorschlägen der EU-Kommission betreffend die Interoperabilität zwischen den EU-Informationssystemen.

Auch in diesem Jahr nahm der EDÖB als nationale Aufsichtsbehörde an den Sitzungen der drei Aufsichtskoordinationsgruppen über die EU-Informationssysteme SIS II, VIS (Vorsitz EDÖB) und Eurodac teil. Diese fanden am 12./13. Juni 2018 sowie 14./15. November 2018 in Brüssel statt. Vertreten sind der europäische Datenschutzbeauftragte (EDSB) sowie die nationalen Datenschutzbehörden der 28 EU-Mitgliedstaaten unter Teilnahme Irlands und des Vereinigten Königreichs als Beobachter. Ergänzt werden die Gruppen mit den nationalen Datenschutzbehörden der Schweiz, Liechtensteins, Norwegens und Islands, da deren Länder an den Informationssystemen teilhaben.

Die Aufsichtskoordinationsgruppen SIS und Eurodac haben u.a. ihre Tätigkeitsberichte 2016/2017 verabschiedet. Zuhanden des EU-Parlaments, des EU-Rats und der EU-Kommission nahmen sie Stellung zu den Vorschlägen der EU-Kommission für eine Verordnung, welche den Rahmen für die Interoperabilität zwischen EU-Informationssystemen festlegen soll. Die Gruppe VIS ihrerseits hat zuhanden dieser Gremien eine Stellungnahme zu den vorgeschlagenen Änderungen der EU-Kommission betreffend das VIS vorbereitet und verschickt. (vgl. www.sis2scg.eu, www.visscg.eu, www.eurodacscg.eu)

Zurzeit wird das Sekretariat der drei Aufsichtskoordinationsgruppen durch den europäischen Datenschutzbeauftragten geführt. In Zukunft soll die Führung dem Europäischen Datenschutzausschuss (EDSA) übertragen werden.

Arbeitsgruppe «Border, Travel & Law Enforcement»

Im Lauf des Berichtsjahrs nahm der EDÖB als Schengen-Mitgliedstaat an sieben Treffen der Unterarbeitsgruppe teil, die namentlich die Interoperabilität der grossen Informationssysteme der Europäischen Union im Bereich Migration, Asyl und Sicherheit, sowie die Zukunft der Überwachungsmodelle der grossen Informatiksysteme der EU im Bereich Justiz und Innenpolitik zum Thema hatten.

Eines der Hauptthemen auf diesen Tagungen war die Interoperabilität der (bereits bestehenden und künftigen) gross angelegten Informationssysteme der europäischen Union im Bereich Migration, Asyl und Sicherheit. Im Dezember 2017 veröffentlichte die EU-Kommission zwei Verordnungsvorschläge zur Schaffung eines Rechtsrahmens für die Interoperabilität der grossen Informationssysteme der Europäischen Union. Dieser neue Ansatz sowie die neu eingeführten Komponenten (Einrichtung eines europäischen Suchportals, eines Servicepools für den Abgleich biometrischer Daten sowie eines gemeinsamen Identitätsdatenverzeichnisses) haben Auswirkungen nicht nur auf den Datenschutz, sondern auch auf die Steuerung und Überwachung der Systeme. Hinsichtlich Datenschutz gab es Bedenken zur Zweckbestimmung einer zentralisierten Datenbank sowie zu den Voraussetzungen und Modalitäten ihrer Nutzung. Der europäische Datenschutzbeauftragte und die nationalen Datenschutzbehörden fordern die Einführung echter Garantien, um die Grundrechte der Staatsbürger von Drittländern zu wahren (vgl. zu diesem Thema die Stellungnahme des

europäischen Beauftragten vom 16. April 2018 auf folgendem Link: edps.europa.eu/data-protection).

Die Zukunft der Modelle zur Überwachung der grossen Informatiksysteme der EU im Bereich Justiz und Polizei wurde auf den verschiedenen Tagungen ebenfalls erörtert. Es wird eine Variante für einen verbesserten Überwachungsmechanismus der verschiedenen Systeme gesucht, z. B. indem diese in eine neue Struktur übertragen wird, die dem Europäischen Datenschutzausschuss (der Nachfolgeeinrichtung der Arbeitsgruppe «Artikel 29», welcher der europäische Beauftragte und die nationalen Datenschutzbehörden angehören) angeschlossen ist und die auch für den Beitritt von Nicht-Mitgliedstaaten mit Beobachterstatus für Themenbereiche im Zusammenhang mit dem Schengen-Besitzstand offen stehen könnte.

Darüber hinaus ist zurzeit die Ausarbeitung von Leitlinien hinsichtlich der EU-Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Polizei und die Strafverfolgungsbehörden (Richtlinie EU 2016/680) im Gange, namentlich in Bezug auf Artikel 47 und die Befugnisse der Aufsichtsbehörden.

Koordinationsgruppe der schweizerischen Datenschutzbehörden im Rahmen von Schengen

Die Koordinationsgruppe Schengen der schweizerischen Datenschutzbehörden ist im Berichtsjahr zweimal zusammengetreten. Der EDÖB informierte die kantonalen Datenschutzbehörden über die bei der Schengen-Evaluierung angesprochenen wichtigsten Punkte und die vom EU-Rat abgegebenen Empfehlungen.

Auf schweizerischer Ebene erfolgt die Koordination der mit Schengen zusammenhängenden Aktivitäten in der «Koordinationsgruppe der schweizerischen Datenschutzbehörden im Rahmen der Umsetzung des Schengen-Assoziierungsabkommens», welcher der EDÖB und die kantonalen Datenschutzbehörden angehören. Sie gibt den vertretenen Behörden die Gelegenheit, sich über die laufenden Entwicklungen im Bereich Schengen zu informieren, Kontrollaktivitäten zu planen und Informationen auszutauschen. So koordinieren wir in Anwendung der Schengen-Zusammenarbeit mit unseren kantonalen Amtskollegen unsere Tätigkeiten bei der Überwachung der in der Schweiz vorgenommenen Datenbearbeitungen im Bereich Migration, Polizei und Justiz.

Die Koordinationsgruppe der Schweizer Datenschutzbehörden ist im Laufe des Berichtsjahrs zweimal zusammengetreten. Auf der ersten Tagung informierte der EDÖB die kantonalen Datenschutzbehörden über die wichtigsten Punkte, die bei der vom 26. Februar bis 2. März 2018 durchgeführten Schengen-Evaluierung der Schweiz angesprochen wurden (s. oben). Die evaluierte kantonale Datenschutzbehörde (Luzern) vermittelte auch einen Überblick über die Elemente, die sie ganz besonders angehen, aber auch die anderen kantonalen Einrichtungen. Wir haben unseren kantonalen Amtskollegen auch die verschiedenen SIS/VIS-Kontrollen erläutert, die wir im Berichtsjahr durchgeführt haben. Die Kantone legten ihrerseits die Ergebnisse ihrer Kontrolltätigkeiten vor.

Bei der zweiten Tagung machte der EDÖB nähere Ausführungen zum Entwurf der an die Schweiz gerichteten Empfehlungen zum Datenschutz in der Schengen-Evaluierung. Wir informierten unsere kantonalen Kollegen auch über die in den Koordinationsgruppen zur Kontrolle des SIS/VIS erörterten Hauptpunkte.

Internationale Konferenz der Datenschutzbeauftragten

Die 40. Internationale Konferenz der Datenschutzbeauftragten befasste sich mit der digitalen Revolution und ihrer Auswirkung auf unsere Gesellschaften, sowie mit der Frage, wie eine neue digitale Ethik dazu beitragen könnte, Achtung und Würde in unserer technologiebeherrschten Welt zu gewährleisten. Es wurde eine Arbeitsgruppe zum Thema künstliche Intelligenz eingesetzt.

Die Konferenz fand vom 22. bis 26. Oktober 2018 in Brüssel unter der Leitung des Europäischen Datenschutzbeauftragten (EDSB) und der bulgarischen Datenschutzkommission statt und war dem Thema «Erörterung ethischer Aspekte: Würde und Respekt in einem von Daten beherrschten Leben» gewidmet. Wie Isabelle Falque-Pierrotin, Präsidentin der CNIL (französische Datenschutzkommission) und Vorsitzende der Internationalen Konferenz in ihrer Eröffnungsrede betonte, haben diese Themen in der Tat eine neue Dimension angenommen; sie erstrecken sich auf neue, vermehrt politische und ethische Problembereiche und treten in einem internationalen Umfeld zutage, das zwar nie besonders harmonisch war, das heute aber ein besonders kontrastreiches Bild abgibt. Selbst zu Fragen, die unseren Kernauftrag betreffen, wie Ortungsdienste, Internetsicherheit, Massenüberwachung oder nachrichtendienstliche Aufklärungstechniken, gehen die Meinungen auseinander. Die Digitalisierung bedeutet weltweit eine einzigartige Entwicklungschance, eine eigentliche Revolution. «Tech for good» oder «AI for humanity» sind mittlerweile von der Agenda unserer Staats- und Regierungschefs nicht mehr wegzudenken, und diese Technologien bieten ein enormes Potenzial an Lösungen für die Menschheit.

Erklärung zu Ethik und Datenschutz in der künstlichen Intelligenz

Die Konferenz wurde erstmals von einer europäischen Institution und einer nationalen Datenschutzbehörde gemeinsam ausgerichtet. Über tausend Teilnehmer diskutierten die aktuellen Datenschutzfragen. An der geschlossenen Konferenz wurden vier Neumitglieder aufgenommen: die Kontrollstelle für Informationszugang von Argentinien, die Datenschutzbehörden von Bayern und von Niedersachsen und die Kommunikationskommission von Korea. Der Konferenz gehören nun 123 Mitglieder an. Elisabeth Denham (Präsidentin der britischen Datenschutzbehörde ICO) wurde zur neuen Präsidentin und Nachfolgerin von Isabelle Falque-Pierrotin (Präsidentin der CNIL) gewählt. Die nächste internationale Konferenz findet vom 21. bis 25. Oktober 2019 in Tirana statt.

Die geschlossene Tagung verabschiedete eine Erklärung zu Ethik und Datenschutz in der künstlichen Intelligenz. Dieser Text stellt sechs Leitsätze auf, die eigentliche Grundwerte für die Wahrung der Menschenrechte bei der Entwicklung der künstlichen Intelligenz darstellen. Schliesslich nahm die Konferenz fünf Resolutionen zu folgenden Themen an: E-Learning-Plattformen, die Änderung der Regeln und Verfahren betreffend die internationale Konferenz, die Kursbestimmung für die Zukunft der internationalen Konferenz, die Zusammenarbeit zwischen den Datenschutzbehörden und den Verbraucherschutzbehörden und eine Bestandsaufnahme der internationalen Konferenzen.

Europäische Konferenz der Datenschutzbeauftragten

Die Konferenz bot die Gelegenheit für eine Gesamtschau über die Probleme bei der Inkraftsetzung der DSGVO, die den 28 Mitgliedstaaten der Europäischen Union eine starke und einheitliche Gesetzgebung bietet.

Diese 28. Auflage unter dem Motto «Datenschutz – besser gemeinsam» fand am 3. und 4. Mai 2018 in Tirana (Albanien) statt. Die Teilnehmer diskutierten auch über die Modernisierung des Übereinkommens 108 des Europarats, die namentlich die Zusammenarbeit zwischen den Parteien erleichtern soll, über die Eingliederung der europäischen Datenschutznormen in die übrigen Regelungssysteme oder auch über die Bearbeitung von Personendaten in der humanitären Arbeit. Die europäische Konferenz hat beschlossen, das Mandat der Arbeitsgruppe über die Zukunft der Konferenz, der auch der EDÖB angehört, zu verlängern und zu präzisieren. Die Arbeitsgruppe muss nun konkrete Vorschläge zur Modernisierung der Funktionsweise dieses Organs ausarbeiten, dem höchstwahrscheinlich eine nicht unbedeutende Rolle in der Zusammenarbeit zwischen den Datenschutzbehörden zukommen wird. Schliesslich prüfte die Konferenz den Entwurf für ein Dokument zur Förderung und Verstärkung der Zusammenarbeit und des Wissensaustausches zwischen den Mitgliedstaaten der EU und den Drittländern im Rahmen der DSGVO.

Arbeitsgruppe der OECD über die Informationssicherheit und den Schutz der Privatsphäre

Die von der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) eingesetzte Arbeitsgruppe über die Informationssicherheit und den Datenschutz widmete ihre Arbeiten verschiedenen Empfehlungen.

