27. Tätigkeitsbericht 2019/20

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Tätigkeitsbericht 2019/2020
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 2019
und 31. März 2020 ab.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra


We'll
show
you
the
way

Vorwort

Am Ende dieser Berichtsperiode dominieren nicht digitale, sondern natürliche Viren die Schlagzeilen. Das Coronavirus dringt in das lebende Gewebe der Menschen ein und thematisiert so unsere Verletzlichkeit als biologische Wesen, die eine natürliche Furcht vor dem Unsichtbaren empfinden.

Unsere digitalisierte Gesellschaft bietet eine Fülle von Diensten an, die unsere Furcht vor der unsichtbaren Welt der Viren und Keime lindern. Gegen Computerviren vertrauen wir auf digitale Brandmauern, und gegen Kontamination mit Keimen leistet das digitale Homeoffice in diesen Tagen wertvolle Dienste. Und Apps, die durch Analyse von Mobilitätsdaten komfortablere Reiseverhältnisse mit einem Minimum an Enge schaffen, helfen mit, unsere Gesundheit im präventiven Sinn zu schützen.

Trotz des offensichtlichen Nutzens digitaler Technologien, trotz der berechtigten Betonung von Gemeinsinn, Disziplin und Krisensolidarität und ungeachtet unserer natürlichen Furcht vor dem unsichtbaren Virus, sollten wir indessen auch jetzt mit unserem selbstbestimmten Denken nicht aussetzen. Gilt es doch gerade während Pandemien und Wirtschaftskrisen wachsam zu verhindern, dass Verschwörungstheorien, Aberglaube oder kaltes Machtstreben Oberhand gewinnen und uns in die Fänge einer digitalen Vormundschaft schubsen.

Wann die Normalität zurückkehren wird, ist im Zeitpunkt der Drucklegung des Berichts nicht absehbar. Wir hoffen alle, dass es bald und mit möglichst wenigen Opfern geschehen kann. Mit dieser Hoffnung verbinde ich auch die Erwartung, dass wir «am Tag danach» auch unsere informationelle Selbstbestimmung unbeschadet wiederfinden werden und dass insbesondere auch das anonyme Bargeld diese Krise überleben wird, obwohl zuweilen Keime an ihm kleben.

Adrian Lobsiger
Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter

Bern, den 31. März 2020

Öffentlichkeitsprinzip

Der EDÖB

Aktuelle Herausforderungen
I Digitalisierung

Die Corona-Krise und die von ihr ausgelöste Verlagerung von Arbeit und Konsum zu Homeoffice und Homeshopping führt vor Augen, wie prägend die IKT und das Internet für die Alltagsgestaltung der Schweizer Bevölkerung geworden sind.

Technologie und Wirtschaft

Das technische und wirtschaftliche Potenzial für Eingriffe in die Privatsphäre und Selbstbestimmungsrechte der Bevölkerung bleibt hoch.

Mit Besorgnis nahm der Beauftragte während der Berichtsperiode zur Kenntnis, dass immer mehr Private dazu übergegangen sind, biometrische Daten in grossen Mengen automatisiert zu bearbeiten. Sei es, indem private Unternehmen solche Daten im direkten Kontakt mit ihren Kunden beschaffen, wenn sich Letztere z.B. über ihre Stimme identifizieren (s. Kap. 1.4). Oder sei es, dass Private riesige Mengen biometrische Daten aus dem Internet beschaffen, indem sie z.B. soziale Netzwerke nach Gesichtsbildern abfischen und die kopierten Bilder mit Gesichtserkennungssoftware weiterbearbeiten sowie mit weiteren Personendaten anreichern (s. Kap. 1.1).

Während die Sicherheitsbehörden autoritärer Staaten direkt oder über die Betreiber von Telekomdiensten und Plattformen nach Belieben auf Personendaten zugreifen, sind den Polizeibehörden westlicher Demokratien Schranken gesetzt, die jedoch recht unterschiedlich ausgestaltet sein können: Während beispielsweise in den USA gewisse Sicherheitsbehörden bereits zahlungspflichtige Gesichtserkennungsdienste Privater nutzen, müssten die Polizeibehörden in der Schweiz automatisierte Gesichtserkennungsprogramme auf gesetzliche Grundlagen abstützen können, welche die Gesetzgeber von Bund und Kantonen zurzeit nicht zur Verfügung stellen.

Die ansteigende Bereitschaft des Auslandes, die verbesserten digitalen Möglichkeiten zur Überwachung der Bevölkerung auszuschöpfen, hat denn auch mit Blick auf die europäische Polizeizusammenarbeit im Rahmen des Prümer Übereinkommens bereits zu Forderungen nach einem Austausch von Bilddaten geführt (s. Kap. 1.9). Der Beauftragte rechnet damit, dass auch die Polizeiorgane von Bund und Kantonen über kurz oder lang von der Politik fordern werden, Gesetze zur breiten polizeilichen Anwendung von Gesichtserkennungstechnologie zu schaffen.

Solche wären aus Sicht des Beauftragten problematisch. Sie drohten die heutige Regel, wonach sich die Menschen im öffentlichen Raum frei und anonym bewegen, zu einer Ausnahme verkommen zu lassen, auch wenn beteuert würde, die automatisierten Abgleiche und Auswertungen von Gesichtsdaten auf besonders schwere Delikte zu beschränkten.

Die Erfahrung zeigt, dass kriminalrechtliche Deliktschwellen nach und nach gesenkt und mit sachfremden Zielen der Sicherheits-, Fremden- und Verwaltungspolizei verwässert werden, wenn entsprechende Gesetzgebungen erst einmal geschaffen sind.

Weiteren Anlass zu Besorgnis geben die auch in dieser Berichtsperiode in erschreckend hoher Anzahl beklagten Verluste von Gesundheitsdaten, Personalkarteien, Kreditanträgen oder Fotodaten, Chat- und Mailkommunikation. Mit jedem unberechtigten Abfluss von Personendaten und der Verbreitung von gestohlenen Daten steigt das Meer ungeschützt zugänglicher Personendaten im Internet an und nimmt die Privatsphäre schaden. Betreiber grosser Clouds, die namentlich auch astronomische Mengen von privaten Bilddaten halten, tragen diesbezüglich eine grosse Verantwortung, die Sicherheit dieser Daten mit angemessenen technischen und organisatorischen Mitteln sicher zu stellen.

Gesellschaft und Datenpolitik

Im Zuge der globalen Bekämpfung des Coronavirus haben Regierungen schwer betroffener Regionen in Asien, wo das Virus ausgebrochen ist, ihre nach westlichen Massstäben teilweise bereits sehr einschneidenden Mittel zur digitalen Überwachung der Bevölkerung weiter ausgebaut, um die weitere Verbreitung des Erregers zu verhindern. Aufgrund des Übergreifens des Virus auf die Schweiz musste auch der Bundesrat gesundheitspolizeiliche Massnahmen anordnen. Nachdem er am 16. März 2020 gestützt auf Art. 7 des Epidemiengesetzes die ausserordentliche Lage ausgerufen hatte, konnte der Bundesrat Massnahmen anordnen, die in diesem Gesetz nicht näher umschrieben sind.

Das Gesetz verlangt einzig, dass die Massnahmen zur Bekämpfung der Seuche «notwendig» sein müssen. In seinen laufend aktualisierten, öffentlichen Stellungnahmen zur Pandemie wies der EDÖB stets darauf hin, dass sich insbesondere der Einsatz digitaler Methoden zur Erhebung und Analyse von Mobilitäts- und Proximity-Daten mit Blick auf den Zweck der Verhinderung von Ansteckungen als verhältnismässig erweisen müsse, was heisst, dass die eingesetzten Methoden epidemiologisch begründet und geeignet sein müssen, im jeweils aktuellen Stadium der Pandemie eine die Eingriffe in die Persönlichkeit der Betroffenen rechtfertigende Wirkung zur Eindämmung der Seuche zu entfalten.

Am 24. März 2020 bestellte der Beauftragte eine EDÖB-interne Task Force Corona, die ab diesem Tag diverse private und staatliche Projekte zur digitalen Bekämpfung der Seuche prüfte. Er informiert über seine Webseite laufend über die Arbeiten der Task Force und deren Ergebnisse (www.edoeb.admin.ch).

Der Beauftragte erwartet, dass das tragische Kollektivereignis des Coronavirus keine bleibenden Beeinträchtigungen der informationellen Selbstbestimmung und Privatsphäre der Schweizer Bevölkerung zur Folge haben wird. In seiner Stellungnahme hat er mit Blick auf die mit der Bekämpfung des Virus verbundenen Personendatenbearbeitungen vorsorglich darauf hingewiesen, dass die entsprechenden Daten nach Abklingen der Pandemie zu löschen oder anonymisieren sind.

Gesetzgebung

Die gesetzgeberischen Arbeiten zur Totalrevision des Datenschutzgesetzes (DSG) sind weit fortgeschritten. Nachdem die Vorlage von beiden Räten durchberaten wurde, steht die Bereinigung der Differenzen am Ende der Berichtsperiode noch an, zumal es auch aufgrund der Pandemie zu Verzögerungen gekommen ist. Der Beauftragte hofft, dass die Differenzen – trotz Coronavirus – bald bereinigt werden und die Schlussabstimmung in der Sommersession stattfinden kann.

«Die Bewältigung der Pandemie darf keine bleibenden Beeinträchtigungen des freien und selbstbestimmten Lebens zur Folge haben.»

II Beratungs- und Kontrolltätigkeit

Damit der EDÖB als Aufsichtsbehörde sicherstellen kann, dass Personendaten nicht mit der technisch machbaren, sondern der 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 aufsichtsrechtliche Begleitung einer Vielzahl von Big Data Projekten von Bundesbehörden und privaten Unternehmen fortgesetzt.

Nicht zuletzt um die eigenen Ressourcen wirksam einsetzen zu können, 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. Der Anteil unserer Gesamtaufwendungen für die beratende Begleitung von privatwirtschaftlichen Projekten ist im Berichtsjahr denn auch etwas zurückgegangen.

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). In der Endphase des Wahlkampfes hat der EDÖB die politischen Parteien mit einer Aktualisierung des Leitfadens der Datenschutzbehörden und einer medial stark beachteten Checkliste zur Nachbesserung ihres Webangebots angehalten.

Ein weiterer Schwerpunkt lag bei der Beratung der Verkehrsbranche bezüglich der Ausgestaltung von Ticketing Apps (s. Kap. 1.8). Die Bearbeitung von Mobilitätsdaten erweist sich als besonders heikel, weil diese leicht zu Persönlichkeitsprofilen führt, die sich nur mit grossem Aufwand pseudonymisieren oder gar anonymisieren lassen (s. Kap. 1.1). Vor diesem Hintergrund ist es zu begrüssen, dass der Ständerat erkannt hat, dass der mit der Revision des DSG wegfallende besondere Schutz vor profilbildenden Bearbeitungen beibehalten und unter der neuen Begrifflichkeit des «Profilings» verankert werden soll. Es ist zu hoffen, dass sich die beiden Kammern dahingehend verständigen können, dass das Schutzniveau des heutigen DSG zumindest beibehalten werden kann (s. Schwerpunkt I).

Nachdem die Aufwendungen für die Kontrollaufgaben in der Periode 2015/16 deutlich absanken, konnten diese in der letzten sowie der aktuellen Periode wieder 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 (s. Kap. 3.1).

Da der betriebliche Datenschutz bei der aufsichtsrechtlichen Begleitung digitaler Grossprojekte eine wichtige Brücke zum behördlichen Datenschutz schlagen kann, haben der Beauftragte und sein Stellvertreter ihre regelmässigen persönlichen Fachgespräche mit den Vereinigungen der Datenschutzberater der privaten Unternehmen der deutschen und französischen Schweiz auch in dieser Berichtsperiode fortgesetzt. Diese Gespräche werden gut besucht und haben sich für alle Beteiligten von grossem praktischen Nutzen erwiesen.

«Der betriebliche Datenschutz schlägt bei der aufsichtsrechtlichen Begleitung digitaler Grossprojekte eine wichtige Brücke zum behördlichen Datenschutz.»

III Nationale und internationale Kooperation

Nationale Kooperation

Der EDÖB hat seine Zusammenarbeit mit den kantonalen Datenschutzstellen weiter intensiviert. Als Beispiele sind hier zu nennen: Fachgespräche mit den kantonalen Datenschutzbeauftragten im Hinblick auf die Einführung des elektronischen Patientendossiers (s. Kap. 1.5), die gemeinsame Kommunikation der Datenschutzbehörden von Bund und Kantonen am internationalen Datenschutztag über die Gefahren für die Privatsphäre im privaten und öffentlichen Verkehr (s. Kap. 3.2), Teilnahme an den verschiedenen Präsidiums- und Plenarsitzungen der Konferenz der schweizerischen Datenschutzbeauftragten (Privatim) und Sitzungen der französischsprachigen Datenschutzbeauftragten. Dabei konnten Positionen zu laufenden Vernehmlassungsverfahren und Erfahrungen in den jeweiligen Beratungs- und Aufsichtskompetenzen ausgetauscht werden.

Unterzeichnung der Konvention 108+

Die Schweiz unterzeichnete nach einem Entscheid des Bundesrates die Konvention 108+ am 21. November 2019 in Strassburg formell. Die entsprechende Botschaft zur Genehmigung des Protokolls wurde vom Bundesrat am 6. Dezember 2019 zuhanden des Parlaments verabschiedet. Mit einem Beitritt zur modernisierten Konvention will die Schweiz ein hohes Datenschutzniveau für die Privatsphäre gewährleisten und den grenzüberschreitenden Datenverkehr im öffentlichen Sektor sowie in der Privatwirtschaft erleichtern. Der Beitritt ist ein wichtiges Element mit Blick auf die vor dem Abschluss stehende Evaluation durch die Europäische Kommission (s. unten).

Neues Europäisches Datenschutzrecht

Die Datenschutzgrundverordnung der EU (DSGVO) ist seit Mai 2018 in Kraft. Der EDÖB verfolgt intensiv die Anwendung in den verschiedenen europäischen Ländern und führt das erstmals im Herbst 2017 veröffentlichte Merkblatt laufend nach. Es ist uns weiterhin ein Anliegen, die betroffenen Schweizer Unternehmen mit Rat und Tat zu unterstützen.

«Arbeit und Konsum verlagern sich zu Homeoffice und Homeshopping.»

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. Der Evaluierungsprozess der EU auf der Basis der DSGVO begann offiziell im März 2019. Während des Berichtsjahres unterstützte der EDÖB die vom Bundesamt für Justiz geleitete Arbeitsgruppe mit seinem Knowhow (s. Kap. 1.9). Der entsprechende Bericht der Kommission wir für Ende Mai 2020 erwartet.

Nach dem Referendum im Vereinigten Königreich über den Austritt aus der EU (Brexit) vom Juni 2016 erfolgte dessen Austritt am 1. Februar 2020. Unsere Behörde hat an zahlreichen Sitzungen mit Behörden des Bundes und des Vereinigten Königreichs teilgenommen, um sicherzustellen, dass der freie Verkehr von Personendaten zwischen der Schweiz und Grossbritannien auch nach dem Brexit möglich bleibt. Das Vereinigte Königreich gilt als Land mit einem angemessenen Datenschutzniveau, und der EDÖB sieht derzeit keine Veranlassung, dessen Status zu ändern. Die EU wird bis Ende Jahr 2020 prüfen, ob dem Vereinigten Königreich eine datenschutzrechtliche Angemessenheit attestiert wird. Der EDÖB beobachtet diese Entwicklungen weiterhin aktiv (s. Kap. 1.9).

Swiss-US Privacy Shield

Im Herbst 2019 haben wir im Rahmen einer vom Seco angeführten Delegation die zweite aufsichtsbehördliche Überprüfung für das Swiss-US Privacy Shield durchgeführt. Die Überprüfung zeigte nach wie vor Schwachstellen auf, die Funktionsweise des Privacy Shields konnte jedoch weiter verbessert werden (s. Kap. 1.9).

Der mit Spannung erwartete Entscheid über die derzeit vor dem Gerichtshof der Europäischen Union (EuGH) hängige Rechtssache betreffend die Übermittlung von Daten von der EU in die USA (Schrems II), bei der gegebenenfalls auch das EU-US Privacy Shield Rahmenabkommen beurteilt wird, steht noch aus. Eine unmittelbare Wirkung auf die Schweiz wird das Urteil nicht haben. Der EDÖB wird nach dessen Ausfällung die mögliche Relevanz auf das Swiss-US Privacy Shield Rahmenabkommen analysieren.

«Unternehmen in der EU können Personendaten ohne weitere Massnahmen mit Firmen in der Schweiz austauschen.»

Datenschutz

1.1 Digitalisierung und Grundrechte

Wahlen und Abstimmungen: Wahl-Features von Facebook

Facebook hat anlässlich der Eidgenössischen Wahlen 2019 Features eingesetzt, um die Stimmberechtigten auf ihrer sozialen Plattform anzusprechen. Das Unternehmen hat dem EDÖB die Einhaltung der datenschutzrechtlichen Anforderungen gemäss dem Leitfaden zu Wahlen und Abstimmungen bestätigt.

Nachdem der Beauftragte durch Medienberichte Kenntnis davon erhalten hatte, dass Facebook im Hinblick auf die Eidgenössischen Wahlen 2019 auf ihrer sozialen Plattform möglicherweise Wahl-Features wie den «Voter-Button» einsetzen werde, hat er die vom Unternehmen vorgängig benannten Kontaktstellen angeschrieben und um Stellungnahme gebeten. In seinem Schreiben hat der EDÖB unter Verweis auf seinen Leitfaden zu Wahlen und Abstimmungen (s. Box) darauf hingewiesen, dass die Betreiber von sozialen Netzwerken dazu aufgerufen sind, fair und vollständig über die im Zusammenhang mit Wahlen eingesetzten digitalen Bearbeitungsmethoden zu informieren. Nur aufgrund einer solchen Transparenz können die Stimmbürgerinnen und -bürger abschätzen, ob und wie sie in ihrer Meinungsbildung oder ihrem Wahlverhalten beeinflusst werden.

Facebook Ireland Ltd. hat daraufhin dem EDÖB schriftlich bestätigt, dass die Plattform einen Tag vor den Wahlen und am Wahltag entsprechende Funktionen einsetzen werde. Das soziale Netzwerk werde zum Wahltermin ohne Ausnahme alle über 18-jährigen Facebook-Nutzerinnen und -Nutzer in der Schweiz an die Wahl erinnern. Weiter versicherte uns das Unternehmen, dass Facebook hinsichtlich der Zustellung dieser Erinnerung keine Selektion von Gruppen oder Personen vornehme. Gemäss den schriftlichen Zusicherungen zielten die Features alleine darauf ab, die Nutzer für die anstehenden Wahlen zu sensibilisieren und die Teilnahme zu fördern – zum Beispiel indem die betroffenen Personen auf ihrem Profil posten können, dass sie an der Wahl teilgenommen haben. Facebook betonte, dass vom Unternehmen in diesem Zusammenhang keine politischen Ansichten der jeweiligen Nutzer bearbeitet werden. Weiter hat Facebook dargelegt, dass das Unternehmen den Transparenzerfordernissen unseres Leitfadens Beachtung schenke. Die betroffenen Personen sollen sich über eine mehrstufige Information mittels Hyperlinks über die eingesetzten Funktionen, Methoden und deren Bearbeitungsgrundlagen informieren können. Der EDÖB hat die Öffentlichkeit über seine Webseite über die Zusicherungen von Facebook informiert.

Aktualisierter Leitfaden und neue Checkliste für Parteien

Der EDÖB hat die politischen Parteien vor der Endphase der Eidgenössischen Wahlen 2019 mit einer Aktualisierung des Leitfadens der Datenschutzbehörden und einer medial stark beachteten Checkliste zur Nachbesserung ihres Webangebots angehalten.

Die Datenschutzbehörden von Bund und Kantonen haben Ende 2018 einen Leitfaden zur Anwendung des Datenschutzrechts auf die digitale Bearbeitung von Personendaten im Zusammenhang mit Wahlen und Abstimmungen publiziert. Dies mit dem Ziel, die politischen Parteien und übrigen Akteure wie Betreiber sozialer Netzwerke oder Datenhändler im Hinblick auf die Eidgenössischen Wahlen 2019 zu einer gesetzeskonformen Datenbearbeitung anzuhalten. Den politischen Parteien zeigt der Leitfaden insbesondere auf, wie sie das datenschutzrechtliche Grundprinzip der Transparenz im Sinne der berechtigten Erwartungen der Stimmbürger zur Anwendung bringen können (s. 26. TB, Kap. 1.1).

Vor der Endphase des Wahlkampfes hat der EDÖB den Leitfaden aktualisiert und mit einer Checkliste für die politischen Parteien ergänzt. Letztere enthielt Kontrollfragen, die bei den Medien auf hohe Resonanz stiessen und dazu führten, dass mehrere Parteien ihre Webseiten im Bemühen einer vorbildlichen Anwendung des Datenschutzgesetzes vor dem Urnengang nachbesserten.

Nach Aufschaltung der Wahl-Features hat der Beauftragte die Umsetzung der Transparenzvorgaben überprüft und dabei festgestellt, dass Facebook die Nutzer in der beschriebenen Weise über die damit verbundenen Datenbearbeitungen informiert. Zudem konnte er sich vergewissern, dass alle weiteren Aktivitäten, wie z.B. Postings zur Wahlbeteiligung bestimmter Personen, von den Nutzern selber und freiwillig vorgenommen werden. Nachdem auch keine Hinweise auf anderweitige datenschutzrechtliche Mängel vorlagen, konnte er auf weiterführende Massnahmen verzichten.

Auch nach den Wahlen 2019 unterstreichen wir die Wichtigkeit, die Persönlichkeitsrechte im politischen Kontext zu wahren. Wir werden die diesbezügliche Situation in der Schweiz weiterhin aufsichtsrechtlich beobachten.

Elektronische Identität: Einsatz für höchstmögliches Schutzniveau

Mit dem Bundesgesetz über anerkannte elektronische Identifizierungsdienste (BGEID) wurde eine gesetzliche Grundlage geschaffen, die eine sichere Identifikation von Personen im Online-Geschäftsverkehr oder bei E-Government-Anwendungen ermöglichen soll. Der EDÖB konnte im Gesetzgebungsprozess seine Anliegen erfolgreich einbringen.

Politisch umstritten blieb in den inzwischen abgeschlossenen parlamentarischen Beratungen des BGEID die Aufgabenteilung zwischen Staat und privaten Unternehmen: Als sogenannte Identity Provider (IdP) können private Unternehmen durch den standardisierten Rechtsrahmen des BGEID zur Ausstellung von elektronischen Identitäten ermächtigt werden. Voraussetzung dafür ist eine staatliche Zulassung durch eine unabhängige Kommission, die EIDCOM. Die Zulassung erteilt die EIDCOM privaten Gesuchstellern, welche Gewähr bieten, dass sie die technischen und sicherheitsrelevanten Anforderungen des BGEID erfüllen. Vor der Anerkennung eines IdP wird der EDÖB von der EIDCOM hinsichtlich der datenschutzrechtlichen Vorgaben angehört. Der zugelassene IdP untersteht der laufenden Aufsicht durch die EIDCOM.

Der Beauftragte hat sich im Rahmen der Vorbereitung der Vorlage durch die Verwaltung und in den Beratungen in den Rechtskommissionen der Eidgenössischen Räte dafür eingesetzt, dass mit dem BGEID keinerlei Pflichten eingeführt werden, sich für den Zugang zum Internet und zum e-Commerce gesichert identifizieren zu müssen. Weiter haben wir darauf hingewirkt, dass jegliche Datenbekanntgabe vom IdP an Dritte zu kommerziellen oder ähnlichen Zwecken ausgeschlossen wird. Eine Datenbekanntgabe an einen Onlinedienstanbieter ist nur dann erlaubt, wenn dies für die Identifizierung der betreffenden Person beim Dienstanbieter zur Erfüllung vertraglicher Pflichten notwendig ist und der Nutzer vor der ersten Datenweitergabe informiert wurde. Diese Datenbekanntgabe muss in einer Vereinbarung zwischen dem IdP und dem Onlinedienstanbieter geregelt und zusätzlich dem EDÖB zur Prüfung vorgelegt werden. Nachdem unsere Anliegen im Gesetzgebungsverfahren berücksichtigt wurden, erachtet der Beauftragte das BGEID als konform mit der Datenschutzgesetzgebung des Bundes.

In den Schlussabstimmungen vom 27. September 2019 haben der Nationalrat und der Ständerat das BGEID verabschiedet. Gegen das Gesetz ist das Referendum zustande gekommen, welches darauf abzielt, die Herausgabe der elektronischen Identität einzig in staatliche Hände zu legen.

Die «SwissID» der SwissSign Group AG

Die SwissSign Group AG hat mit der «SwissID» eine systemrelevante Bedeutung. Der EDÖB begleitet die Projekte des Unternehmens im Rahmen seiner aufsichtsrechtlichen Beratungstätigkeit.

Die SwissSign Group AG bietet mit der «SwissID» ein Produkt für den Online-Geschäftsverkehr an, das sowohl reine Single-Sign-On (SSO) Dienste als auch die Herausgabe einer elektronischen Identität (s. Haupttext) auf privater Basis beinhaltet. Das Produkt soll im Hinblick auf das kommende BGEID ausgebaut werden, damit die Nutzer identitätspflichtige Rechtsgeschäfte mit einer staatlich anerkannten elektronischen Identität online abschliessen und staatliche Dienstleistungen im Internet beziehen können.

Nachdem die SwissSign Group AG eine datenschutzverantwortliche Stelle im Unternehmen bestimmt und diese mit der Analyse der datenschutzrechtlichen Risiken beauftragt hat, wirkte der EDÖB im Berichtsjahr in regelmässigen Sitzungen mit den Projektverantwortlichen zunächst darauf hin, dass für reine SSO-Dienste eine anonyme Anmeldung möglich sein wird. Die Kunden müssen sich hierfür mit selbstdeklarierten Angaben einloggen können und dürfen weder einer Wahrheitspflicht noch einem Identifizierungsverfahren unterliegen.

Weiter muss das Unternehmen sicherstellen, dass identifizierende Personendaten nur dann an den Onlinedienstanbieter weitergegeben werden, wenn dieser die Daten für die Abwicklung seines Rechtsgeschäftes zwingend benötigt. Dieser Grundsatz soll nicht durch weitergehende Zustimmungen der Nutzer umgestossen werden können.

Die SwissSign Group AG hat dem EDÖB zugesichert, diese Grundsätze in ihre Datenpolicy aufzunehmen und in den Verträgen mit den Onlinedienstanbietern und den Nutzern der «SwissID» umzusetzen.

De-Anonymisierung als Gefahr der KI

Eine Arbeitsgruppe des Bundes formulierte unter Mitwirkung des EDÖB datenschutzrechtliche Anforderungen an die künstliche Intelligenz (KI). Zu den besonderen Risiken von KI-Systemen gehört, dass aus der Kombination unpersönlicher Daten persönliche Informationen abgeleitet werden können.

In Zusammenhang mit der überarbeiteten Strategie «Digitale Schweiz» beschloss der Bundesrat, eine interdepartementale Arbeitsgruppe zur künstlichen Intelligenz (KI) einzusetzen. Dabei wurden zu einzelnen Themenbereichen der KI Projektgruppen gebildet. Der EDÖB nahm in der Projektgruppe Datenverfügbarkeit/Datennutzung und Rahmenbedingungen/Rechtssicherheit Einsitz. Der Gesamtbericht hält fest, dass KI-Systeme aus der Kombination unpersönlicher Datenelemente, die sie aus riesigen Datenmengen filtern (Big Data), Informationen abzuleiten vermögen, die zur Bestimmbarkeit von Personen führen und somit deren Identifizierung möglich machen (sog. De-Anonymisierung). Der Bericht wurde vom Bundesrat im Dezember 2019 zur Kenntnis genommen und vom Staatssekretariat für Bildung, Forschung und Innovation (SBFI) veröffentlicht (vgl. Website des SBFI).

Bundesamt für Statistik: mehr Transparenz und Vor-ort-Audits bei der Bekanntgabe von Personendaten ins Ausland gefordert

Das Bundesamt für Statistik (BFS) setzt neuerdings für Scanning-Dienstleistungen auf einen Anbieter, welcher Teile der vertraglich zugesicherten Leistung im Ausland erbringt. Bei der dadurch entstehenden Bekanntgabe von Personendaten ins Ausland erachtet der EDÖB die Massnahmen zum Schutz der Personendaten im Ausland, mittels den vertraglich getroffenen Vereinbarungen, datenschutzrechtlich als angemessen. Er fordert jedoch mehr Transparenz für betroffene Personen und Vorort-Audits beim Auftragsdatenbearbeiter.

Aufgrund der Schliessung des Digitalisierungs- und Scanning Services des Bundesamtes für Informatik und Telekommunikation per Ende 2018 hat das Bundesamt für Statistik zusammen mit dem Bundesamt für Bauten und Logistik den Auftrag erhalten, im Rahmen eines WTO-Verfahrens einen neuen Leistungserbringer für Scanning-Dienstleistungen zu evaluieren. Nach der Durchführung des WTO-Verfahrens erhielt die «Tessi document solutions GmbH» den Auftrag. Das Scanning der Papierdokumente erfolgt bei dieser Dienstleistung am Standort Genf, wo sie anschliessend entweder sicher vernichtet, oder an das BFS zurückgeliefert werden. Die Papierfragebögen verlassen somit die Schweiz nicht.

Nach dem Scanvorgang werden als fehlerhaft erkannte Textfelder (Ausschnitte der Dokumente) im Ausland manuell korrigiert. Die dazu verwendete elektronische Verarbeitungslösung stellt dem Anwender im Ausland lediglich das Bild der zu korrigierenden Textfelder dar, wobei die Gesamtdokumente auf Systemen innerhalb der Schweiz verbleiben.

Es kommt dadurch zu einer grenzüberschreitenden Datenbekanntgabe gemäss Art. 6 DSG. Das BFS hat dem EDÖB dazu umfangreiche Dokumentationen und auch die vertraglichen Vereinbarungen übermittelt, welche aufzeigen, dass massgebliche Vorkehrungen technischer und organisatorischer sowie vertraglicher Art zum Schutz der Personendaten im Ausland getroffen wurden.

Der EDÖB stellte daraufhin in seiner Stellungnahme fest, dass das BFS als Auftraggeber die Verantwortung für den Datenschutz und die Datensicherheit über die gesamte Verarbeitungskette trägt und sich gemäss Art. 10a Abs. 2 DSG auch darüber vergewissern muss, dass der Datenschutz und die Datensicherheit beim Auftragnehmer gewährleistet sind. Aufgrund der Tragweite dieses Projekts erachtete der EDÖB zudem die stichprobenartige Kontrolle der Räumlichkeiten, in denen die Daten bearbeitet werden, als angezeigt.

Weiter erachtet es der Beauftragte im Sinne des datenschutzrechtlichen Grundsatzes der Transparenz als unabdingbar, dass die betroffenen Personen, über den Sachverhalt der Bekanntgabe von Daten ins Ausland, durch das BFS aktiv informiert werden. Die Information der Betroffenen hat gemäss seiner

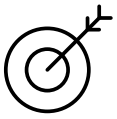
Auffassung mittels eines entsprechenden Hinweises auf den Erhebungsfragebögen des BFS zu erfolgen.