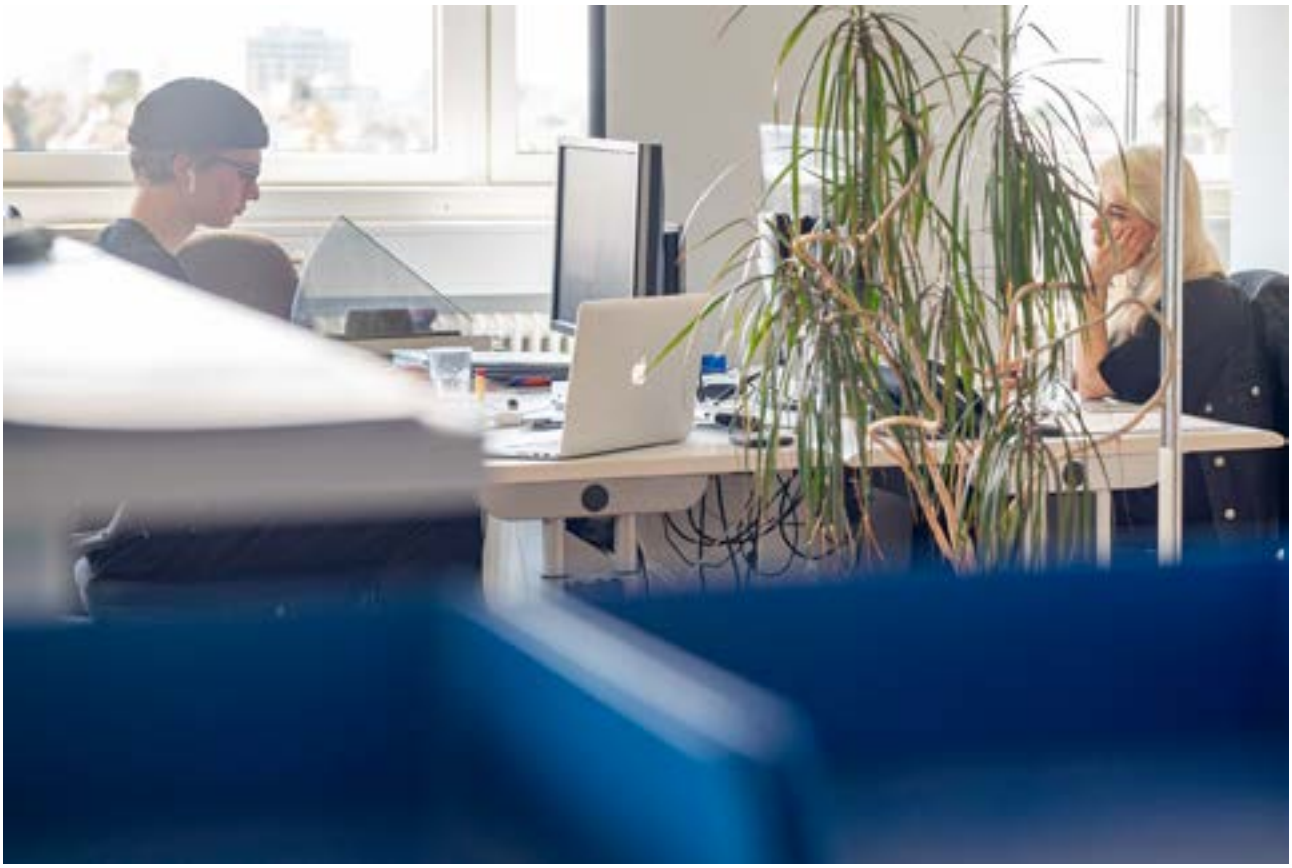
Die Gruppe befasste sich mit der überarbeiteten Fassung des Empfehlungsentwurfs der OECD zum Schutz kritischer Informationsinfrastrukturen (CII). Der Entwurf macht die Relevanz der Sicherheitsrichtlinien für die CII deutlich; er zeigt Ansätze für einzelstaatliche Massnahmen auf und schlägt Mittel zur Verbesserung der internationalen Zusammenarbeit für den Schutz der CII vor. Angesichts der Bedeutung des Internet als weltumspannende Infrastruktur betont sie die Notwendigkeit einer verstärkten internationalen Zusammenarbeit zur Bewältigung grenzüberschreitender Probleme. Die Delegierten berieten sich über Themen zur Verbesserung der Daten für die Ausarbeitung von Strategien im Bereich Sicherheit und Schutz der Privatsphäre, namentlich betreffend die Vergleichbarkeit der Meldeberichte im Falle von Datenschutzverletzungen. Des Weiteren beschäftigten sie sich mit der derzeit in Überarbeitung befindlichen Empfehlung aus dem Jahr 2012 zum Schutz der Kinder im Internet.

2013 verabschiedete die OECD die überarbeiteten Richtlinien für den Schutz der Privatsphäre und den grenzüberschreitenden Datenverkehr; damit wurde die ursprüngliche Fassung von 1980 aktualisiert. Diese überarbeiteten Richtlinien sehen eine Überprüfung ihrer Umsetzung und eine Berichterstattung nach fünf Jahren vor. Die Arbeitsgruppe hat daher bei ihrer Tagung am 13. und 14. November ein Prüfungsverfahren für diese Richtlinien bestimmt und wurde mit der Einsetzung einer Expertengruppe beauftragt, der auch der EDÖB angehören wird.

Französischsprachige Vereinigung der Datenschutzbehörden (AFAPDP)

Die AFAPDP organisierte unter anderem ein Podiumsgespräch über den Einfluss der sozialen Netzwerke auf Wahlprozesse, an dem Wahlexperten und Vertreter von politischen Parteien teilnahmen.

Die französischsprachige Vereinigung der Datenschutzbehörden (AFAPDP) traf am 18. und 19. Oktober 2018 in Paris. Der EDÖB ist seit ihrer Gründung im Jahr 2007 ausserordentliches Mitglied der Vereinigung. Bei dieser Gelegenheit verabschiedeten die Mitglieder eine Resolution über das Eigentum an den persönlichen Daten und wiesen damit auf die Tatsache hin, dass Personendaten Bestandteile des Menschen als Person sind. Es ist daher notwendig, im französischsprachigen Raum den Erlass von Gesetzgebungen zum Schutz der Personendaten und der Privatsphäre zu unterstützen, um die Wahrung der Demokratie und der Rechtsstaatlichkeit in unseren Gesellschaften zu garantieren. Diese Rechtsvorschriften müssen es den Einzelpersonen ermöglichen, die mit den persönlichen Daten verbundenen unveräusserlichen Rechte umfassend wahrzunehmen, indem ihnen eine weitreichende Kontrolle über ihre Daten gewährleistet wird. Schliesslich konnten die verschiedenen Behörden in einer weiteren Sitzung ihre Erfahrungen mit der DSGVO, fünf Monate nach deren Inkrafttreten, diskutieren.



Die DSGVO – in gewissen Fällen auch in der Schweiz anwendbar

Die neue EU-Datenschutz-Grundverordnung (DSGVO) ist am 25. Mai 2018 in der Europäischen Union in Kraft getreten. Unter gewissen Bedingungen gilt sie auch für Datenbearbeitungen durch Schweizer Unternehmen. Der EDÖB hat im Rahmen seiner Beratungs- und Sensibilisierungstätigkeit ein Merkblatt zu dem Thema herausgegeben und an zahlreichen Informationssitzungen teilgenommen.

Die am 27. April 2016 verabschiedete europäische Datenschutz-Grundverordnung (DSGVO) ist seit dem 25. Mai 2018 in allen Mitgliedstaaten der Europäischen Union direkt anwendbar. Ihr Geltungsbereich erstreckt sich indessen über das Gebiet der EU hinaus: soweit nämlich der für die Datenbearbeitung Verantwortliche (oder der Subunternehmer) Waren oder Dienstleistungen Personen in der Europäischen Union anbietet, oder wenn er das Verhalten dieser Personen beobachtet, um deren Präferenzen zu analysieren, hat er sich an die Vorgaben der DSGVO zu halten, selbst wenn er nicht in der Union niedergelassen ist. Aufgrund der neuen Bestimmungen erhalten Personen in der EU mehr Kontrolle über ihre Personendaten; die Unternehmen werden vermehrt in die Verantwortung genommen, während gleichzeitig ihre Meldepflichten abgebaut werden und die Rolle der Datenschutzbehörden gestärkt wird.

Eine der grössten Schwierigkeiten für eine Datenschutzbehörde eines Drittlandes wie der Schweiz liegt zunächst in der mangelnden Klarheit der Begriffe des «Anbietens von Waren und Dienstleistungen an Personen in der Union» oder der «Beobachtung des Verhaltens der betroffenen Personen». Es ist nicht unproblematisch, der Definition des Anwendungsbereichs eines nicht von uns verfassten Textes vorzugreifen und ihn zu interpretieren. Da die Schweiz von diesem neuen Rechtsakt jedoch unmittelbar betroffen ist, hat der EDÖB ein Merkblatt veröffentlicht, das insbesondere auf die extraterritoriale Anwendung des neuen europäischen Rechts Bezug nimmt. Daraus geht hervor, dass die Beantwortung der Frage nach der Geltung der DSGVO immer im Einzelfall beurteilt werden muss und namentlich von der Absicht des für die Bearbeitung Verantwortlichen abhängt, Waren oder Dienstleistungen Personen in der EU anzubieten, oder deren Verhalten zu beobachten.

Leitlinien zum Geltungsbereich der DSGVO

Der EDÖB hat sowohl bei der Bundesverwaltung als auch bei Privaten an zahlreichen Informationssitzungen zu diesem Thema mitgewirkt. Im Rahmen seiner Beratungstätigkeit beantwortete er ausserdem eine Vielzahl von mündlichen und schriftlichen Anfragen von Bürgerinnen und Bürgern sowie von Medienschaffenden.
Da die französischsprachigen europäischen Behörden der Nicht-Mitgliedstaaten der EU vor den gleichen Schwierigkeiten stehen wie die Schweiz, sind wir im Laufe des Jahres mehrmals zusammengekommen, um unsere Erfahrungen auszutauschen und offene Fragen zu diskutieren und die Antworten aufeinander abzustimmen.
Mehr als sechs Monate nach Inkrafttreten der DSGVO veröffentlichte der Europäische Datenschutzausschuss (EDSA), der als unabhängiges Organ für die einheitliche Anwendung der Datenschutzvorschriften in der Europäischen Union zuständig ist, seine Leitlinien zum Anwendungsbereich der DSGVO. Diese waren Gegenstand einer öffentlichen Konsultation, an der sich der EDÖB in Zusammenarbeit mit der monegassischen Behörde (CCIN) beteiligte, um gewisse Punkte zu klären, welche für die in der Unionslandschaft integrierten Drittländer wichtig sind.

Evaluation des Datenschutzniveaus

Die Europäische Kommission überprüft das Datenschutzniveau von Drittländern und hat der Schweiz letztmals im Jahre 2000 attestiert, dass ihr Datenschutzniveau angemessen ist. Unternehmen in der EU können deshalb Personendaten ohne weitere Massnahmen mit Firmen in der Schweiz austauschen. Zurzeit ist die Kommission daran, die Angemessenheit des Schweizer Datenschutzniveaus gestützt auf die in der DSGVO aufgelisteten Kriterien erneut zu evaluieren. Sie hat angekündigt, den Angemessenheitsentscheid im Mai 2020 in Berichtsform zu veröffentlichen (vgl. Ziff. IV)

Europarat – Die Schweiz sollte das angepasste Übereinkommen so bald wie möglich unterzeichnen

Das Übereinkommen 108 ist modernisiert und zur Unterzeichnung aufgelegt worden. 22 Staaten haben den Text bisher unterzeichnet. Die Schweiz, die bei der Ausarbeitung und Verabschiedung massgeblich mitwirkte, gehört noch nicht zu den Unterzeichnerstaaten.

Die Arbeiten zur Modernisierung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen 108) wurden am 18. Mai 2018 mit der Annahme eines Änderungsprotokolls im Ministerkomitee des Europarats abgeschlossen (CETS 223). Das modernisierte Übereinkommen (Übereinkommen 108+) wurde am 10. Oktober 2018 zur Unterzeichnung durch die Parteien aufgelegt und inzwischen von 22 Staaten paraphiert. Angesichts des noch nicht absehbaren Abschlusses der Totalrevision des DSG hat der Bundesrat mit der Unterzeichnung des Protokolls zugewartet.

Das Übereinkommen 108+ bekräftigt die grundlegenden Prinzipien des Datenschutzes, stärkt gewisse Grundsätze wie das Verhältnismässigkeitsprinzip, präzisiert die Bedingungen für die Rechtmässigkeit der Bearbeitung von Personendaten und führt neue Garantien und Rechte für die betroffenen Personen ein – beispielsweise das Recht, nicht einer automatisch gefällten Entscheidung unterworfen zu werden, das Recht auf Information über die der Bearbeitung zugrundeliegende Logik, das Widerspruchsrecht der Betroffenen sowie das Beschwerderecht bei der Datenschutzbehörde.

Es führt auch neue Pflichten für die Bearbeitungsverantwortlichen ein, etwa die Meldung von Datenverletzungen, die Mängelbehebung, eine Risikofolgenabschätzung, eine Ausgestaltung der Datenbearbeitung, welche die Risiken einer Verletzung der Grundrechte und -freiheiten verhindert bzw. minimiert, oder auch Informationspflichten (Transparenzgebot). Es regelt die internationalen Datenübermittlungen, präzisiert und erweitert die Kompetenzen und Befugnisse der Kontrollbehörden sowie ihre Pflichten im Bereich der Zusammenarbeit. Es schafft ausserdem einen Mechanismus, mit dem die Einhaltung der Bestimmungen überwacht und beurteilt werden kann.

Eine Modernisierung, die der globalen und digitalen Realität Rechnung trägt

Die Modernisierung wurde notwendig, um den seit 1981 erfolgten technologischen und rechtlichen Entwicklungen in einer globalisierten und digitalen Welt Rechnung zu tragen. Dank seiner offenen Ausgestaltung kommt dem international verbindlichen Übereinkommen eine universelle Bedeutung zu. Dies wurde bei den Modernisierungsarbeiten durch allgemein gehaltene und einfache Formulierungen ohne technologische Bezugnahmen berücksichtigt. In seiner heutigen Fassung umfasst das Übereinkommen 53 Staaten (47 Mitgliedstaaten des Europarats und 6 Drittstaaten: Kap Verde, Mauritius, Mexiko, Senegal, Tunesien und Uruguay). Drei weitere Staaten wurden zum Beitritt eingeladen, und elf Staaten haben einen Beobachterstatus im beratenden Ausschuss.