Es zeigt sich, dass datenschutzrechtliche Überlegungen bereits in der WTO-Evaluierungsphase von Projekten mit Personendatenbearbeitungen einzubeziehen sind. Der EDÖB wird das Projekt weiter begleiten und die Umsetzung der geforderten Massnahmen überprüfen.

Die Vermarktung von Bewegungsdaten aus dem Mobilfunknetz erachtet der EDÖB trotz aufwendiger Anonymisierung nach wie vor als problematisch

Die Art und Weise, wie sich die Menschen bewegen, ist einzigartig. Aus diesem Grund kann auch nach Anwendung von ausgeklügelten Anonymisierungsmethoden nicht ausgeschlossen werden, dass anhand dieser eindeutigen Bewegungsmuster und zusätzlichen Angaben mindestens in Einzelfällen Personen mit wenig Aufwand bestimmt werden können. Die Daten sind daher als Personendaten zu qualifizieren, benötigen zur Bearbeitung die Einwilligung der Betroffenen und sind entsprechend zu schützen.

Der Trend in der Geschäftswelt, Bewegungsdaten aus dem Mobilfunknetz zu statistischen Zwecken zu nutzen, hält weiter an. Mit Hilfe von Bewegungsdaten können Datenbearbeiter heute exakt bestimmen, wo Menschen zu Fuss unterwegs sind, auf welchen Strecken sie fahren, fliegen oder öffentliche Verkehrsmittel nutzen.



Die Bewegungsdaten werden verwendet, um beispielsweise Verkehrsflüsse zu verbessern oder den optimalen Standort für ein Ladenlokal zu planen.

So erhielt der EDÖB im 2019 die Anfrage einer Firma betreffend Nutzung solcher Bewegungsdaten. Dabei ging es um die Frage, ob die nach Anwendung einer ausführlich in der Dokumentation beschriebenen Anonymisierungsmethode trotzdem noch als Personendaten klassifizierten Daten vom Mobilfunkanbieter an die Firma übertragen werden dürfen.

Die Methode sieht vor, dass bereits beim Fernmeldedienstanbieter mehrere Anonymisierungsschritte durchgeführt werden, so dass der Firma nur statistische Gesetzmässigkeiten des Verhaltens von Individuen übermittelt werden. Dazu gehört unter anderem, dass einerseits die Informationen zu den Standorten von Mobilfunkgeräten nicht punktgenau erfasst werden. Andererseits werden aus diesen ungenauen Standortdaten mögliche Bewegungspfade berechnet und jener mit der grössten Wahrscheinlichkeit ausgewählt. Das Ergebnis sind Bewegungsprofile, welche den Gesetzmässigkeiten der realen Bevölkerung entsprechen, jedoch nicht das tatsächliche Verhalten eines Individuums abbilden sollen.

Gemäss der Einschätzung des EDÖB reduziert die angewandte Anonymisierungsmethode die Möglichkeiten einer Re-Identifikation von Personen erheblich.

Es kann jedoch nicht ausgeschlossen werden, dass basierend auf den übermittelten Daten und durch die Aggregation von Wohnsitz und Arbeitsort ein Rückschluss auf ein tatsächliches Individuum gemacht werden kann.

Die Problematik liegt insbesondere in den ländlichen Regionen mit geringen Bevölkerungsdichten. Der Aufwand für eine Re-Identifikation erscheint dem EDÖB jedoch nicht sehr gross. Es muss deshalb damit gerechnet werden, dass ein Interessent diesen auf sich nehmen wird. Aus diesem Grund kann nicht ausgeschlossen werden, dass mindestens im Einzelfall anhand von vorhanden Daten und zusätzlichen Angaben eine Person mit wenig Aufwand bestimmbar ist, und hier folglich Personendaten im Sinne von Art. 3 Bst. a DSG vorliegen.

In casu sollen Personendaten, welche zum Zweck der Erbringung von Fernmeldediensten und deren Abrechnung erfasst wurden, für weitere Zwecke genutzt werden. Diese Änderung des Bearbeitungszwecks hat zur Folge, dass die Einwilligung der betroffenen Personen vorliegen muss sowie Massnahmen zum Schutz der Personendaten zu treffen sind.

5G Standard: EDÖB kontrolliert Datenschutzmassnahmen der Fernmeldedienstanbieter zur sicheren Implementierung

Der EDÖB hat technische Abklärungen zur datenschutzkonformen Implementation des neuen Fernmeldestandards 5G aufgenommen.

Der neue Fernmeldestandard 5G, Nachfolger des aktuellen Standards 4G /LTE verspricht nicht nur mehr Bandbreite und mehr gleichzeitig verbundene Geräte, sondern auch Datenübertragungen in nahezu Echtzeit. So bildet der Fernmeldestandard 5G die Grundlage für eine Vielzahl zukünftiger Anwendungen sei es in der Industrie mit IoT-Sensoren (Internet der Dinge) oder Connected Cars bzw. autonom fahrenden Autos. Obschon 5G ein internationaler Standard für mobiles Internet und Mobiltelefonie darstellt, bestehen teilweise grosse Unterschiede bei der Umsetzung der einzelnen Anbieter. Weiter zeigen öffentliche Berichte von Forschern der ETH Zürich [arXiv:1806.10360v3 [cs.CR] 18 Oct 2018] einerseits und der Universitäten Purdue und Iowa [NDSS '19, 24-27 February 2019, San Diego, CA, USA Copyright 2019 Internet Society, ISBN 1-891562-55-X] Sicherheitslücken im neuen 5G Standard auf (u.a. im Paging Protocol mit ToRPEDO und PIERCER Angriffen). Den Berichten zufolge soll der neue Standard jedoch in der Gesamtheit sichererer als der bisherige 4G Standard sein.

Mit der Lieferung der Unterlagen zu den gewählten Implementationen und der Einsicht vor Ort, kann sich der EDÖB ein detailliertes Bild über das Sicherheitsniveau und die getroffenen Massnahmen machen. Die Abklärungen wurden im Berichtsjahr noch nicht abgeschlossen.

Falsche E-Mail-Adressen bei Swisscom

Eine Datenpanne in einem Kundensystem der Swisscom führte dazu, dass E-Mails an falsche Adressen versandt wurden. Das Unternehmen hat rasch geeignete Massnahmen ergriffen.

Aufgrund einer Bürgermeldung hat der EDÖB erfahren, dass ein Kunde von Swisscom verschiedenste E-Mails erhalten hat, die nicht für ihn bestimmt waren. Der EDÖB hat das Unternehmen daraufhin zur Stellungnahme aufgefordert. Es führte aus, dass ihm dieses Problem bereits bekannt sei und es eine Task Force beauftragt habe, eine Risikoanalyse vorzunehmen. Es habe sich gezeigt, dass in einem Kundensystem der Swisscom generisch erfasste E-Mail-Adressen nicht den korrekten Kunden zugewiesen waren. In der Folge gingen einige E-Mails von Swisscom an ein fremdes Konto. Nach Bekanntwerden des Vorfalls hat das Unternehmen die E-Mails bei dem unberechtigten Empfänger gelöscht.

Nach Angaben von Swisscom wurden die falsch zugewiesenen E-Mail-Adressen in der Zwischenzeit identifiziert und umgehend sichergestellt, dass keine weiteren E-Mails zugestellt werden. Gemäss dem Unternehmen liegen zudem keine Hinweise vor, wonach die fehlgeleiteten E-Mails missbräuchlich verwendet worden seien. Das Unternehmen ist zudem daran, die Prozesse anzupassen, damit derartige Vorfälle verhindert werden können.

Der EDÖB hat die Sofortmassnahmen auf Grundlage der Risikoanalyse der Swisscom zur Kenntnis genommen. Aufgrund der durch das Unternehmen sofort eingeleiteten Massnahmen konnte er von weiteren Handlungsempfehlungen absehen.

«Tiktok» im Fokus der Datenschützer

Die Videoplattform Tiktok ist bei Kindern und Jugendlichen enorm beliebt. Der EDÖB hat die chinesische Betreiberin der App kontaktiert, da die Nutzungsbestimmungen für Schweizer Kunden unklar sind. Zudem ist er mit der britischen Datenschutzbehörde ICO in Kontakt, um Fragen betreffend den Persönlichkeitsschutz der Nutzerinnen und Nutzer zu klären.

«Tiktok» ist eine vor allem bei Jugendlichen beliebte Videoplattform mit rasant steigenden Download-Raten in den jeweiligen App-Stores. Mit «Tiktok» können kurze, selbst erstellte Clips mit verschiedenen Effekten und Filtern versehen und mit anderen geteilt werden. Die Social-Media-Funktionen der Plattform erlauben es, auf sehr einfachem Weg mit anderen Usern in Kontakt zu treten, auf deren Videos zu reagieren und diese zu kommentieren.

Die App gehört dem chinesischen Internet-Technologie-Unternehmen Bytedance mit Sitz in Peking. In den Medien werden verschiedene Vorbehalte und Kritiken gegen den Inhaber des Videoportals laut. Es wird ihm beispielsweise vorgeworfen, zu wenig für den Persönlichkeitsschutz von Kindern zu unternehmen oder gewisse Inhalte nach chinesischen Vorgaben zu zensieren oder zu filtern.

Der EDÖB hat festgestellt, dass für Schweizer User unklar ist, welche Nutzungsbestimmungen für sie anwendbar sind, da sich diese auf den EU-Raum beziehen. Er hat die verantwortliche Stelle bei «Tiktok» zu dieser Frage und zu den Massnahmen zum Schutz der Kinder und Jugendlichen um eine Stellungnahme gebeten. Daneben hat er verlangt, dass das Unternehmen eine für ihn zuständige Stelle angibt, welche in Fragen des Datenschutzes kompetent Auskunft geben kann.

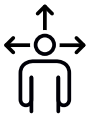
Das Unternehmen hat zu den Fragen Stellung genommen und eine Ansprechstelle genannt. Der EDÖB steht mit der britischen Datenschutzbehörde ICO in Kontakt, welche im Berichtsjahr zum Thema des Schutzes von Kindern und Jugendlichen und dem Umgang mit deren Daten eine Abklärung gegen «Tiktok» eröffnet hat.

Musik-Streamingdienst – Analyse der Personendaten auf Basis eines Auskunftsgesuches des EDÖB

Ein Musik-Streamingdienst fragte zur Kontrolle der Wohnadresse auch nach dem Zugriff auf die GPS-Daten seiner Nutzer. Der EDÖB hat im Rahmen seiner Abklärungen ein Auskunftsgesuch gestellt und die erhaltenen Daten eingehend analysiert. Die Abklärungen konnten ohne formelle Massnahmen abgeschlossen werden.

Im Berichtsjahr erschienen diverse Zeitungsberichte über einen verbreiteten Musik-Streamingdienst. Laut diesen Berichten würden Nutzer neuerdings aufgefordert, zum Zweck der Überprüfung der Zugehörigkeit zu einem Haushalt für die Rechnungsstellung, mittels Übertragung der GPS-Daten ihres Smartphones ihren Standort zu verifizieren. Dieser Umstand bewog den EDÖB dazu, die Rechtmässigkeit der Datenbearbeitung zu prüfen, indem per Auskunftsgesuch konkrete Nutzungsdaten bei diesem Musik-Streamingdienst beantragt wurden. Unsere Analyse der erhaltenen Daten ergab, dass der Anbieter die bei ihm anfallenden Nutzerdaten konform zu seinen eigenen Nutzungs- und Datenschutzbestimmungen bearbeitet. Die ebenfalls geprüften Bestimmungen sind aus unserer Sicht verständlich formuliert und entsprechen den gesetzlichen Vorgaben. Es wurden diesbezüglich keine Auffälligkeiten festgestellt.

Die Einwilligung der Kunden zur Übermittlung von GPS-Daten an den Anbieter wird in dessen Datenschutzerklärung als freiwillig bezeichnet. Tatsächlich haben die Nutzer bei der Anfrage die Wahl, ob sie die Bestätigung per GPS-Signal oder lieber per



Angabe der Postleitzahl vornehmen möchte. Somit besteht für die Kunden keine Pflicht, die GPS-Daten an den Musik-Streamingdienst zu übertragen und daher aus Sicht des EDÖB auch kein Grund zu einer Beanstandung.

Geprüft wurde auch die Aufbewahrungsdauer der Nutzerdaten. Dabei wird zwischen den Angaben zur Person und den Nutzungsdaten unterscheiden:

- Die Angaben zur Person (Nutzerdaten) werden beim Erstellen des Benutzerkontos erfasst und enthalten Identitäts- und Kontaktdaten, welche über die gesamte Nutzungsdauer des Dienstes verwendet und aufbewahrt werden. Diese Angaben sind für die Kontaktaufnahme und die korrekte Rechnungsstellung nötig. Was die vom Streamingdienst angefragten GPS-Daten zur Standortbestimmung betrifft, so wurden keine solchen Daten in den erhaltenen Nutzerdaten gefunden. Eine Löschung der eigenen Nutzerdaten kann nur durch das endgültige Schliessen des Kontos und somit dem Verzicht der Nutzung des Streamingdienstes erreicht werden. Dieses Vorgehen ist nicht zu beanstanden, da auf Grund urheberrechtlicher Vorgaben eine Nutzung ohne Registrierung für das vorliegende Streaming-Angebot nicht möglich ist.
- Anders sieht es bei den Nutzungsdaten aus. Diese werden während der Verwendung des Diensts angelegt und enthalten Informationen zu dessen Nutzung. Diese Angaben sollen zwar das Erlebnis der Nutzer verbessern, sind aber nicht zwingend für die Benutzerverwaltung erforderlich. Daher kann eine Kontrolle der Nutzungsdaten erfolgen, indem der Benutzer die von ihm selber erstellten Daten, wie beispielsweise Playlists, jederzeit auch selber wieder löschen kann. Weitere Nutzungsdaten wie beispielsweise der Hörverlauf, werden für den Zeitraum von neunzig Tagen gespeichert und danach automatisch gelöscht. Dieses Vorgehen ist verhältnismässig und widerspricht nicht den gesetzlichen Vorgaben.

Nachdem der EDÖB keine Unverhältnismässigkeiten seitens des Musik-Streamingdienstes feststellen konnte, wurde die Abklärung ohne formelle Massnahmen abgeschlossen.

Clearview beschafft ungefragt Gesichtsbilder

Der EDÖB warnte auf seiner Internetseite wiederholt vor drohenden Persönlichkeitsverletzungen von Personen in der Schweiz durch die ungefragte Beschaffung von Gesichtsbildern im Internet.

Die US-amerikanischen Anbieter der Applikation Clearview betreiben gemäss Medienberichten eine Datenbank mit rund drei Milliarden Gesichtsbildern, die sie durch Abfischen des Internets und der sozialen Netzwerke beschaffen. Das Geschäftsmodell besteht darin, dass Clearview für seine zahlenden Kunden beliebige Gesichtsaufnahmen mit der Datenbank abgleicht und die Treffer aufgrund weiterer Informationen identifizierbaren Personen zuweist. Zur US-Kundschaft von Clearview sollen namentlich Polizeibehörden gehören.

Da wir damit rechnen mussten, dass in der Datenbank von Clearview auch Gesichtsbilder von Einwohnern der Schweiz bearbeitet werden, nahm unsere Behörde im Januar 2020 auf der Webseite wiederholt zur Applikation Clearview Stellung: An die Adresse von Clearview hielten wir fest, dass das schweizerische Datenschutzrecht und die Persönlichkeit der betroffenen Personen in der Schweiz in schwerer Weise verletzt würden, falls ihre Gesichtsbilder ungefragt beschafft und für fremde Polizeibehörden weiterbearbeitet würden.

Zuhanden der sozialen Netzwerke, deren Nutzungsbedingungen das ungefragte Abfischen ihrer Plattformen durch Dritte oder deren Roboter in aller Regel untersagen, hielten wir fest, dass sie die Bilddaten ihrer Kunden technisch besser schützen müssen. Und den Benutzern von sozialen Netzwerken rieten wir, eigenverantwortlich zu handeln und in den Voreinstellungen die Zugänglichmachung von Fotomaterial für Suchmaschinen zu unterbinden.

Um die Betroffenheit der Schweizer Bevölkerung einschätzen zu können, stellte der Beauftragte am 24. Januar 2020 bei Clearview ein Auskunfts- und Löschgesuch zu den über seine Person bearbeiteten Daten. Dieses blieb, trotz Mahnschreiben bis zum Abschluss der Berichtsperiode unbeantwortet. Die Direktionen des Bundesamtes für Polizei (fedpol), die Eidgenössische Zollverwaltung (EZV) und der Nachrichtendienst des Bundes (NDB) bestätigten dem EDÖB auf dessen Anfrage hin demgegenüber innert nützlicher Frist, dass sie in ihrer Tätigkeit weder Clearview noch vergleichbare Anwendungen einsetzen oder einzusetzen beabsichtigen.

Der Beauftragte wird im Rahmen seiner gesetzlichen Möglichkeiten alles unternehmen, um die Schweizer Bevölkerung vor ungefragten Beschaffungen ihrer Gesichtsbilder zu schützen, damit sie sich sowohl im virtuellen wie auch realen Raum weiterhin anonym bewegen kann.

Revision des Datenschutzgesetzes

Im Berichtsjahr erreichte die Totalrevision des Bundesgesetzes über den Datenschutz vom 19. Juni 1992 (DSG) wichtige Meilensteine. Nachdem die Vorlage von der Staatspolitischen Kommission des Nationalrates und von der entsprechenden Kommission des Ständerates geprüft wurde, steht nun die Differenzbereinigung an. Das Gesetzgebungsverfahren ist wegen der derzeitigen ausserordentlichen Lage, die durch die Covid-19-Pandemie bedingt ist, beeinträchtigt. Mit einer Verzögerung der Verabschiedung der Revision ist zu rechnen. Dementsprechend muss auch mit der formellen Aufhebung des Bundesgesetzes über den Datenschutz im Rahmen der Anwendung des Schengen-Besitzstands in Strafsachen (SDSG), das am 1. März 2019 provisorisch in Kraft trat und formal in das neue DSG integriert werden soll, zugewartet werden.

Bei den Anhörungen in den parlamentarischen Kommissionen, zu denen er eingeladen wurde, setzte sich der Beauftragte für die Einführung von Massnahmen ein, mit denen die dynamische Technologieentwicklung und die dazugehörigen Risiken bewältigt werden können. Er befürwortete die Vorschläge, die Schweizerinnen und Schweizern ein Datenschutzniveau bieten, welches demjenigen der Datenschutzkonvention des Europarats (Konvention 108+) entspricht und ähnlich ist wie in der Datenschutzgrundverordnung der EU; diese wird von vielen Akteuren in der Schweiz im Sinne einer besten Praxis bereits jetzt für ihre Schweizer Kundschaft angewandt. Im Hinblick auf eine Fortentwicklung des bestehenden Datenschutzansatzes sieht die Vorlage einen Ausbau der Grundkonzepte des Gesetzes vor.

Die bestehenden Grundsätze sollen namentlich durch den datenschutzfreundliche Voreinstellungen (privacy by default) und entsprechende Technikgestaltung (privacy by design) ergänzt werden. Zudem wurde die Terminologie modernisiert und auf jene des europäischen Rechts abgestimmt. Allerdings bleiben Divergenzen bestehen, die zu einem gewissen Mass an Rechtsunsicherheit und zu Schwierigkeiten in der praktischen Handhabung führen könnten. In einigen Fällen handelt es sich um echte konzeptionelle Unterschiede, beispielsweise bei den Begriffen «Profiling» bzw. «Profiling mit hohem Risiko», einer vom Ständerat vorgeschlagenen Neuerung, die im klaren Widerspruch zur Auffassung des Nationalrats steht.

Mit dieser Revision kann die Schweiz den Verpflichtungen nachkommen, die sie unlängst mit der Unterzeichnung des Übereinkommens 108+ eingegangen ist, sowie in den Genuss des erhofften Angemessenheitsbeschlusses kommen, der für die hiesige Wirtschaft die Aufrechterhaltung des vollen Zugangs zum europäischen Markt bedeuten würde.

Datenschutzkonvention 108+ des Europarates

Der Bundesrat entschied im Oktober 2019, das Änderungsprotokoll zur Datenschutzkonvention 108 des Europarats (Konvention 108+) zu unterzeichnen. Die Schweiz hat daraufhin die Konvention 108+ am 21. November 2019 in Strassburg formell unterzeichnet. Die entsprechende Botschaft zur Genehmigung des Protokolls wurde vom Bundesrat am 6. Dezember 2019 zuhanden des Parlaments verabschiedet. Die Schweiz will damit einen international anerkannten Datenschutzstandard garantieren.

Der EDÖB hat im 26. Tätigkeitsbericht 2018/19 darauf hingewiesen, dass es angezeigt wäre, dass der Bundesrat das modernisierte Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten des Europarates, unterzeichnet.

Die Schweiz ratifizierte die im Jahr 1985 in Kraft getretene ursprüngliche Datenschutzkonvention am 2. Oktober 1997. Um sie den technologischen Entwicklungen und den Herausforderungen der Digitalisierung anzupassen, wurde sie in den letzten Jahren vom Europarat überarbeitet und liegt seit Oktober 2018 zur Unterzeichnung auf. Das Änderungsprotokoll wurde bisher von mehr als 30 Staaten unterzeichnet und bereits von den ersten Staaten ratifiziert.

Ein Beitritt zur modernisierten Datenschutzkonvention des Europarates ist für die Schweiz von grosser Bedeutung. Die Konvention verstärkt den Schutz der Personen in unserem Land, deren Personendaten in einem der Vertragsstaaten bearbeitet werden. Zudem wird der Datenaustausch zwischen den Vertragsstaaten vereinfacht. Weiter wird sichergestellt, dass die grenzüberschreitende Datenübermittlung ohne zusätzliche Hürden möglich bleibt. Ferner kommt der Konvention auch im Rahmen der bevorstehenden Angemessenheitsprüfung des schweizerischen Datenschutzniveaus durch die EU eine wichtige Bedeutung zu, weil die EU bei ihrem Entscheid jeweils auch berücksichtigt, ob die zu prüfenden Staaten der Konvention beigetreten sind.

Gemäss Konvention 108+ werden die Pflichten des für die Datenbearbeitung Verantwortlichen ausgeweitet. Dieser ist insbesondere verpflichtet, der zuständigen Aufsichtsbehörde gewisse Datenschutzverletzungen zu melden. Die Rechte der betroffenen Personen werden zudem gestärkt, da der Dateninhaber die betroffene Person über die Beschaffung von Personendaten in gewissen Fällen informieren muss. Der Datenbearbeiter hat zudem im Vorfeld bestimmter Bearbeitungen eine Datenschutzfolgenabschätzung durchzuführen. Der Datenschutz ist in Projektvorhaben von Beginn weg zu berücksichtigen (privacy by design) und die Voreinstellungen sind datenschutzfreundlich zu konfigurieren. Das Änderungsprotokoll sieht auch einen Ausbau der Rechte der betroffenen Personen vor, insbesondere in Bezug auf ihr Auskunftsrecht und Widerspruchsrecht bei automatisierten Einzelfallentscheidungen. Die Vertragsstaaten werden auch verpflichtet, ein Sanktionen- und Rechtsmittelsystem einzuführen und den Aufsichtsbehörden eine Befugnis zum Erlass von verbindlichen Entscheidungen einzuräumen.

Der Bundesrat hat am 30. Oktober 2019 entschieden, die Konvention 108+ zu unterzeichnen. Die Unterzeichnung durch die Schweiz erfolgte dann am 21. November 2019 formell in Strassburg. In der Folge verabschiedete der Bundesrat an seiner Sitzung vom 6. Dezember 2019 die Botschaft über die Genehmigung des Protokolls zur Änderung der Datenschutzkonvention des Europarates zuhanden des Parlaments, welches über die Ratifikation zu befinden hat.

Mit einem Beitritt zur modernisierten Konvention kann die Schweiz ein hohes Datenschutzniveau für die Privatsphäre gewährleisten und den grenzüberschreitenden Datenverkehr im öffentlichen Sektor sowie in der Privatwirtschaft erleichtern, was auch für die Schweizer Wirtschaft wichtig ist.


Arrival 2
Taxi
Lost & Found 1|2
Check-in 2

1.2 Justiz, Polizei, Sicherheit

DNA-Profile: ein strenger Gesetzesrahmen ist unerlässlich

Im Zusammenhang mit der Ämterkonsultation zum Entwurf über die Änderung des DNA-Profil-Gesetzes begrüsste der EDÖB grundsätzlich die vorgeschlagenen Änderungen und Neuerungen, betonte jedoch die Notwendigkeit eines strengen gesetzlichen Rahmens für die neuen Instrumente «Phänotypisierung» und «erweiterter Suchlauf mit Verwandtschaftsbezug» (Verwandtenrecherche).

Der Änderungsentwurf des EJPD sieht vor, die Vorschriften des Gesetzes über DNA-Profile von denjenigen der Zivil- und Militärstrafprozessordnung loszulösen. Der EDÖB zeigte sich über diesen Klärungsvorschlag erfreut.

Ferner steht eine neue Lösung betreffend die Dauer der Aufbewahrung der DNA-Profile zur Diskussion, die das Verhältnismässigkeitsprinzip und die spezifischen Anforderungen des Jugendstrafrechts berücksichtigt.

Hinsichtlich der erweiterten Verwandtenrecherche und der Phänotypisierung fordert der EDÖB strenge Auflagen, um die Verhältnismässigkeit des Eingriffs in die Grundrechte der betroffenen Personen zu gewährleisten. Laut Auffassung des EDÖB sollten diese Instrumente nur als ultima ratio zur Anwendung kommen. Sie sollten ausschliesslich zur Aufklärung schwerer Verbrechen im Verhältnis zur Bedeutung des jeweiligen Rechtsguts, namentlich bei Gefährdung von Leib und Leben bzw. Verletzung der Freiheit oder der sexuellen Integrität eingesetzt werden. Bei Straftaten gegen das Eigentum sollten der erweiterte Suchlauf mit Verwandtschaftsbezug, die Phänotypisierung sowie Massenuntersuchungen hingegen in der Regel nicht angewandt werden. Für das Herauslesen einiger Merkmale, beispielsweise der Haarfarbe, ist die Phänotypisierung zu unpräzise und demnach hinsichtlich der Anforderung der Datenrichtigkeit potenziell problematisch. Die Ermittlung von Daten im Rahmen einer Verwandtschaftsrecherche unterläuft ihrerseits das Zeugnisverweigerungsrecht und ist somit nur bei besonders schwerwiegenden Straftaten vertretbar.

Der erweiterte Suchlauf mit Verwandtschaftsbezug und die Phänotypisierung dürfen wie oben erwähnt nur bei besonders schwerwiegenden Verbrechen und im Verhältnis zur Schwere der Rechtsgutverletzung durchgeführt werden. Da die Erstellung eines entsprechenden abschliessenden Deliktskatalogs schwierig ist schlug der EDÖB vor, die Anordnungsbefugnis für die betreffenden Massnahmen analog zum Fall der Massenuntersuchungen dem Zwangsmassnahmengericht zu übertragen. Der Bundesrat hat dem Antrag des EDÖB nicht zugestimmt. Dieser wird sich im Rahmen des parlamentarischen Prozesses dazu äussern, falls er dazu aufgefordert wird.

Gesetz zur Bekanntgabe von Flugpassagierdaten in EU-Staaten verzögert sich

Der EDÖB begleitete weiterhin die Arbeiten zur Schaffung einer gesetzlichen Grundlage für die Bekanntgabe von Fluggastdaten durch Fluggesellschaften an EU-Staaten. Wir wiesen verschiedentlich auf die Dringlichkeit der baldigen Schaffung dieser Grundlagen hin.

Wie der EDÖB im Tätigkeitsbericht 2018/2019 festhielt, planten verschiedene EU-Staaten, von Luftfahrtgesellschaften deren Passagierdaten von Flügen aus der Schweiz zu verlangen. Sie stützen sich dabei auf die EU-Richtlinie 2016/681 vom 27. April 2016 über die Verwendung von Fluggastdatensätzen zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität (EU-PNR-Richtlinie).

Wir wiesen die zuständigen Bundesbehörden darauf hin, dass dafür eine gesetzliche Grundlage zu schaffen sei. 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 zu schaffen (s. 26. TB, Kap. 1.2).

In der Folge begann das Bundesamt für Zivilluftfahrt (BAZL) als zuständiges Bundesamt mit den entsprechenden Gesetzgebungsarbeiten. Der EDÖB stand dem BAZL von Anfang an beratend zur Seite, bis das Amt entschied, seine Arbeiten aufzuschieben. Zur Begründung führte das BAZL an, einerseits hätten die bisherigen Arbeiten ergeben, dass zuerst eine gesetzliche Grundlage in einem for-

mellen Gesetz geschaffen werden müsse. Andererseits sei davon auszugehen, dass der Bundesrat in nächster Zeit in einem separaten Gesetzgebungsprojekt über das weitere Vorgehen in Zusammenhang mit der Nutzung von Flugpassagierdaten zur Bekämpfung der schweren Kriminalität und des Terrorismus durch die Schweiz entscheiden werde. Es sei deshalb sinnvoll, beide Vorlagen zusammenzulegen und gleichzeitig zu behandeln.

Der EDÖB wies dabei erneut auf die Dringlichkeit der Schaffung einer gesetzlichen Grundlage hin. Ohne eine solche sei die Bekanntgabe von PNR-Daten durch Fluggesellschaften an Behörden der EU unrechtmässig. Der Vollständigkeit halber hielten wir weiter fest, dass für die Bekanntgabe von PNR-Daten durch Fluggesellschaften in Drittstaaten (d.h. ausserhalb des Anwendungsbereichs der EU-PNR-Richtlinie) Abkommen geschaffen werden müssten. In der Folge nahm das Bundesamt für Polizei erste Arbeiten zur gesetzlichen Regelung der Nutzung von Flugpassagierdaten zur Bekämpfung der schweren Kriminalität und des Terrorismus durch die Schweiz auf.

Dabei wurde auch die Frage der Bekanntgabe von Flugpassagierdaten an EU-Staaten gestützt auf die EU-PNR-Richtlinie integriert. Der EDÖB nahm auch hier im Rahmen der Ämterkonsultation Stellung und hielt an seiner bisherigen Position fest. Im Februar 2020 hat sich der Bundesrat in einem Grundsatzentscheid für die Nutzung von Flugpassagierdaten in der Schweiz zur Terrorismus- und Kriminalitätsbekämpfung ausgesprochen. Der EDÖB wird die Gesetzgebungsarbeiten weiterhin beratend begleiten.

Swiss Buchungssystem – Massnahmen gegen Datenmissbrauch in Umsetzung

Bereits im letzten Tätigkeitsbericht berichtete der EDÖB über das Buchungssystem der Fluggesellschaft Swiss. Das Unternehmen versprach, gewisse Anpassungen – wie die teilweise Maskierung der Passnummer – mit der Einführung ihrer neuen Internetseite umzusetzen. Die Einführung verzögerte sich allerdings.

Wie im letzten Tätigkeitsbericht erwähnt, hat die Fluggesellschaft Swiss auf Einwirken des Beauftragten hin ihre allgemeinen Beförderungsbestimmungen (ABB) angepasst, um ihre Kunden besser auf die Schutzwürdigkeit der auf dem Boarding Pass ersichtlichen bzw. gespeicherten Personendaten hinzuweisen. Weiter sollte die Passnummer, die in bestimmten Fällen beim Buchungsaufruf ersichtlich ist, teilweise unkenntlich gemacht werden (s. 26. TB, Kap. 1.2). Die Swiss hielt gegenüber dem EDÖB fest, dass mit der Inbetriebnahme ihrer neuen Webseite die Anpassungen umgesetzt würden. Die Umstellung auf die neue Webseitenarchitektur und die damit zusammenhängende Maskierung der Passnummer verzögerten sich allerdings. Daher beschloss die Swiss, die Maskierung der Passnummern und neu auch Visa-/Greencard-Daten auf ihrer Internetseite separat und vorgängig einzuführen, indem die ersten zwei Zeichen der Passnummern und Visa-/Greencard-Daten beim Buchungsaufruf lesbar belassen und alle folgenden durch ein «x» ersetzt werden. Diese Änderung hat die Swiss Ende 2019 umgesetzt.