Brexit und Übermittlung personenbezogener Daten

Nach dem Referendum im Vereinigten Königreich über den Austritt aus der EU (Brexit) im Juni 2016 teilte die britische Regierung der Union ihre Entscheidung zum Austritt mit. Das Verfahren für den Austritt hätte am 29. März 2019 abgeschlossen werden sollen, wurde aber auf einen späteren Zeitpunkt verschoben.

Der EDÖB hat an zahlreichen Sitzungen mit Behörden des Bundes und des Vereinigten Königreichs teilgenommen, um sicherzustellen, dass der freie Verkehr personenbezogener Daten zwischen der Schweiz und Grossbritannien auch nach dem Austritt möglich bleibt. Das Vereinigte Königreich gilt als Land mit einem angemessenen Niveau, und der EDÖB sieht derzeit keine Veranlassung, dessen Status zu ändern.

Das Übereinkommen 108+ gilt als Referenz für ein angemessenes Datenschutzniveau

Das Änderungsprotokoll zum Übereinkommen 108 tritt in Kraft, sobald es von allen Parteien angenommen wurde, oder wenn 38 Parteien es binnen einer Frist von fünf Jahren angenommen haben. Bei der Verabschiedung des Textes forderte das Ministerkomitee sämtliche Parteien auf, sich mit allen Mitteln um eine rasche Inkraftsetzung zu bemühen. Die Ratifizierung des Übereinkommens 108+ ist ein wesentliches Kriterium für die Europäische Union, damit ein Entscheid, das Datenschutzniveau eines Drittstaates als angemessen anzuerkennen, weiterhin gilt. Dies ist insbesondere für Wirtschafts- und Finanzplätze von Drittstaaten wie der Schweiz unerlässlich, weil davon der freie Datenverkehr zwischen der Schweiz und der EU abhängig ist.

Nicht zuletzt auch mit Blick auf die voranschreitende Evaluation durch die Europäische Kommission (s. Ziff. III), liegt es im Interesse der Schweiz, das Änderungsprotokoll baldmöglichst zu unterzeichnen und nachfolgend zu ratifizieren. Dies setzt voraus, dass die in den eidgenössischen Räten hängige Revision des Bundesgesetzes über den Datenschutz in Einklang mit den Bestimmungen des Übereinkommens 108+ vorgenommen wird, wie das der Bundesrat in seiner Botschaft vorgeschlagen hat. Auch die Kantone müssen ihre Gesetzgebungen zeitgerecht anpassen.

Der Beratende Ausschuss zum Übereinkommen 108 (T-PD) hat den Entwurf für eine Empfehlung zum Datenschutz im Gesundheitsbereich angenommen. Diese Empfehlung, die das Ministerkomitee im Laufe dieses Jahres verabschieden sollte, wird die Empfehlung R (97) 5 über den Schutz medizinischer Daten ersetzen. Sie soll den seit 1997 eingetretenen technologischen Entwicklungen und dem Übereinkommen 108+ Rechnung tragen. Der T-PD hat zudem einen praktischen Leitfaden zum Datenschutz im Polizeisektor angenommen, der sich in erster Linie an die Polizeikräfte richtet und die Datenschutzprinzipien und -bestimmungen veranschaulicht. Der T-PD hat auch Leitlinien zum Schutz der Privatsphäre und zu den Medien herausgegeben, die gemeinsam mit dem Lenkungsausschuss für die Medien und die Informationsgesellschaft (CDMSI) ausgearbeitet wurden, sowie einen Leitfaden zu den Grundsätzen der Achtung der Privatsphäre und des Datenschutzes bei der Datenbearbeitung im Zusammenhang mit der ICANN (Internet Corporation for Assigned Names and Numbers) herausgegeben. Er ist ausserdem daran, Leitlinien betreffend den Datenschutz und die künstliche Intelligenz zu erarbeiten, sowie zu den im Übereinkommen 108+ vorgesehenen Überwachungs- und Beurteilungsmechanismen.

Öffentlichkeitsprinzip

2.1 Allgemein

Die Konsolidierung des mit der Einführung des Öffentlichkeitsprinzips angestrebten Paradigmenwechsels hin zu einer offenen und transparenten Verwaltung schreitet weiter voran: Die Umsetzung des Öffentlichkeitsgesetzes durch die Bundesbehörden ist insgesamt als positiv zu werten. Dies zeigt sich insbesondere auch daran, dass die Zahl der vollständig gewährten Zugänge mit der steigenden Gesamtzahl der Gesuche mithält und der Prozentsatz der kompletten Zugangsverweigerungen über die Jahre stetig abnimmt (s. nachfolgend Ziffer 2.2).

Erfreulich zu sehen ist auch, dass das Öffentlichkeitsgesetz einen positiven Einfluss auf die aktive Informationspolitik der Bundesbehörden hat: Ausgelöst durch Zugangsgesuche und Schlichtungsanträge veröffentlicht das ENSI nunmehr monatlich den Verlauf der Emissionsmesswerte der Schweizer Kernkraftwerke (sog. ANPA-EMI-Daten) und das BFE jährlich die Vollzugsresultate der CO_2 Emissionsvorschriften für Personenwagen. Zur Förderung der Transparenz wiederum publiziert armasuisse ein Register der Kompensationsgeschäfte («Offset-Register») und die Interne Revision VBS ihre Prüfberichte.

Dank der Überführung des erfolgreichen Pilotversuchs «Beschleunigung Schlichtungsverfahren» in den ordentlichen Betrieb konnten auch in diesem Berichtsjahr positive Ergebnisse hinsichtlich Bearbeitungsdauer und Einigungsquoten erzielt werden (s. nachfolgend Ziffer 2.2).

Als herausfordernd für alle Beteiligten erweisen sich Drei- oder gar Mehrparteienverfahren. Darunter fallen etwa Verfahren betreffend Berichte von Administrativ- oder Disziplinaruntersuchungen, Unterlagen mit möglichen Geschäftsgeheimnissen von Unternehmen oder mit Bezug zum Persönlichkeitsschutz von Privaten und Verwaltungsmitarbeitenden. Diese Schlichtungsverfahren zeichnen sich oft durch komplexe Abklärungen mit den betroffenen Dritten aus. Dazu trägt nicht zuletzt auch die Tendenz bei, dass die betroffenen Dritten bereits im Stadium des Zugangs- und Schlichtungsverfahrens vermehrt Rechtsanwälte beiziehen. Dies führt zu einer Verrechtlichung dieser – informellen – Verfahrensabschnitte und zu einer Verzögerung der Zugangsgewährung für die Gesuchstellenden. Diese Entwicklung steht in Widerspruch zur Intention des Gesetzgebers eines einfachen und raschen Zugangs- und Schlichtungsverfahrens. Für die Klärung von Rechtsfragen hat er das ordentliche Verwaltungsverfahren vorgesehen, d.h. den Erlass einer Verfügung durch die Behörde und anschliessend die Beschwerdemöglichkeit beim Bundesverwaltungsgericht.

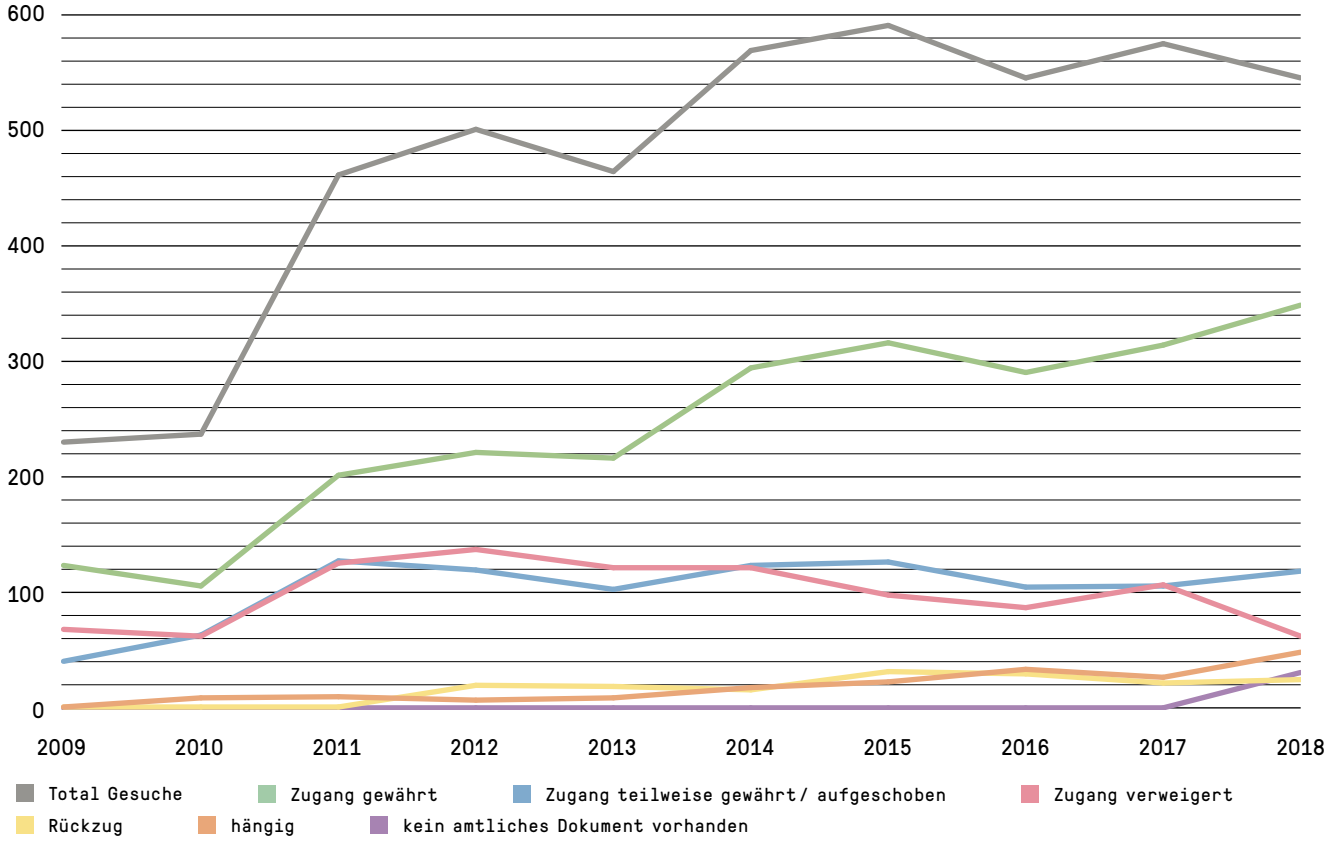
2.2 Zugangsgesuche – stetige Zunahme

Laut den uns für das Jahr 2018 gemeldeten Zahlen wurden bei den Bundesbehörden 636 Zugangsgesuche gestellt (gegenüber 581 für 2017). Dies entspricht einem Zuwachs von 9,5 Prozent. Unter Einbezug der Bundesanwaltschaft (8) und der Parlamentsdienste (3) beläuft sich die Zahl insgesamt auf 647.

Die Behörden gewährten in 352 Fällen einen vollständigen Zugang, was einem Anteil von 55 Prozent entspricht (gegenüber 317 oder ebenfalls 55 Prozent im Jahr 2017), während in 119 Fällen (19 Prozent) nur ein Teilzugang gewährt wurde (gegenüber 106 oder 18 Prozent im Jahr 2017). In 62 Fällen (zehn Prozent) wurde der Zugang vollständig verweigert (gegenüber 107 oder 18 Prozent im Jahr 2017). Des Weiteren teilten uns die Behörden mit, dass 24 Zugangsgesuche (vier Prozent) zurückgezogen wurden (gegenüber 26 bzw. lediglich vier Prozent im Jahr 2017), dass 48 Gesuche (acht Prozent) am Ende des Jahres 2018 noch hängig waren (gegenüber 21 oder vier Prozent im Jahr 2017), und dass in 31 Fällen (fünf Prozent) kein amtliches Dokument vorhanden war.

Departemente und Bundesämter

Aufgrund der von den Ämtern vorgelegten Zahlen stellt der Beauftragte fest, dass das BAG im Jahr 2018 am meisten Gesuche erhalten hat (42), gefolgt vom BAV (27) und von Swissmedic (24). Die Departemente mit den meisten eingegangenen Gesuchen sind das EDA (156) und das EDI (112). 16 Behörden meldeten dagegen, dass bei ihnen im Laufe des Jahres 2018 kein einziges Gesuch eingereicht worden sei. Im selben Zeitraum gingen beim EDÖB selber sieben Gesuche ein. Er gewährte in vier Fällen den vollständigen und in einem Fall einen teilweisen Zugang, ein Fall ist noch hängig und im letzten Fall war kein Dokument vorhanden.



2018 wurden bei 17 Zugangsgesuchen Gebühren erhoben, was 2.6 Prozent aller eingegangen Gesuche (gegenüber 1,9 Prozent im Jahr 2017) entspricht. Es ist anzumerken, dass nur acht Behörden Gebühren verlangt haben. Die Gesamtsumme der für den Zugang zu Dokumenten erhobenen Gebühren beläuft sich auf 13 358 Schweizer Franken. Dieser Betrag ist zwar höher als im Jahr 2017 (CHF 6160), liegt aber im Vergleich zu den Vorjahren weiterhin in der Norm (2016: CHF 22 700, 2015: CHF 13 663). Wie in den früheren Jahren bildete die Erhebung einer Gebühr die Ausnahme; in fast 98 Prozent der Fälle wurde darauf verzichtet. Während die Bundeskanzlei, das EJPD, das EDA und das EFD keinerlei Gebühren erhoben haben, stellten die übrigen vier Departemente den Gesuchstellern ihre Arbeitszeit bei einzelnen Fällen in Rechnung. Der grösste Teil der Gebühren entfiel auf das EDI (CHF 10 900 für acht Gesuche) und das UVEK (CHF 1300 für drei Gesuche).

Bezüglich der Verbuchung der für die Behandlung der Gesuche aufgewendeten Arbeitszeit weist der EDÖB erneut darauf hin, dass die Behörden nicht verpflichtet sind, sie zu registrieren, und dass es in der Bundesverwaltung keine Richtlinie für eine einheitliche Erfassung gibt. Die dem EDÖB gelieferten Angaben erfolgen auf freiwilliger Basis und geben die für die Behandlung der Gesuche aufgewendete Arbeitszeit nicht vollständig wieder. Gemäss diesen Angaben nahm die aufgewendete Arbeitszeit im Vergleich zum Vorjahr um 63 Prozent zu (2018: 4827 Stunden; 2017: 2968 Stunden). Diese Steigerung lässt sich auf eine im Vergleich zu den Vorjahren höhere Anzahl Zugangsgesuche zurückführen. Jedoch ging die für die Vorbereitung der Schlichtungssitzungen aufgewendete Arbeitszeit deutlich zurück (2018: 672 Stunden; 2017: 914 Stunden; 2016: 857 Stunden). Die für den Erlass einer Verfügung oder für ein Beschwerdeverfahren aufgewendete Arbeitszeit wurde in den meisten Fällen dem EDÖB nicht mitgeteilt.

Parlamentsdienste

Die Parlamentsdienste meldeten uns für 2018 drei Zugangsgesuche. In zwei Fällen wurde der Zugang vollständig verweigert, und im dritten Fall gab es keine amtlichen Dokumente.

Bundesanwaltschaft

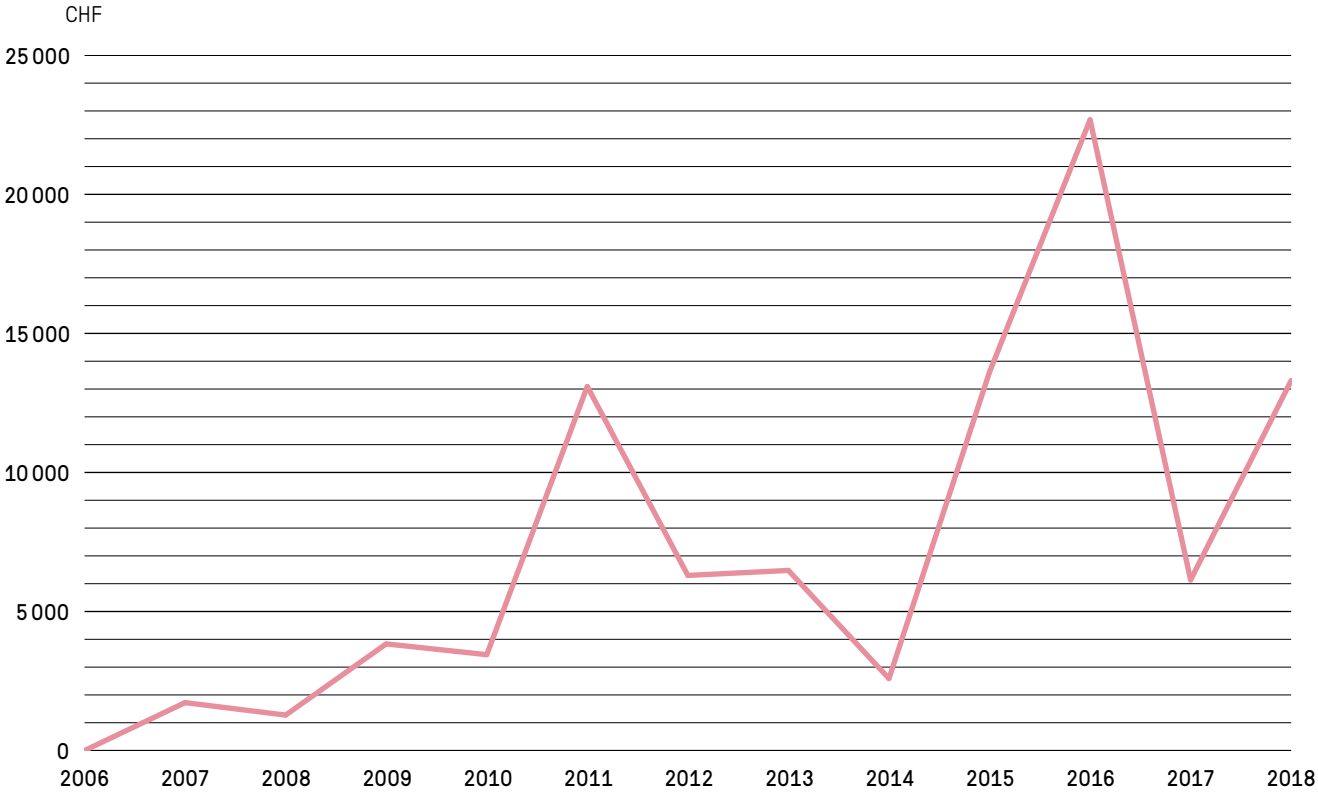
Laut Mitteilung der Bundesanwaltschaft gingen bei ihr acht Gesuche ein; der Zugang wurde in drei Fällen vollständig gewährt, in zwei Fällen vollständig verweigert. Von den verbleibenden Fällen sind zwei noch hängig, und in einem Fall waren keine amtlichen Dokumente vorhanden.

Schlichtungsanträge

Im Jahr 2018 wurden 76 Schlichtungsanträge beim Beauftragten eingereicht, drei weniger als 2017 (79), darunter nahezu gleich viele von Privatpersonen (26) wie von den Medienschaffenden (24).

Diese Zahlen lassen folgende Schlüsse und Bemerkungen zu: in 212 Fällen verweigerte die Bundesverwaltung den Zugang vollständig (62) oder teilweise (119), oder sie konnte den Zugang in Ermangelung der Dokumente nicht gewähren (31). Diese Angaben sind in Beziehung zu den 76 beim Beauftragten eingegangenen Schlichtungsanträgen zu setzen. 36 Prozent der teilweise oder vollständig verweigerten Zugangsgesuche waren Gegenstand eines Schlichtungsantrags (gegenüber 37 Prozent im Jahr 2017).

Insgesamt konnten im Berichtsjahr 64 Schlichtungsverfahren abgeschlossen werden. Davon stammen 61 Anträge aus dem Berichtsjahr selbst und drei aus 2017. In 26 Fällen konnte zwischen den Beteiligten eine Einigung erzielt werden. In 22 Fällen, in denen eine einvernehmliche Lösung nicht möglich war, erliessen wir Empfehlungen. Drei Schlichtungsanträge wurden zurückgezogen und in sechs Fällen waren die Voraussetzungen für die Anwendung des Öffentlichkeitsgesetzes nicht gegeben. In weiteren sechs Fällen wurde der Schlichtungsantrag nicht fristgerecht eingereicht.



2.3 Schlichtungsverfahren – hoher Anteil einvernehmlicher Lösungen

Wie im letzten Tätigkeitsbericht erwähnt, war im Jahr 2017 ein Pilotversuch durchgeführt worden, um die Schlichtungsverfahren zu beschleunigen. Die Gesuche wurden mehrheitlich in mündlichen Schlichtungsverfahren in Anwesenheit der betroffenen Personen und Behörden behandelt. Kam in der Verhandlung keine Einigung zustande, wurde den Parteien eine schriftliche Empfehlung mit einer summarischen Begründung zugestellt. Da die getroffenen Massnahmen die erwünschte Beschleunigung des Verfahrens brachten, wurde die neue Methode ab Januar 2018 in den ordentlichen Betrieb überführt. Die drei folgenden Kapitel veranschaulichen die Ergebnisse des Pilotversuchs von 2017 im Vergleich zu den Zahlen von 2018.

Dauer der Schlichtungsverfahren

In Tabelle 1 wurden die Schlichtungsverfahren aufgrund der für die Erledigung erforderlichen Zeit in drei Kategorien unterteilt: gesetzliche Frist von 30 Tagen eingehalten, Bearbeitungsdauer zwischen 31 und 99 Tagen, Bearbeitungsdauer länger als hundert Tage. Die mittlere Dauer der Behandlung der in den Jahren 2014 bis 2016, 2017 und 2018 gestellten Schlichtungsanträge wurde in den oben genannten Kategorien prozentmässig angegeben. Bei der Berechnung der Bearbeitungsdauer eines Schlichtungsverfahrens wird die Dauer einer allfälligen Sistierung nicht beachtet.

Wie bereits während des Pilotversuchs konnte auch im Berichtsjahr die Bearbeitungsdauer im Vergleich zu den Vorjahren verkürzt werden. Die gesetzliche Frist von dreissig Tagen wurde bei der Hälfte der Schlichtungsverfahren (32 von 64) eingehalten. In keinem Fall betrug die Bearbeitungsdauer mehr als hundert Tage.

Die Überschreitung der gesetzlichen Frist von dreissig Tagen war häufig der Abwesenheit der betroffenen Personen oder Behörden infolge Ferien, Krankheit oder Reisen, der grossen Zahl der am Verfahren beteiligten Drittpersonen oder der Komplexität der rechtlichen Fragestellung zuzuschreiben. Hinzuzufügen ist auch, dass die oben erwähnten Gründe oft einen erheblichen Mehraufwand verursachen und dass in diesem Fall der Beauftragte gemäss Artikel 12a der Verordnung über das Öffentlichkeitsprinzip er Verwaltung (VBGÖ; SR 152.31) die ordentliche Frist angemessen verlängern kann. Der Beauftragte stellt aber fest, dass die Bearbeitungsdauer innerhalb von 30 Tagen im Vergleich zu 2017 konstant bleibt.

Tabelle 1: Bearbeitungsdauer Schlichtungsverfahren

Bearbeitungsdauer in Tagen	Zeitraum 2014 – August 2016*	Pilotphase 2017	Pilotphase 2017
innert 30 Tagen	11 %	59 %	50 %
zwischen 31 und 99 Tagen	45 %	37 %	50 %
mehr als 100 Tage	44 %	4 %	0 %

*Quelle: Präsentation des Beauftragten, Veranstaltung zum 10. Jahrestag des BGÖ, 2. September 2016

Anteil einvernehmlicher Lösungen

Um die Auswirkungen der Überführung des Pilotversuchs in das ordentliche Verfahren abzuschätzen, wurden die drei oben definierten Kategorien bzw. Zeiträume analysiert. Der erste betrifft die Periode von 2013 bis 2016, der zweite das Jahr der Durchführung des Pilotversuchs (2017) und der dritte das Jahr der konkreten Umsetzung des Pilotversuchs (2018).

Tabelle 2: Verhältnis Empfehlungen und einvernehmliche Lösungen

2013 – 2016	40 %
2017	60 %
2018	55 %

Der Beauftragte stellt fest, dass die Steigerung des Anteils einvernehmlicher Lösungen im Vergleich zu den Empfehlungen konstant geblieben ist und dass somit die positiven Auswirkungen des Pilotversuchs von 2017 auch 2018 weiter andauerten. Die Durchführung der mehrheitlich mündlichen Schlichtungspraxis führte im Vergleich zu den Vorjahren zu einer signifikanten Zunahme der einvernehmlichen Lösungen.

Zur Information: Sämtliche Empfehlungen werden auf der Website des Beauftragten publiziert und sind dort jederzeit abrufbar.

Anzahl hängiger Fälle

Tabelle 3: Hängige Schlichtungsverfahren

Ende 2016	33
Ende 2017	3 (2 in Bearbeitung; 1 Sistierung)
Ende 2018	15 (davon 13 im Februar 2019 erledigt und 2 sistiert)

Am Ende des Pilotversuchs (2017) waren nur drei Verfahren hängig (gegenüber 33 im Jahr 2016). Ende 2018 waren noch 15 Fälle hängig, wobei zehn Schlichtungsanträge im Dezember gestellt worden waren. Es ist anzumerken, dass bereits im Februar 2019 dreizehn dieser Verfahren erledigt und zwei sistiert worden sind. Eine Sistierung des Schlichtungsverfahrens erfolgt, wenn eine Behörde insbesondere nach der Schlichtungssitzung ihre Stellungnahme erneut überprüfen möchte oder wenn sie betroffene Dritte anhören muss.

Obwohl die Anzahl hängiger Verfahren im Vergleich zum Vorjahr gestiegen ist, stellt der Beauftragte fest, dass es sich nicht um einen Leistungsabfall, sondern um einen statistischen Zufall handelt, da zahlreiche Schlichtungsanträge im Dezember eingereicht wurden. Der Rückgang der hängigen Fälle gegenüber den früheren Jahren ist demnach weiterhin offenkundig.

2.4 Ämterkonsultation und weitere Stellungnahmen

Totalrevision des Bundesgesetzes über das öffentliche Beschaffungswesen

Das Parlament hat eine umfassende Revision des Bundesgesetzes über das öffentliche Beschaffungswesen beraten. Der Vorschlag des Bundesrates, das Öffentlichkeitsprinzip im Beschaffungswesen vollständig aufzuheben, wurde verworfen. Der Beauftragte hat sich in der zuständigen Kommission und in den Medien dezidiert gegen dieses Vorhaben gewandt.