Polizeiliche Massnahmen zur Bekämpfung von Terrorismus

Aus Sicht des EDÖB stellt die Schaffung einer Polizeigesetzgebung auf Bundesebene eine unerlässliche Voraussetzung dar, die zu erfüllen wäre, bevor neue Regularien ausgearbeitet werden. Er erhebt folglich Zweifel an der Gesamtheit des Entwurfs über polizeiliche Massnahmen zur Bekämpfung von Terrorismus.

Seit mehreren Jahren bemängelt der EDÖB in seinen Tätigkeitsberichten, dass die Regelungen betreffend die polizeiliche Tätigkeit des Bundes auf zahlreiche Erlasse verstreut sind. In der Tat verfügt der Bund im Gegensatz zu den Kantonen nicht über ein eigentliches Polizeigesetz, das die Aufgaben, Befugnisse und die Bearbeitung personenbezogener Daten umfassend abbilden würde. Das Bundesamt für Polizei ist für eine grosse Anzahl von Datenbanken zuständig, die eine zentralisierte Bearbeitung äusserst schützenswerter Daten ermöglichen, zu denen zwischen Polizeibehörden des Bundes und der Kantone sowie mit anderen Ländern ein Austausch stattfindet.

Die Bearbeitung der Daten erfolgt auf der Grundlage eines Wirrwarrs an polizeirechtlichen Spezialgesetzen, deren Handhabung sogar für spezialisierte Juristen und erst recht für das Polizeipersonal an der Front unübersichtlich ist, so dass selbst Untersuchungsverfahren betreffend die Bearbeitung von Daten aufgrund der vorhandenen Komplexität längst an ihre Grenzen stossen. Anstatt ein Gesetz über die Polizeiaufgaben oder zumindest ein Gesetz über Information und Zusammenarbeit auf Bundesebene auf den Weg zu bringen, erarbeitet das EJPD immer wieder neue Bestimmungen, etwa über polizeiliche Massnahmen zur Bekämpfung von Terrorismus oder über Vorläuferstoffe für explosionsfähige Stoffe. Dadurch steigt die Schwerfälligkeit der ohnehin bereits unzumutbar komplexen Vorschriften, während bestimmte Fragen dennoch offen bleiben: In welchen Systemen sollen Vorratsdaten auf welche Weise und über welchen Zeitraum bearbeitet werden?

Angesichts dieses Sachverhalts ist der EDÖB nicht mehr bereit, Gesetzesvorhaben in sensiblen Bereichen, beispielsweise auf dem Gebiet der Polizeimassnahmen zur Terrorismusbekämpfung, in der parlamentarischen Phase zu unterstützen. Der EDÖB stellt den gesamten vom EJPD vorgelegten Entwurf grundsätzlich in Frage. Die vorberatende Kommission des erstberatenden Ständerates hat indessen trotz unserer bereits im letzten Jahresbericht (s. 26. TB, Kap. 1.2) und in den Medien publizierten Kritik davon abgesehen, den EDÖB zu diesem Geschäft anzuhören.

Technische Aufsicht der Nutzung des Schengener Informationssystems (SIS) bei fedpol und ISC-EJPD

Das N-SIS ist die nationale Kopie des zentralen Schengener Informationssystems (C-SIS) für die Schweiz. Die Datenbearbeitung innerhalb des N-SIS und die Übermittlung der Daten an das zentrale SIS sind im Bearbeitungsreglement «Informationssystem N-SIS und dessen Teilsysteme» geregelt. Das N-SIS wird in der Schweiz von über 30 000 Nutzern aus verschiedenen Dienststellen des Bundes (z.B. RIPOL, SEM), der Kantone (z.B. Kantonsverwaltungen und -polizeien) und der Gemeinden verwendet.
Das ISC-EJPD ist der Entwickler des Systems, und es erbringt Dienstleistungen für das Bundesamt für Polizei (fedpol), das die Verantwortung für das System trägt. Unsere technische Kontrolle betraf beide Gremien. Dabei wurden Anfragen an weitere Organe gerichtet, beispielsweise an das RIPOL, das ZEMIS sowie an Kantonspolizeien; diese Organe wurden jedoch nicht kontrolliert.

Erstes Ziel dieser Kontrolle ist, die Konformität mit dem neuesten Stand der vorwiegend an der Norm ISO 27 001 angelehnten technischen und organisatorischen Massnahmen für die Sicherheit und den Schutz der Daten innerhalb des Systems und bei dessen Nutzung zu überprüfen. Das zweite Ziel ist die Überprüfung der Durchführung der betreffenden Massnahmen.

Die Gespräche über unseren Fragenkatalog und über die geprüften Elemente veranlassten uns dazu, spezifische Punkte zu vertiefen. Die Auswertung der Kontrolle war am Ende der Berichtsperiode noch nicht abgeschlossen.


Check-in 3
Zuschauerterrasse
Observation Deck

Eröffnung einer Untersuchung des fedpol betreffend die Tätigkeiten im Rahmen des SIRENE-Büros

Anfang 2018 wurden die Umsetzung und die Anwendung des Schengen-Besitzstands durch die Schweiz im Bereich Datenschutz überprüft. In diesem Zusammenhang eröffnete der Beauftragte, der zugleich die Funktion der nationalen Kontrollinstanz des N-SIS ausübt, eine Untersuchung zur Aufsicht über die Tätigkeiten des SIRENE-Büros des fedpol.

Gestützt auf den Vorschlag der Kommission gab der Rat der EU am 7. März 2019 eine Reihe von Empfehlungen im Hinblick auf die Beseitigung von Mängeln ab, die anlässlich der Evaluierung der Schweiz festgestellt wurden. Einige Empfehlungen betreffen den Beauftragten, namentlich jene, die sich auf seine Tätigkeit als Kontrollinstanz des SIS bezieht. Demnach wird der Beauftragte aufgefordert, die Rechtmässigkeit der Bearbeitungen von personenbezogenen Daten im Zusammenhang mit dem SIS häufiger zu prüfen und mindestens alle vier Jahre ein Audit über die Datenbearbeitungsvorgänge im nationalen Teil des SIS (N-SIS) durchzuführen.

Diese Inspektionen sollten sich nicht auf die Überprüfung der Logdateien beschränken, sondern auch auf andere datenschutzrelevante Aspekte der Struktur und der Funktionsweise des N-SIS ausgedehnt werden und Datenbearbeitungen des fedpol, das für das N-SIS verantwortlich ist, einschliesslich des SIRENE-Büros und des N-SIS-Servers, umfassen.

In diesem Zusammenhang und im Rahmen seiner Kontrolltätigkeit sowie als nationale Instanz für die Aufsicht über die Datei des N-SIS eröffnete der Beauftragte im Juni 2019 eine Kontrolle betreffend die Tätigkeiten des SIRENE-Büros des fedpol in Verbindung mit SIS-Ausschreibungen und mit dem Austausch von Zusatzinformationen zwischen dem SIRENE-Büro und entsprechenden ausländischen Amtsstellen.

Nach dem Versand eines Fragebogens über die allgemeinen Tätigkeiten des SIRENE-Büros liess sich der Beauftragte den Umgang mit einer Ausschreibung im System des SIRENE-Büros sowie den Austausch von Zusatzinformationen bei einem Besuch vor Ort zeigen.

Im Anschluss an seine Kontrolle befand der Beauftragte, dass das SIRENE-Büro bei der Bearbeitung von Daten betreffend Ausschreibungen und den Austausch von Zusatzinformationen die Datenschutzbestimmungen einhält, die im schweizerischen Recht für die durch das Schengener Durchführungsübereinkommen (DSÜ) vom 19. Juni 1990 abgedeckten Bereiche gelten, und dass es sich an das europäische Recht hält. Dementsprechend fällte der Beauftragte hierzu keine Beschlüsse und ergriff keine einschlägigen Massnahmen.

Seine Prüfung bezog sich auf:

- die Struktur und die Funktionsweise des N-SIS
- die Zusammensetzung des SIRENE-Büros und sein Informatiksystem SIRENE-IT
- die Gewährung und Ausübung der Zugriffsrechte im N-SIS
- die Kontrolle des Zugriffs der Mitarbeitenden des SIRENE-Büros auf das N-SIS
- die Aufgaben des SIRENE-Büros im Rahmen von Ausschreibungen im N-SIS und im Rahmen des Austauschs von Zusatzinformationen mit den entsprechenden Ämtern im Ausland sowie die Beschreibung der Aufgaben des Büros im Rahmen des Missbrauchs der Identität
- die Aufbewahrung der Ausschreibungen und Zusatzinformationen
- die Auskunfts-, Berichtigungs- und Löschungsrechte
- die Schulung und Sensibilisierung der Mitarbeitenden

Auf diese Weise konnte er die Empfehlung der Schengen-Evaluierung 2018 umsetzen und die Verpflichtungen aus Art. 44 der Verordnung SIS II[1] und aus Art. 60 des Beschlusses SIS II[2] erfüllen.

Eine zweite Kontrolle betreffend das Informatik Service Center des EJPD (ISC-EJPD), die sich spezifisch mit technischen und sicherheitsrelevanten Aspekten der Server befasst, wurde eröffnet.

[1] Verordnung (EG) Nr. 1987/2006 des Europäischen Parlaments und des Rates vom 20. Dezember 2006 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II) [Verordnung SIS II].

[2] Beschluss 2007/533/JI des Rates vom 12. Juni 2007 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II) [Beschluss SIS II].

Das Schengen-Datenschutzgesetz

Das Bundesgesetz über den Datenschutz im Rahmen der Anwendung des Schengen-Besitzstands in Strafsachen (SDSG) trat am 1. März 2019 in Kraft und mit ihm diverse Neuerungen, die unter anderem die bisherigen Zuständigkeiten des EDÖB betreffen (s. 26. TB, Kap. 1.2).

Das SDSG gilt insbesondere für die Bearbeitung von Personendaten durch Bundesorgane zur Verhütung und Verfolgung von Strafsachen im Rahmen der Anwendung des Schengen-Besitzstands. Angesichts der neuen Erfordernisse und des transversalen Charakters dieses neuen Gesetzes für die Tätigkeiten der betreffenden Bundesämter nahm der Beauftragte Kontakt mit den Datenschutzverantwortlichen der Bundesorgane auf, die potenziell unter den Geltungsbereich des SDSG fallen und an erster Stelle betroffen wären, insbesondere mit dem Bundesamt für Polizei (fedpol), dem Bundesamt für Justiz (BJ) im Bereich der internationalen Rechtshilfe in Strafsachen und mit der Bundesanwaltschaft, aber auch mit dem Staatssekretariat für Migration und der Eidgenössischen Zollverwaltung. Im Mittelpunkt standen dabei die Klärung des Geltungsbereichs und die Neuerungen, die sich aus diesem Gesetz ergeben. Der Meinungsaustausch bezog sich hauptsächlich auf die Datenbearbeitungsvorgänge und auf die Bundesorgane, die dem SDSG unterstellt sind, sowie auf die Zuständigkeiten des Beauftragten. Letzterer bleibt mit den betroffenen Bundesorganen im Hinblick auf die Umsetzung des SDSG in deren jeweiligem Tätigkeitsbereich in ständigem Kontakt.

Der EDÖB hat gemäss Artikel 21 SDSG die Aufgabe, die Anwendung der bundesrechtlichen Datenschutzvorschriften zu beaufsichtigen. Bevor er die Planung der Kontrollen nach Artikel 21 bis 25 SDSG an die Hand nimmt, möchte er sich einen Überblick über die Tätigkeiten verschaffen, die unter das SDSG fallen (Dateien/Informationssysteme).

Aus diesem Grund bat er das Bundesamt für Polizei (fedpol) und die Eidgenössische Zollverwaltung (EZV), uns eine Kopie des Verzeichnisses der Bearbeitungstätigkeiten gemäss Artikel 12 SDSG und, sofern sie vorliegen oder generiert werden können, nach Bearbeitungstätigkeit (Datei/Informationssystem) gegliederte statistische Angaben für die vergangenen fünf Jahre (2015 bis 2019) zu unterbreiten, unter anderem über die Anzahl der registrierten natürlichen oder juristischen Personen, die Staatsangehörigkeit der registrierten Personen und die Anzahl der Nutzer.

Zweiter Review Privacy Shield

Im September 2019 fand der zweite Swiss-US Privacy Shield Review in Washington D.C. statt. Dieser erfolgte im Anschluss an die dritte Überprüfung des EU-US Privacy Shield Rahmenwerks und zeigte weitere Fortschritte, aber auch Verbesserungspotenzial auf.

Seit Inkraftsetzung des Swiss-US Privacy Shield Rahmenwerks 2017 haben sich über 3300 Unternehmen dem Swiss-US Privacy Shield Programm angeschlossen, seit dem letzten Review (s. 26. TB, Kap. 1.2) ist die Anzahl um fast 1000 Zertifizierungen angestiegen. Bei über 70 Prozent der Mitglieder handelt es sich um KMU, aber auch Konzerne wie Facebook Inc. und Google LLC sind nach wie vor unter Privacy Shield zertifiziert (vgl. https://www.privacyshield.gov/list).

Im Berichtsjahr ist beim EDÖB ein Fall zur Weiterleitung an das US-Handelsministerium eingegangen. Es handelte sich hierbei um eine «false claim», also ein Unternehmen, das sich fälschlicherweise als Privacy Shield zertifiziert ausgibt. Der Fall konnte in Zusammenarbeit mit dem US-Handelsministerium (Departement of Commerce) gelöst werden (s. 26. TB, Kap. 1.2).

Weiter sind rund zehn berechtigte Beschwerden gegen zertifizierte Unternehmen bei privaten, unabhängigen Stellen für die alternative Streitbeilegung (ADR) eingereicht worden. Bezüglich den Zugriff auf Personendaten durch US Behörden zum Zweck der nationalen Sicherheit ist bei uns seit Inkraftsetzung des Rahmenwerks kein Fall eingegangen.

Seit der ersten jährlichen Überprüfung des Swiss-US Privacy Shield und der zweiten seitens der EU wurde die Funktionsweise des Rahmenwerks verbessert. So nimmt das US-Handelsministerium systematischere Überprüfungen der zertifizierten Unternehmen vor und prüft beispielsweise monatlich mit Stichproben, ob Unternehmen bestimmte im Rahmenwerk festgelegte Grundsätze einhalten. Auch wird die für die Durchsetzung zuständige Federal Trade Commission nun vermehrt von Amtes wegen tätig.

Weitere Fortschritte gegenüber dem letzten Berichtsjahr sind die Ernennungen für die Aufsichts- und Schlichtungsgremien. So wurden eine permanente Ombudsperson für das Rahmenwerk sowie die letzten zwei fehlenden Mitglieder des Privacy and Civil Liberties Oversight Board (Gremium zur Überwachung des Schutzes der Privatsphäre und der bürgerlichen Freiheiten) ernannt. Es verbleiben jedoch auch verbesserungswürdige Punkte: Für den EDÖB wie auch den Europäischen Datenschutzausschuss ist unklar, wie die Kompetenzen der Ombudsperson ausgestaltet sind. Der Wunsch nach Klärung wurde formuliert. Ebenso konnte die Divergenz bezüglich der Frage, was genau unter dem Begriff der HR-Daten zu verstehen sei, noch nicht bereinigt werden.

Eine gewisse Unsicherheit besteht derzeit wegen eines vor dem Gerichtshof der Europäischen Union (EuGH) hängigen Rechtsstreits über die Übermittlung von Daten zwischen der EU und den USA, der Auswirkungen auf das EU-US Privacy Shield Rahmenabkommen haben könnte. Auch wenn EuGH-Urteile für die Schweiz nicht anwendbar sind, wird der EDÖB mit Blick auf die analoge Ausgestaltung der Abkommen analysieren müssen, ob die Erwägungen des EuGH auch für die Beurteilung des Swiss-US Privacy Shield Rahmenabkommens relevant sein könnten.

1.3 Steuer- und Finanzwesen

Bekanntgabe von Personendaten an ausländische Steuerbehörden – problematische Ausdehnung auf weitere Staaten

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.

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. Das Schweizer AIA-Netzwerk soll auf 18 zusätzliche Partnerstaaten ausgeweitet werden, mit denen der AIA ab 2020/2021 umgesetzt werden soll, darunter befinden sich Staaten wie Ghana, Kasachstan, Libanon oder Nigeria. Wie bei den vorausgegangenen Ausdehnungen des AIA auf weitere Staaten wies der EDÖB auch im aktuellen Berichtsjahr mehrfach auf das Erfordernis der Gewährleistung eines angemessenen Datenschutzniveaus im jeweiligen Partnerstaat hin. Besteht ein solches nicht von Gesetzes wegen, muss der Datenschutz durch zureichende Datenschutzgarantien (vgl. Art. 6 Abs. 2 DSG) sichergestellt sein. Im Zusammenhang mit dem AIA wurden indessen gemäss unserer Einschätzung keine hinreichenden Garantien geschaffen (s. 26. TB, Kap. 1.3).

In einer Ämterkonsultation zum Entwurf einer Änderung des Bundesgesetzes über den AIA (AIAG) äusserte sich der EDÖB zur neu vorgesehenen Kompetenzregelung für den Fall, dass ein Partnerstaat die Anforderungen der OECD an die Vertraulichkeit und Datensicherheit nicht erfüllt. Er schlug mit Erfolg eine Neuformulierung vor, die klarstellt, dass bei Nichterfüllung der Anforderungen an die Vertraulichkeit und Datensicherheit die zuständige Schweizer Behörde den AIA gegenüber dem Partnerstaat nicht in eigener Kompetenz aussetzen kann, sondern aussetzen muss. Die Bundesversammlung hat die Vorlage des Bundesrats im Berichtsjahr noch nicht behandelt.

Austausch länderbezogener Berichte multinationaler Konzerne (ALBA)

Die Schweiz wird ab 2020 erstmals mit ihren Partnerstaaten länderbezogene Berichte multinationaler Konzerne austauschen (s. 24. TB, Kap. 1.9.1). Im Berichtsjahr äusserte sich der EDÖB im Rahmen einer Ämterkonsultation zur jüngst vorgesehenen Erweiterung der Länderliste der Partnerstaaten für die Aktivierung des Austauschs von länderbezogenen Berichten multinationaler Konzerne. Dabei wies er darauf hin, dass die Erweiterung Staaten und Territorien betrifft, die auf der Staatenliste des EDÖB mit einem ungenügenden Datenschutzniveau aufgeführt sind (so etwa Armenien, Bosnien und Herzegowina sowie die Cook-Inseln). Der EDÖB hielt deshalb wie bereits bei früheren Ämterkonsultationen fest, dass mit Blick auf solche Länder zusätzliche Garantien nach Art. 6 Abs. 2 DSG notwendig sind, um ein angemessenes Datenschutzniveau zu gewährleisten (s. 26. TB, Kap. 1.3).

Das Bundesverwaltungsgericht heisst die Beschwerde des Beauftragten im ESTV-Fall gut: Betroffene Dritte haben das Recht auf vorgängige Information

Das Bundesverwaltungsgericht hiess eine Beschwerde des EDÖB zum Recht auf Information in der internationalen Steueramtshilfe gut. Das diesbezügliche Beschwerdeverfahren vor Bundesgericht wurde vorläufig sistiert.

Ende Dezember 2017 erliess der EDÖB eine formelle Empfehlung, wonach die Eidgenössische Steuerverwaltung (ESTV) in der internationalen Steueramtshilfe auch die vom Amtshilfeersuchen nicht betroffenen Personen (d.h. Drittpersonen), deren Namen ungeschwärzt an die ersuchende ausländische Behörde übermittelt werden sollen, vorgängig zu informieren hat (s. 25. TB, Kap. 1.9.2). Die ESTV lehnte diese Empfehlung ab, worauf der EDÖB die Angelegenheit zuerst dem Eidgenössischen Finanzdepartement (EFD) vorlegte und dann dessen ablehnende Verfügung an das Bundesverwaltungsgericht weiterzog (s. 26. TB, Kap. 1.3).

Das Bundesverwaltungsgericht gelangte in seinem Urteil vom 3. September 2019 zum Schluss, dass in der internationalen Steueramtshilfe die vom Amtshilfeersuchen nicht betroffenen Personen (Drittpersonen), deren Daten ungeschwärzt übermittelt werden sollen, grundsätzlich vorgängig zu informieren sind. Für Fälle, in welchen mit der erforderlichen Information unverhältnismässiger Aufwand verbunden ist und der Vollzug der Amtshilfe verunmöglicht oder unverhältnismässig verzögert würde, sind gemäss Bundesverwaltungsgericht Ausnahmeregelungen zu erarbeiten. Der EDÖB begrüsst das Urteil, da es die Grundrechte der Bank-Mitarbeitenden und weiterer Drittpersonen schützt. Er ist bereit, mit der ESTV nach praktischen Lösungen zur Umsetzung des Urteils zu suchen, was er anlässlich eines Treffens mit der ESTV Ende 2019 bekräftigt hat.

Die ESTV hat beim Bundesgericht Beschwerde erhoben. Aktuell ist das Verfahren auf deren Antrag hin sistiert, da das Urteil vom Entscheid in einem anderen Rechtsstreit beeinflusst werden kann. Der Beauftragte hat im Berichtsjahr keine Gelegenheit erhalten, von der gegnerischen Beschwerdeschrift Kenntnis zu nehmen.

1.4 Handel und Wirtschaft

Fehlerhafte Datenbankeinträge bei Inkassounternehmen

Der EDÖB hat bei einer führenden Inkassofirma eine Sachverhaltsabklärung wegen angeblich fehlerhafter Einträge eröffnet.

Durch Bürgeranfragen und Medienberichte wurde der EDÖB auf ein Unternehmen aufmerksam, welches Bonitäts- und Kreditauskünfte sowie Inkassodienstleistungen anbietet. Angeblich soll es dort aufgrund von fehlerhaften Datenbankeinträgen zu Verwechslungen von Personen mit gleichen oder ähnlichen Namen beziehungsweise Adressen kommen.

Als Folge davon sollen Zahlungsaufforderungen an falsche Personen verschickt oder unzutreffende negative Bonitätsinformationen gespeichert und bekannt gegeben worden sein. Auch wurde über Schwierigkeiten bei der Korrektur solcher Fehleinträge berichtet. Um diesen Vorhaltungen nachzugehen, hat der Beauftragte im Februar 2020 eine Sachverhaltsabklärung eingeleitet. Diese war zum Ende des Berichtsjahres noch im Gang.

Verwendung der Daten von ricardo.ch innerhalb der Tamedia-Gruppe (TX Group)

Der EDÖB hat die Sachverhaltsabklärung bezüglich der Verwendung der auf der Plattform ricardo.ch erhobenen Daten fortgesetzt, insbesondere innerhalb der Tamedia-Gruppe (TX Group).

Im Juli 2017 hatten wir ein Verfahren zur Abklärung des Sachverhalts eröffnet, um die Transparenz und die Konformität der Bearbeitungen von Daten der Nutzerinnen und Nutzer von ricardo.ch innerhalb der Tamedia-Gruppe sowie die Möglichkeit zu prüfen, der Nutzung von Daten zum Zweck der gezielten Werbung zu widersprechen (s. 25. TB, Kap. 1.8.8).

Die Sachlage hat seit Beginn der Abklärung erhebliche Veränderungen erfahren; unter anderem führte das Inkrafttreten der europäischen Datenschutzgrundverordnung zu einer Anpassung der Datenschutzerklärung (s. 26. TB, Kap. 1.4). Weitere Änderungen folgten im Mai 2019 und im Februar 2020.

Personendaten, die auf der Online-Auktionsplattform ricardo.ch gesammelt werden, werden von der Tamedia AG (inzwischen TX Group AG) unter anderem zu Marketingzwecken (zielgruppenspezifische Werbung) bearbeitet, analysiert und zusammengeführt. Folglich haben wir unser Abklärungsverfahren formell auf die Tamedia AG ausgedehnt. Wir reichten unsere Sachverhaltsfeststellung erneut zur Prüfung ein und nahmen einige Anpassungen vor. Unsere rechtliche Beurteilung des Sacherhalts wird gestützt auf die entsprechend festgestellten Tatsachen erfolgen.

Fehlerhafte Adressen bei der Serafe AG – Massnahmen zur Datenrichtigkeit nötig

Die Serafe AG hat im Berichtsjahr tausende fehlerhafte Rechnungen verschickt. Das Unternehmen hat die Problematik erkannt und erste Massnahmen getroffen. Der EDÖB prüft, ob aus datenschutzrechtlicher Sicht weitere Empfehlungen nötig sind.

Seit Anfang 2019 ist die Serafe AG die schweizerische Erhebungsstelle für die Radio- und Fernsehabgabe. Nach einem öffentlichen Ausschreibungsverfahren hat ihr das Eidgenössische Departement für Umwelt, Verkehr, Energie und Kommunikation (UVEK) das Mandat bis Ende 2025 erteilt.

Gemäss Meldungen von betroffenen Personen an den EDÖB und verschiedenen Medienberichten hat die Serafe AG im Berichtsjahr Tausende fehlerhafte Rechnungen verschickt. Die Rechnungen wurden beispielsweise an veraltete Zustelladressen oder an die falschen Adressaten geschickt oder den Empfängern mehrfach zugestellt. Angeblich seien die für die Erhebung der Haushaltabgabe nötigen Daten aus den Einwohnerregistern von den Kantonen und Gemeinden zum Teil fehlerhaft geliefert worden. Die Problematik sei jedoch erkannt und Massnahmen getroffen worden, um in Zukunft die Datenrichtigkeit zu gewährleisten.

Der Beauftragte hat die Serafe AG um Stellungnahme gebeten. Aufgrund der Antworten wird er prüfen, ob er eine datenschutzrechtliche Abklärung vornehmen und den Verantwortlichen gegebenenfalls weitere Massnahmen empfehlen soll, um die gesetzeskonforme Datenbearbeitung sicherzustellen.

Analyse von Transaktionsdaten zu Planungszwecken

Eine Handelsfirma ersuchte den EDÖB um Beratung betreffend die Auswertung ihrer Kundentransaktionsdaten für nicht personenbezogene Zwecke. Wir haben dieses Vorhaben im Rahmen unserer beratenden Tätigkeit aus technischer und aus juristischer Sicht beurteilt.

Die Handelsfirma, die im Einzelhandel tätig ist und mehrere Geschäfte in der Schweiz betreibt, stellte uns ihr Projekt vor, dessen Ziel es ist, im Rahmen der betrieblichen Planung die Transaktionsdaten ihrer Kundschaft zu nicht personenbezogenen Zwecken zu verwenden.

Beim vorgelegten Konzept ging es darum, einerseits die von der Firma erfassten Daten im Zeitpunkt der Transaktion zu nutzen sowie andererseits die vom Zahlungsdienstleister erfassten Daten zu verarbeiten. Anhand der Verknüpfung der beidseits verfügbaren Daten liessen sich die Transaktionen verfolgen, die von einer bestimmten Zahlkarte ausgehen, und es könnte ein längerfristiges Konsumprofil (Querschnittsprofil) angelegt werden; ein derartiges Profil kann die Firma anhand der ihr zur Verfügung stehenden Daten nicht erstellen. Die Handelsfirma betonte, dass die Analyse ausdrücklich zu Zwecken erfolgen würde, die nicht personenbezogen sind (insbesondere keine gezielte Werbung).

Da die Handelsfirma die Zahlkartendaten nicht erfasst, bedürfte es einer vorgängigen Übermittlung dieser Daten durch den Zahlungsdienstleister. Dazu sah das vorgelegte Konzept vor, die Nummer der Zahlkarte vorgängig durch einen eindeutigen Identi-

fikator («Token») zu ersetzen, der durch ein Hash-Verfahren generiert wird (Pseudonymisierung).

In Ausübung unserer Beratungsfunktion beurteilten wir die vorgelegten Unterlagen aus technischer und juristischer Sicht und kamen zum Schluss, dass sowohl die Datenverarbeitung durch den Zahlungsdienstleister als auch jene durch die Handelsfirma dem DSG unterworfen sind, da es sich in beiden Fällen bei den bearbeiteten Daten in der Tat um Personendaten handelt. Die Festlegung eines eindeutigen Identifikators, die mittels einer Hashfunktion erfolgt, erschwert die Bestimmbarkeit der Daten und ermöglicht eine Minimierung der Persönlichkeitsverletzung; dies gemäss dem Prinzip der Verhältnismässigkeit und der Sicherheit. Die übrigen allgemeinen Grundsätze des Datenschutzes, etwa das Prinzip der Zweckbestimmung und das Öffentlichkeitsprinzip, sind ebenfalls anwendbar.

Die Übermittlung der Daten durch den Zahlungsdienstleister ist als Änderung der Zweckbestimmung gegenüber dem ursprünglichen Zweck der Datenbearbeitung (der Durchführung der Zahlungsdienstleistung) zu werten. Für eine derartige Änderung der Zweckbestimmung bedarf es eines Rechtfertigungsgrunds; im vorliegenden Fall ist es die freiwillige Einwilligung nach angemessener Information des betroffenen Kunden. Was die technischen Vorkehrungen anbelangt, hielten wir fest, dass zur Gewährleistung der Sicherheit eine Hashfunktion mit Salt oder geheimem Schlüssel notwendig ist.

Für die Handelsfirma gilt, dass sie sich unserer Auffassung nach auf Art. 13 Abs. 2 lit. e DSG berufen und ein überwiegendes privates Interesse geltend machen kann, solange sie sich an die angeführten Bedingungen hält: Die Personendaten dürfen nur zu Zwecken verarbeitet werden, die nicht personenbezogen sind, im Rahmen der Forschung, der Planung oder der Statistik. Zudem müssen die Ergebnisse in einer Form veröffentlicht werden, die die Identifizierung der betroffenen Personen verunmöglicht. Im konkreten Fall bedeutet dies, dass die Erkenntnisse aus Profilanalysen nicht unter Verweis auf diesen Rechtfertigungsgrund für gezielte Werbung eingesetzt werden dürfen; die Handelsfirma darf sie ferner auch nicht mit anderen personenbezogenen Daten verknüpfen, über die sie allenfalls verfügt (Kundenkarte, E-Shop u.ä.). Für eine derartige Nutzung wäre angesichts des durchgeführten Profilings die ausdrückliche Einwilligung der betroffenen Personen erforderlich.

Die Handelsfirma hat unsere Beurteilung zur Kenntnis genommen und wird uns gegebenenfalls über die Umsetzung des Projekts informieren.

Sportwarenhändler Decathlon informierte mangelhaft über Datenbeschaffung

Im Rahmen einer Sachverhaltsabklärung forderte der Beauftragte von Decathlon eine verbesserte Kundeninformation bei der Datenbeschaffung. Der Sportwarenhändler hat seine Datenschutzerklärung überarbeitet.