Ausschreibungen und Zuschläge des Bundes werden auf der Beschaffungsplattform simap.ch publiziert. Zu den Beschaffungsunterlagen besteht während des Vergabeverfahrens kein Einsichtsrecht. Die Unterlagen werden gemäss Öffentlichkeitsgesetz erst nach Abschluss des Verfahrens auf Gesuch hin einsehbar (s. auch 24. Tätigkeitsbericht 2016/17, Ziffer 2.3.2).

Das Parlament hat die Vorlage im Lauf des Jahres 2018 beraten und die geplante Sonderregelung abgelehnt. Damit bleiben die Beschaffungsunterlagen mit Ausnahme von wettbewerbsrelevanten Inhalten wie bis anhin dem Öffentlichkeitsgesetz unterstellt und damit grundsätzlich zugänglich. Unternehmen, Medien und Bevölkerung können somit weiterhin überprüfen, wie die Behörden bei der Beschaffung von Gütern und Dienstleistungen mit Steuergeldern umgehen. Zudem soll mit der Umsetzung der parlamentarischen Motion 14.3045 in der Beschaffungsverordnung eine Regelung eingeführt werden, die vorsieht, dass alle Beschaffungen mit einem Vertragsvolumen ab CHF 50 000 mindestens einmal jährlich publiziert werden. Insgesamt wird die Transparenz mit der Revision somit gestärkt.

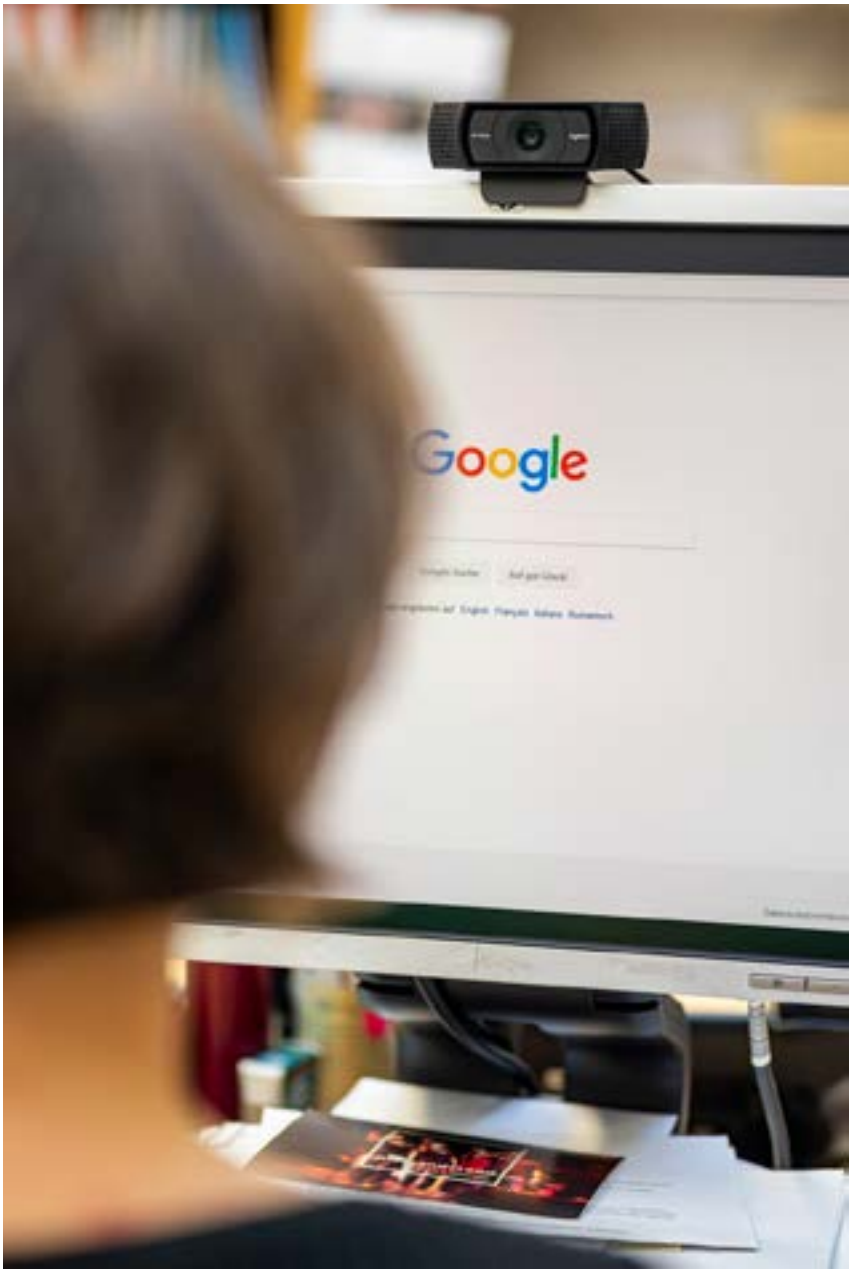
Die Vorlage befindet sich zurzeit im Stadium der parlamentarischen Differenzbereinigung, wovon die Transparenzbestimmungen jedoch nicht betroffen sind.

Ämterkonsultation zur Genehmigung von Tarifstrukturen in der Krankenversicherung

Das Bundesamt für Gesundheit wollte eine Ausnahme vom Zugangsrecht zu Dokumenten der zwei Ämterkonsultationsverfahren zu Tarifgenehmigungen einführen. Der Beauftragte hat sich erfolgreich dagegen ausgesprochen.

Der Bundestrat genehmigt regelmässig Tarifstrukturen im Bereich der stationären Spitalbehandlung. Im Berichtsjahr wurden dem Bundesrat vom Bundesamt für Gesundheit (BAG) zwei solche Genehmigungsanträge im Psychiatriebereich vorgelegt. Darin hat das BAG vorgeschlagen, dass sämtliche in die Ämterkonsultation geschickten Berechnungsgrundlagen der betroffenen Tarifstrukturen nach der Genehmigung durch den Bundesrat vom Zugangsrecht nach dem Öffentlichkeitsgesetz ausgeschlossen bleiben, um Geschäftsgeheimnisse der Akteure zu schützen. Das Bundesamt stützte seine Argumentation auf eine Bestimmung des Öffentlichkeitsgesetzes, wonach «amtliche Dokumente des Ämterkonsultationsverfahrens» ausnahmsweise auch nach dem Entscheid des Bundesrates nicht zugänglich bleiben.

Wir haben im Rahmen der Konsultationen jeweils beantragt, auf diese Regelung zu verzichten, da die in Frage stehenden Unterlagen vor Beginn des Ämterkonsultationsverfahrens erstellt bzw. dem BAG eingereicht wurden und somit aus diesem Grund schon gar keine «amtlichen Dokumente des Ämterkonsultationsverfahrens» darstellen. Die Voraussetzungen für einen endgültigen Ausschluss vom Öffentlichkeitsgesetz waren somit nicht erfüllt. Hinzu kommt, dass das Öffentlichkeitsgesetz bereits eine spezifische Bestimmung für den Schutz von Geschäftsgeheimnissen der Unternehmen kennt. Das BAG hat in der Folge auf die Sonderregelung verzichtet.



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 zwanzig 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 unsere Behörde auf das bereits bestehende Personal des EDÖB und teilweise auf Mittel der Bundeskanzlei zurückgreifen. 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 nie im vollen Umfang rekrutiert werden.

In seiner Botschaft zur Totalrevision des DSG hat der Bundesrat dem EDÖB die Schaffung zusätzlicher Mittel im Umfang von zehn Stellen in Aussicht gestellt (BBl 2017 7172). Aufgrund des schwer vorhersehbaren Abschlusses der parlamentarischen Arbeiten zur Totalrevision (vgl. Ziff. I) ist zurzeit nicht absehbar, ob und wann zusätzliche Stellen rekrutiert werden können. Nachdem mit dem neuen Bundesgesetz über die Umsetzung der Schengen Richtlinie (EU) 2016/680 ein Teilaspekt der Totalrevision vorweggenommen wurde und per 1. März 2019 in Kraft getreten ist, sieht sich unsere Behörden bezüglich der besonders sensiblen Bearbeitung von Personendaten im Polizeibereich mit zusätzlichen Aufgaben und Befugnissen betraut (vgl. Ziff. 1.2). Ob der Bundesrat dem EDÖB dafür die beantragten, zusätzlichen Mittel zusprechen wird, stand zur Zeit der Drucklegung dieses Berichts noch nicht fest.

Tabelle 4: Für DSG-Belange einsetzbare Stellen

2005	22
2010	23
2018	24
2019	24

Leistungen

Die Aufgaben des EDÖB als für die Bundesorgane und die Privatwirtschaft zuständige Datenschutzbehörde werden gemäss dem Neuen Führungsmodell Bund (NFB) den vier Leistungsgruppen Beratung, Aufsicht, Information und Gesetzgebung zugewiesen. Im Berichtsjahr vom 1.4.2018 bis 31.3.2019 wurden die beim EDÖB für den Datenschutz einsetzbaren Personalressourcen wie folgt auf diese Gruppen aufgeteilt:

Tabelle 5: Leistungen Datenschutz

Beratung Private	21,1%	
Beratung Bund	21,3%	
Zusammenarbeit mit Kantonen	2,1%	
Zusammenarbeit mit ausl. Behörden	9,8%	
Total Beratung		**54,3%**
Aufsicht	14,1%	
Zertifizierung	0,2%	
Register Datensammlung	0,7%	
Total Aufsicht		**15,0%**
Information	17,6%	
Ausbildung/ Referate	5,0%	
Total Information		**22,6%**
Gesetzgebung	8,1%	
Total Gesetzgebung		**8,1%**
Total Datenschutz		**100,0%**

Die Schweiz sieht sich nach der letzten Evaluation durch die EU damit konfrontiert, dass die Datenschutzaufsicht des Bundes die Personendatenbearbeitungen in den schengen-relevanten Datenbanken häufiger kontrollieren und dafür mit ausreichenden Ressourcen ausgestattet werden sollte (vgl. Ziff. 1.2, Schwerpunkt Schengen).

Beratung

Wie im Eingangskapitel «Aktuelle Herausforderungen und Schwerpunkte» dargelegt, sieht sich der EDÖB im Leistungsbereich der Beratung, aufgrund der Notwendigkeit immer umfangreichere und komplexere Projekte zu begleiten, mit einer weiter anwachsenden Nachfrage konfrontiert. In der Berichtsperiode hat sich der Anstieg der für die Beratung aufgewendeten personellen Mittel weiter auf 53,9 Prozent erhöht. Gemäss dem Kontrollplan des EDÖB für das Jahr 2019 ist die beratende Begleitung von elf grossen Projekten im Gang.

Tabelle 6: Beratungen in umfangreicheren Projekten für 2018

Verkehr	2
Finanzen	1
Gesundheit und Arbeit	3
Sicherheit	2
Telekom/Internet of Things (IOT)	3

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. In der Berichtsperiode haben die drei Teams des Direktionsbereichs Datenschutz insgesamt monatlich rund achtzig Anfragen und Anzeigen von Bürgerinnen und Bürgern mit einem Standardschreiben beantwortet, das die Betroffenen auf den zivilprozessualen Weg verweist. Zudem musste unsere Behörde 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 bei Staat und Wirtschaft auszugehen.

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 wie bereits mehrfach ausgeführt der Dichte der Kontrollen enge Grenzen. Im Jahr 2018 wurden für die Aufsichtstätigkeit rund zwölf Prozent der Personalressourcen aufgewendet, was deutlich unter dem langjährigen Mittelwert von rund zwanzig Prozent lag. In der aktuellen Berichtsperiode konnte der Anteil wieder auf rund 15 Prozent angehoben werden, was dem Stand der Periode von 2016/17 entspricht. Gemäss Kontrollplan für das Jahr 2019 werden mit diesen Mitteln noch zwölf umfassendere Kontrollen bestritten. Im Vergleich zu der Anzahl von rund 12 000 grossen und mittleren Unternehmen in der Schweiz erweist sich die aktuelle Kontrolldichte nach wie vor als tief. Für den Beauftragten bleibt es 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 Grundlagen zulässig ist. Diese zieht demzufolge eine Vielzahl von neuen Bearbeitungsvorschriften im Bundesrecht nach sich, zu denen der EDÖB in diversen Konsultationsverfahren Stellung beziehen muss. Der diesbezügliche Aufwand ist in den letzten zehn Jahren deutlich angestiegen, was ebenfalls zum weiteren Absinken der Kontrolldichte beigetragen hat. Zwar ist es uns in der Berichtsperiode gelungen, diesen Trend zu stoppen. Angesichts unserer knappen Mittel, sahen wir uns jedoch gezwungen, unsere Stellungnahmen im Rahmen von Konsultation zunehmend summarisch zu begründen sowie unsere Leistungen in anderen Aufgabenbereichen zu kürzen.

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 momentan nicht absehbar ist, wann der in der Botschaft in Aussicht gestellte Stellenausbau erfolgen kann, muss unsere Behörde die neuen Arbeitsinstrumente mit den bestehenden Personalressourcen so pragmatisch wie möglich umsetzen.

Dienststellenbesuche und Anhörungen durch die Geschäftsprüfungskommissionen

Anlässlich des Dienststellenbesuchs der Subkommission EJPD/BK der Geschäftsprüfungskommission des Ständerats im 2018 präsentierten wir die Ergebnisse des Pilotversuchs «Beschleunigung Schlichtungsverfahren». Am 11. April 2019 schliesslich konnten wir die Subkommission bei einer Anhörung nunmehr über die erfolgreiche Überführung des Pilotversuchs in den ordentlichen Betrieb informieren.