Im Jahr 2018 eröffneten wir beim Sportwarenhändler Decathlon eine Sachverhaltsabklärung, nachdem wir aus unterschiedlichen Quellen 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 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. Dies veranlasste den EDÖB, sich der Frage zuzuwenden, ob die Freiwilligkeit für die Kundschaft denn auch tatsächlich erkennbar sei und diese bei der Datenbeschaffung angemessen informiert würde. Da die Informationen von Decathlon uneinheitlich und zu wenig klar formuliert waren, unterbreitete der EDÖB dem Sportwarenhändler Vorschläge für eine Verbesserung der Information (s. 26. TB, Kap. 1.4). Decathlon hat sämtliche Hinweise des EDÖB berücksichtigt und die Überarbeitung seiner Datenschutzerklärung abgeschlossen.

Authentifizierung mit Stimmerkennung bei der PostFinance AG

Im Berichtsjahr ist die PostFinance AG an den EDÖB herangetreten und hat ihm ihr Projekt zur Stimmerkennung in ihrem Kontaktcenter vorgestellt. Der Beauftragte wies das Unternehmen darauf hin, dass Stimmabdrücke als biometrische Daten über einzelne Personen ein erhöhtes Risiko bergen und deshalb besonders geschützt werden müssten.

Die PostFinance AG hat dem EDÖB im Berichtsjahr ein Vorhaben präsentiert, das bezweckt, Anrufende im Kontaktcenter mittels Stimmerkennung zu identifizieren. Die Identität des Anrufenden wird dabei anhand eines Abgleichs mit einem aufgezeichneten Stimmabdruck verifiziert. Die PostFinance AG hat betont, dass die erhobenen Stimmabdrücke einzig und ausschliesslich zur Authentifizierung der Kunden am Telefon verwendet würden. Sie hätte aktuell keine Absichten, diese Daten für weitergehende Analysen zu nutzen.

Im Gegensatz zur Datenschutzgrundverordnung der EU (DSGVO) sind im schweizerischen DSG biometrische Daten nicht bei den besonders schützenswerten Personendaten aufgeführt – dies obwohl deren Bearbeitung mit besonderen Risiken verbunden ist. Biometrische Merkmale sind untrennbar mit einer bestimmten Person verbunden und können nach einer Panne oder einem Missbrauch im Gegensatz zu Passwörtern nicht ausgewechselt werden. Aufgrund des technischen Fortschritts von Stimm- und Gesichtserkennungsprogrammen (s. Kap. 1.1, Beitrag zu Clearview) und der dadurch gestiegenen Risiken für die Persönlichkeitsrechte der betroffenen Personen muss die Bearbeitung von biometrischen Daten unter Anwendung solcher Technologien einen erhöhten datenschutzrechtlichen Schutz gewährleisten. In den Fällen, bei denen gemäss DSG eine Einwilligung vorliegen muss, ist diese deshalb nach Auffassung des EDÖB ausdrücklich einzuholen, bevor eine Datenbeschaffung erfolgen darf. Der verantwortliche Dateninhaber muss zudem vorab transparent und ausführlich über die Datenbearbeitung informieren.

Der EDÖB hat von der PostFinance AG im Rahmen seiner Beratungstätigkeit ein entsprechendes Vorgehen verlangt, und das Unternehmen hatte dies zunächst so umgesetzt. Die PostFinance AG hat den Prozess jedoch zu einem späteren Zeitpunkt geändert und gewährt den Schweizer Kundinnen und Kunden seither nur ein sog. Opt-Out. Damit wird die Stimmerkennung bei diesen Anrufenden grundsätzlich eingesetzt, ausser sie sprechen sich explizit dagegen aus.

Wir haben die PostFinance AG daraufhin um eine schriftliche Stellungnahme gebeten, zumal wir festgestellt haben, dass bei ausländischen Kunden weiterhin erst nach deren ausdrücklichen Zustimmung eine Stimmerkennung vorgenommen wird – also mittels Opt-In. Das Unternehmen hat in seiner Stellungnahme bestätigt, dass es nach Einholung einer Drittmeinung im Rahmen einer erneuten Prüfung der rechtlichen Konformität Ende 2018 den Prozess angepasst hätte. Demnach würden die Schweizer Kundinnen und Kunden mittels einer automatischen Ansage über die Aufzeichnung ihres Stimmabdrucks informiert. Wenn die Kunden mit der Erstellung ihres Stimmabdrucks nicht einverstanden seien, müssten sie selber aktiv werden und ihre Ablehnung dem Kundenberater mitteilen oder die Funktion zu einem späteren Zeitpunkt in ihrem E-Finance-Portal deaktivieren. Bei Auslandkunden könne gemäss der PostFinance AG nicht ausgeschlossen werden, dass für sie strengere Datenschutzregeln zu Anwendung gelangen, wie namentlich die DSGVO, weshalb bei diesen weiterhin eine vorgängige explizite Einwilligung eingeholt würde.

Der EDÖB hat die Ausführungen der PostFinance AG zur Kenntnis genommen und öffentlich auf die Notwendigkeit einer baldigen Anhebung des Datenschutzniveaus für die Schweizer Bevölkerung hingewiesen. Solange die Totalrevision des DSG nicht in Kraft tritt (s. Schwerpunkt I), können Schweizer Kunden offenbar nicht darauf zählen, dass alle hiesigen Unternehmen davon absehen, sie schlechter zu stellen als ausländische Kunden.

Videoüberwachung mit intelligenten Kameras bei Migros

Die Migros hat im Berichtsjahr versuchsweise ein neues Kamerasystem zur Überwachung ihrer Ladenflächen eingeführt. Der EDÖB prüft die Datenschutzkonformität.

Der EDÖB wurde durch Medienberichte darauf aufmerksam, dass die Migros neuartige Überwachungskameras im Einsatz habe. Auf Nachfrage hin gab die Migros bekannt, dass sie in bestimmten Filialen ein neues System in einem Pilotprojekt prüfe. Die eingesetzte Software erlaube es, im Ereignisfall Kunden anhand von bestimmten Erscheinungskriterien zu analysieren und die relevanten Videosequenzen zu eruieren. Mit den neuen Kameras werde aber keine Gesichtserkennung vorgenommen.

Für den EDÖB stellen sich im Hinblick auf eine datenschutzkonforme Ausgestaltung solcher Systeme verschiedene Fragen. Von zentraler Bedeutung sind namentlich die Transparenz gegenüber den betroffenen Personen und die Gewährleistung von hohen Sicherheitsstandards bei der Datenbearbeitung. Im Anschluss an seine Vorabklärungen eröffnete der EDÖB eine Sachverhaltsabklärung, um das System vertieft zu prüfen und gegebenenfalls datenschutzrechtliche Empfehlungen zu erlassen. Diese Untersuchung war zum Ende des Berichtjahres noch im Gang.

1.5 Gesundheit

Intensivierte Kontakte im Hinblick auf die Einführung des elektronischen Patientendossiers

Ab dem 15. April 2020 sollte Bürgerinnen und Bürgern schweizweit ein elektronisches Patientendossier (EPD) zur Verfügung stehen. Aufgrund der bevorstehenden Einführung hat sich der EDÖB im Berichtsjahr erneut vertieft damit beschäftigt – namentlich mit den Anbietern, den sog. Stammgemeinschaften.

Mit dem EPD können Privatpersonen über ihre persönlichen Gesundheitsdaten wie bspw. Krankheiten oder einzunehmende Medikamente in digitaler Form verfügen und selber bestimmen, wer diese einsehen darf. Die per 15. April 2020 geplante Einführung des elektronischen Patientendossiers führe zu erneut ansteigenden Bürgeranfragen an den EDÖB. Zudem verstärkten wir unsere Koordinationsbemühungen mit den kantonalen Datenschutzbeauftragten und wirkten bei diversen Fachveranstaltungen mit.

Aufgrund der Wichtigkeit und Aktualität des Themas hat sich der EDÖB zudem von einer der grössten Stammgemeinschaften in der Schweiz aus erster Hand über den Stand der Arbeiten, die Umsetzung und die Schwierigkeiten bei der Einführung des EPD informieren lassen. Diese Körperschaften sind gemäss Gesetz exklusiv befugt, das EPD anzubieten, und stehen unter Aufsicht des EDÖB, während die zumeist kantonalen Institutionen wie Spitäler von den kantonalen Datenschutzbeauftragten beaufsichtigt werden. Der EDÖB verschaffte sich so einen Überblick über die Aufbauarbeiten sowie die komplexen technischen Abläufe und Instrumente, die für den Betrieb des EPD nötig sind. Dabei zeigte sich, dass nicht nur der Aufbau der Stammgemeinschaften technisch anspruchsvoll ist, sondern auch der Zertifizierungsprozess mit einem hohen Aufwand verbunden ist, den die Stammgemeinschaften sowie die Herausgeber der Identifikationsmittel für die elektronische Identität im EPD durchlaufen müssen.

Nach Auskunft der zuständigen Stellen wird sich der Roll-Out bis Sommer 2020 verzögern. Der EDÖB wird die Entwicklung weiterhin verfolgen und diesbezügliche Kontrollaktivitäten ins Auge fassen, sobald die Stammgemeinschaften ihren Betrieb aufgenommen haben.

Bonusprogramm Helsana+ – Umsetzung des Bundesverwaltungsgerichtsurteils

Das Bundesverwaltungsgericht beurteilte im Jahr 2019 bestimmte Datenbearbeitungen als rechtswidrig, die im Rahmen des Bonusprogramms Helsana+ durch den Versicherer vorgenommen wurden. Der EDÖB stand im Berichtsjahr mehrmals in Kontakt mit Helsana um sicherzustellen, dass das Urteil vollständig umgesetzt wird und dass auch zukünftige Anpassungen der Nutzungsbestimmungen den datenschutzrechtlichen Anforderungen gerecht werden.

Mit Urteil vom 19. März 2019 qualifizierte das Bundesverwaltungsgericht die in der ursprünglichen Ausgestaltung erfolgte Datenbeschaffung beim Grundversicherer mangels rechtsgültiger Einwilligung als rechtswidrig (s. 26. TB, Kap. 1.5). In seinen Erwägungen stellte das Gericht gewisse Mängel der Nutzungs- und Datenschutzbestimmungen von Helsana+ fest, welche nach Auffassung des EDÖB unabhängig von der Frage der rechtsgültigen Einwilligung bestehen.

Nach Inkrafttreten des Urteils verlangte der EDÖB deshalb vom Versicherer, die festgestellten Defizite der Nutzungs- und Datenschutzbestimmungen von Helsana+ zu beseitigen, damit die Bestimmungen die Anforderungen an Transparenz und Verständlichkeit erfüllen.

Der Versicherer hat die Nutzungsbestimmungen des Bonusprogramms in der Zwischenzeit einer umfassenden Überarbeitung unterzogen. Insbesondere mit Blick auf die neuen Regelungen ist der EDÖB weiterhin im Austausch mit dem Versicherer, um die datenschutzkonforme Umsetzung der Datenbearbeitungen sicherzustellen.

«Swiss National Cohort»: weiterführende Schutzmassnahmen erforderlich

Das Projekt «Swiss National Cohort» (SNC) hat an Umfang zugenommen. Damit entstehen nunmehr Verknüpfungen in einem Ausmass, das die Anonymität der bearbeiteten Daten nicht mehr gewährleistet: Ein Ausbau des Vertraulichkeitsdispositivs drängt sich auf.

Gemeinsam mit dem Bundesamt für Statistik (BFS) lancierten das Institut für Epidemiologie, Biostatistik und Prävention (EBPI) der Universität Zürich und das Institut für Sozial- und Präventivmedizin (ISPM) der Universität Bern bereits 2006 die erste Kohorte, die die gesamte Schweizer Bevölkerung langfristig abbildet, und schufen damit eine vielseitige Forschungsplattform. Auf Ersuchen des ISPM nahmen wir zur Frage der Einhaltung datenschutzrechtlicher Bestimmungen durch die SNC Stellung. Dies unter Beachtung sowie vorbehaltlich der Befugnisse der betroffenen kantonalen Datenschutzbehörden.

Auf diese Weise konnten wir feststellen, dass die technischen und organisatorischen Massnahmen geeignet waren, die Sicherheit und Genauigkeit der Daten zu garantieren. Im Unterschied zu den früheren Projektphasen stellten wir hingegen fest, dass umfangreiche und zahlreiche Personendaten, einschliesslich Gesundheitsdaten, nunmehr verknüpft werden, wodurch eine Anonymisierung verunmöglicht wird. Dementsprechend empfahlen wir den Projektträgern, mittels zusätzlicher Schutzvorkehrungen für die Vertraulichkeit der Daten der betroffenen Personen zu sorgen.

Untersuchung zu IQOS, die elektronische Zigarette der neuen Generation von Philip Morris

Bei IQOS, den E-Zigaretten von Philip Morris, entstehen weder Verbrennung noch Asche, dafür aber jede Menge Daten. Der Beauftragte prüfte, ob deren Bearbeitung datenschutzkonform ist.

Während der Markt für E-Zigaretten derzeit weiter an Fahrt gewinnt und das Parlament über ein Bundesgesetz über Tabakprodukte und elektronische Zigaretten (TabPG) berät, entwickelte der Hersteller Philip Morris in den letzten Jahren mit IQOS ein neues Produkt, das aus Tabaksticks, «Heets» genannt, und einem Heizelement besteht, welches den Tabak erhitzt, aber nicht verbrennt. Zudem lassen sich bei IQOS via Bluetooth-Verbindung Daten des Systems exportieren. Folglich ist IQOS nicht nur eine E-Zigarette, sondern auch ein smarter Gegenstand. Nachdem in mehreren Presseartikeln Bedenken hinsichtlich des Schutzes der mit IQOS gesammelten Daten laut wurden, leitete unsere Behörde am 11. Juli 2019 ein Verfahren zur Sachverhaltsabklärung ein, um zu prüfen, inwiefern die Nutzung der mit IQOS erzeugten Daten einen Eingriff in die Privatsphäre der Konsumenten in der Schweiz darstellt.

Im Mittelpunkt unserer Untersuchung stand die Frage, ob die gesetzlichen Vorschriften bezüglich Information, Einwilligung und grenzüberschreitende Übermittlung von Daten, sowohl innerhalb als auch ausserhalb des multinationalen Unternehmens, eingehalten werden.

Wir konnten feststellen, dass die von Philip Morris getroffenen technischen und organisatorischen Vorkehrungen ausreichen, um den Schutz der Personendaten von Nutzerinnen und Nutzern in der Schweiz zu gewährleisten.

1.6 Arbeit

Zeiterfassung und Tracking mit Apps im Arbeitsbereich

Smartphones werden zunehmend auch betrieblich eingesetzt, etwa mithilfe von Apps zur Arbeitszeiterfassung oder zur Aufzeichnung der während der Arbeit zurückgelegten Wege. Eine datenschutzkonforme Ausgestaltung verlangt insbesondere, dass sich die Datenbearbeitung auf das Notwendige beschränkt und dass die Mitarbeitenden angemessen informiert werden.

Im Berichtsjahr nahmen Anfragen aus der Bevölkerung zu mobilen Anwendungen im Arbeitsbereich wiederum zu. Zeiterfassung, GPS-Tracking, Zugriff auf die geschäftlichen E-Mails – es gibt kaum Bereiche des Arbeitslebens, die nicht auch über das Handy bearbeitet werden können. Das mobile Büro in der Hosentasche bringt neben Vereinfachungen im Arbeitsalltag auch einige datenschutzrechtliche Herausforderungen mit sich, zumal sich nicht wenige dieser technischen Funktionen zusätzlich zur Überwachung der Mitarbeitenden einsetzen lassen.

Ein datenschutzkonformer Einsatz mobiler Apps im Arbeitsbereich bedingt, dass der Arbeitgeber nur diejenigen Personendaten seiner Angestellten bearbeitet, welche für die Durchführung des Arbeitsverhältnisses notwendig sind. Weiter müssen stets die Bearbeitungsgrundsätze des DSG beachtet werden, wie die Verhältnismässigkeit und die Transparenz. Insbesondere beim letztgenannten Punkt beobachten wir oftmals insofern Mängel, als die Mitarbeitenden häufig nicht angemessen über den Einsatz oder den Zweck von Überwachungsmassnahmen orientiert werden.

Ein weiteres anspruchsvolles Thema sind die technischen und organisatorischen Massnahmen, welche einen Missbrauch der Daten und Zugriffe durch Unbefugte – auch innerhalb des Unternehmens – verhindern sollten. Und schliesslich ist häufig unklar, was etwa mit erfassten Daten eines GPS-Trackings nach Arbeitsende oder während der Pausen geschieht – solche Datenbearbeitungen verletzen grundsätzlich die Privatsphäre der Mitarbeitenden. Entsprechend häufig fragten Betroffene unsere Behörde in diesem Zusammenhang um Rat.

Die Problematik rund um mobil genutzte Funktionen des Arbeitslebens ist noch zusätzlich verschärft, wenn dasselbe Smartphone für private und berufliche Zwecke verwendet wird. Hier stellt sich insbesondere die Frage, wie bei der Beendigung des Arbeitsverhältnisses korrekterweise vorgegangen werden soll.

Der EDÖB verfolgt die Entwicklungen im Bereich der mobilen Applikationen im Arbeitsalltag weiterhin aufmerksam und hat hierzu auch eine Sachverhaltsabklärung eingeleitet (s. Box).

Sachverhaltsabklärung im Bereich Zeiterfassung

Der EDÖB hat bei einem grossen Unternehmen im Bereich Gebäudereinigung und -unterhalt eine Sachverhaltsabklärung eingeleitet. Das Unternehmen beschäftigt eine grosse Zahl von Mitarbeitenden und hat die Arbeitszeiterfassung vor Kurzem weitgehend digitalisiert. Bei der nunmehr internetbasierten Registrierung der Arbeitszeiten stellen sich verschiedene datenschutzrechtliche Fragen, vor allem in Bezug auf die Datensicherheit, Zugriffsregelungen und die Datenflüsse innerhalb des Unternehmens sowie auch an allfällige Dritte. Der EDÖB wird nach Abschluss des Verfahrens über die Ergebnisse der Sachverhaltsabklärung informieren.

Einsatz von künstlicher Intelligenz im Bewerbungsverfahren

Künstliche Intelligenz (KI) kommt immer häufiger auch bei Bewerbungsverfahren zum Zug. Der Eingriff in die Persönlichkeitsrechte wiegt dabei regelmässig schwerer als bei konventionellen Anstellungsprozessen.

Mehrere Medienberichte und Anfragen im Berichtsjahr lassen den Schluss zu, dass auch hierzulande im Rahmen von Bewerbungsverfahren vermehrt auf künstliche Intelligenz (KI) zurückgegriffen wird. Dabei werden beispielsweise Bewerbungsgespräche auf Video aufgezeichnet und durch eine Software analysiert.

Der datenschutzrechtliche Rahmen beim Einsatz dieser neuen Instrumente ist zunächst derselbe wie bei konventionellen Bewerbungsverfahren: Der Arbeitgeber darf nur jene Daten erheben und bearbeiten, welche für die Abklärung der Eignung einer Person für die betreffende Stelle benötigt werden, und er muss sich stets an die datenschutzrechtlichen Prinzipien halten.

Angesichts der Fülle von Analysemöglichkeiten, die sich durch die KI-gestützten Prozesse bieten, wiegen die Eingriffe in die Persönlichkeitsrechte tendenziell schwerer als bei konventionell geführten Bewerbungsgesprächen. Aus diesem Grund muss insbesondere den Prinzipien der Erkennbarkeit und der Verhältnismässigkeit besondere Beachtung geschenkt werden.

Abklärungen beim Eidgenössischen Personalamt (EPA) haben ergeben, dass der Bund bei seinen Bewerbungsverfahren derzeit noch nicht auf künstliche Intelligenz zurückgreift. Sollte dies zukünftig geplant sein, wird sich der EDÖB frühzeitig einbringen und einen massvollen und datenschutzkonformen Einsatz der entsprechenden Technologien fordern.

1.7 Versicherungen

Neue rechtliche Bestimmungen zu den Observationen im Bereich der Sozialversicherungen in Kraft

Die neuen gesetzlichen Grundlagen für die Überwachung von Versicherten wurden in das Bundesgesetz über den Allgemeinen Teil des Sozialversicherungsrechts (ATSG) übernommen und traten mit den dazugehörigen Verordnungsbestimmungen auf den 1. Oktober 2019 in Kraft. Im Berichtsjahr berieten wir Rechtssuchende, die sich betreffend Überwachung an uns wandten.

Mit dem sog. Observationsartikel wurde im Berichtsjahr die Überwachung im Sozialversicherungsbereich neu geregelt. Mit den Artikeln 43a und 43b des Bundesgesetzes über den Allgemeinen Teil des Sozialversicherungsrechts (ATSG) und den dazugehörigen Ausführungsbestimmungen der Verordnung in den Artikeln 7a – 9b ATSV traten die entsprechenden rechtlichen Grundlagen auf den 1. Oktober 2019 in Kraft.

Diese regeln die Voraussetzungen und die zulässigen Mittel einer verdeckten Observation von versicherten Personen, bei denen ein Verdacht auf Versicherungsmissbrauch besteht. Der Erlass von rechtlichen Bestimmungen in diesem Bereich war nötig geworden, nachdem der Europäische Gerichtshof für Menschenrechte (EGMR) in Strassburg in seinem Urteil «Vukota-Bojic gegen Schweiz» vom 18. Oktober 2016 (Beschwerde Nr. 61838/10) festgehalten hatte, dass in der Schweiz eine ausreichende gesetzliche Grundlage für den Einsatz von Privatdetektiven im Bereich der Sozialversicherungen fehle. Somit verstiessen gemäss Auffassung des EGMR die Überwachungsmassnahmen von Versicherungen gegen das Recht auf Privatleben, das durch Artikel 8 der Europäischen Menschenrechtskonvention (EMRK) geschützt ist.

Weil der Beauftragte bei derartigen Observationen den Schutz der Privatsphäre wesentlich tangiert sieht, brachte er sich früh in den Gesetzgebungsprozess ein. Er forderte unter anderem, dass eine Observation nur durch eine Person mit Direktionsfunktion im fallbearbeitenden Bereich bzw. im Leistungsbereich des jeweils zuständigen Versicherungsträgers angeordnet werden darf. Weiter verlangte er, dass die Dauer der Überwachung gesetzlich begrenzt sein muss. Beide Aspekte fanden Eingang in den Artikel 43a ATSG. Vor dieser Gesetzesänderung konnten Privatdetektive zwecks Observationen nur in der Invalidenversicherung (IV) und der Unfallversicherung (UV) eingesetzt werden.

Observationen sind neu auch in den übrigen Sozialversicherungszweigen möglich: in der Arbeitslosenversicherung (ALV), der obligatorischen Krankenversicherung (KV), der Militärversicherung (MV), bei den Ergänzungsleistungen (EL), beim Erwerbsersatz für Dienstleistende und bei Mutterschaft (EO) sowie in der Alters- und Hinterlassenenversicherung (AHV). Da etliche dieser Versicherungen durch kantonale Stellen durchgeführt werden und diese dementsprechend Observationen anordnen können, werden diese Überwachungstätigkeiten von den jeweiligen kantonalen Datenschutzbeauftragten beaufsichtigt. Der EDÖB ist demgegenüber für die Aufsicht und Beratung in datenschutzrechtlichen Fragen bei der UV, KV und MV zuständig und somit für Observationen, die im Rahmen dieser Sozialversicherungen angeordnet werden.

Gesetzesvorlage zur systematischen Verwendung der AHV-Nummer

Am 30. September 2019 unterbreitete der Bundesrat den Eidgenössischen Räten eine Botschaft zu einer Änderung des AHV-Gesetzes. Der Entwurf sieht vor, die Verwaltungen von Bund, Kantonen und Gemeinden zu ermächtigen, die AHV-Nummer systematisch als eindeutiges Identifikationsmerkmal ausserhalb des Sozialversicherungsbereichs zu verwenden.

Diese Vorlage setzt gleichsam den Schlusspunkt einer langjährigen Entwicklung, die dazu geführt hat, dass der Bundesgesetzgeber die Verwendung der AHV-Nummer durch zahlreiche Spezialgesetze weit über den Sozialversicherungsbereich hinaus ausgeweitet hat. Solche Ausweitungen standen auch im Rahmen der Beratungen der Modernisierung des Handelsregister- und Grundbuchrechts zur Diskussion, zu denen die Rechtskommissionen beider Räte den EDÖB beizogen. Nachdem wir das Bundesamt für Justiz dafür gewinnen konnten, bei der ETH Zürich eine Studie zur Beurteilung der datenschutzrechtlichen Risiken in Auftrag zu geben und in die Beratungen der Modernisierung des Grundbuchs einfliessen zu lassen, wurde einerseits klar, dass die Personenregister von Bund, Kantonen und Gemeinden anfällig sind für nicht autorisierte und missbräuchliche Zugriffe. Der Gutachter bestätigte aber auch, dass sich diese Datenschutzrisiken allein mit sektoriellen Identifikatoren wie sie die Bundesgesetzgebung z.B. bei der Verwaltung des elektronischen Patientendossiers vorsieht, nicht signifikant senken lassen. Nach Kenntnisnahme dieser Ergebnisse hat die nationalrätliche Rechtskommission den Bundesrat im Jahre 2017 mit einem Postulat beauftragt, ein Konzept zur Senkung der von der Studie aufgezeigten Risiken vorzulegen und dabei die Meinung des EDÖB einzubeziehen (s. 25. TB, Kap. 1.1.2).

Diesen Auftrag hat der Bundesrat im Rahmen der erwähnten Botschaft erfüllt, und unsere Behörde wurde vom Bundesamt für Sozialversicherung bei der Erarbeitung von Botschaft und Gesetzesentwurf denn auch umfassend einbezogen. Unsere Vorschläge und Bemerkungen wurden berücksichtigt: Angesichts der hohen Datenschutzrisiken begrüssen wir es, dass der Gesetzesentwurf ausdrücklich die Pflicht zu periodischen Risikoanalysen vorsieht für Behörden, die über Datenbanken verfügen, in denen die AHV-Nummer systematisch verwendet wird, wobei insbesondere die Gefahr eines unberechtigten Datenabgleichs berücksichtigt werden soll.

Auf Basis dieser Risikoanalysen sind Sicherheits- und Datenschutzmassnahmen zu definieren und umzusetzen, die der Risikosituation angemessen sind und dem Stand der Technik entsprechen. Wir begrüssen auch die Pflicht für die im Gesetzesentwurf bezeichneten Behörden, welche die AHV-Nummer systematisch verwenden, ein Verzeichnis über die relevanten Datenbanken zu führen, die als Grundlage für die Risikoanalysen dienen. Weiter begrüssen wir das Versprechen des Bundesrates, dass die rechtsstaatlichen Zuständigkeitsgrenzen der Verwaltung durch die einheitliche Verwendung der AHV-Nummer nicht übersteuert werden dürfen, auf dem der EDÖB die Bundesverwaltung behaften wird. Weiter betont der Bundesrat, dass der einheitliche Gebrauch der AHVN nicht dazu führen darf, dass die Sozialversicherungsnummer als allgemeines Identifizierungsmittel verwendet wird, wie in den USA oder Skandinavien, wo es immer wieder zu massenhaften Identitätsdiebstählen gekommen ist. Dem will er entgegenwirken, indem er den Gebrauch der Nummer durch Private einschränkt und gesetzlich vorschreibt, dass die Staatsangestellten so geschult werden, dass die AHVN nur aufgabenbezogen verwendet wird. Zu Zwecken der Identifizierung im Behördenverkehr soll inskünftig die elektronische Identität zur Verfügung stehen, die auf einer von de AHV-Nummer unabhängigen E-ID-Registrierungsnummer basieren soll, was durch die Neufassung des AHVG weiterhin möglich bleibt. Auch dies wird vom EDÖB begrüsst.

Bedeutsam sind auch die technischen Vorgaben der Vorlage, die u.a. verlangen, dass Datensätze mit der AHVN inskünftig nur noch verschlüsselt über das öffentliche Netz übertragen werden.

Anlässlich der Anhörung an der Sitzung der Staatspolitischen Kommission des Ständerates vom 18. Februar 2020 konnten wir die Wichtigkeit von Garantien und konkreten Massnahmen betonen, die eine möglichst weitgehende Risikominimierung bezwecken, sowie die Notwendigkeit, dass Bund, Kantone und Gemeinden die Ausgestaltung ihrer Datenbankarchitekturen regelmässig überprüfen und neu beurteilen.

1.8 Verkehr

ÖV-App SmartWay erstellt Persönlichkeitsprofile

Das Angebot an Apps im öffentlichen Verkehr nimmt stetig zu. Der EDÖB hat in diesem Kontext namentlich die SBB beraten, welche im Berichtsjahr Mobilitäts-Apps wie EasyRide für elektronisches Ticketing oder SmartWay als elektronischen Reiseassistenten lanciert haben.

Der EDÖB hat im Hinblick auf das zunehmende Angebot an Mobilitäts-Apps bereits in den vergangenen Jahren verschiedene Transportunternehmen insbesondere betreffend das elektronische Ticketing beraten (s. 24. TB). Auch in diesem Berichtsjahr stand der EDÖB im Austausch mit Transportunternehmen, namentlich mit dem Datenschutzverantwortlichen der SBB, unter anderem bezüglich der Technologie von Fairtiq für elektronisches Ticketing. Der EDÖB wirkte unter anderem darauf hin, dass die Nutzungsbedingungen für die auf Fairtiq basierende EasyRide-App kundenfreundlicher und unter Wahrung der Verhältnismässigkeit ausgestaltet werden. Zudem liess er sich versichern, dass die Beschränkungen für die Datenweitergabe und -weiterbearbeitung durch Dritte tatsächlich beachtet werden.

Ferner stellten die SBB dem EDÖB die äusserst datenintensive Anwendung SmartWay vor, welche sich noch in der Testphase befindet. Diese App schlägt den Nutzenden personalisierte Reiseempfehlungen mit passenden Verbindungen vor. Die App erfasst Daten durchgehend während 24 Stunden, unabhängig davon, ob sie gerade genutzt wird oder nicht. Die Nutzenden können diese Funktion nicht ablehnen und sofern sie die Daten nicht aktiv löschen oder die App während mehrerer Monate nie benutzen, werden die Daten erst nach vier Jahren gelöscht.

Bereits schon nach wenigen Tagen entstehen Persönlichkeitsprofile und die Möglichkeit einer Anonymisierung von Bewegungsprofilen ist praktisch unmöglich. Folglich sind sehr hohe Anforderungen an den Datenschutz, insbesondere an die Verhältnismässigkeit und die Information zu stellen. Der EDÖB hat darauf hingewiesen, dass die Nutzenden vor der Registrierung vollständig und verständlich über sämtliche Personendatenbearbeitungen informiert werden müssen, damit ihre Einwilligung freiwillig erfolgen kann. Es muss klar sein, wer welche Daten zu welchem Zweck bearbeitet. Einwilligungen sind zudem ausdrücklich (opt-in) sowie zweckbezogen und nicht pauschal einzuholen. Es muss transparent gemacht werden wie das Auskunftsrecht– auch bei Auftragsdatenbearbeitung durch Dritte – ausgeübt werden kann und ob die Profile bei einer Löschung in der App auch bei allfälligen Dritten gelöscht werden. Wenn nicht, muss informiert werden, wie die Nutzenden die Löschung sämtlicher Daten vornehmen können.

Wenn Daten im Ausland weiterbearbeitet werden, zum Beispiel in einer Cloud, müssen die Nutzenden unter Angabe des Landes für Auskunfts- und Löschungsbegehren angemessen informiert werden.