Bemessungskriterien

Ob dem EDÖB mit Blick auf die im Berichtsjahr hinzugekommenen Aufgaben und die Resultate der letzten Schengen-Evaluation 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, welches 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:

Leistungen und Ressourcen im Bereich Öffentlichkeitsgesetz

Die Einheit BGÖ, wo unverändert 3,6 Stellen eingesetzt werden, ist nach Durchführung eines einjährigen Versuchs zu einem beschleunigten und summarischen Verfahren übergegangen, das sich dadurch charakterisiert, dass in der Regel mündliche Schlichtungsverhandlungen durchgeführt werden. Dieses Verfahren bewährt sich weiterhin, indem der Anteil der einvernehmlich abgeschlossenen Schlichtungen nach wie vor hoch und die Überschreitung der gesetzlichen Fristen im Wesentlichen auf prozessual und inhaltlich komplexe Fälle beschränkt werden konnten. Bei einem Anstieg der Zahl der Schlichtungsanträge, mehreren Anträgen innert eines kurzen Zeitraums und personellen Vakanzen kommt es indes rasch zu Arbeitsrückständen.

Tabelle 7: Wirkungsziele EDÖB

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 unter Anwendung digitalisierungstauglicher Arbeitsinstrumente.
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.

3.2 Kommunikation

Rege Sensibilisierungstätigkeit und grosse mediale Aufmerksamkeit

Der EDÖB strebt eine wahrnehmbare Sensibilisierung für die Themen des Datenschutzes und des Öffentlichkeitsprinzips an. Die Formen des Dialoges mit der Bevölkerung sollen weiter verstärkt werden. Zentrales Element der Kommunikation bleibt die Website – sie wird täglich von rund 2000 Personen besucht.

Das gesteigerte Interesse der Öffentlichkeit am Wirken des EDÖB hat sich im Berichtsjahr bestätigt. Die mediale Aufmerksamkeit manifestierte sich in zahlreichen Stellungnahmen des Beauftragten wie auch seines Stellvertreters und des Mediendienstes. In den vom EDÖB beobachteten Medien erschienen rund 3000 Beiträge und Artikel, die sich vorwiegend mit Datenschutzfragen befassten, aber auch das Öffentlichkeitsprinzip in der Verwaltung thematisierten. Insgesamt haben wir über 400 Medienanfragen bearbeitet. Bürger/innen und Unternehmen nutzten Mail, den Postweg oder die telefonische Hotline, um ihre Anliegen und Fragen bei unseren Fachleuten anzubringen – insgesamt verzeichneten wir über diese Kanäle gegen 3500 Eingänge. Diese Zahl ist als Richtgrösse zu betrachten, da wir im Berichtsjahr das Geschäftsverwaltungssystem abgelöst haben.

Auch nahm der Beauftragte bei rund vierzig Veranstaltungen als Referent oder Podiumsteilnehmer teil. Unter den Veranstaltern befanden sich Verbände und Vereine, Bildungsinstitutionen, Behörden oder Unternehmen sowie Organisationen im Umfeld der Digitalisierung. Im Chat des SRF-Themenabends Dataland vom 21. November 2018 hat er ebenfalls mitgewirkt. Weiter nahm der EDÖB am zweiten Schweizer Digitaltag teil und veröffentlichte im Vorfeld ein Video, das die Wirtschaft aufforderte, im Rahmen ihrer digitalen Projekte in datenschutzfreundliche Technologien zu investieren.

Datenschutzbehörden von Bund und Kantonen traten am Internationalen Datenschutztag gemeinsam auf

Der Internationale Datenschutztag wird auf Initiative des Europarates seit 2007 jedes Jahr am 28. Januar durchgeführt. Er hat zum Ziel, das Bewusstsein der Bürgerinnen und Bürger für den Schutz der Privatsphäre und das Recht auf informationelle Selbstbestimmung zu stärken und eine nachhaltige Verhaltensänderung im Umgang mit neuen Technologien zu bewirken.

Der EDÖB und die kantonalen Datenschutzbehörden informierten an einer Medienorientierung in Bern gemeinsam über die datenschutzrechtlichen Aspekte im Kontext der Wahlen sowie die Datenschutzrisiken einer systematischen Verwendung der AHV-Nummer. Ausserdem sensibilisierten wir die Öffentlichkeit für die bevorstehende Inkraftsetzung des Schengen-Datenschutzgesetzes und die nötig werdende Verstärkung der Datenschutzaufsicht von Bund und Kantonen über die Polizei.

Diverse Leitfäden und Empfehlungen publiziert

Im Berichtsjahr erstellte der Beauftragte diverse umfassendere Publikationen und machte diese zugänglich.

- So haben wir einen Leitfaden zur EU-Datenschutzgrundverordnung (DSGVO) aufgeschaltet, bevor diese am 25. Mai 2018 in Kraft getreten war. Erste Guidelines zur DSGVO seitens EU-Behörden wurden Ende 2018 ebenfalls publiziert und vom EDÖB auf Twitter geteilt.
- Damit Kinder und Jugendliche für den sicheren Umgang mit den neuen Medien sensibilisiert werden, haben wir – mit Unterstützung des Bundesamts für Sozialversicherungen BSV – per Anfang August 2018 unser Lehrmittel vollständig erneuert. Es richtet sich an Lehrpersonen für den Unterricht mit 13- bis 19-jährigen Schüler/innen und ist in den drei Landessprachen auf unserer Website verfügbar.
- Im Dezember 2018 hat der EDÖB gemeinsam mit den kantonalen Datenschutzbehörden (Privatim) einen Leitfaden zu Wahlen und Abstimmungen in den Sprachen Deutsch, Französisch, Italienisch und Englisch veröffentlicht.
- Im Januar 2019 haben wir erläuternde Informationen zum Schengen-Datenschutzgesetz aufgeschaltet, bevor dieses am 1. März 2019 in Kraft trat.
- Auf der Website des EDÖB publizierten wir 18 Empfehlungen betreffend das Öffentlichkeitsprinzip. Im Bereich Datenschutz waren es deren zwei. Weiter haben wir diverse Merkblätter und Leitfäden aktualisiert wie bspw. jene zu Dashcams oder der Datenübermittlung ins Ausland.

Mit der bei uns verlinkten interaktiven Plattform Think Data konnten wir ein breiteres Publikum für den Datenschutz bzw. mehr Transparenz sensibilisieren. Anhand von konkreten Szenarien werden hier datenschutzrechtliche Empfehlungen abgegeben. Think Data ist ein Projekt einer interdisziplinären Arbeitsgruppe (Thinkservices), an dem der EDÖB mitgewirkt hat und es heute noch unterstützt.

Die Publikation des jährlichen Tätigkeitsberichts erfolgt erstmals auch vollumfänglich in den Sprachen Italienisch und Englisch. Zudem haben wir die Lesefreundlichkeit auf den Ebenen Layout und Text verbessert. Um einen Schritt Richtung digitales Publishing zu gehen, wurde der Bericht erstmals auch als e-Paper herausgegeben.

Website nach wie vor wichtigster Kanal unserer Kommunikation

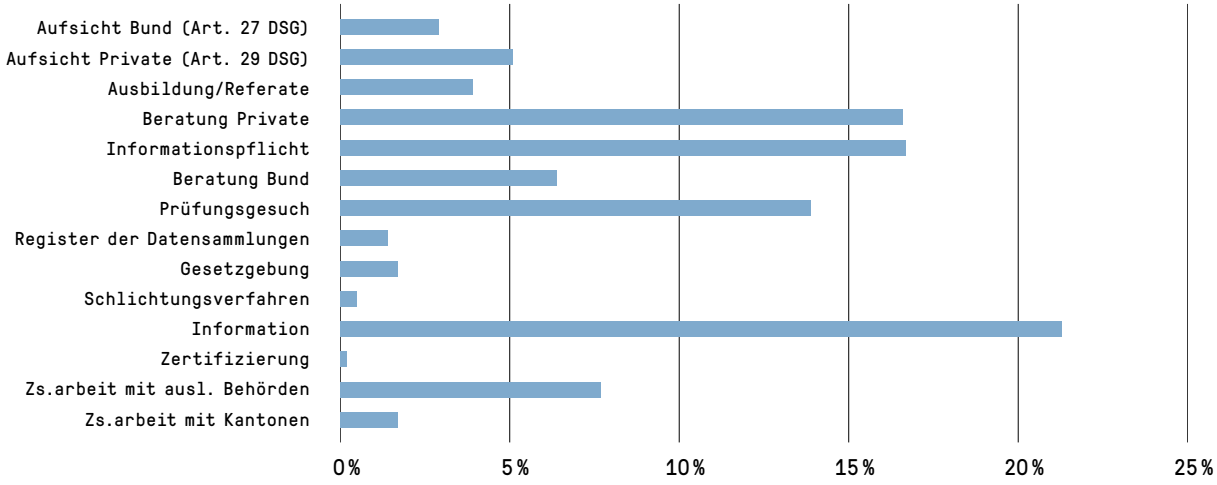
Die Webseite ist der zentrale Kommunikationskanal des EDÖB. Wir zählen jährlich 480 000 Besucher/innen oder rund 2000 an einem Arbeitstag. Zwei von fünf Besuchern kommen aus dem Ausland – mehrheitlich aus europäischen Staaten, aber auch aus Übersee oder Asien. Die Inhalte sind in der Regel in den drei Sprachen Deutsch, Französisch und Italienisch abrufbar – Inhalte, die für ausländische Nutzerinnen und Nutzer relevant sind, auch in Englisch. Es ist vorgesehen, den Webauftritt schrittweise zu optimieren: Er soll einfacher und visueller aufbereitet werden und den Nutzern vermehrt Dialogformate anbieten.

Unter @derBeauftragte kommunizieren wir zudem via den Microblog Twitter. Ziel ist es, unseren Followern den raschen Zugang zu relevanten Informationen zu erleichtern und Teil der am Datenschutz interessierten Community zu sein. Auf die Nutzung anderer Social Media Plattformen wurde aufgrund unserer knappen Ressourcen, teilweise aber auch aus anderen Gründen verzichtet.

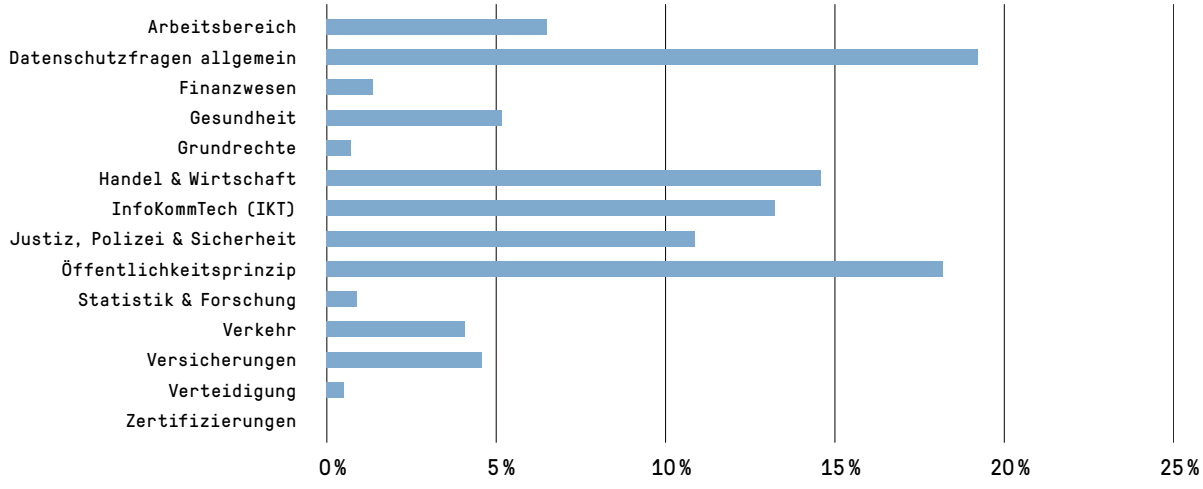
3.3 Statistiken

Statistiken über die Tätigkeiten des EDÖB vom 1. April 2018 bis 31. März 2019 (Datenschutz)