Generell müssen Dritte, welche die Personendaten bearbeiten, ihrerseits die Datenschutzgrundsätze und die Datensicherheit einhalten.

Der EDÖB hat darauf hingewiesen, dass die Datenbearbeiter dafür verantwortlich sind, den Datenschutz von Anfang an sicherzustellen und während der Projektentwicklung laufend Risikofolgeabschätzungen durchzuführen.

Kontrolle eines Pilotprojekts von SBB und Axon Vibe

Anlässlich eines längeren Unterbruchs der Bahnstrecke zwischen Lausanne und Puidoux-Chexbres starteten die SBB ein Pilotprojekt zur Entschädigung der Kunden. Der EDÖB hat eine Sachverhaltsabklärung betreffend die korrekte Datenbearbeitung durchgeführt.

Im Sommer 2018 musste die SBB die Bahnstrecke zwischen Lausanne und Puidoux-Chexbres aufgrund von Bauarbeiten während mehrerer Monate sperren. Um Bahnkunden, welche mehrfach von grossen Verspätungen betroffen waren, eine faire Entschädigung zu erstatten, starteten die SBB ein Pilotprojekt. Damit wurden die Fahrten der sich am Entschädigungsprojekt beteiligenden SBB-Kunden automatisch via die Smartphone-Funktionen Geolokalisation und «Bewegung und Fitness» erfasst. So wurden unter anderem Bewegungsdaten der Kunden bearbeitet. Da sich hierbei auch datenschutzrechtliche Fragen stellen, entschied der EDÖB, eine Sachverhaltsabklärung betreffend die Personendatenbearbeitung durchzuführen.

Mit der Kontrolle wollten wir überprüfen, ob die SBB die Personendatenbearbeitung rechtskonform vornahmen, wie sie dies zugesichert hatten. Insbesondere interessierte uns die ausschliessliche Verwendung der Personendaten für dieses Pilotprojekt sowie die Löschung der Daten. Ferner wurde der Fokus auf die Übertragung von Daten von den SBB an Axon Vibe und deren weitere Bearbeitung durch dieses Drittunternehmen gesetzt.

Während der Sachverhaltsabklärung wurde deutlich, dass diverse datenschutzrechtliche Aspekte über das Pilotprojekt hinausgingen. Zum Beispiel wurden die für das Pilotprojekt relevanten Daten über ein weitergehendes System (Reise-Cockpit) von Axon Vibe erfasst, welches bereits Kundendaten beinhaltete. Eine klare Trennung dieser Daten von jenen die im Pilotprojekt erhoben wurden, war nicht ersichtlich.

Auch war unter anderem nicht klar, ob die SBB oder Axon Vibe für die Datenbearbeitung verantwortlich war.

Eine detaillierte Analyse hätte eine neue, erweiterte Sachverhaltsabklärung erfordert. Das Pilotprojekt war örtlich und zeitlich eng abgesteckt, sodass vergleichsweise wenige Kunden betroffen waren. Zudem hatten die SBB zwischenzeitlich datenintensivere Apps lanciert, auf die der EDÖB den Fokus legt. Er beschränkte sich darum in der Folge auf die Kontrolle der korrekten, unwiederbringlichen Löschung aller im Rahmen des Pilotprojekts erhobenen Personendaten.

Unser Schriftverkehr mit den SBB resp. Axon Vibe war am Ende der Berichtsperiode noch im Gang.

Schutz der Privatsphäre im Projekt Mobility Pricing

Das Bundesamt für Strassen (ASTRA) plant mit Blick auf das Anwachsen der Einwohnerzahl der Schweiz auf zehn Millionen eine Steuerung des Mobilitätsverhaltens der Bevölkerung über die Reisekosten. Ein solches Mobility Pricing soll von der Uhrzeit und der zurückgelegten Distanz sowie dem genutzten Verkehrsmittel abhängen. Das Projekt befindet sich in der Anfangsphase. Der EDÖB fordert, dass datenschutzrechtliche Anforderungen frühzeitig berücksichtigt werden.

Das Bundesamt für Strassen nimmt an, dass die bis in rund zwanzig Jahren zu erwartende Einwohnerzahl der Schweiz von zehn Millionen das heutige Verkehrssystem als Ganzes überfordern würde. Weder könne die traditionelle Infrastruktur im notwendigen Mass baulich ausgebaut werden, noch stünden visionäre Systeme wie unterirdische Bauten rechtzeitig zur Verfügung. Daher will sich das ASTRA zur Brechung von Verkehrsspitzen auf Lösungen fokussieren, die das Mobilitätsverhalten der Bevölkerung beeinflussen. Mit dem sog. Mobility Pricing sollen die Verkehrsteilnehmenden gemäss der von ihnen in der Schweiz zurückgelegten Distanz je nach Uhrzeit und genutztem Verkehrsmittel belastet werden.

Die Umsetzung eines solchen Mobility Pricings bedingt die Erfassung des Mobilitätsverhaltens der Verkehrsteilnehmenden und damit die Bearbeitung von teilweise sensiblen Personendaten und Bewegungsprofilen (s. oben).

Der Beauftragte geht zurzeit davon aus, dass eine datenschutzkonforme Ausgestaltung des Mobility Pricings möglich ist. Anlässlich mehrerer Sitzungen mit dem ASTRA und schriftlichen Stellungnahmen wirkte der EDÖB im Berichtsjahr darauf hin, dass der Datenschutz im Projekt frühzeitig erkannt und umgesetzt wird. Insbesondere legen wir Wert darauf, dass alle projektbeteiligten Amtsstellen und privaten Unternehmen über einen mit genügend Ressourcen ausgestatteten internen Datenschutzberater verfügen. Die Datenschutzberater sind frühzeitig in das Projekt einzubeziehen und sollen gewährleisten, dass die

nötigen Risikofolgeabschätzungen erstellt und datenschutzfreundliche Technologien entwickelt werden. Die dafür notwendigen Mittel müssen von Anfang an eingeplant werden. Ferner sind datenschutzrechtliche Dokumentationen zu erstellen.

App Cyclomania von Pro Velo Schweiz

Eine neue App zur Förderung der Fahrradbenutzung soll die registrierten Nutzer während eines Monats im Jahr tracken. Der EDÖB hat Pro Velo Schweiz zu Datenschutzaspekten beraten.

Der nationale Dachverband der lokalen und regionalen Verbände für die Interessen der Velofahrenden in der Schweiz (Pro Velo Schweiz) entwickelt, unterstützt vom Bundesamt für Energie, die neue App Cycolmania. Diese soll mithelfen, das Velo als Verkehrsmittel zu fördern. Die App erstellt von den registrierten Nutzerinnen und Nutzern während eines Monats im Jahr ein Bewegungsprofil. Die erhobenen Daten werden zum einen für die persönliche Statistik der Cycolmania-Nutzenden und Verlosung von Preisen verwendet, zum anderen sollen die Daten in anonymer oder aggregierter Form den Gemeinden zur Verfügung gestellt werden, damit diese ihre Infrastruktur dem Verhalten der Bevölkerung entsprechend verbessern können. Bei Einwilligung der Nutzer sollen die Daten gegebenenfalls für Forschungszwecke über den zeitlichen Rahmen der Aktion hinaus aufbewahrt werden.

Der EDÖB beriet Pro Velo Schweiz zu den datenschutzrechtlichen Aspekten des Projekts. Unter anderem ist wichtig, dass die Nutzer transparent und angemessen über alle Personendatenbearbeitungen informiert werden und das Verhältnismässigkeitsprinzip eingehalten wird. Beispielsweise soll die Löschung der Daten erfolgen, sobald diese für die angegebenen Zwecke nicht mehr benötig werden. Es soll dem Nutzer ferner die Abschaltung wie auch die gezielte Verwendung der App durch datenschutzfreundliche (Vor-)Einstellungen möglichst einfach gemacht werden. Sinnvoll wäre es, die Information und ausdrückliche Einwilligung kurz und übersichtlich zu gestalten, mit anklickbaren Links zu weitergehenden Informationen. Zu beachten ist weiter die Unmöglichkeit Bewegungsprofile zu anonymisieren (s. Kap. 1.1).

1.9 International

Internationale Konferenz der Datenschutzbeauftragten in Tirana

Die 41. Internationale Konferenz der Datenschutzbeauftragten fand vom 21. bis 24. Oktober 2019 in Tirana unter der Leitung der albanischen Datenschutzbehörde statt und war dem Thema «Convergence and connectivity: raising global data protection standards in the digital age» gewidmet.
Zu Beginn der Konferenz einigten sich die Mitglieder in einer geschlossenen Sitzung auf ein Rahmenkonzept, um die Stellung des Gremiums als internationales Forum weiter zu stärken. Konkret wurde ein neuer Schritt in der Zusammenarbeit zwischen den Datenschutzbehörden weltweit eingeleitet: Neu trägt die Internationale Konferenz nun die Bezeichnung «Global Privacy Assembly – Assemblée globale de la vie privée (GPA)» und unternimmt damit eine grundlegende Reform im Bereich der internen Organisation, der Funktionsweise und der zukunftsgerichteten Koordinierung. Die Konferenz verfolgt drei strategische Prioritäten: 1. Weltweiter Ausbau des Schutzes der Privatsphäre im digitalen Zeitalter; 2. Bedeutung und Einfluss der Konferenz maximieren, namentlich durch die Stärkung der Rolle der Konferenz in der digitalen Politik und die Intensivierung der Beziehungen zu anderen internationalen Gremien und Netzwerken; 3. Kapazitätserweiterung, damit die Mitglieder ihr Fachwissen während des Jahres laufend austauschen können.

An der geschlossenen Sitzung vom 21. und vom 22. Oktober 2019 wurden sechs Grundsatzdokumente verabschiedet :

- Entschliessung über die strategische Orientierung der Konferenz (2019 – 2021);
- Entschliessung über die Privatsphäre als grundlegendes Menschenrecht und als Grundvoraussetzung für die Demokratie;
- Entschliessung über die Förderung von neuen praktischen, langfristig angelegten Instrumenten sowie über die Weiterführung juristischer Bestrebungen im Hinblick auf eine wirksame Zusammenarbeit im Bereich der grenzüberschreitenden Kontrolle;
- Entschliessung über soziale Medien und extremistische, gewaltgeprägte Webinhalte;
- Entschliessung zur Unterstützung und Erleichterung der Zusammenarbeit in Regulierungsfragen für Datenschutz-, Verbraucherschutz- und Wettbewerbsbehörden, damit klare, einheitliche Datenschutznormen in der digitalen Wirtschaft eingeführt werden können;
- Entschliessung über die Bedeutung des menschlichen Versagens im Zusammenhang mit der Verletzung personenbezogener Daten.

An der Eröffnung der Konferenz hielt der albanische Premierminister Edi Rama eine Ansprache. Diese öffentlich zugängliche Sitzung war vor allem durch den Austausch und die Zusammenarbeit zwischen Vertretern der Datenschutzbehörden, der Hochschulen, der Industrie sowie der Bürgergesellschaft und der Medien geprägt. Nebst anderen Fragen kamen folgende Themen zur Sprache: gemeinsame Datenschutznormen im Bereich der Privatsphäre; weltweite Herausforderungen für den Schutz der Privatsphäre im Zusammenhang mit datenbasierten Handelsmodellen; konvergierende digitale Regulierungen in den Bereichen Datenschutz und Wettbewerb; Verantwortungsbewusstsein als globale Brücke, die zur Einhaltung strenger Datenschutznormen beiträgt; zukünftige Herausforderungen für Datenschutzbehörden und -beauftragte.

Über 700 Personen nahmen an der Konferenz teil. Die nächste Auflage der Konferenz ist für 2020 in Mexiko-Stadt vorgesehen.

Europäische Konferenz der Datenschutzbeauftragten in Tiflis

Wir haben an der Europäischen Konferenz der Datenschutzbeauftragen teilgenommen, deren Fokus auf den Herausforderungen im Zusammenhang mit der Umsetzung der DSGVO und auf den wesentlichen Neuerungen des Übereinkommens 108+ lag. Diese Urkunde ist nach wie vor das einzige internationale, rechtlich bindende Instrument auf dem Gebiet des Datenschutzes.

Die 29. Europäische Konferenz der Datenschutzbeauftragten fand vom 8. bis 10. Mai 2019 auf Einladung der georgischen Datenschutzbeauftragten in Tiflis (Georgien) statt. Sie bot Gelegenheit, Rückschau über das erste Jahr der Datenschutz-Grundverordnung zu halten. Im Rahmen von Debatten konnten sich die Vertreter der Datenschutzbehörden über die Herausforderungen bei der Umsetzung und Anwendung der DSGVO austauschen. Dabei wurden diverse Initiativen der Datenschutzbehörden vorgestellt, namentlich die Software für Datenschutz-Folgenabschätzungen der CNIL, die in 16 Sprachen vorliegt. Auch der territoriale Geltungsbereich und die Mechanismen der Zusammenarbeit wurden anlässlich einer Paneldiskussion erörtert, an der eine Vertreterin des EDÖB teilnahm.

Die Teilnehmer diskutierten zudem über das Übereinkommen 108+ des Europarats, das unter anderem die Zusammenarbeit zwischen den Parteien erleichtern wird, über den Schutz der Daten von Kindern, den Datenschutz, die internationalen Organisationen sowie über die Zukunft der Konferenz. Die Panelexperten stellten die wichtigsten Neuerungen des Übereinkommens 108+ vor und wiesen nachdrücklich darauf hin, wie wichtig das Inkrafttreten dieser Urkunde des Europarats für alle Beteiligten ist, da es sich dabei um den bislang einzigen völkerrechtlich bindenden Vertrag auf dem Gebiet des Datenschutzes handelt.

Französischsprachige Vereinigung der Datenschutzbehörden

Eine Vertreterin des EDÖB hat an der Jahreskonferenz der Vereinigung der französischsprachigen Datenschutzbehörden in Dakar teilgenommen, die sich mit dem «digitalen Bürger» befasste. Den Schutz der Persönlichkeitsrechte zu wahren und dabei den technologischen Fortschritt im Blick zu behalten, stellt die grösste Herausforderung der Datenschutzbehörden dar.

Die Konferenz der französischsprachigen Vereinigung der Datenschutzbehörden (AFAPDP) fand am 16. und 17. September 2019 auf Einladung der senegalesischen Datenschutzkommission und mit Unterstützung der Internationalen Organisation der Frankophonie (OIF) in Dakar statt. An diesem Anlass waren vierzehn Delegationen vertreten. Die Präsidenten, Datenschutzbeauftragen und Vertreter der französischsprachigen Datenschutzbehörden nahmen die Datenschutzbehörde der Insel Jersey (OIC) als einundzwanzigstes Mitglied in die Vereinigung auf. Die Internationale Konferenz der Datenschutzbeauftragten und die Regulierungsbehörde für Telekommunikation Kameruns (ART) erhielten Beobachterstatus. Ausserdem wählten die Mitglieder einen neuen Vorstand, und es wurde eine Handlungsstrategie 2025 verabschiedet. Letztere soll zur Erreichung der drei Schwerpunktziele der Vereinigung beitragen: Förderung des Datenschutzrechts im französischsprachigen Raum, Unterstützung und Kapazitätsaufbau für die Mitglieder der AFAPDP sowie Verbreitung der Expertise und Betrachtungsweise der Frankophonie über den französischsprachigen Raum hinaus.

Thema der Jahreskonferenz war der «digitale Bürger». Im digitalen Raum wird der Rechtsträger als Verbraucher, Untersuchungsobjekt oder als anonymer «Troll» wahrgenommen. Es ist, als ob der digitale Raum und das reale Leben zwei verschiedene Sphären wären und als müsste das Individuum einer dieser Kategorien zugeordnet werden können. Für Datenschutzbehörden besteht die permanente Herausforderung darin, einen Ausgleich zwischen dem Schutz von Persönlichkeitsrechten und der Wahrung der Interessen der für die Datenverarbeitung Verantwortlichen herbeizuführen, ohne dabei die Fortschritte und die unendlichen Möglichkeiten der digitalen Technologie aus dem Blickwinkel zu verlieren. Die personenbezogenen Daten sind ein untrennbarer Bestandteil der menschlichen Person. Für unsere Behörden ist es wichtig, immer wieder an ihren Kernauftrag zu erinnern: den Schutz der Privatsphäre des Menschen.

.

Aufsichtskoordinationsgruppen über die Informationssysteme SIS II, VIS und Eurodac

Im Berichtsjahr trafen sich die Aufsichtskoordinationsgruppen in Brüssel. Sie besprachen unter anderem den enormen Anstieg von Auskunftsgesuchen betreffend das Informationssystem SIS und nahmen zwei Berichte an.

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 19./20. Juni 2019 sowie 26./27. November 2019 in Brüssel statt. Vertreten waren der europäische Datenschutzbeauftragte (EDSB) sowie die nationalen Datenschutzbehörden der Mitgliedstaaten.

Die Aufsichtskoordinationsgruppe SIS beschäftigte sich insbesondere mit dem Thema des enormen Anstiegs von Auskunftsgesuchen betreffend das Informationssystem SIS. Dieser Anstieg konnte in vielen Mitgliedstaaten, vor allem aber in der Schweiz, festgestellt werden. Die Aufsichtskoordinationsgruppe wird sich weiterhin mit diesem Thema beschäftigen. Die Aufsichtskoordinationsgruppe Eurodac hat den Bericht zu den Rechten der betroffenen Personen und die Aufsichtskoordinationsgruppe VIS den Bericht zur Datenschutzschulung der auf das VIS zugriffsberechtigten Personen angenommen.

Besprochen wurde in allen drei Gruppen auch die geplante Änderung ihrer Ausgestaltung. In Zukunft werden die drei Aufsichtskoordinationsgruppen als «Coordinated Supervision Committee» in den europäischen Datenschutzausschuss (EDSA) eingegliedert, der auch das Sekretariat führen wird. Auch wenn die Schweiz nicht Mitglied des EDSA ist, kann sie auch inskünftig in den Schengen und Dublin relevanten Bereichen teilnehmen.

OECD: Arbeitsgruppe «Data Governance and Privacy in the Digital Economy»

Die von der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) neu eingesetzte Arbeitsgruppe «Data Governance and Privacy in the Digital Economy (WPDGP)» tagte erstmals im November 2019 in Paris.

Neben der Konstituierung der neu geschaffenen Arbeitsgruppe fand eine ganztätige Expertensitzung über das Thema «Bewältigung neuer Herausforderungen bei der Durchsetzung des Datenschutzes» statt. Am zweiten Tag wurden diverse Themen und Arbeitspapiere diskutiert und zur weiteren Bearbeitung an das Sekretariat und danach zur Konsultation bei den Mitgliedern weitergeleitet.

Der erste runde Tisch beschäftigte sich mit den Auswirkungen der künstlichen Intelligenz (KI) auf den Schutz von Personendaten und auf die Umsetzung der Datenschutzleitlinien. Dabei wurden u.a. folgende Fragestellungen erörtert: Was sind die Herausforderungen für die Datenschutzbehörden bei der Durchsetzung der grundlegenden Datenschutzprinzipien der Datenschutzrichtlinien und bei Audits im Zusammenhang mit künstlicher Intelligenz? Inwieweit berücksichtigen die derzeitigen Richtlinien der KI-Politik die Privatsphäre und den Datenschutz? Wie kann die individuelle Rechtsausübung gewährleistet werden?

Der zweite runde Tisch erörterte den zunehmenden grenzüberschreitenden Fluss von Personendaten und die wachsende Bedeutung der internationalen Zusammenarbeit zur Durchsetzung des Schutzes der Privatsphäre und des Datenschutzes. Es wurden verschiedene Möglichkeiten der Zusammenarbeit aufgezeigt und u.a. folgende Fragen erörtert: Wie kann die internationale Zusammenarbeit zu einem vertrauensvollen grenzüberschreitenden Fluss von Personendaten beitragen? Was sind die Hindernisse für die internationale Zusammenarbeit und wie können sie abgebaut werden? Was sind die Lehren aus Kooperationen?

Am dritten runden Tisch wurde eine Bilanz der Diskussionen des Tages gezogen und besprochen, wie die OECD am besten auf die Herausforderungen reagieren kann.

An der geschlossenen Sitzung wurden erste Entwürfe von Zwischenberichten, Umfragen und Arbeitspapieren besprochen und zwar zu den Themen: Verbesserung des Zugangs zu und gemeinsame Nutzung von Daten, Datenportabilität, Datenethik, eine praktische Anleitung für die Umsetzung der künstlichen Intelligenz, sowie die Förderung der Vergleichbarkeit der Meldung von Datenschutzverstössen. Des Weiteren beschäftigte sich die Arbeitsgruppe mit der derzeit in Überarbeitung befindlichen Empfehlung aus dem Jahr 2012 zum Schutz der Kinder im Internet. Schliesslich präsentierte das Sekretariat einen ersten Zwischenbericht zur Umsetzung der Datenschutzrichtlinien.

Plenarsitzungen des Europäischen Datenschutzausschusses (EDSA)

Der EDÖB nahm im Jahr 2019 an zwei Plenarsitzungen des Europäischen Datenschutzausschusses – EDSA (European Data Protection Board, EDPB) über Schengen-relevante Themen teil sowie an der letzten Plenarsitzung des Jahres 2019 für einen allgemeinen Informationsaustausch.

Der mit der DSGVO eingeführte EDSA hielt im Jahr 2019 insgesamt zwölf Plenarsitzungen ab. Unsere Teilnahme als Beobachter in den Plenarsitzungen beschränkte sich auf Schengen-relevante Themen.

So nahmen wir erstmalig seit der Konstituierung des EDSA an zwei Plenarsitzungen teil und konnten unsere Position zu den innerstaatlichen Zuständigkeiten zusammen mit anderen Datenschutzbehörden vertreten. Zudem informierte der Beauftragte den Ausschuss auf dessen Einladung Anfang Dezember 2019 summarisch über den Stand seines Aufsichtsverfahrens gegen den in Genf ansässigen Verein Libra (s. Schwerkpunkt II).

Europäische Arbeitsgruppe für die Behandlung datenschutzrelevanter Fälle

Ein Vertreter des EDÖB nahm an der 31. Ausgabe des jährlichen europäischen «Case Handling Workshops» teil.

Der neue Europäische Datenschutzbeauftragte, Wojciech Wiewiórowski, organisierte als Gastgeber am 28. und 29. November 2019 in Brüssel die 31. Ausgabe des jährlichen europäischen Workshops zur Bearbeitung von Datenschutzfällen («Case Handling Workshop»). Am Workshop nahmen Mitarbeitende von 28 EU- und Nicht-EU-Datenschutzbehörden – einschliesslich eines Vertreters des EDÖB – teil.

Der Workshop bot die Gelegenheit, die Erfahrungen bei der Untersuchung von Beschwerden, der Beratung von für die Bearbeitung Verantwortlichen und der Durchsetzung von Datenschutzgesetzen auszutauschen. An den zwei Veranstaltungstagen wurden insgesamt Anwendungsfälle aus sechs Themenbereichen besprochen: Nutzung von IT-Dienstleistern durch öffentliche Einrichtungen; Behandlung von offenkundig unbegründeten oder exzessiven Anfragen nach Artikel 57 Absatz 4 DSGVO; Behandlung von Fällen nach Artikel 56 Absatz 2 DSGVO (zusätzliche lokale Zuständigkeit, neben einer federführenden Behörde); Bewertung von Anträgen auf vorherige Konsultation gemäß Artikel 36 Absatz 3 DSGVO; Kreditauskunftssysteme und Datenvermittler; Ausübung von Untersuchungs- und Korrekturbefugnissen sowie Abwägung zwischen alternativen Optionen nach Artikel 58 DSGVO.

Unterarbeitsgruppe BTLE «Border, Travel & Law Enforcement»

Im Verlauf des Berichtsjahrs nahm der EDÖB an den sieben Treffen der «Border, Travel & Law Enforcement Subgroup» (BTLE) teil. Diese Unterarbeitsgruppe beobachtete die dritte Überprüfung des EU-US Privacy Shield aufmerksam und setzt sich weiterhin mit dem Umbrella Agreement auseinander, welches als Rahmenabkommen den Austausch von personenbezogenen Daten zwischen Polizei- und Justizbehörden im Zusammenhang mit Flugpassagierdaten (PNR) regelt.

Bei der «Border, Travel & Law Enforcement» (BTLE) handelt es sich um eine Unterarbeitsgruppe, die von der vormaligen Arbeitsgruppe «Artikel 29» über den Datenschutz eingesetzt wurde. Ihre Aufgabe besteht darin, die gesetzgeberischen Entwicklungen in den Bereichen Polizei, Grenzen und Strafjustiz mitzuverfolgen und dabei den Fokus besonders auf den Schengen-Besitzstand zu legen. Sie fertigt diesbezügliche Gutachten und Stellungnahmen an und legt sie dem Europäischen Datenschutzausschuss zur Genehmigung vor.

Die Unterarbeitsgruppe richtete ihr besonderes Augenmerk auf die Zukunft der Überwachungsmodelle der grossen Informatiksysteme der EU im Bereich Justiz und Innenpolitik. Sie setzte sich mit der Erarbeitung neuer Verfahrensregeln auseinander.

Die Gruppe befasste sich intensiv mit dem dritten jährlichen Review über die Funktionsweise des EU-US Privacy Shield. Sie verfolgte die Arbeiten am Zusatzprotokoll zum Übereinkommen über Cyberkriminalität, bei dem es um die Kriminalisierung rassistischer und fremdenfeindlicher Handlungen geht, die über Informatiksysteme ausgeübt werden, aufmerksam mit. Zudem fertigte sie eine gemeinsame Position zu Handen der Octopus Konferenz an.

Die Gruppe begleitete weiterhin das Umbrella Agreement, das einen Rahmen für den Austausch personenbezogener Daten zwischen Polizei- und Justizbehörden festlegt, indem es die Rechte US-amerikanischer Behörden im Umgang mit europäischen Daten begrenzt, sowie die Schaffung eines europäischen Rahmens für die Bekanntgabe von PNR-Daten an Drittländer und für die Verwendung von PNR-Daten zur Verfolgung von Straftaten.

Europäische Datenschutz-Grundverordnung (DSGVO)

Die neue EU-Datenschutz-Grundverordnung (DSGVO) gilt unter bestimmten Voraussetzungen auch für Datenverarbeitungen durch Schweizer Unternehmen. Der EDÖB nahm an diversen internationalen Konferenzen teil und konnte somit die Debatten über die Herausforderungen, die sich im Zusammenhang mit dem Vollzug der neuen europäischen Verordnung ergeben, mitverfolgen. Mehr als ein Jahr nach deren Inkrafttreten sind zahlreiche Fragen nach wie vor offen, namentlich was den territorialen Geltungsbereich angeht.

Die europäische Datenschutz-Grundverordnung (DSGVO) wurde am 27. April 2016 verabschiedet und ist in sämtlichen Mitgliedstaaten der Europäischen Union seit dem 25. Mai 2018 anwendbar. Ihr Geltungsbereich erstreckt sich jedoch weit über das Gebiet der EU hinaus: Wenn ein für die Datenbearbeitung Verantwortlicher (oder ein Subunternehmer) Waren oder Dienstleistungen Personen in der Europäischen Union anbietet bzw. das Verhalten dieser Personen beobachtet, namentlich um ihre Präferenzen zu analysieren, gelten die Vorgaben der DSGVO für ihn auch dann, wenn er nicht in der EU niedergelassen ist. Im Berichtsjahr nahm der EDÖB an mehreren internationalen Konferenzen teil und konnte somit den Debatten über Erfolge und Herausforderungen im Zusammenhang mit der Umsetzung und Anwendung dieses Grundlagentextes beiwohnen. Dabei wurden auch die extraterritoriale Anwendung der Verordnung und die Zusammenarbeitsmechanismen erörtert. Während des ganzen Jahres tauschten sich die französischsprachigen europäischen Behörden der Nicht-Mitgliedstaaten der EU, die vor den gleichen Schwierigkeiten stehen wie die Schweiz, über das Inkrafttreten der DSGVO und über die diesbezüglichen Erfahrungen aus, um Fragen, die an sie gerichtet wurden, im Hinblick auf eine koordinierte Antwort gemeinsam anzugehen.

Der EDÖB nahm auch in diesem Berichtsjahr an zahlreichen Informationssitzungen zu diesem Thema teil, die von der Bundesverwaltung oder von privaten Akteuren veranstaltet wurden. Im Rahmen seiner beratenden Tätigkeit beantwortete er zudem zahlreiche mündliche und schriftliche Anfragen aus der Bevölkerung und den Medien.

Über ein Jahr nach Inkrafttreten der DSGVO veröffentlichte der EDSA, der als unabhängiges europäisches Organ an der einheitlichen Einhaltung der Datenschutzvorschriften in der Europäischen Union mitwirkt, seine seit langem erwarteten Leitlinien zum Anwendungsbereich der DSGVO. Der EDÖB beteiligte sich zusammen mit der monegassischen Behörde (CCIN, Commission de contrôle des informations nominatives) an der öffentlichen Konsultation, die den Leitlinien vorausging, um eine Reihe von Aspekten dieser Frage abzuklären, die für Drittländer, welche in das EU-Gefüge eingebunden sind, eminent wichtig ist. Im Februar 2020 wurde zudem die neue Fassung an einem Treffen in Bern analysiert. Auf unserer Website werden die Informationen zur Anwendung der DSGVO regelmässig aktualisiert.

Brexit und Übermittlung von Personendaten

Nach dem Referendum im Vereinigten Königreich über den Austritt aus der EU (Brexit) im Juni 2016 teilte die britische Regierung der Union ihren Entscheid mit. Nach einigen Verzögerungen erfolgte der Austritt am 1. Februar 2020. Wie bereits im letzten Tätigkeitsbericht ausgeführt, hat der EDÖB an zahlreichen Sitzungen mit Behörden des Bundes und des Vereinigten Königreichs teilgenommen, um sicherzustellen, dass der freie Verkehr von Personendaten zwischen der Schweiz und Grossbritannien auch nach dem Brexit möglich bleibt. Das Vereinigte Königreich gilt als Land mit einem angemessenen Datenschutzniveau, und der EDÖB sieht derzeit keine Veranlassung, dessen Status zu ändern.

Die EU wird bis Ende Jahr 2020 prüfen, ob dem Vereinigten Königreich eine datenschutzrechtliche Angemessenheit attestiert wird. Der EDÖB beobachtet diese Entwicklungen aktiv.

Beratender Ausschuss zum Übereinkommen 108 – T-PD

Der Beratende Ausschuss zum Übereinkommen 108 (T-PD) verabschiedete Leitlinien betreffend die künstliche Intelligenz (KI) und den Datenschutz. Mit diesen Leitlinien soll politischen Entscheidungsträgern, Entwicklern für künstliche Intelligenz, Herstellern und Dienstleistern geholfen werden, dafür zu sorgen, dass KI-Anwendungen nicht zu Verletzungen des Rechts auf Datenschutz führen. Sie knüpfen an Grundsatzfragen an, mit denen sich bereits die Leitlinien über den Schutz des Menschen bei der Verarbeitung von Personendaten in Zeiten von Big Data befassen. Ausserdem bezog der Ausschuss Position zum Empfehlungsentwurf des Ministerkomitees an die Mitgliedstaaten betreffend die «Folgen algorithmischer Systeme für die Menschenrechte», der vom Lenkungsausschuss für die Medien und die Informationsgesellschaft zur Stellungnahme vorgelegt wurde.

Er erstellte das Arbeitsprogramm des Ausschusses für 2020–2021. Es beinhaltet unter anderem die Begleitung der Modernisierung des Übereinkommens, die Förderung des Übereinkommens, eine spezifische Empfehlung betreffend die Gesichtserkennung, die Bearbeitung von Personendaten im Zusammenhang mit Bildungssystemen sowie eine erneute Prüfung des Profilings.

Zudem sollen die Mechanismen zur Überwachung und Beurteilung des Übereinkommens 108+ bearbeitet werden, und es wird eine Arbeitsgruppe gebildet, um die Ausarbeitung von Vorschlägen für den neuen Mechanismus voranzutreiben. Diese Arbeitsgruppe setzt sich aus den Mitgliedern des Büros zusammen und steht allen interessierten Delegationen offen.

Angemessenheitsbeschluss betreffend das Schweizer Datenschutzniveau

Die Europäische Kommission setzte die Überprüfung ihres aus dem Jahr 2000 stammenden Angemessenheitsbeschlusses für die Schweiz fort. Die entsprechenden Schlussfolgerungen werden für Mai 2020 erwartet. Die Beibehaltung des Angemessenheitsbeschlusses der EU ist für den Bundesrat ein vorrangiges Ziel.

Mit einem Angemessenheitsbeschluss attestiert die Europäische Kommission einem Drittland, dass dessen innerstaatliche Gesetzgebung oder internationalen Verpflichtungen einen mit dem Niveau der Europäischen Union vergleichbaren Schutz der Personendaten gewährleisten. Personendaten können dank eines solchen Beschlusses sicher zwischen dem Europäischen Wirtschaftsraum (EWR) und dem betreffenden Drittland übertragen werden, ohne dass die Bearbeitungsverantwortlichen eigene zusätzliche sichernde Massnahmen vorsehen müssen.

In Anwendung von Artikel 45 Abs. 3 und 4 DSGVO überwacht die Europäische Kommission fortlaufend die Entwicklungen des Datenschutzniveaus in Drittländern, denen sie, wie im Falle der Schweiz, die Angemessenheit ihres Schutzniveaus in einem Entscheid bestätigt hat. Das Verfahren zur Überprüfung des Angemessenheitsbeschlusses ist für alle betroffenen Drittländer gleich.

Die Kommission muss insbesondere die Rechtsstaatlichkeit, die Achtung der Menschenrechte und Grundfreiheiten, die einschlägigen Rechtsvorschriften, das Bestehen und die wirksame Funktionsweise einer oder mehrerer unabhängiger Aufsichtsbehörden sowie die internationalen Verpflichtungen, die das Drittland eingegangen ist, prüfen. Für die Beibehaltung des Beschlusses, die für den Bundesrat ein vorrangiges Ziel darstellt (siehe Interpellation 17.4088), werden die Unterzeichnung des Übereinkommens 108+ im November 2019 und die Revision des DSG eine wesentliche Rolle spielen.

Das Überprüfungsverfahren begann offiziell im März und wird sich im Rahmen eines regelmässigen Austauschs bis zum Frühjahr 2020 fortsetzen. Im Berichtsjahr brachte sich der EDÖB in die vom Bundesamt für Justiz (BJ) geleitete Arbeitsgruppe ein. Die Europäische Kommission hat bis zum 25. Mai 2020 Zeit, um die Schlussfolgerungen ihrer Prüfung vorzulegen und um ihren Beschluss betreffend die Schweiz zu erneuern. Gemäss DSGVO bleiben Angemessenheitsbeschlüsse so lange in Kraft, bis sie geändert, ersetzt oder aufgehoben werden.

Projekt Libra

Das Kryptowährungsprojekt Libra hat bei Medien und Datenschützern weltweit für grosses Aufsehen gesorgt. Der EDÖB hat in einem Vorverfahren seine Zuständigkeit als Aufsichtsorgan für die von Libra Association mit Sitz in Genf durchgeführten Datenbearbeitungen bejaht und eine entsprechende Dokumentation einverlangt. Die Libra Association hat dem EDÖB zugesichert, die für den Persönlichkeitsschutz notwendigen Massnahmen umzusetzen.

Der EDÖB wurde durch Medienberichte auf das Projekt Libra, die geplante weltweite Kryptowährung unter der Schirmherrschaft von Facebook, aufmerksam. So nahm er insbesondere Kenntnis von den Ausführungen, welche der Vizepräsident für Messaging-Produkte bei Facebook, David Marcus, bei der Anhörung vom 16. Juli 2019 vor einem US-Senatsausschuss zum Kryptowährungsprojekt der Libra Association sowie zur Leitungsfunktion des Vereins und zur Rolle des EDÖB als deren Aufsichtsbehörde machte.

Da der EDÖB von den Promotoren des Projekts vorgängig nicht kontaktiert worden war, gelangte er mit Schreiben vom 17. Juli 2019 an die Libra Association in Genf. Darin teilte er mit, dass er die Aussagen von David Marcus zur Kenntnis nehme, wonach der Datenschutz als grundlegendes Element des Projektes berücksichtigt werde. Gleichzeitig machte der EDÖB klar, dass er im Fall der Bearbeitung von Personendaten eine Risikofolgeabschätzung erwarte, welche unter anderem die vorgesehenen Datenbearbeitungen beschreibt, die Datenschutzrisiken für die betroffenen Personen bewertet und die zweckmässigen Massnahmen zu deren Minderung aufzeigt. Zudem forderte er die Libra Association auf, ihm Unterlagen zum aktuellen Stand des Projektes einzureichen.

Nachdem die Libra Association fristgerecht die vom EDÖB einverlangten Informationen zum Libra-Projekt eingereicht hatte, fand am 17. September 2019 ein persönliches Treffen zwischen dem EDÖB und Vertretern der Libra Association in Bern statt. Der Verein bekräftigte, einen global einheitlichen Datenschutzstandard für das System zu entwickeln, welcher insbesondere den Anforderungen der Datenschutzgrundverordnung der EU genügen werde. Damit wird der Haltung des Beauftragten entsprochen, der auf diese Weise ein hohes Schutzniveau für die Personendaten der Nutzerinnen und Nutzer erreichen will. Weiter beteuerte der Verein, den EDÖB in einem frühen Stadium in ihre laufenden Entwicklungsarbeiten einbeziehen, um die datenschutzrechtlichen Anforderungen im Sinne des Grundsatzes von Privacy by design von Beginn an zu erfüllen. Die Libra Association hat dem EDÖB schriftlich zugesichert, rechtzeitig vor Lancierung der Währung die für die Schaffung des einheitlichen Datenschutzstandards nötigen Massnahmen wie die Ernennung einer Datenschutzstelle zu treffen und Letztere mit der Erstellung einer Risikofolgenabschätzung zu beauftragen. Mit Schreiben vom 17. Februar 2020 hat die Libra Association den EDÖB darüber informiert, dass die diesbezüglichen Arbeiten noch im Gang sind. Sie hat zudem noch einmal bekräftigt, dass sie die dem EDÖB zugesicherten Massnahmen zum Schutz der Persönlichkeitsrechte im Projekt Libra umsetzen wird.

Der EDÖB tauscht sich seit Bekanntwerden seiner Zuständigkeit für die Aufsicht über das Projekt Libra mit den Kollegen der EU-Datenschutzbehörden aus und informiert das EU Board regelmässig über den Stand des Projektes. Am 23. August 2019 fand ausserdem ein vom Staatssekretariat für internationale Finanzfragen (SIF) geleitetes Treffen mit dem U.S. House Committee on Financial Services statt, an dem der Beauftragte über den Stand seines Aufsichtsverfahrens informierte (s. unten). Der Beauftragte steht zudem in Kontakt mit der Schweizerischen Nationalbank und der Eidg. Finanzmarktaufsicht (FINMA), um die Tätigkeiten der beteiligten Bundesstellen zu koordinieren und einen Informationsaustausch sicherzustellen. Letztere hat zugesichert, den Beauftragten über den Stand des bei ihr anhängigen Verfahrens zur Erteilung einer Bankenbewilligung auf dem Laufenden zu halten. Dies erlaubt es dem EDÖB, sein Verfahren zeitlich abzustimmen.

Wie bis anhin wird der EDÖB die Weltöffentlichkeit weiterhin mit Updates über relevante Weiterentwicklungen des Aufsichtsverfahrens auf dem Laufenden halten.

Internationale Tätigkeiten und Treffen

Gemeinsam mit weiteren Bundesbehörden nahm der EDÖB am 23. August 2019 an einem vom SIF organisierten Anlass in Bern teil, an dem sechs Mitglieder des U.S. House Committee on Financial Services, angeführt von deren Vorsitzenden Maxine Waters, empfangen wurden. Letztere interessierten sich für die behördliche Aufsicht über die Tätigkeiten des in Genf ansässigen Vereins Libra und die rechtlichen Rahmenbedingungen von Kryptowährungen in der Schweiz sowie mögliche Auswirkungen auf die Persönlichkeitsrechte von betroffenen Personen in den USA. Der Beauftragte informierte die Delegation summarisch über das hängige Aufsichtsverfahren gegen den Verein Libra und beantwortete deren Verständnisfragen.

Der Beauftragte erklärte, dass er wie alle anderen Datenschutzbehörden vom Libra-Projekt und seinem globalen Netzwerk betroffen und bestrebt sei, die globale Gemeinschaft der Datenschutzbehörden bei ihren gemeinsamen Bemühungen zum Schutz der Bevölkerung zu unterstützen. Er stand deshalb mit dem Europäischen Datenschutzausschuss (EDSA) und der Global Privacy Association (GPA, damals noch ICDPPC) und weiteren Datenschutzbehörden in engem Kontakt. Er bekräftigte dabei insbesondere, dass das schweizerische Verfahren in keiner Weise die Kompetenzen und Befugnisse der anderen Datenschutzbehörden in anderen Ländern präjudizieren oder beeinflussen würde. Weiter werde er mögliche Versuche verhindern, dass einzelne Datenschutzbehörden gegeneinander ausgespielt würden. Er informierte die Vorsitzenden des EDSA und der GPA, dass er sie über das Verfahren in der Schweiz summarisch auf dem Laufenden halten werde.

Ein Vertreter des EDÖB nahm in der Folge auch an einem Panel zum Datenschutz an der «Conference on global stablecoins» von der Bank für Internationalen Zahlungsausgleich am 16. September 2019 in Basel teil. Die Teilnehmer waren vornehmlich Vertreter von Nationalbanken und Finanzaufsichtsregulatoren, und so konnte erstmals in einem solchen Rahmen auf die Datenschutzaspekte hingewiesen und mitdiskutiert werden.

Der Beauftragte stand verschiedentlich mit Vertretern der GPA und dem EDSA in Kontakt. Anlässlich der Internationalen Konferenz der Datenschutzbeauftragten in Tirana hatte der EDÖB die Gelegenheit zu persönlichen Treffen mit den Datenschutzbeauftragten diverser europäischer Staaten und mit der amerikanischen Federal Trade Commission (FTC). Der Beauftragte stand auch mit Vertretern der Schweizerischen Nationalbank und der FINMA in Kontakt, die ihm zugesichert haben, seine Behörde über den zeitlichen Verlauf finanzrechtlicher Bewilligungsverfahren, die den Verein Libra betreffen, auf dem Laufenden zu halten. Ferner nahm der Beauftragte am 3. Dezember 2019 an einer Sitzung des EDSA in Brüssel für einen Informationsaustausch teil (s. Kap. 1.9).

Öffentlichkeitsprinzip

2.1 Allgemein

Der Paradigmenwechsel, der mit der Einführung des Öffentlichkeitsgesetzes begann, schreitet klar voran, und das Öffentlichkeitsprinzip wird von den meisten Bundesbehörden mit Erfolg umgesetzt. Dies belegen die nachstehend aufgeführten Zahlen. Sie bestätigen die Entwicklung der letzten Jahre: Es überwiegt der vollständige Zugang zu den gewünschten Dokumenten, und die Zahl der Zugangsgesuche steigt deutlich (s. Kap. 2.2).

Dass sich mündliche Schlichtungsverhandlungen bewähren, konnte 2019 besonders deutlich festgestellt werden: Nicht weniger als 61 Prozent der Fälle wurden einvernehmlich abgeschlossen. Diese Vorgehensweise muss weiterhin gefördert und privilegiert werden. In mehreren Fällen erhielten die Antragstellenden nicht nur innerhalb kurzer Zeit die verlangten Informationen, sondern auch die Möglichkeit, in einen direkten Austausch mit der Verwaltung zu treten und somit eventuell sogar enge Beziehungen zu den Bundesbehörden zu knüpfen, die für eine zukünftige Zusammenarbeit wertvoll sind.

Die Durchführung von Schlichtungsverfahren innert der gesetzlichen Frist von 30 Tagen bleibt je nach Konstellation des Einzelfalles herausfordernd. Dies ist insbesondere der Fall bei komplexen Drei- oder Mehrparteienverfahren betreffend Zugangsgesuche zu Unterlagen mit geschäftsgeheimnisrelevanten Informationen oder mit Bezug zum Persönlichkeitsschutz von Privatpersonen oder Verwaltungsangestellten. Diese Schlichtungsverfahren bringen umfangreiche und bisweilen komplexe Abklärungen mit den Betroffenen mit sich, was sich direkt auf eine längere Bearbeitungsdauer des Verfahrens auswirkt (s. Kap. 2.3).

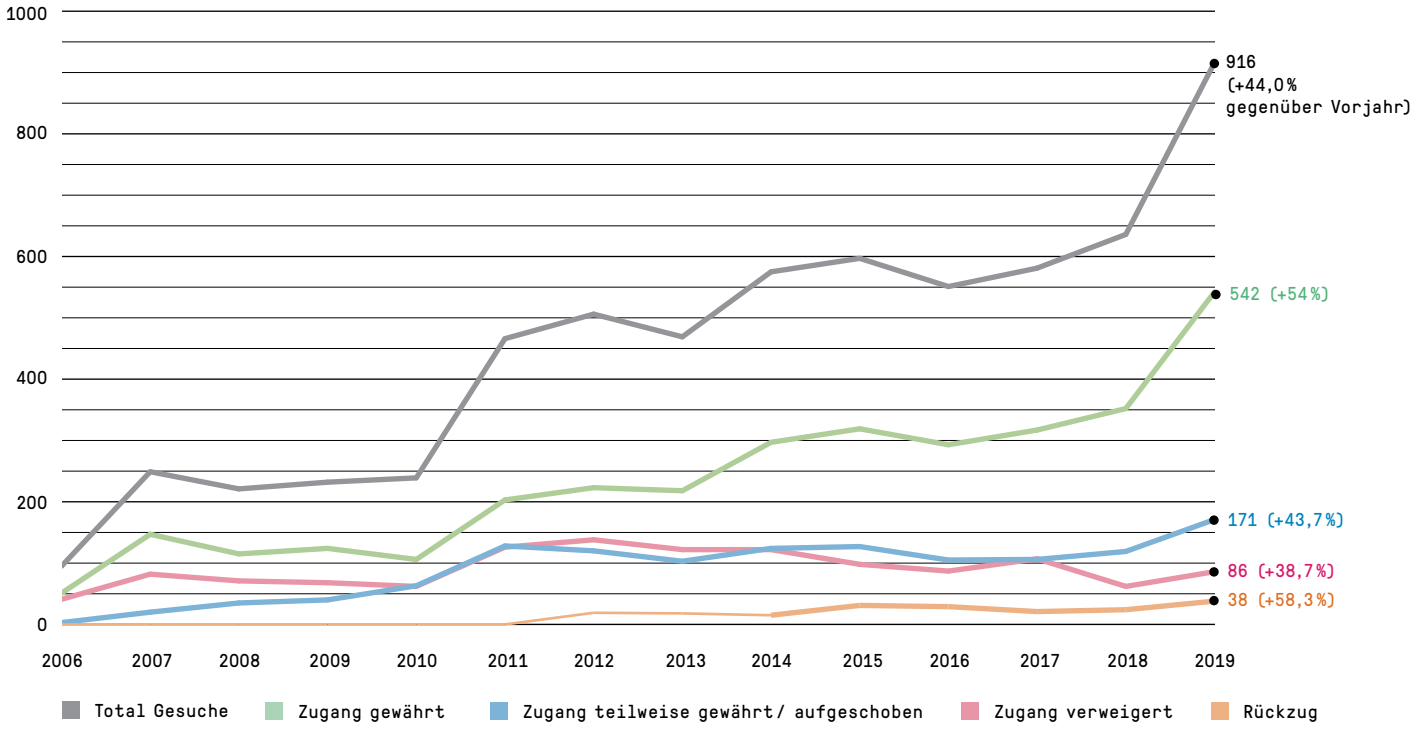
Auch in diesem Berichtsjahr bewies das Öffentlichkeitsgesetz seinen hohen Wert für die Förderung der Transparenz, der Information, sowie als Aufsichtsinstrument im Dienste der Bevölkerung. Folglich gilt es, wachsam zu sein und zu verhindern, dass es durch die Einführung neuer Bestimmungen verwässert wird, die auf die Einschränkung seines Geltungsbereichs abzielen. In diesem Berichtsjahr gab es wiederum verstärkte Bestrebungen der Verwaltung (z.B. die Eidg. Zollverwaltung und das Bundesamt für Gesundheit), Teilbereiche ihrer Tätigkeit oder bestimmte Kategorien von Dokumenten von der Verwaltungsöffentlichkeit auszunehmen. Demgegenüber hat der Bundesgesetzgeber mit seinem Bekenntnis zur Transparenz beim Bundesgesetz über das öffentliche Beschaffungswesen (BÖB) im Juni 2019 sowie mit dem Entscheid der Staatspolitischen Kommission des Nationalrates zum Grundsatz der Gebührenfreiheit für Zugangsgesuche gezeigt, dass er am Öffentlichkeitsprinzip festhält. Leider hat der Bundesrat die gegen seinen Willen geschaffene Transparenz im BÖB in seinen Ausführungsbestimmungen zu diesem Gesetz wieder teilweise eingeschränkt (s. Kap. 2.4).

2.2 Zugangsgesuche – erneute Zunahme im 2019

Gemäss den Zahlen, die von ihnen gemeldet wurden, gingen im Berichtsjahr 905 Zugangsgesuche bei den Bundesbehörden ein (für 2018 waren es 636 Gesuche). Grund für diese Zunahme ist unter anderem die Tatsache, dass allein beim BASPO 175 Zugangsgesuche eingingen. Rechnet man die Bundesanwaltschaft (10) und die Parlamentsdienste (1) mit ein, beträgt die Gesamtzahl 916; dies entspricht einer Steigerung um 44 Prozent gegenüber 2018. Zu den höheren Zahlen hat wohl auch die Tatsache beigetragen, dass die Bevölkerung nicht zuletzt dank Medienberichten über die Jahre hinweg immer bessere Kenntnisse über das Öffentlichkeitsprinzip hat und nun die Möglichkeiten, die dieses bietet, auch selber vermehrt aktiv nutzt. Es ist davon auszugehen, dass diese Tendenz auch in den kommenden Jahren anhalten wird, zumal in der Gesellschaft eine allgemeine Zunahme der Transparenzansprüche gegenüber Verwaltung und Politik festzustellen ist.

In 542 Fällen (59 Prozent) gewährten die Behörden einen vollständigen Zugang (gegenüber 352 bzw. 55 Prozent im Jahr 2018), währenddem bei 171 Gesuchen (19 Prozent) ein teilweiser Zugang zu den Dokumenten genehmigt wurde. In 86 Fällen (9 Prozent) wurde die Einsichtnahme vollständig verweigert (gegenüber 62 bzw. 10 Prozent im Jahr 2018). Nach Angaben der Behörden wurden 38 Zugangsgesuche zurückgezogen (gegenüber 24 bzw. vier Prozent im Jahr 2018), 43 Gesuche waren Ende 2019 noch hängig, und in 36 Fällen war kein amtliches Dokument vorhanden. Seit 2015 wird in mehr als 50 Prozent der Fälle ein vollständiger Zugang zu den Dokumenten gewährt. Demgegenüber sind die vollständigen Zugangsverweigerungen in der Minderzahl und pendeln sich im Laufe der Jahre auf rund zehn Prozent ein. Der EDÖB stellt fest, dass sich die Praxis der Behörden in Richtung mehr Transparenz entwickelt. Mit ihren einschlägigen Massnahmen haben mehrere Bundesbehörden zur Zunahme der gewährten Zugänge und zur Unterstützung des vom Gesetzgeber gewollten Paradigmenwechsels beigetragen (s. Kap. 3.3).

Grafik 1: Beurteilung Zugangsgesuche – Entwicklung seit 2006



Departemente und Bundesämter

Auf Stufe Amt zeigen die gemeldeten Zahlen, dass das BASPO mit 175 Fällen 2019 am meisten Zugangsgesuche erhielt. Danach folgen das BAFU und das BAG mit je 35 Gesuchen sowie das SECO (34). Bei den Departementen liegen das VBS (225) und das EDA (168) an der Spitze. Zehn Behörden meldeten hingegen, dass im Berichtsjahr bei ihnen kein einziges Zugangsgesuch eingegangen sei. Der Beauftragte selbst sah sich mit zehn Zugangsgesuchen konfrontiert, wobei er den Zugang in sechs Fällen vollständig gewährte. In einem Fall war das angeforderte Dokument nicht vorhanden, und in drei Fällen wurde das Gesuch zurückgezogen.

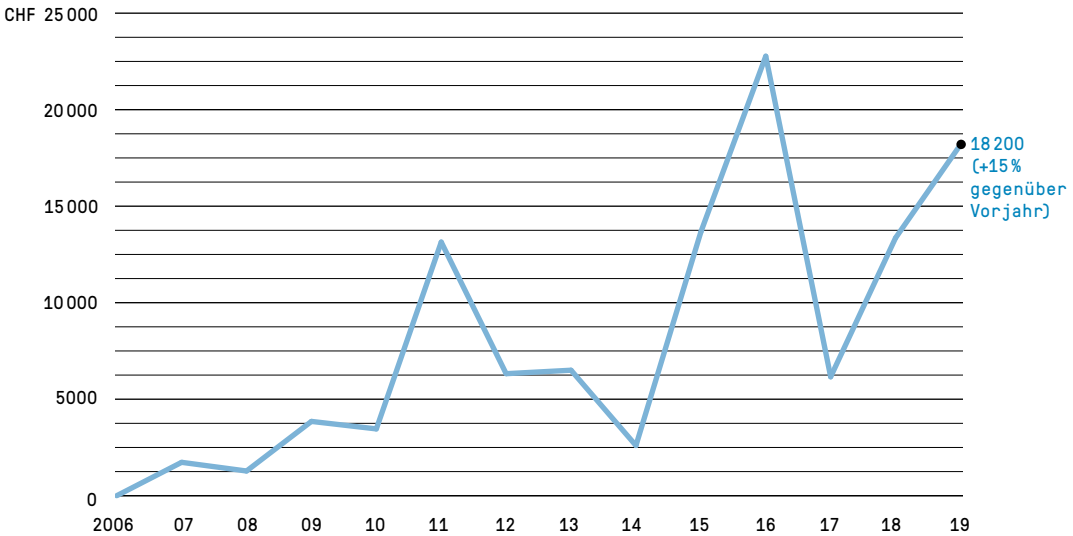
Der 2019 für den Zugang zu amtlichen Dokumenten erhobene Gebührenbetrag beläuft sich auf insgesamt CHF 18 185 und liegt damit über der Vorjahressumme (CHF 13 358), weicht jedoch gemessen an den zurückliegenden Jahren nicht von der Norm ab.

Während das EJPD und die Bundeskanzlei überhaupt keine Gebühren erhoben, verrechneten die übrigen sechs Departemente den Gesuchstellenden einen Teil ihres Zeitaufwands (DFI: CHF 8710; VBS: CHF 300; EFD: CHF 3750; WBF: CHF 700; UVEK: CHF 2750). Dazu sei vermerkt, dass lediglich bei 31 der 916 eingereichten Zugangsgesuche eine Gebühr erhoben wurde. Gegenüber dem Vorjahr, in dem nur in 17 Fällen eine Gebühr verlangt wurde, stellt dies zwar eine Zunahme dar, allerdings bei einer merklich gestiegenen Zahl der Zugangsgesuche. Wie bereits in den Vorjahren stellt die Erhebung von Gebühren weiterhin eine Ausnahme dar: In beinahe 97 Prozent besteht Gebührenfreiheit. Der EDÖB stellt jedoch bezogen auf das Berichtsjahr fest, dass die Bundesbehörden nunmehr häufiger dazu tendieren, Gebühren zu erheben, die entsprechende Betragshöhe aber eher abnimmt.

Im Zusammenhang mit der Bearbeitung der Initiative Graf Litscher (16.432 n Pa. Iv. Graf-Litscher «Gebührenregelung. Öffentlichkeitsprinzip in der Bundesverwaltung») stellte die Staatspolitische Kommission des Nationalrates fest, dass in einigen Departementen bereits Rechnungen über mehrere Tausend Franken gestellt wurden, was zu einer Aushöhlung des Prinzips des Zugangs zu amtlichen Dokumenten führt. Sie kommt zum Schluss, dass der Grundsatz der Gebührenfreiheit im Öffentlichkeitsgesetz verankert sein sollte und hat zu diesem Zweck am 14. Februar 2020 einen entsprechenden Vorschlag zur Gesetzesänderung in die Vernehmlassung geschickt.

Was den Zeitaufwand für die Bearbeitung von Zugangsgesuchen anbelangt, weist der Beauftragte erneut darauf hin, dass die Behörden nicht verpflichtet sind, diesen zu erfassen, und dass es keine für die gesamte Bundesverwaltung geltenden Vorgaben für eine einheitliche Erfassung gibt.

Grafik 2: Erhobene Gebühren seit Inkrafttreten des BGÖ



Die ihm auf freiwilliger Basis übermittelten Angaben widerspiegeln die tatsächlich geleisteten Arbeitsstunden daher nur bedingt. Gemäss diesen Angaben hat der Zeitaufwand für das Berichtsjahr mit 4375 Stunden im Vergleich zu 2018 (4827 Stunden) abgenommen. Ebenfalls rückläufig ist der Zeitaufwand für die Vorbereitung von Schlichtungsverfahren: 473 Stunden (gegenüber 672 Stunden für 2018 und 914 Stunden für 2017). Diese geringe Stundenzahl steht im Kontrast zur deutlichen Zunahme der Zahl der Schlichtungsverfahren. Es ist davon auszugehen, dass der Aufwand für die Vorbereitung der Verfahren nicht vollumfänglich erfasst wurde. Zudem wurden die Arbeitsstunden, die für den Erlass einer Verfügung oder für ein Beschwerdeverfahren geleistet wurden, dem Beauftragten oftmals nicht mitgeteilt.

Parlamentsdienste

Die Parlamentsdienste meldeten den Eingang eines einzigen Zugangsgesuchs. Es wurde vollumfänglich abgelehnt.

Bundesanwaltschaft

Die Bundesanwaltschaft meldete für 2019 den Eingang von zehn Gesuchen. In drei Fällen wurde dem Antrag stattgegeben, in einem Fall wurde der Zugang vollumfänglich verweigert. Für die übrigen Gesuche gilt, dass in zwei Fällen keine Dokumente vorhanden waren; drei weitere Fälle wurden zurückgezogen; der letzte Fall ist hängig.

2.3 Schlichtungsverfahren – bedeutende Zunahme der Schlichtungsanträge

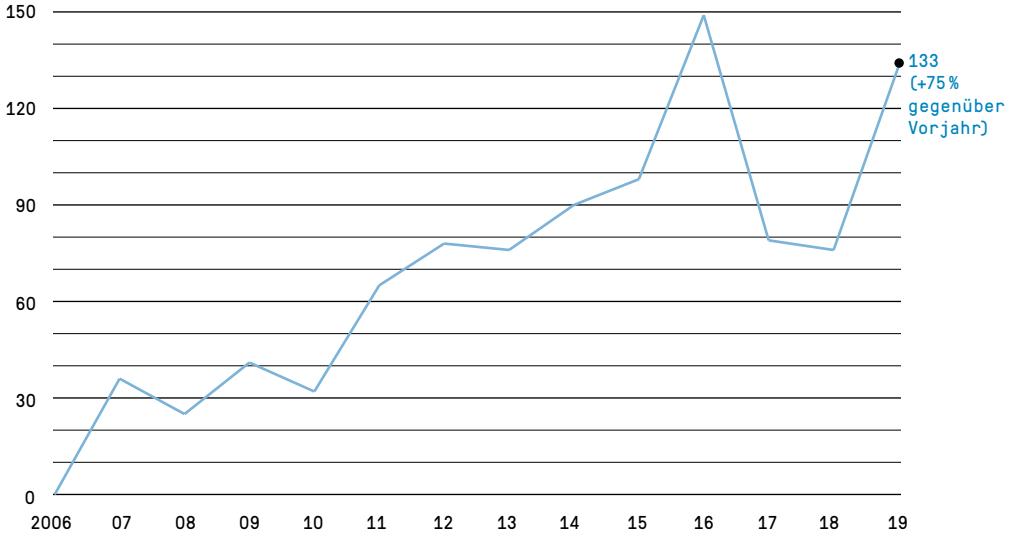
2019 erhielt der Beauftragte 133 Schlichtungsanträge. Im Vergleich zu den 2018 eingegangenen 75 Anträgen entspricht dies einer Zunahme um 75 Prozent. Die meisten Schlichtungsanträge wurden von Medienschaffenden (34), Privatpersonen (40) und Unternehmen (47) eingereicht. Diese Zahlen lassen folgende Feststellungen zu: In den 258 Fällen, in denen die Bundesverwaltung den Zugang vollständig oder teilweise verweigerte, kam es 133 Mal bzw. in 51 Prozent der Fälle, in denen das Gesuch abschlägig beschieden wurde, zur Einreichung eines Schlichtungsantrags beim Beauftragten.

Zum Teil rührt die Zunahme der Schlichtungsanträge daher, dass ein spezifisches Zugangsgesuch Abklärungen mit einer überaus grossen Zahl von betroffenen Dritten nach sich zog, von denen 28 anschliessend Schlichtungsanträge beim Beauftragten einreichten. 108 Schlichtungsanträge wurden 2019 abgearbeitet, von denen 93 im Berichtsjahr und 15 im Jahr davor eingegangen waren.

In den meisten Fällen (48) konnten sich die Beteiligten auf eine Konsenslösung einigen. Ausserdem erliess der Beauftragte 26 Empfehlungen, durch die 31 Fälle erledigt werden konnten, in denen eine einvernehmliche Lösung zwischen den Partei nicht ersichtlich war.

Zu den abgeschlossenen Fällen zu zählen sind auch sechs Schlichtungsanträge, die zurückgezogen wurden, ohne dass der Beauftragte tätig wurde, acht Fälle, in denen die Voraussetzungen für die Anwendung des Öffentlichkeitsgesetzes nicht gegeben waren sowie zwölf Anträge, die nicht fristgerecht eingereicht wurden. Per Ende Jahr war in vier Schlichtungsverfahren auf Wunsch der Beteiligten eine Sistierung erfolgt.

Grafik 3: Schlichtungsanträge seit Inkrafttreten des BGÖ



Dauer der Schlichtungsverfahren

Untenstehende Tabelle ist in drei von der Behandlungsdauer abhängige Spalten aufgeteilt. Aus ihr wird ersichtlich, dass die Mehrheit der Verfahren 2019 innerhalb der ordentlichen Frist von 30 Tagen abgearbeitet wurden. Der Genauigkeit halber sei festgehalten, dass die Zeit, in der ein Schlichtungsverfahren mit Einverständnis der Beteiligten sistiert ist, nicht zur Behandlungsdauer gezählt wird. Eine Sistierung des Schlichtungsverfahrens erfolgt insbesondere dann, wenn eine Behörde nach der Schlichtungssitzung ihre Position überprüfen möchte, oder wenn sie betroffene Dritte anhören muss.