Aufwand nach Aufgabengebiet

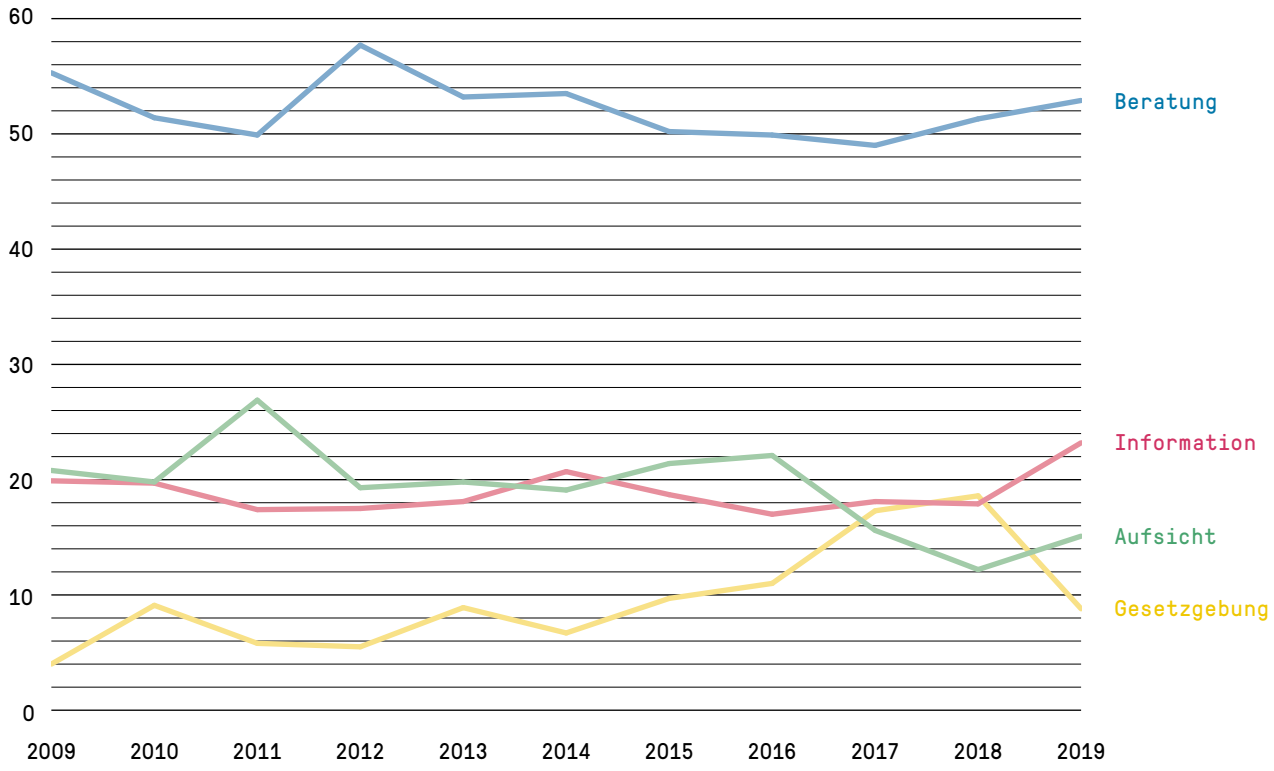


Aufwand nach Sachgebiet



Mehrjahresvergleich Aufwand

(Angaben in Prozent)



Statistiken über eingereichte Zugangsgesuche nach Öffentlichkeitsgesetz vom 1. Januar 2018 bis am 31. Dezember 2018

	Betroffener Fachbereich	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt/aufgeschoben	Zugangsgesuch zurückgezogen	Zugangsgesuch hängig	kein amtliches Dokument vorhanden
Bundeskanzlei BK	BK	**18**	9	4	4	0	0	1
	EDÖB	**7**	4	0	1	0	1	1
	Total	**25**	**13**	**4**	**5**	**0**	**1**	**2**
Eidg. Departement für Auswärtige Angelegenheiten EDA	EDA	**156**	107	2	28	6	8	5
	Total	**156**	**107**	**2**	**28**	**6**	**8**	**5**
Eidg. Departement des Inneren EDI	GS EDI	**0**	0	0	0	0	0	0
	EBG	**2**	0	1	1	0	0	0
	BAK	**7**	2	1	3	1	0	0
	BAR	**6**	6	0	0	0	0	0
	METEO CH	**0**	0	0	0	0	0	0
	NB	**0**	0	0	0	0	0	0
	BAG	**42**	15	4	11	2	10	0
	BFS	**5**	1	3	1	0	0	0
	BSV	**11**	7	0	1	1	1	1
	BLV	**15**	8	1	4	0	1	1
	SNM	**0**	0	0	0	0	0	0
	SWISS MEDIC	**24**	9	2	3	2	8	0
	SUVA	**0**	0	0	0	0	0	0
	Total	**112**	**48**	**12**	**24**	**6**	**20**	**2**
Eidg. Finanz-departement EFD	GS	**23**	12	7	2	0	0	2
	ISB	**3**	1	0	2	0	0	0
	EFV	**0**	0	0	0	0	0	0
	EPA	**1**	1	0	0	0	0	0
	ESTV	**7**	3	2	0	0	1	1
	EZV	**6**	3	1	0	1	1	0
	BBL	**6**	5	0	0	0	1	0
	BIT	**0**	0	0	0	0	0	0
	EFK	**19**	5	7	3	0	0	4
	SIF	**0**	0	0	0	0	0	0
	PUBLICA	**0**	0	0	0	0	0	0
	ZAS	**3**	2	0	1	0	0	0
	Total	**68**	**32**	**17**	**8**	**1**	**3**	**7**

	Betroffener Fachbereich	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt/aufgeschoben	Zugangsgesuch zurückgezogen	Zugangsgesuch hängig	kein amtliches Dokument vorhanden
Eidg.Justiz- und Polizeidepartement EJPD	GS EJPD	**5**	3	0	0	0	0	2
	BJ	**3**	3	0	0	0	0	0
	FEDPOL	**4**	3	1	0	0	0	0
	METAS	**2**	2	0	0	0	0	0
	SEM	**13**	7	1	2	0	1	2
	Dienst ÜPF	**1**	1	0	0	0	0	0
	SIR	**1**	1	0	0	0	0	0
	IGE	**0**	0	0	0	0	0	0
	ESBK	**1**	1	0	0	0	0	0
	ESchK	**2**	1	1	0	0	0	0
	RAB	**0**	0	0	0	0	0	0
	ISC	**1**	1	0	0	0	0	0
	NKVF	**0**	0	0	0	0	0	0
	Total	**33**	**23**	**3**	**2**	**0**	**1**	**4**
Eidg.Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK	GS	**5**	4	1	0	0	0	0
	BAV	**27**	10	0	15	2	0	0
	BAZL	**6**	2	0	3	0	0	1
	BFE	**12**	11	1	0	0	0	0
	ASTRA	**6**	5	0	0	0	1	0
	BAKOM	**10**	4	0	3	0	0	3
	BAFU	**10**	3	0	1	0	3	3
	ARE	**3**	1	1	0	0	0	1
	ComCom	**1**	0	0	1	0	0	0
	ENSI	**20**	10	1	2	6	1	0
	PostCom	**3**	3	0	0	0	0	0
	UBI	**2**	2	0	0	0	0	0
	Total	**105**	**55**	**4**	**25**	**8**	**5**	**8**

Statistiken über eingereichte Zugangsgesuche nach Öffentlichkeitsgesetz vom 1. Januar 2018 bis am 31. Dezember 2018

	Betroffener Fachbereich	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt/aufgeschoben	Zugangsgesuch zurückgezogen	Zugangsgesuch hängig	kein amtliches Dokument vorhanden
Eidg. Departement für Verteidigung, Bevölkerungsschutz und Sport VBS	GS VBS	**6**	5	0	1	0	0	0
	Verteidig./ Armee	**14**	6	0	4	1	3	0
	NDB	**9**	2	2	2	1	2	0
	armasuisse	**6**	4	0	0	0	2	0
	BASPO	**4**	3	0	0	0	1	0
	BABS	**2**	2	0	0	0	0	0
	swisstopo	**0**	0	0	0	0	0	0
	OA	**0**	0	0	0	0	0	0
	Total	**41**	**22**	**2**	**7**	**2**	**8**	**0**
Eidg. Departement für Wirtschaft, Bildung und Forschung WBF	GS	**6**	3	2	1	0	0	0
	SECO	**12**	4	3	4	0	0	1
	SBFI	**11**	8	3	0	0	0	0
	BLW	**17**	4	3	6	1	1	2
	BWL	**2**	1	0	1	0	0	0
	BWO	**0**	0	0	0	0	0	0
	PUE	**6**	5	0	1	0	0	0
	WEKO	**20**	12	4	4	0	0	0
	ZIVI	**2**	2	0	0	0	0	0
	BFK	**1**	1	0	0	0	0	0
	SNF	**1**	0	1	0	0	0	0
	EHB	**2**	2	0	0	0	0	0
	ETH Rat	**16**	10	2	3	0	1	0
	Innosuisse	**0**	0	0	0	0	0	0
	Total	**96**	**52**	**18**	**20**	**1**	**2**	**3**
Bundesanwaltschaft BA	BA	**8**	3	2	0	0	2	1
	Total	**8**	**3**	**2**	**0**	**0**	**2**	**1**
Parlamentsdienste PD	PD	**3**	0	2	0	0	0	1
	Total	**3**	**0**	**2**	**0**	**0**	**0**	**1**

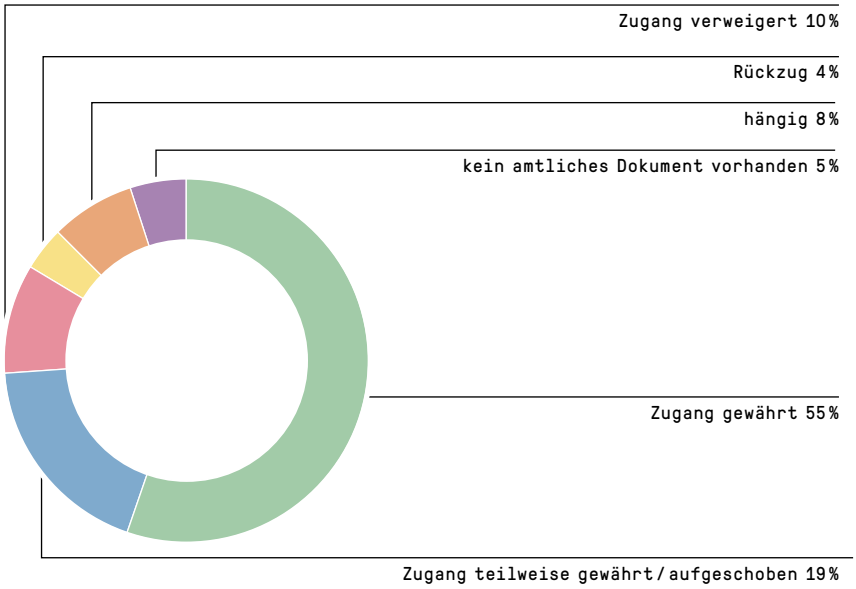
Übersicht der Zugangsgesuche der Departemente und der Bundeskanzlei

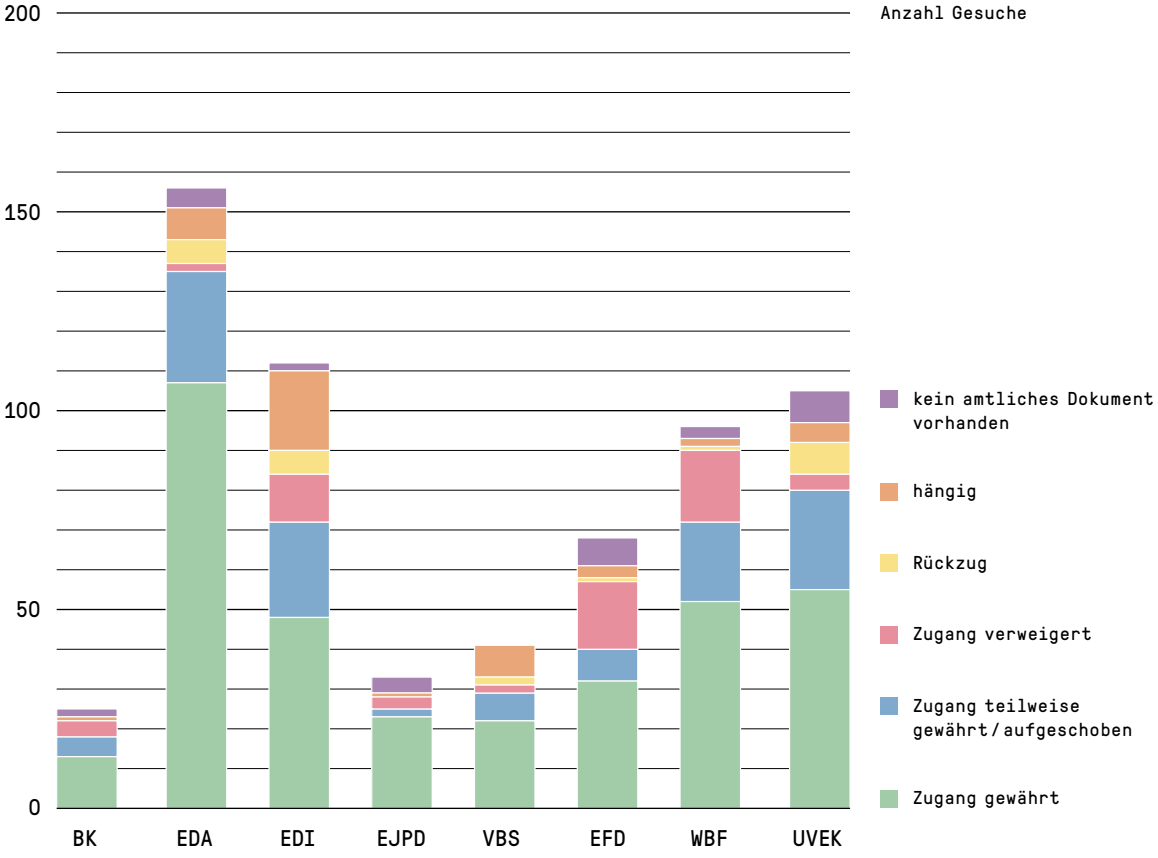
Departement	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt/aufgeschoben	Zugangsgesuch zurückgezogen	Zugangsgesuch hängig	kein amtliches Dokument vorhanden
BK	25	13	4	5	0	1	2
EDA	156	107	2	28	6	8	5
EDI	112	48	12	24	6	20	2
EFD	68	32	17	8	1	3	7
EJPD	33	23	3	2	0	1	4
UVEK	105	55	4	25	8	5	8
VBS	41	22	2	7	2	8	0
WBF	96	52	18	20	1	2	3
Total 2018 (%)	636 (100)	352 (55)	62 (10)	119 (19)	24 (4)	48 (7)	31 (5)
Total 2017 (%)	581 (99)	317 (55)	107 (18)	106 (18)	26 (4)	21 (4)	–
Total 2016 (%)	551 (99)	293 (53)	87 (16)	105 (19)	33 (6)	29 (5)	–
Total 2015 (%)	597 (100)	319 (53)	98 (16)	127 (21)	31 (5)	22 (4)	–
Total 2014 (%)	575 (100)	297 (52)	122 (21)	124 (22)	15 (3)	17 (3)	–
Total 2013 (%)	469 (100)	218 (46)	122 (26)	103 (22)	18 (4)	8 (2)	–
Total 2012 (%)	506 (100)	223 (44)	138 (27)	120 (24)	19 (4)	6 (1)	–
Total 2011 (%)	466 (100)	203 (44)	126 (27)	128 (27)	0 (0)	9 (2)	–
Total 2010 (%)	239 (100)	106 (44)	62 (26)	63 (26)	0 (0)	8 (3)	–
Total 2009 (%)	232 (100)	124 (53)	68 (29)	40 (17)	0 (0)	–	–