Häufige Gründe für eine Fristüberschreitung sind eine Abwesenheit der betroffenen Personen oder Behörden (Ferien, Krankheit, Reisen), eine grosse Zahl der am Verfahren beteiligten Drittpersonen oder die juristische Komplexität der Fragestellung. Diese Gründe treffen auch auf jene vier Fälle zu, deren Bearbeitung länger als 100 Tag in Anspruch nahm, wobei drei dieser Verfahren zusammengelegt wurden. Ausserdem wurde die Einhaltung der Fristen wegen Konsultationen im Ausland, wegen zahlreicher Verhandlungsbestrebungen zwischen den Beteiligten und wegen der Fülle an Dokumenten oder der Vielzahl betroffener Personen zusätzlich verunmöglicht. Weil die Bearbeitung in derartigen Fällen oftmals besonders aufwändig ist, steht es dem Beauftragten gemäss Artikel 12a der Verordnung über das Öffentlichkeitsprinzip der Verwaltung (VBGÖ; SR 152.31) frei, die ordentliche Frist angemessen zu verlängern.

Der Vergleich mit den Vorjahren zeigt, dass die Bearbeitungsdauer der Schlichtungsverfahren seit dem Pilotprojekt 2017 stark zurückging. Diese deutliche Verkürzung geht aus den Zahlen für 2019 eindeutig hervor und bestätigt in Verbindung mit dem Anteil an einvernehmlichen Lösungen die Wirksamkeit der eingeleiteten Massnahmen, die namentlich darin bestanden, den Fokus auf die mündliche Schlichtung zu legen.

Die Vorgabe der gesetzlichen Frist von 30 Tagen für die Durchführung von Schlichtungsverfahren kann in der Regel respektiert werden, wenn die Schlichtungssitzungen planmässig, d.h. ohne Gesuch auf Verschiebung durch die Beteiligten, innert der Frist nach Eingang des Antrags erfolgreich mit einer Einigung abgeschlossen werden können. Kommt keine Einigung zustande, kann die schriftliche Empfehlung den Beteiligten nicht in jedem Fall innert 30 Tagen nach Eingang des Antrags zugestellt werden. Demgegenüber ist eine Einhaltung der Frist bereits aus Ressourcengründen nicht möglich, wenn innert einer kurzen Zeitspanne zahlreiche Schlichtungsanträge eingereicht werden. Besteht bereits ein Rückstand in der Bearbeitung von Schlichtungsverfahren, trägt jeder neu eingehende Antrag zu einem grösseren Rückstau bei. Bei komplexen Fällen und bei Mehrparteienverfahren (d.h. mehrere Drittbetroffene) erweisen sich die 30 Tage ebenfalls als (zu) kurz. Die Erfahrung zeigt zudem, dass der Beizug von Rechtsvertretungen durch angehörte Drittbetroffene bereits im Stadium des Zugangs- und Schlichtungsverfahrens einer einfachen, pragmatischen und raschen Lösungsfindung wenig förderlich ist.

Tabelle 1: Bearbeitungsdauer Schlichtungsverfahren

Bearbeitungsdauer in Tagen	Zeitraum 2014 – August 2016*	Pilotphase 2017	Zeitraum 2018	Zeitraum 2019
innert 30 Tagen	11%	59%	50%	57%
zwischen 31 und 99 Tagen	45%	37%	50%	38%
mehr als 100 Tage	44%	4%	0%	5%

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

Anteil einvernehmlicher Lösungen

Wie wirksam sich die 2017 eingeführten Massnahmen und Schlichtungssitzungen erwiesen haben, lässt sich vor allem am Anteil der einvernehmlichen Lösungen im Verhältnis zu den Empfehlungen ablesen. Zu den vielen Vorteilen der einvernehmlichen Lösungen gehört, dass sie eine Klärung der Sachlage und eine Beschleunigung des Zugangsverfahrens ermöglichen und zudem die Basis für eine allfällige zukünftige Zusammenarbeit zwischen den an der Schlichtungssitzung Beteiligten schaffen. Im Berichtsjahr konnten 48 einvernehmliche Lösungen erzielt werden, und der Beauftragte gab 26 Empfehlung zur Lösung von 31 Fällen ab. Im Verhältnis zu den Empfehlungen machen die einvernehmlichen Lösungen somit einen Anteil von 61 Prozent aus. Der Beauftragte begrüsst die weitere Zunahme der Schlichtungsverfahren, die einer einvernehmlichen Lösung zugeführt werden konnten.

Hinweis: Sämtliche Empfehlungen aus dem Berichtsjahr sind auf der Website des Beauftragten abrufbar (www.derbeauftragte.ch)

Tabelle 2: Einvernehmliche Lösungen

2013 – 2016	40 %
2017	60 %
2018	55 %
2019	61 %

Anzahl hängiger Fälle

Die unten aufgeführten Angaben geben Auskunft über die Anzahl der Fälle, die am Ende der Berichtsjahre hängig waren. Anfang Januar 2020 waren noch 43 Fälle aus dem Jahr 2019 hängig, wovon vier Verfahren sistiert wurden.

Dazu sei vermerkt, dass im November und Dezember 42 Schlichtungen beantragt wurden, von denen 40 bis zum Zeitpunkt des Redaktionsschlusses geregelt werden konnten. Dass die Zahl der hängigen Fälle deutlich über dem Vorjahr liegt, ist allerdings die logische Folge der starken Zunahme der Schlichtungsanträge und der knappen Ressourcen, die dem Beauftragten zur Verfügung stehen. In Ermangelung zusätzlicher Mittel ist die Gefahr gross, dass sich die Bearbeitungsdauer erhöht, dass die ordentliche Frist nicht mehr eingehalten werden kann und dass die Zahl der hängigen Fälle am Ende des kommenden Jahres abermals steigt.

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)
Ende 2019	43 (davon 40 bis zum Redaktionsschluss erledigt und 3 sistiert)

2.4 Ämterkonsultationen

Ämterkonsultation zum Entwurf für ein Gesetz über Zoll und Grenzsicherheit, Eröffnung des Vernehmlassungsverfahrens

Die EZV will wesentliche Bereiche ihrer Tätigkeit vom Öffentlichkeitsgesetz ausnehmen. Dies schlägt sie im Entwurf für ein neues Bundesgesetz über Zoll und Grenzsicherheit (BGZG) vor. Der Beauftragte hat sich in seiner Stellungnahme im Rahmen der Ämterkonsultation gegen diese Pläne ausgesprochen.

Im Entwurf für ein Gesetz über Zoll und Grenzsicherheit (BGZG) präsentierte die EZV Bestimmungen und Massnahmen, um wesentliche Bereiche ihrer öffentlichen Aufgabeerfüllung vom Öffentlichkeitsgesetz auszunehmen. So schlug die EZV etwa die Einführung einer Bestimmung vor, wonach die Behörde «auf freiwilliger Basis gelieferte Daten von Privaten» beziehen kann. Laut erläuterndem Bericht sollten diese «freiwillig» gelieferten Personendaten der besonderen Geheimhaltung im Sinne von Art. 7 Abs. 1 Bst. h BGÖ unterliegen. Insbesondere sollten diese Daten bearbeitet werden, um den jeweiligen Wirtschaftsbeteiligten zusätzliche Verfahrenserleichterungen einräumen zu können.

In seiner Stellungnahme hat der Beauftragte die EZV darauf hingewiesen, dass für das Vorliegen der erwähnten Ausnahmebestimmung drei Voraussetzungen kumulativ gegeben sein müssen: Erstens muss die Information von einer Privatperson mitgeteilt worden sein. Zweitens muss diese Mitteilung freiwillig und spontan erfolgt sein. Keine Freiwilligkeit liegt vor, wenn die Information im Rahmen einer gesetzlichen oder vertraglichen Verpflichtung abgegeben wurde. Drittens muss die Behörde die Geheimhaltung auf ausdrückliches Verlangen der Informantin bzw. des Informanten zugesichert haben. Die Behörde darf die Zusicherung weder von sich aus anbieten, noch darf sie diese leichtfertig abgeben. Angesichts der in Aussicht stehenden zusätzlichen Verfahrenserleichterungen durch die EZV bezweifelte der Beauftragte bereits das Vorliegen des Kriteriums der Freiwilligkeit. Zudem darf die Geheimhaltungszusicherung nur auf Anfrage der Privatperson und nur im Einzelfall abgegeben werden. Eine proaktive und generelle Zusicherung durch eine Behörde ist nicht möglich, hat doch selbst der Bundesrat in seiner Botschaft zum Öffentlichkeitsgesetzes explizit festgehalten, dass sonst der Zweck des Gesetzes, nämlich die Erleichterung des Zugangs der Öffentlichkeit zu amtlichen Dokumenten und die Förderung der Transparenz der Verwaltung, unterlaufen wird.

Der Vorschlag der EZV widerspricht somit dem Sinn und Zweck des Öffentlichkeitsgesetzes und der Ausnahmeklausel von Art. 7 Abs. 1 Bst. h BGÖ.

Des Weiteren sah der Entwurf eine Schweigepflicht vor, wonach Personen, die mit dem Vollzug dieses Gesetzes betraut sind oder dazu beigezogen werden, gegenüber anderen Behörden und Privaten über die in Ausübung ihres Amtes gemachten Wahrnehmungen Stillschweigen zu bewahren und den Einblick in amtliche Dokumente zu verweigern haben. Diese weitreichende Schweigepflicht soll nach Vorstellung der EZV auch für das Automobilsteuergesetz, Mineralölsteuergesetz und Alkoholgesetz jeweils analog gelten. Laut erläuterndem Bericht der EZV gehen heute zahlreiche Zugangsgesuche ein, die nicht die Tätigkeit der Verwaltung zum Gegenstand haben, sondern einzig darauf abzielen, heikle Wirtschaftsdaten Dritter in Erfahrung zu bringen. Die EZV verkennt hierbei, dass der Gesetzgeber den Schutz von heiklen «Wirtschaftsdaten» im Öffentlichkeitsgesetz bereits selber sichergestellt hat. So werden entsprechende Unternehmensinformationen bereits heute mit Art. 7 Abs. 1 Bst. g BGÖ (Berufs-, Geschäfts- oder Fabrikationsgeheimnisse) umfassend geschützt. Entsprechende Dokumente können bei begründetem Nachweis entsprechender Geheimnisse geschwärzt oder, wenn eine Schwärzung nicht möglich ist, gänzlich dem Zugang entzogen werden. Ausserdem können sich die betroffenen Unternehmen auf dem Rechtsweg gegen eine von der Verwaltung vorgesehene Zugangsgewährung zur Wehr setzten. Es besteht hierzu eine lanjährige bundesgerichtliche Rechtsprechung.

Zudem ignoriert die EZV mit ihrem umfassenden Vorbehalt zur Geheimhaltung den klaren Willen des Gesetzgebers, wonach das Öffentlichkeitsgesetz die Transparenz über den Auftrag, die Organisation und die Tätigkeit der Verwaltung fördern soll. Mit der Einführung des Öffentlichkeitsprinzips beabsichtigte der Gesetzgeber sogar explizit, dass die Bevölkerung Zugangsgesuche einreicht, nicht zuletzt zur Kontrolle der Behörden im Umgang mit Dritten. Das Öffentlichkeitsprinzip verfolgt somit auch das Ziel, Misswirtschaft und Korruption in der Verwaltung vorzubeugen. Indirekt schützt es somit also auch davor, dass sich einzelne Bereiche der

Bundesverwaltung dem Verdacht ausgesetzt sehen könnten, mit den Wirtschaftsbeteiligten Geheimabsprachen resp. unlautere Machenschaften zum Nachteil von anderen resp. auf Kosten der Steuerzahlenden getätigt zu haben.

Der Beauftragte hat die EZV auch darauf hingewiesen, dass missliebige Zugangsgesuche oder allfälliger Arbeitsaufwand alleine weder ausreichende noch stichhaltige Argumente für die Forderung nach einer umfassenden Schweigepflichtbestimmung sind.

Aus diesen Gründen hat der Beauftragte von der EZV in der Ämterkonsultation die Streichung dieser transparenzfeindlichen Schweigepflichtnorm für alle betroffenen Gesetze gefordert.

Aufgrund der Rückmeldungen der konsultierten Behörden überarbeitete die EZV die Vorlage und führte eine zweite Ämterkonsultation durch. Im überarbeiteten Gesetzesentwurf wurde die Bestimmung betreffend der Schweigepflicht für Personen, die mit dem Vollzug des Gesetzes betraut sind, gestrichen und der erläuternde Bericht an verschiedenen Stellen angepasst. Im übrigen hielt die EZV indes an ihrem Vorhaben fest.

Würden der Bundesrat und das Parlament der Absicht der EZV folgen, hätte diese zur Folge, dass grosse Bereiche der gesetzlichen Hauptaufgaben der EZV von der Verwaltungsöffentlichkeit ausgeschlossen wären.

Konsultationen zur Vereinbarung zwischen dem Bund und den Kantonen über die Harmonisierung und die gemeinsame Bereitstellung der Polizeitechnik und -informatik

Die Konferenz der kantonalen Justiz- und Polizeidirektoren (KKJPD) hat in einer Vereinbarung zwischen dem Bund und den Kantonen über die Harmonisierung und die gemeinsame Bereitstellung der Polizeitechnik und -informatik (VPTI Schweiz) eine Rechtswahlklausel aufgenommen, nach deren Wortlaut im Zusammenhang mit der Polizeitechnik und -informatik für die Verwaltungsöffentlichkeit nicht das Öffentlichkeitsgesetz des Bundes, sondern das kantonale bernische Recht gelten soll.

Die KKJPD hat im Jahr 2010 das Programm zur Harmonisierung der schweizerischen Polizeiinformationen (HPI) geschaffen. Mit der operativen Umsetzung des Programms wurde eine Geschäftsstelle beauftragt, die beim Schweizerischen Kompetenzzentrum für Polizeitechnik und -informatik (PTI) angesiedelt ist. Die beiden Geschäftsfelder HPI und PTI sollten nunmehr mit einer einzigen Vereinbarung zwischen dem Bund und den Kantonen geregelt werden. In den Entwurf dieser Vereinbarung wurde eine Rechtswahlklausel aufgenommen, nach welcher für alle beteiligten kantonalen und Bundesbehörden (u.a. auch) für die Verwaltungsöffentlichkeit einzig das bernische Recht über die Information der Bevölkerung anwendbar sein soll.

Bereits früher im Berichtsjahr stellte der Beauftragte im Rahmen einer Vorkonsultation durch das Bundesamt für Justiz BJ klar, dass die vorgeschlagene Rechtswahlklausel – soweit Bundesbehörden betroffen sind – das Öffentlichkeitsgesetz des Bundes umgeht und damit gegen Bundesrecht verstösst, was wiederum Art. 48 Abs. 3 der Bundesverfassung verletzt, wonach Verträge zwischen Kantonen dem Recht und den Interessen des Bundes sowie den Rechten anderer Kantone nicht zuwiderlaufen dürfen.

In einer späteren Konsultation stellte der Beauftragte gegenüber der KKJPD fest, dass zwar zwischenzeitlich seine gegenüber dem BJ vorgebrachten Bemerkungen in die Erläuterungen zur Vereinbarung aufgenommen wurden, die Rechtswahlklausel im Vereinbarungsentwurf jedoch unverändert geblieben ist. Demnach gilt – nach dem Wortlaut der Rechtswahlklausel – weiterhin für die an der Vereinbarung beteiligten Bundesbehörden das kantonale bernische Recht, so etwa in Bezug auf die Verwaltungsöffentlichkeit, für datenschutzrechtliche Belange oder für Beschaffungen. Gegenüber der KKJPD erklärte der Beauftragte, der Vorbehalt der Anwendbarkeit des Öffentlichkeitsgesetzes des Bundes für Bundesbehörden müsse nicht zuletzt aus Gründen der Rechtssicherheit in der Vereinbarung selbst stehen und nicht lediglich in den Erläuterungen, die erfahrungsgemäss erst bei der Unklarheit einer Norm gelesen würden. Abschliessend wies der Beauftragte darauf hin, wonach ungeachtet der Beteiligung einer oder mehrerer Bundesbehörden an der geplanten Vereinbarung diese weiterhin dem Öffentlichkeitsgesetz des Bundes unterstellt bleiben, sofern

sie Dokumente erstellen oder Dokumente als Hauptadressatinnen erhalten. Mit anderen Worten bedeutet dies, dass für Bundesbehörden bei der Beurteilung von Zugangsgesuchen zu amtlichen Dokumenten betreffend die Harmonisierung und die gemeinsame Bereitstellung der Polizeitechnik und -informatik nicht das kantonalbernische Recht über die Information der Bevölkerung, sondern einzig das Öffentlichkeitsgesetz des Bundes massgebend ist.

Ämterkonsultation Zentraler Nachweis amtlicher Dokumente

Das Schweizerische Bundesarchiv BAR hat beim Bundesrat die Erstellung einer Studie zum Zweck einer Entscheidungsgrundlage betreffend den Zentralen Nachweis amtlicher Dokumente beantragt. Die Präzisierungen des Beauftragten wurden im Antrag an den Bundesrat aufgenommen.

Der Bundesrat beschloss im Jahr 2008 die Einführung von GEVER und die Errichtung eines zentralen Nachweises von amtlichen Dokumenten in der Bundesverwaltung («Single Point of Orientation SPO»). SPO sollte die Metadaten der elektronischen Geschäftsverwaltung GEVER nutzen, um einen Katalog zu erstellen. Die Suchergebnisse in diesem zentralen Nachweis sollten Gesuchstellenden nach Öffentlichkeitsgesetz auch dazu dienen, präzise Zugangsgesuche stellen zu können. Das BAR entwickelte und testete im Jahr 2012 dafür eine entsprechende Pilot-Webanwendung. Das Projekt wurde in der Folge zweimal sistiert. Ende 2019 musste das BAR dem Bundesrat die aktuelle Ausgangslage darlegen und einen Vorschlag für das weitere Vorgehen präsentieren. Der Beauftragte hat im Rahmen einer Ämterkonsultation zum Vorschlag «Zentraler Nachweis amtlicher Dokumente» des BAR Stellung genommen

Ein «Zentraler Nachweis amtlicher Dokumente» samt den Metainformationen würde der Verwirklichung des Öffentlichkeitsprinzips dienen und zu einer transparenteren Verwaltung beitragen. Der Beauftragte begrüsst daher diese Bestrebungen. In seiner Stellungnahme an das BAR hat er darauf hingewiesen, dass es wichtig ist, beim Projekt «Zentraler Nachweis amtlicher Dokumente» klar zwischen dem Öffentlichkeitsgesetz und dem allgemeinen Informationsauftrag der Behörden zu unterscheiden. Das Öffentlichkeitsgesetz enthält in Art. 21 BGÖ zwar eine Vollzugsbestimmung zur Information über amtliche Dokumente. Diese schafft aber keine eigenständige Gesetzesgrundlage, sondern konkretisiert lediglich die bereits bestehende allgemeine Informationspflicht der Behörden.

Ein «Zentraler Nachweis amtlicher Dokumente» ist ein Instrument der aktiven Behördeninformation: Die Behörden haben gemäss Verfassung und des Regierungs- und Verwaltungsorganisationsgesetzes bereits heute eine allgemeine Informationspflicht, von sich aus über ihre Aufgabenbereiche und über wichtige Geschäfte zu informieren und dafür geeignete Informationen zur Verfügung zu stellen (aktive Information). Demgegenüber gelangt das Öffentlichkeitsgesetz dann zur Anwendung, wenn eine Person ein Zugangsgesuch bei einer Behörde stellt (passive Information).

Der Bundesrat hat an seiner Sitzung vom 6. Dezember 2019 beschlossen, eine Studie über die Einrichtung eines zentralen Registers der amtlichen Dokumente durchzuführen. Die Studie soll unter anderem die Art der Umsetzung eines solchen Systems, die technischen Lösungen sowie die Zuständigkeiten innerhalb der Bundesverwaltung klären. Die Ergebnisse der Studie sollen Ende 2020 präsentiert werden.

Ämterkonsultation zum Tarifvertrag CAR-T-Zelltherapie

Das Bundesamt für Gesundheit (BAG) wollte mittels eines Bundesratsbeschlusses die Tarifgenehmigung betreffend Behandlung der autologen CAR-T-Zelltherapie vom Öffentlichkeitsgesetz ausnehmen. Der Beauftragte hat sich gegen dieses Vorgehen ausgesprochen.

Das BAG beantragte dem Bundesrat die Genehmigung des Tarifvertrages zwischen den Spitälern und den Krankenversicherern (Vertragspartner) betreffend die Behandlung der autologen CAR-T-Zelltherapie. Dieser Vertrag enthält eine Vertraulichkeitsabrede, wonach die vereinbarten variablen Vergütungshöhen für die autologen CAR-T-Zelltransplantate neben den Vertragsparteien nur den Genehmigungsbehörden und den zuständigen Gesundheitsbehörden des Wohnkantons des Patienten zugänglich sein dürfen. Das BAG argumentierte u.a., der Vergütungspreis stelle ein Geschäftsgeheimnis dar. Weiter schlug es vor, dass der Bundesratsantrag sowie die in der Beilage aufgeführten Vergütungsvereinbarungen auch nach Genehmigung des Tarifvertrages durch den Bundesrat vom Zugangsrecht nach Öffentlichkeitsgesetz ausgeschlossen bleiben sollen.

In der Ämterkonsultation wies der Beauftragte das BAG zunächst darauf hin, dass die Kranken- und Unfallversicherer für den Bereich der obligatorischen Versicherung als Behörden im Sinne des Öffentlichkeitsgesetzes gelten. Die dem BAG von Dritten zum Zwecke der Tarifgenehmigung gelieferten Informationen basieren auf gesetzlichen Vorgaben (Bundesgesetz über die Krankenversicherung), weshalb diesbezüglich eine Vertraulichkeitsabrede in einem Tarifvertrag weder rechtsgültig vereinbart noch vom Bundesrat genehmigt werden kann. Zudem hielt der Beauftragte fest, dass das Öffentlichkeitsgesetz bereits sowohl den Geschäftsgeheimnisschutz als auch den Schutz der Privatsphäre gewährleistet, weshalb eine Ausnahme zum Öffentlichkeitsgesetz nicht notwendig ist. Weiter erklärte er, dass der unterzeichnete Bundesratsantrag Teil des Mitberichtsverfahrens ist und daher bereits gemäss Art. 8 Abs. 1 BGÖ vom Zugangsrecht nach Öffentlichkeitsgesetz ausgeschlossen ist, im Gegensatz zu den ihm beigefügten Beilagen.

Der Vollständigkeit halber wies der Beauftragte auch darauf hin, dass kein Anwendungsfall von Art. 8 Abs. 3 BGÖ gegeben ist, da der Tarifvertrag und die mit ihm verbundenen Vergütungsvereinbarungen bereits vor Beginn des Ämterkonsultationsverfahrens erstellt wurden und somit nicht als Dokumente dieses Verfahrens gelten (der Beauftragte äusserte sich bereits in gleicher Sache dazu, s. 26. TB, Kap. 2.4). Nach Art. 8 Abs. 3 BGÖ kann der Bundesrat zwar ausnahmsweise amtliche Dokumente des Ämterkonsultationsverfahrens nach seinem Entscheid endgültig vom Zugang ausschliessen. Er muss sich in seinem Ermessen jedoch an den Ausnahmegründen nach Öffentlichkeitsgesetz orientieren.

Der Beauftragte hat das BAG insbesondere darauf aufmerksam gemacht, dass das Öffentlichkeitsgesetz den Bundesrat nicht dazu berechtigt, amtliche Dokumente mittels Beschluss vom Anwendungsbereich des Öffentlichkeitsgesetzes auszunehmen, indem er – unter Umgehung des ordentlichen Gesetzgebungsprozesses – den Geltungsbereich des Öffentlichkeitsgesetzes nach seinem Willen und Ermessen einschränkt.

Das BAG modifizierte in der Folge den Bundesratsantrag. Indessen lancierte es nur wenige Wochen später die Forderung nach einer Bereichsausnahme vom Öffentlichkeitsgesetz erneut und schlug eine entsprechende Teilrevision des Krankenversicherungsgesetzes vor (s. unten).

Ämterkonsultation Vernehmlassung der Teilrevision des KVG betreffend Massnahmen zur Kostendämpfung – 2. Paket

Der Beauftragte wehrte sich gegen die Absicht des Bundesrates, eine Ausnahme vom Öffentlichkeitsprinzip für Dokumente betreffend Preismodelle bei Arzneimitteln in der Krankenversicherung einzuführen.

Das Bundesamt für Gesundheit BAG hat im Rahmen einer Ämterkonsultation u.a. eine Ausnahme der Zugänglichkeit zu den Unterlagen betreffend die Höhe, die Berechnung und die Modalitäten im Rahmen von Preismodellen und Rückvergütungen in der obligatorischen Krankenpflegeversicherung vorgeschlagen.

Bei der Preisfestlegung von Medikamenten der Spezialitätenliste (SL) können zwischen den Pharmaunternehmen als Zulassungsinhaber und den Krankenversicherern Rabatte verhandelt werden (sogenannte Preismodelle). Bei Preismodellen unterscheidet sich der offizielle Preis auf der SL vom tatsächlichen Preis, den der Krankenversicherer dem Pharmaunternehmen auszuzahlen hat (Rückerstattung).

Mit seinem Vorhaben will der Bundesrat sämtliche Unterlagen im Zusammenhang mit Preismodellen neu vom Geltungsbereich des Öffentlichkeitsgesetzes ausnehmen. Die vereinbarten Rabatte und der vollständige Rückvergütungsmechanismus sollen der Bevölkerung nicht bekannt gegeben werden.

Der Bundesrat vertritt die Auffassung, dass die Pharmaunternehmen bei einer Offenlegung der tatsächlichen Preise nicht mehr bereit wären, solche Preismodelle zu verhandeln. Der Bundesrat argumentiert auch damit, dass die Mehrheit der Zugangsgesuche im Zusammenhang mit Unterlagen von Arzneimitteln der Spezialitätenliste nicht von Bürgern gestellt werden, die sich über staatliches Handeln informieren wollen, sondern insbesondere von Pharmaunternehmen, welche Einsicht in Geschäftsinformationen von konkurrierenden Unternehmen verlangen. Dem ist entgegenzuhalten, dass auch Mitkonkurrenten ein legitimes Interesse daran haben, die Genehmigungspraxis des BAG bei Konkurrenzprodukten überprüfen zu können. Geschäfts- und Fabrikationsgeheimnisse und die Privatsphäre der betroffenen Unternehmen bleiben auch bei Anwendung des Öffentlichkeitsgesetzes explizit geschützt.

Die Verankerung einer Geheimhaltungsbestimmung im Krankenversicherungsgesetz geht nach Ansicht des Beauftragten in die falsche Richtung. In seiner Stellungnahme im Rahmen der Ämterkonsultation erinnerte er daran, dass mit dem Öffentlichkeitsprinzip das Verständnis für die Verwaltung und ihr Funktionieren gefördert sowie die Akzeptanz staatlichen Handelns erhöht werden soll.

Der Einsatz von solchen Preismodellen durch das BAG ist ein Instrument der Preispolitik, das immer öfter zur Anwendung gelangt. Demgegenüber besteht ein breit abgestützter Konsens nach Kostentransparenz im Gesundheitswesen, zumal die kontinuierlich steigenden Krankenkassenprämien von der Bevölkerung seit Jahren als eine ihrer grössten Sorgen bezeichnet werden. Vor diesem Hintergrund ist es unabdingbar, dass sowohl für die Bevölkerung als auch für die Mitbewerberinnen weiterhin die Möglichkeit besteht, die Genehmigungspraxis des BAG umfassend nachvollziehen und kontrollieren zu können. Mittel- und langfristig würde eine aktive Transparenzstrategie, insbesondere auf internationaler Ebene, zu tieferen Preisen führen. Eine starke Kooperation unter den Staaten ist für eine echt wirksame Preispolitik langfristig unabdingbar.

Das BAG hat den Bedenken des Beauftragten nicht Rechnung getragen. Der Bundesrat wird demnächst eine Vernehmlassung für eine Teilrevision des KVG eröffnen.

Ämterkonsultation zur Totalrevision der Verordnung über das öffentliche Beschaffungswesen

Im Rahmen der Erarbeitung der Totalrevision der Verordnung über das öffentliche Beschaffungswesen hat sich eine Differenz zwischen dem Beauftragten und dem Bundesrat in Bezug auf die Zugänglichkeit der neuen Liste der sanktionierten Anbieterinnen ergeben.

Das Parlament hat am 21. Juni 2019 die Totalrevision des Bundesgesetzes über das öffentliche Beschaffungswesen (BöB) verabschiedet (Geschäftsnr. 17.019). Entgegen der vom Bundesrat geplanten vollständigen Ausnahme bleibt das Öffentlichkeitsprinzip im öffentlichen Beschaffungswesen in der neuen Vorlage – wie bereits im aktuell geltenden BöB – weiterhin verankert. Der Beauftragte hatte sich im Ämterkonsultationsverfahren und im Verlauf der parlamentarischen Beratungen dezidiert dafür eingesetzt (vgl. 26. Tätigkeitsbericht 2018/19, Ziffer 2.4). Im ersten Teil des Berichtsjahres präsentierte das BBL den Entwurf der totalrevidierten dazugehörigen Verordnung im Rahmen einer Ämterkonsultation. Mit Art. 45 Abs. 3 des vom Parlament verabschiedeten Gesetzes wurde eine Liste der sanktionierten Anbieterinnen und Subunternehmerinnen eingeführt, die als «nicht öffentlich» bezeichnet wird. Auf der Liste werden diejenigen Unternehmen aufgeführt, gegen welche ein rechtskräftiger Ausschluss von künftigen öffentlichen Aufträgen ausgesprochen wurde, weil sie zum Beispiel die Bestimmungen über die Bekämpfung der Korruption verletzt oder unzulässige Wettbewerbsabreden getroffen haben.

Art 25 Abs. 3 der revidierten Verordnung regelt ein gesondertes Zugangsrecht zu dieser Liste einzig für die Vergabestellen, nicht aber ein allgemeines Recht auf Einsicht für die Bevölkerung. Im erläuternden Bericht zur Verordnung wird dazu präzisiert, dass laut Botschaft zum BöB kein Zugangsrecht zur Liste nach Öffentlichkeitsgesetz besteht.

Der Beauftragte hat sich im Rahmen der Ämterkonsultation gegen diese Auslegung ausgesprochen: Im bundesrätlichen Entwurf zum revidierten BöB waren sämtliche Dokumente im Zusammenhang mit der Beschaffung vollständig vom Anwendungsbereich des Öffentlichkeitsgesetzes ausgeschlossen. Das Parlament hat sich jedoch für vollständige Transparenz im öffentlichen Beschaffungswesen entschieden und die Pläne des Bundesrates nach Geheimhaltung abgelehnt. Dem klaren Willen des Gesetzgebers zur Transparenz folgend muss somit das Öffentlichkeitsgesetz ohne jede Einschränkung auf das revidierte BöB Anwendung finden.