Anzahl Schlichtungsgesuche nach Kategorien der Antragssteller

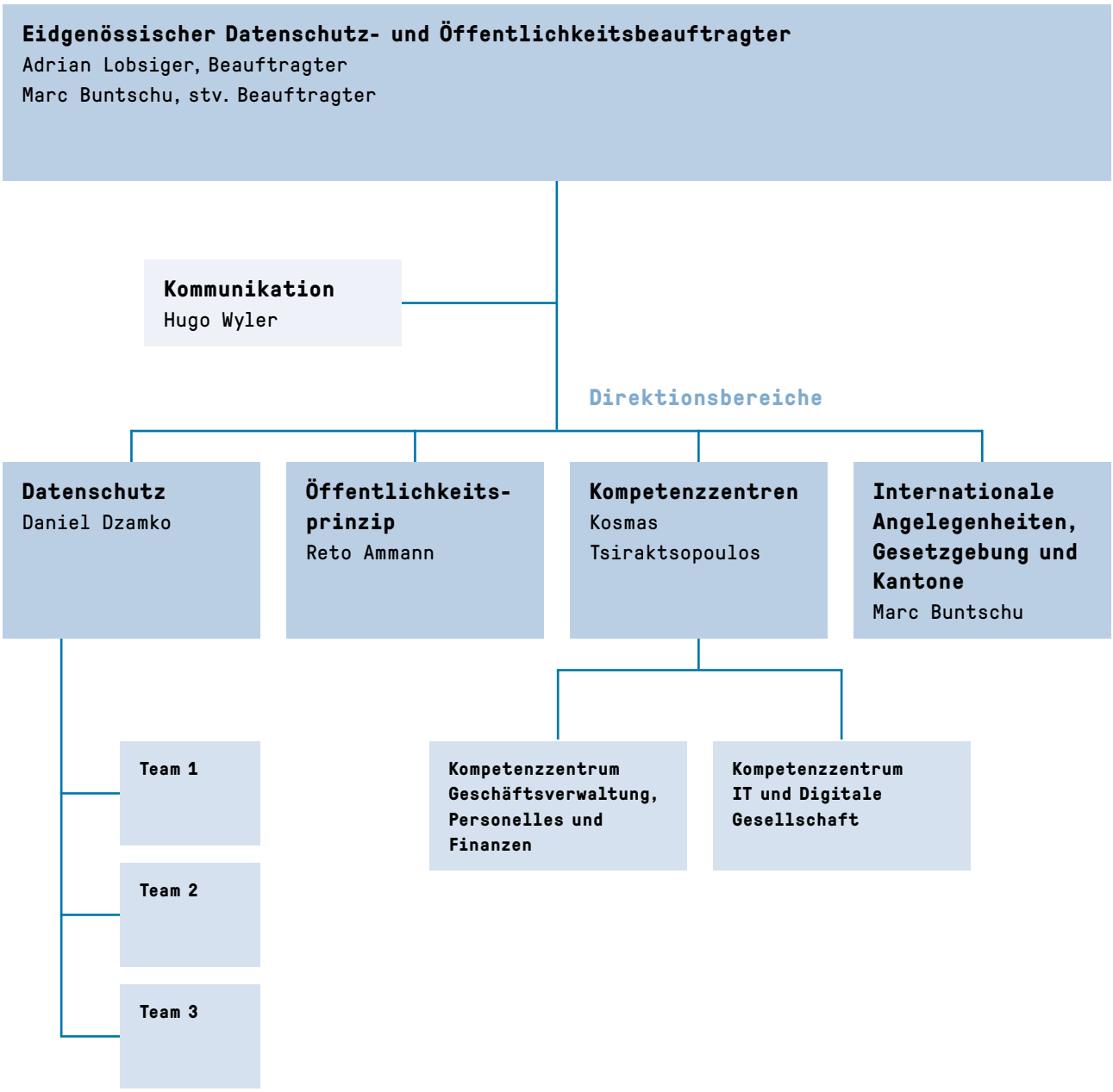
Kategorie Antragsteller	2018
Medien	24
Privatpersonen (bzw. keine genaue Zuordnung möglich)	26
Interessenvertreter (Verbände, Organisationen, Vereine usw.)	9
Rechtsanwälte	4
Unternehmen	13
Total	**76**

Zugangsgesuche der gesamten Bundesverwaltung





3.4 Organisation EDÖB (Stand 31. März 2019)



Abkürzungsverzeichnis

ADR Alternative Dispute Resolution body (unabhängigen Stellen für die alternative Streitbeilegung im Rahmen des Privacy Shield)

AFAPDP Französischsprachige Vereinigung der Datenschutzbehörden

AHVN13 13-stellige AHV-Nummer

AIA Automatischer Informationsaustausch über Finanzkonten

ALBA Austausch länderbezogener Berichte multinationaler Konzerne

BGEID Bundesgesetz über staatlich anerkannte elektronische Identifizierungsdienste (E-ID-Gesetz)

BGÖ Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsgesetz)

BPI Bundesgesetz über die polizeilichen Informationssysteme des Bundes

CNIL Commission Nationale de l'Informatique et des Libertés (Datenschutzbehörde Frankreich)

DoC U.S. Department of Commerce (US-Handelsministerium)

DSG Bundesgesetz über den Datenschutz (Datenschutzgesetz)

DSGVO Datenschutzgrundverordnung der EU

EDSA Europäischer Datenschutzausschuss (Engl. EDPB, European Data Protection Board)

EDPS Europäischer Datenschutzbeauftragter (European Data Protection Supervisor)

ENSI Eidgenössisches Nuklearsicherheitsinspektorat

Eurodac EU-Biometrische Datenbank im Asylwesen

ICO Information Commissioner's Office (Datenschutzbehörde des Vereinigten Königreichs)

IRM Independent Recourse Mechanism (unabhängiger Streitbeilegungsmechanismus im Rahmen des Privacy Shield)

NDB Nachrichtendienst des Bundes

NDG Bundesgesetz über den Nachrichtendienst (Nachrichtendienstgesetz)

OECD Organisation für wirtschaftliche Zusammenarbeit und Entwicklung

PCLOB Privacy and Civil Liberties Oversight Board (Stelle zur Überwachung des Schutzes der Privatsphäre und der bürgerlichen Freiheiten)

PMT Bundesgesetz über polizeiliche Massnahmen zur Bekämpfung von Terrorismus

Privatim Konferenz der Schweizer Datenschutz-Beauftragten (kantonale Datenschutzbehörden)

RIPOL Automatisiertes Fahndungssystem der Polizei

SDSG Bundesgesetz über den Datenschutz im Rahmen der Anwendung des Schengen-Besitzstands in Strafsachen (Schengen-Datenschutzgesetz)

SIF Staatssekretariat für internationale Finanzfragen

SIS Schengener Informationssystem

SIS II Schengener Informationssystem der zweiten Generation

SPK Staatspolitische Kommission (für DSG-Beratung zuständig)

StAhiG Steueramtshilfegesetz

VBGÖ Verordnung zum BGÖ

VIS Visa-Informationssystem

Abbildungsverzeichnis

Tabellen

Tabelle 1: Bearbeitungsdauer Schlichtungsverfahren ..... S. 64

Tabelle 2: Verhältnis Empfehlungen und einvernehmliche Lösungen ..... S. 65

Tabelle 3: Hängige Schlichtungsverfahren ..... S. 65

Tabelle 4: Für DSG-Belange einsetzbare Stellen ..... S. 70

Tabelle 5: Leistungen Datenschutz ..... S. 70

Tabelle 6: Beratungen in umfangreicheren Projekten für 2018 ..... S. 71

Tabelle 7: Wirkungsziele EDÖB ..... S. 73

Bilder (Aufnahmeorte)

ps architektur, perroneschneider GmbH, 4051 Basel ..... Umschlag

Terres des Hommes Schweiz, 4018 Basel ..... S. 15, 62, 67

Die Medienmacher AG, 4132 Muttenz ..... S. 21, 30, 34, 48, 53

restudio AG, 4053 Basel ..... S. 27, 55

Duplex Design GmbH, 4053 Basel ..... S. 43

Impressum

Dieser Bericht ist in vier Sprachen vorhanden und über das Internet (www.derbeauftragte.ch) aufrufbar.
Vetrieb: BBL, Verkauf Bundespublikationen, CH-3003 Bern
www.bundespublikationen.admin.ch
Art.-Nr. 410.026.d

Layout: Duplex Design GmbH, Basel
Fotografie: Maya Valentin
Schriften: Pressura, Documenta
Druck: Ast & Fischer AG, Wabern
Papier: PlanoArt®, holzfrei hochweiss

MIX
Papier aus verantwortungsvollen Quellen
FSC® C004050

Kennzahlen

Aufwand Datenschutz

8,1 % Gesetzgebung

22,6 % Information

15 % Aufsicht

54,3 % Beratung

Zugangsgesuche (BGÖ) Öffentlichkeitsprinzip

55 % gewährt

19 % teilweise gewährt / aufgeschoben

10 % verweigert

4 % Rückzug

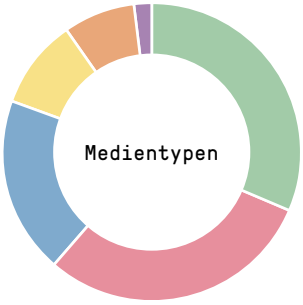
8 % hängig

5 % kein amtliches Dokument vorhanden

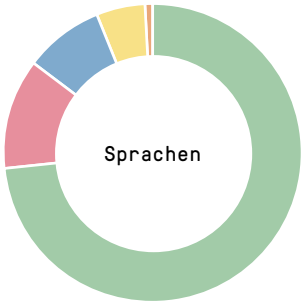
Mediale Resonanz des Beauftragten im Online

526 untersuchte Beiträge

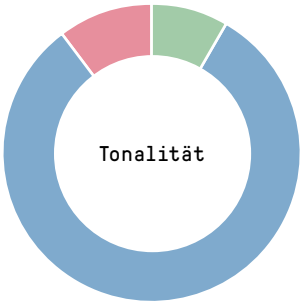
4925 Engagement*



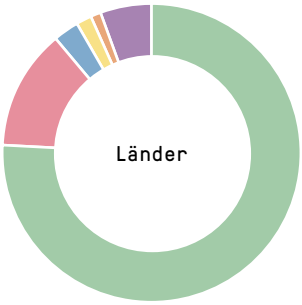
Onlinenews	31 %
Tageszeitung	30 %
Twitter	19 %
Blogs	10 %
TV/Radio	8 %
Andere	2 %



Deutsch	74 %
Französisch	12 %
Italienisch	8 %
Englisch	5 %
Andere	1 %



Positiv	9 %
Negativ	10 %
Neutral	81 %



Schweiz	76 %
Deutschland	13 %
USA	3 %
Ungarn	2 %
Frankreich	1 %
Andere	5 %

*Anzahl aller Interaktionen der untersuchten Beiträge (Likes, Retweets, etc.)

Anliegen des Datenschutzes

Faire Information
Unternehmen und Bundesorgane informieren transparent über ihre Datenbearbeitung: verständlich und vollständig.

Wahlmöglichkeit
Betroffene geben ihre Einwilligung informiert und erhalten eine echte Wahlfreiheit.

Risikoanalyse
Bereits im Projekt werden die möglichen Datenschutzrisiken identifiziert und deren Auswirkungen mit Massnahmen minimiert.

Datenrichtigkeit
Die Bearbeitung erfolgt mit zutreffenden Daten.

Verhältnismässigkeit
Kein Datensammeln auf Vorrat, sondern nur so weit wie nötig zur Erreichung des Zwecks.
Die Datenbearbeitung wird umfangmässig und zeitlich limitiert.

Zweckgebundenheit
Die Daten werden nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist.

Datensicherheit
Die Datenbearbeiter stellen technisch und organisatorisch sicher, dass die Personendaten hinreichend geschützt sind.

Dokumentation
Alle Datenbearbeitungen werden durch den Datenbearbeiter dokumentiert und klassifiziert.

Eigenverantwortung
Private und Bundesorgane nehmen ihre Pflicht zur Beachtung der Datenschutzgesetzgebung eigenverantwortlich wahr.