Der Beauftragte ist ausserdem der Ansicht, dass die blosse Bezeichnung der Liste im Gesetz als «nicht öffentlich» nicht ausreicht, um sie als «geheim» im Sinne einer Spezialbestimmung von Art. 4 BGÖ zu qualifizieren. Dafür bräuchte es einen expliziten formell-gesetzlichen Vorbehalt zum Öffentlichkeitsgesetz im BöB selber. Vielmehr bedeutet «nicht öffentlich» lediglich, dass die Liste durch die Behörde nicht aktiv publiziert wird. Aus dem Wortlaut der Gesetzesbestimmung ergibt sich keineswegs, dass die Liste auf Zugangsgesuch hin als geheim zu halten ist. Diese Differenz konnte nicht beseitigt werden. Der Bundesrat hat die Einwände des Beauftragten verworfen.

Das revidierte Gesetz und die dazu gehörige Verordnung werden am 1. Januar 2021 in Kraft treten.

Der EDÖB

3.1 Aufgaben und Ressourcen

Der Beauftragte

An seiner Sitzung vom 10. April 2019 hat der Bundesrat Adrian Lobsiger für eine zweite Amtsdauer (51. Legislatur) wiedergewählt. Diese dauert bis Ende 2023.

Leistungen und Ressourcen im Bereich Datenschutz

Personalbestände

Von 2005 bis 2019 hat der Stellenetat für den Vollzug des Datenschutzgesetzes (DSG) zwischen zwanzig und 24 Vollzeitstellen 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 neun bis zehn Stellen in Aussicht gestellt (BBl 2017 7172). Inzwischen hat der Bundesgesetzgeber mit dem neuen Bundesgesetz über den Datenschutz im Rahmen der Anwendung des Schengen-Besitzstands in Strafsachen (SDSG, SR 235.3) einen Teilaspekt dieser Totalrevision vorweggenommen. Das SDSG betraut unsere Behörden bezüglich der besonders sensiblen Bearbeitung von Personendaten im Polizeibereich mit zusätzlichen Aufgaben und Befugnissen (s. 26. TB, Kap 1.2). Nachdem der Bundesrat dieses Gesetz am 1. März 2019 in Kraft setzte, hat er dem EDÖB für die Umsetzung der neuen Aufgaben und Befugnisse drei zusätzliche Stellen zugesprochen. Damit hat sich der Stellenetat für das Datenschutzpersonal seit 2005 erstmals erhöht. Diese drei zusätzlichen Stellen konnten bis im Frühjahr 2020 besetzt werden, sodass sich der Stellenetat des EDÖB neu auf 27 Vollzeitstellen beläuft. Aufgrund des engen Geltungsbereiches des SDSG wird das zusätzlich rekrutierte Personal schwerpunktmässig im Bereich unserer Aufsicht über die Polizeibehörden des Bundes einzusetzen sein. Aufgrund von Abgängen hat sich die Altersstruktur der Behörde verjüngt, was den Personalkredit entlastet und in der folgenden Berichtsperiode voraussichtlich eine zusätzliche Erhöhung unseres Mitarbeiterbestandes erlauben wird.

Wann der EDÖB das weitere, zur Umsetzung der Totalrevision in Aussicht gestellte Personal beantragen und rekrutieren kann, hängt vom nach wie vor ungewissen Zeitpunkt des Inkrafttretens des neuen DSG ab. Gemäss dem von beiden Kammern der Eidgenössischen Räte genehmigten Art. 40a der Vorlage wird der Beauftragte den Entwurf seines Budgets erstmals im Frühjahr nach Inkrafttreten des Gesetzes dem Bundesrat einreichen. Im Frühling welchen Jahres dies sein wird, ist zurzeit offen. Der Bundesrat wird den Entwurf dannzumal unverändert an die Bundesversammlung leiten, und Letztere wird dann bis im darauffolgenden Winter entscheiden, ob und in welchem Umfang sie unser Budget erhöht.

Tabelle 4: Für DSG-Belange einsetzbare Stellen

2005	22
2010	23
2018	24
2019	24
2020	27

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 1.4.2019 bis 31.3.2020 wurden die beim EDÖB für den Datenschutz einsetzbaren Personalressourcen wie folgt auf diese Gruppen aufgeteilt:

Tabelle 5: Leistungen Datenschutz

Beratung Private	16,5%	
Beratung Bund	18,8%	
Zusammenarbeit mit Kantonen	2,5%	
Zusammenarbeit mit ausl. Behörden	12%	
Total Beratung		**49,8%**
Aufsicht	16%	
Zertifizierung	0,1%	
Register Datensammlung	0,6%	
Total Aufsicht		**16,7%**
Information	18,7%	
Ausbildung/Referate	5,5%	
Total Information		**24,2%**
Gesetzgebung	9,3%	
Total Gesetzgebung		**9,3%**
Total Datenschutz		**100,0%**

Beratung

Wie im Eingangskapitel «Aktuelle Herausforderungen und Schwerpunkte» dargelegt, sieht sich der EDÖB im Leistungsbereich der Beratung, aufgrund der Notwendigkeit digitale Grossprojekte zu begleiten, mit einer weiter anwachsenden Nachfrage konfrontiert. Aufgrund der Notwenigkeit, unsere Aufsichtstätigkeit zu stärken, haben sich die für die Beratung aufgewendeten personellen Mittel um rund vier Prozent auf 49,8 Prozent vermindert. Gemäss dem Kontrollplan des EDÖB für das Jahr 2020 ist die beratende Begleitung von zwölf grossen Projekten im Gang.

Tabelle 6: Beratungen in umfangreicheren Projekten für 2019

Grundrechte	1
Verkehr	1
Finanzen	1
Gesundheit und Arbeit	3
Sicherheit	2
Telekom	1
Medien	1
Handel und Wirtschaft	2
Total	**12**

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 65 Anfragen und Meldungen von Bürgerinnen und Bürgern mit einem Standardschreiben beantwortet, das die Betroffenen auf den zivilprozessualen Weg verweist.

Das führt zunehmend auf Unverständnis, weil einerseits die Datenschutzgrundverordnung der EU die dortigen Datenschutzbehörden verpflichtet, allen Bürgerklagen nachzugehen, und andrerseits die Vorlage zur Totalrevision des DSG auch für den EDÖB eine ausweitende Pflicht vorsieht, Einzelanliegen der Schweizer Bevölkerung materiell zu behandeln.

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 cloudgestützten Applikationen müssen Kontrollen heute rasch durchgeführt werden. Diese Beschleunigung sowie die immer wichtiger werdende Kombination von juristischem und technischem Fachwissen schliessen längere Unterbrüche bei den Sachverhaltsklärungen aus, sodass umfassendere Kontrollen von mehreren Mitarbeitenden betreut werden müssen. Die aktuellen Personalbestände setzen der Dichte der Kontrollen enge Grenzen. Im Jahr 2018 wurden für die Aufsichtstätigkeit rund zwölf Prozent der Personalressourcen aufgewendet, was deutlich unter dem langjährigen Mittelwert von rund zwanzig Prozent lag. In der letzten und aktuellen Berichtsperiode ist der Anteil nun wieder auf rund 17 Prozent gestiegen.

Gemäss Kontrollplan für das Jahr 2020 werden mit diesen Mitteln fünfzehn umfassendere Kontrollen bestritten. Im Vergleich zu der Anzahl von rund 12 000 grossen und mittleren kaufmännischen Unternehmen sowie rund 100 000 Stiftungen und Vereinen 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 von 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 Absinken der Kontrolldichte beigetragen hat. Dennoch ist es uns in der vorletzten Berichtsperiode gelungen, diesen Trend zu stoppen. Angesichts unserer knappen Mittel, sehen wir uns gezwungen, unsere Stellungnahmen im Rahmen von Konsultationen summarisch zu begründen sowie unsere Leistungen in anderen Aufgabenbereichen zu kürzen.

Totalrevision des DSG

Wie im letzten Jahresbericht ausgeführt 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. Tab. 6) 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 das in Totalrevision stehende DSG denn auch vorsieht. Da nach wie vor nicht absehbar ist, wann das neue DSG in Kraft treten wird, muss unsere Behörde die neuen Arbeitsinstrumente mit den bestehenden Personalressourcen pragmatisch umsetzen.

Teilnahme an Kommissionsberatungen und Anhörungen durch parlamentarische Kommissionen

Nachdem wir der Subkommission EJPD/BK der Geschäftsprüfungskommission des Ständerats (GPK-S) in der Vorperiode im Rahmen eines Dienststellenbesuches die Ergebnisse des Pilotversuchs «Beschleunigung Schlichtungsverfahren» präsentiert hatten, konnten wir die Subkommission im April 2019 bei einer Anhörung nunmehr über die erfolgreiche Überführung des Versuchs in den ordentlichen Betrieb informieren.

Weitere Anhörungen im Berichtsjahr betrafen die systematische Verwendung der AHV-Nummer durch Behörden (Änderung AHVG) im Februar 2020 in der Staatspolitischen Kommission des Ständerats sowie im Oktober 2019 von der Subkommission EDI/Uvek der GPK-N zum Elektronischen Patientendossier EPD. Teilgenommen haben wir ausserdem im April und Mai 2019 an der Beratung zum Bundesgesetz über elektronische Identifizierungsdienste in der Rechtskommission des Ständerates (RK-S).

Bemessungskriterien

Ob und in welchem Mass dem EDÖB 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 (s. Tab. 7):

Leistungen und Ressourcen im Bereich Öffentlichkeitsgesetz

Der Direktionsbereich Öffentlichkeitsprinzip, wo unverändert 3,6 Stellen eingesetzt werden, ist nach Durchführung eines einjährigen Versuchs im Jahr 2017 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 in der Regel auf prozessual und inhaltlich komplexe Fälle beschränkt werden konnten. Das laufende Berichtsjahr hat indes auch gezeigt, dass ein Anstieg der Zahl der Schlichtungsanträge, zahlreiche Anträge innerhalb eines kurzen Zeitraums und personelle Vakanzen rasch Arbeitsrückstände verursachen, welche zur Folge haben, dass die gesetzlichen Fristen für die Durchführung des Schlichtungsverfahrens nicht mehr eingehalten werden können (s. Kap. 2.3).

Hält die Tendenz bei der Zunahme von (komplexen) Schlichtungsanträgen an, besteht das Risiko, dass sich der Rückstau bei der Bearbeitung von Verfahren negativ auf die neu eröffneten Fälle auswirken wird.

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

Ausbau aufgrund von zusätzlichen Aufgaben und fehlender kritischer Grösse

Unsere Behörde ist bestrebt, Medienschaffende und die breite Öffentlichkeit wirksam über die Themen zum Schutz der Privatsphäre und des Öffentlichkeitsprinzips in der Verwaltung zu informieren und den entsprechenden Dialog zu pflegen. Wir nutzen dafür als zentralen Kommunikationskanal die Website, die jeden Tag rund 2000 Personen besuchen. Im Berichtsjahr hat das Eidgenössische Parlament die Beratung der Totalrevision des Datenschutzgesetzes (DSG) vorangetrieben. Mit Blick auf das zu erwartende Inkraftsetzen wird auch der Informationsbedarf von Bevölkerung, Unternehmen und Behörden weiter ansteigen.

Der Fachbereich Kommunikation musste sich mit seinen eineinhalb Vollzeitstellen auch in diesem Berichtsjahr auf die mediale Begleitung der wichtigen operativen Geschäfte konzentrieren. Weil das revidierte DSG neue Pflichten für die Wirtschaft und zusätzliche Aufgaben und Befugnisse für unsere Behörde vorsieht, soll der Kommunikationsdienst auf zweieinhalb Stellenprozente ausgebaut werden. Die entsprechende Stellenausschreibung konnte vor Ablauf der Berichtsperiode eingeleitet werden.

Vorrangig wird es darum gehen, das revidierte Gesetz kommunikativ zu begleiten und im Sinne der Information und Sensibilisierung die dafür geeigneten Massnahmen zu ergreifen. Dazu gehören auch crossmediale Inhalte und audiovisuelle Formate. In erster Priorität aber müssen unsere bestehenden Merkblätter, Erläuterungen und Leitfäden im Hinblick auf die neuen Gesetzes- und Verordnungsbestimmungen überprüft und überarbeitet sowie gänzlich neue Wegleitungen geschaffen werden.

Hohes mediales Interesse – auch im Ausland

Das Interesse der medialen Öffentlichkeit am Datenschutz hat sich weiter verstärkt – aufgrund unserer aufsichtsrechtlichen Zuständigkeit über das Libra-Projekt gelangten zudem vermehrt ausländische Medien an den EDÖB und wurde der Austausch mit den internationalen Datenschutzbehörden intensiviert. Die mediale Aufmerksamkeit zeigte sich in zahlreichen Stellungnahmen des Beauftragten – namentlich auch in einer zeitweise hohen Präsenz in TV-Formaten. In den vom EDÖB beobachteten Print- und Radio-/TV-Medien erschienen rund 2000 Beiträge und Artikel, die sich vorwiegend mit Datenschutzfragen befassten, aber auch das Öffentlichkeitsprinzip in der Verwaltung thematisierten. Bei der Beobachtung der wichtigsten sozialen Medien und Online-Plattformen (Social Web) wurden 2019 rund 8800 Erwähnungen des Beauftragten oder der Sprecher gezählt – doppelt soviel wie im 2018 und mit einer sehr hohen Aktivität im englischsprachigen Raum vornehmlich wegen Libra. Insgesamt haben wir rund 450 Medienanfragen bearbeitet.

Bürgerinnen und Bürger sowie Unternehmen nutzten Mail, den Postweg oder die telefonische Hotline, um ihre Anliegen und Fragen bei unseren Fachleuten anzubringen – insgesamt erreichten uns über diese Kanäle rund 3000 Anfragen.

Wiederum nahm der Beauftragte bei gegen 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.

Weiter trat der Beauftragte auf einem Podium am dritten Schweizer Digitaltag auf und nahm in auflagestarken Unternehmensmagazinen die Gelegenheit wahr, um für den Schutz der Privatsphäre zu sensibilisieren wie zum Beispiel in Verkehrs-, Finanz- oder Gesundheitspublikationen.

Gemeinsame Kommunikation der Datenschutzbehörden von Bund und Kantonen am Internationalen Datenschutztag

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 im Januar 2020 gemeinsam über zunehmende Gefahren für die Privatsphäre im privaten und öffentlichen Verkehr. Auslöser der datenschutzrechtlichen Risiken sind namentlich die Vermessung durch Videoaufzeichnungen und die Erstellung von Bewegungsprofilen, welche etwa durch die Entwicklung immer neuerer Mobilitäts-Apps und intelligente Fahrzeuge (Stichwort «Connected Cars») Einzug in den Alltag halten bzw. gehalten haben.

Stellungnahmen, Empfehlungen und Publikationen

Im Berichtsjahr veröffentlichte der Beauftragte diverse Stellungnahmen und Statements zu aktuellen Projekten und Ereignissen – unter anderem zu folgenden Themen:

- in Bezug auf die Libra Association mit Sitz in Genf, welche im Juli 2019 bekannt gab, ein Projekt für eine weltweite Kryptowährung lanciert zu haben;
- betreffend der amerikanischen Applikation Clearview, welche, wie im Januar 2020 bekannt wurde, massenhaft Gesichtsdaten aus öffentlich zugänglichen Quellen abschöpft und kommerzialisiert;
- zum Wahlfeature von Facebook, das bei den Eidgenössischen Wahlen im Oktober 2019 in der Schweiz eingesetzt worden ist;
- zu den Folgen des Brexit für den internationalen Datenverkehr der Schweiz ab dem 31. Januar 2020;
- zur Ungleichbehandlung von Schweizerinnen und Schweizern gegenüber Bürgern der EU durch die Postfinance bei deren Anwendung eines Stimmabdrucks (sog. Voiceprint) im Kundencenter;
- zu verschiedensten Aspekten, welche im Zusammenhang mit der Coronakrise ein starkes Interesse erzeugten wie beispielsweise die Proximity Tracing App, der Zugang des BAG auf Standortdaten der Swisscom oder die Nutzung von Videochats.

Auf der Website des EDÖB publizierten wir 23 Empfehlungen betreffend das Öffentlichkeitsprinzip.

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

Die Publikation des jährlichen Tätigkeitsberichts erfolgt wie im Vorjahr in vier Sprachen – sowohl als gedruckte Version wie auch als auf der Website verlinktes E-Paper.

Website nach wie vor wichtigster Kanal unserer Kommunikation

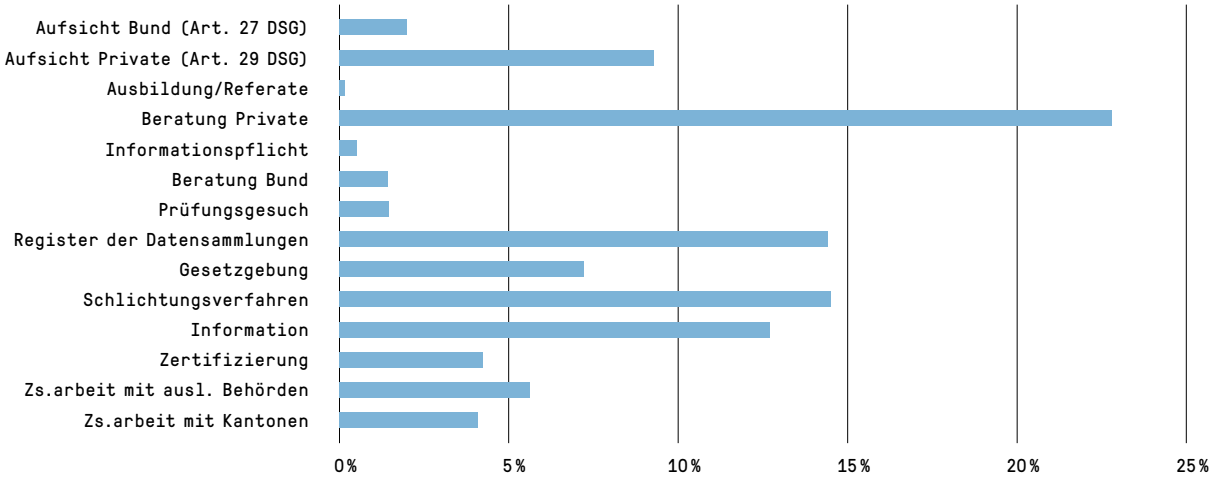
Die Webseite ist der zentrale Kommunikationskanal des EDÖB. Wir zählen jährlich rund eine halbe Million Besucherinnen und Besucher oder etwa 2000 an einem Arbeitstag. Zwei von fünf Besuchern kommen aus dem Ausland – mehrheitlich aus europäischen Staaten, aber auch aus Übersee oder Asien. Die Inhalte sind in der Regel in den drei Sprachen Deutsch, Französisch und Italienisch abrufbar. Inhalte, die für ausländische Nutzerinnen und Nutzer relevant sind, publizieren wir zusätzlich in Englisch. Der Webauftritt wird schrittweise optimiert.

Unter @derBeauftragte kommunizieren wir zudem via Twitter. Ziel ist es, unseren Followern und einer weiteren, am Datenschutz interessierten Community den raschen Zugang zu relevanten Informationen zu erleichtern. Auf die offizielle Nutzung anderer Social Media Plattformen hat unsere Behörde aufgrund knapper Ressourcen – aber auch aus anderen Gründen – verzichtet.

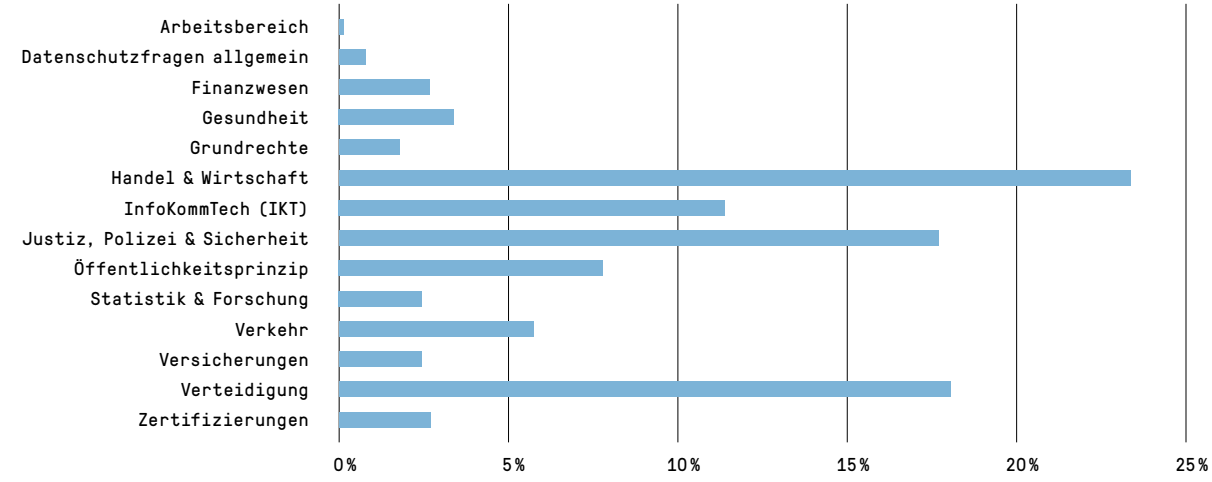
3.3 Statistiken

Statistiken über die Tätigkeiten des EDÖB vom 1. April 2019 bis 31. März 2020 (Datenschutz)

Aufwand nach Aufgabengebiet

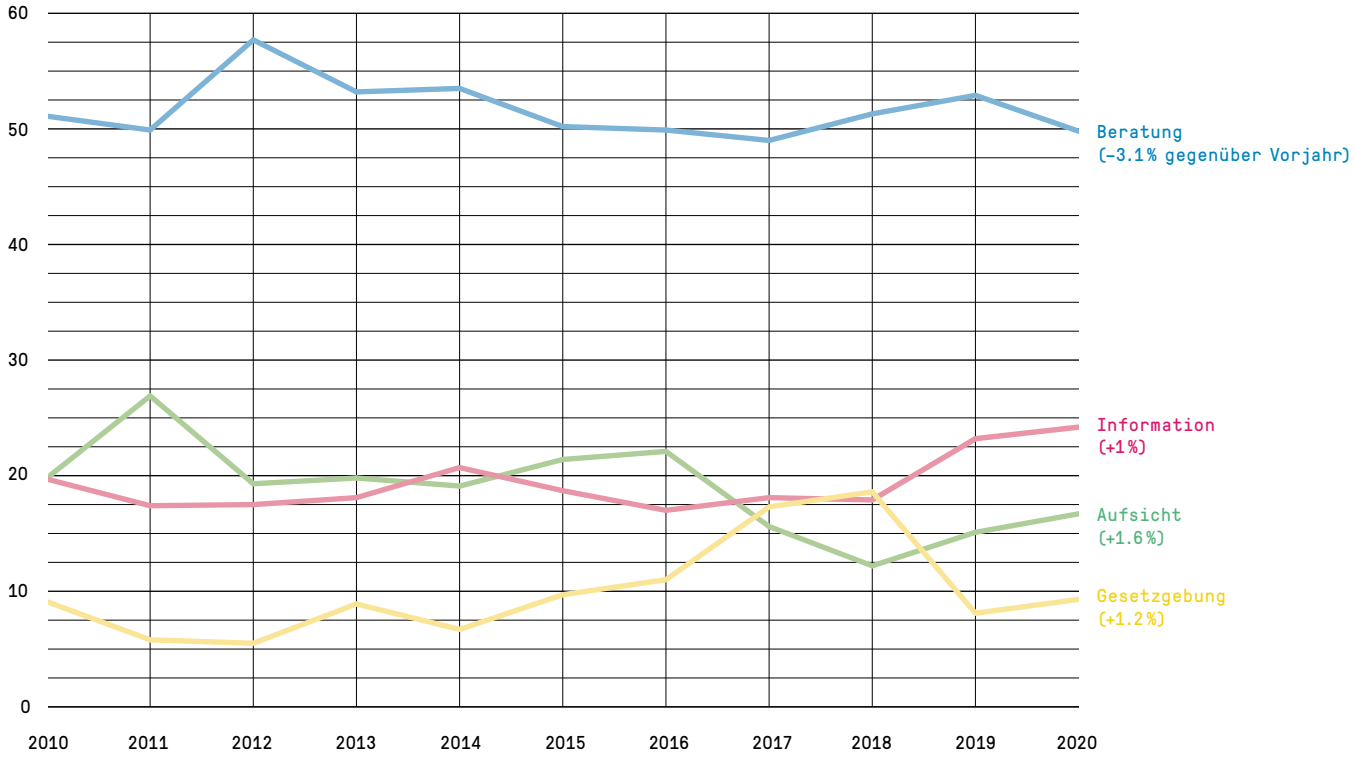


Aufwand nach Sachgebiet



Mehrjahresvergleich Aufwand

(Angaben in Prozent)



Übersicht der Zugangsgesuche vom 1. Januar bis 31. Dezember 2019

Departement	Anzahl Gesuche		Zugang vollständig gewährt		Zugang vollständig verweigert		Zugang teilweise gewährt/aufgeschoben		Zugangsgesuch zurückgezogen		Zugangsgesuch hängig		kein amtliches Dokument vorhanden	
BK	24		12		3		2		4		0		3	
EDA	168		89		15		38		7		10		9	
EDI	126		52		15		31		8		9		11	
EJPD	48		27		8		9		2		1		1	
VBS	225		193		6		14		6		4		2	
EFD	102		49		17		25		2		4		5	
WBF	100		50		11		27		3		7		2	
UVEK	112		67		9		25		3		7		1	
BA	10		3		1		0		3		1		2	
PD	1		0		1		0		0		0		0	
Total 2019 (%)	916	(100)	542	(59)	86	(9)	171	(19)	38	(4)	43	(5)	36	(4)
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)	–	

Statistiken über eingereichte Zugangsgesuche nach Öffentlichkeitsgesetz vom 1. Januar bis 31. Dezember 2019

	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	**14**	6	3	2	1	0	2
	EDÖB	**10**	6	0	0	3	0	1
	Total	**24**	**12**	**3**	**2**	**4**	**0**	**3**
Eidg.Departement für Auswärtige Angelegenheiten EDA	EDA	**168**	89	15	38	7	10	9
	Total	**168**	**89**	**15**	**38**	**7**	**10**	**9**
Eidg.Departement des Inneren EDI	GS EDI	**8**	3	2	3	0	0	0
	EBG	**3**	2	0	0	0	0	1
	BAK	**4**	3	0	1	0	0	0
	BAR	**2**	2	0	0	0	0	0
	METEO CH	**1**	1	0	0	0	0	0
	NB	**0**	0	0	0	0	0	0
	BAG	**35**	6	3	14	3	2	7
	BFS	**6**	3	3	0	0	0	0
	BSV	**15**	12	0	0	0	3	0
	BLV	**14**	3	1	7	0	0	3
	SNM	**0**	0	0	0	0	0	0
	SWISS MEDIC	**31**	14	3	5	5	4	0
	SUVA	**7**	3	3	1	0	0	0
	Total	**126**	**52**	**15**	**31**	**8**	**9**	**11**
Eidg.Justiz- und Polizeidepartement EJPD	GS EJPD	**6**	5	0	1	0	0	0
	BJ	**12**	8	0	4	0	0	0
	FEDPOL	**5**	2	0	3	0	0	0
	METAS	**4**	3	1	0	0	0	0
	SEM	**9**	3	3	0	1	1	1
	Dienst ÜPF	**2**	0	2	0	0	0	0
	SIR	**4**	2	0	1	1	0	0
	IGE	**0**	0	0	0	0	0	0
	ESBK	**3**	3	0	0	0	0	0
	ESchK	**0**	0	0	0	0	0	0
	RAB	**2**	0	2	0	0	0	0
	ISC	**1**	1	0	0	0	0	0
	NKVF	**0**	0	0	0	0	0	0
	Total	**48**	**27**	**8**	**9**	**2**	**1**	**1**

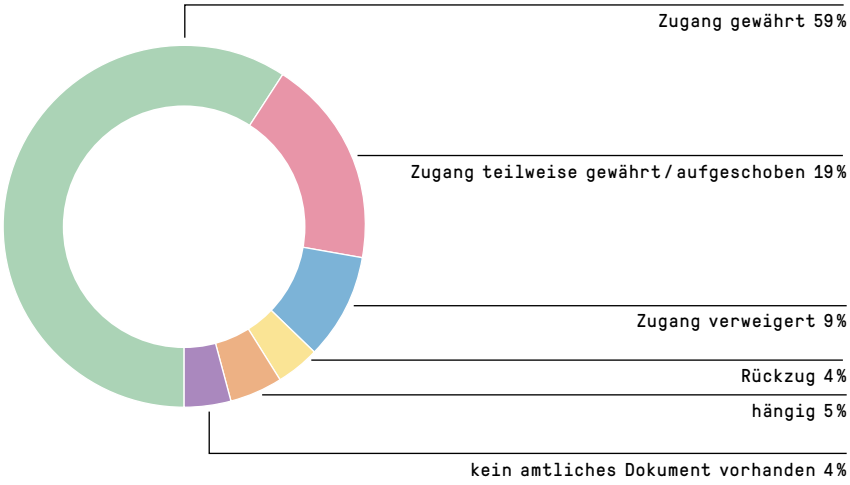
	Betroffener Fachbereich	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt/aufgeschoben	Zugangsgesuch zurückgezogen	Zugangsgesuch hängig	Kein amtliches Dokument vorhanden
Eidg.Departement für Verteidigung, Bevölkerungsschutz und Sport VBS	GS VBS	**5**	4	0	1	0	0	0
	Verteidig./ Armee	**24**	9	1	9	3	1	1
	NDB	**10**	1	3	3	1	1	1
	armasuisse	**7**	4	1	1	0	1	0
	BASPO	**175**	172	1	0	1	1	0
	BABS	**2**	2	0	0	0	0	0
	swisstopo	**2**	1	0	0	1	0	0
	OA	**0**	0	0	0	0	0	0
	Total	**225**	**193**	**6**	**14**	**6**	**4**	**2**
Eidg.Finanz-departement EFD	GS	**16**	4	7	3	0	2	0
	ISB	**4**	1	2	1	0	0	0
	EFV	**6**	4	0	2	0	0	0
	EPA	**3**	3	0	0	0	0	0
	ESTV	**14**	8	3	2	0	0	1
	EZV	**16**	5	3	6	2	0	0
	BBL	**4**	4	0	0	0	0	0
	BIT	**5**	5	0	0	0	0	0
	EFK	**10**	6	1	1	0	1	1
	SIF	**4**	2	1	1	0	0	0
	PUBLICA	**0**	0	0	0	0	0	0
	ZAS	**20**	7	0	9	0	1	3
	Total	**102**	**49**	**17**	**25**	**2**	**4**	**5**
Eidg.Departement für Wirtschaft, Bildung und Forschung WBF	GS	**10**	4	1	4	0	1	0
	SECO	**34**	14	7	11	1	1	0
	SBFI	**3**	2	0	0	0	0	1
	BLW	**14**	5	2	2	1	3	1
	BWL	**1**	0	0	1	0	0	0
	BWO	**0**	0	0	0	0	0	0
	PUE	**4**	1	1	1	0	1	0
	WEKO	**15**	12	0	3	0	0	0
	ZIVI	**1**	1	0	0	0	0	0
	BFK	**2**	2	0	0	0	0	0
	SNF	**1**	0	0	1	0	0	0
	EHB	**0**	0	0	0	0	0	0
	ETH Rat	**9**	7	0	1	0	1	0
	Innosuisse	**6**	2	0	3	1	0	0
	Total	**100**	**50**	**11**	**27**	**3**	**7**	**2**

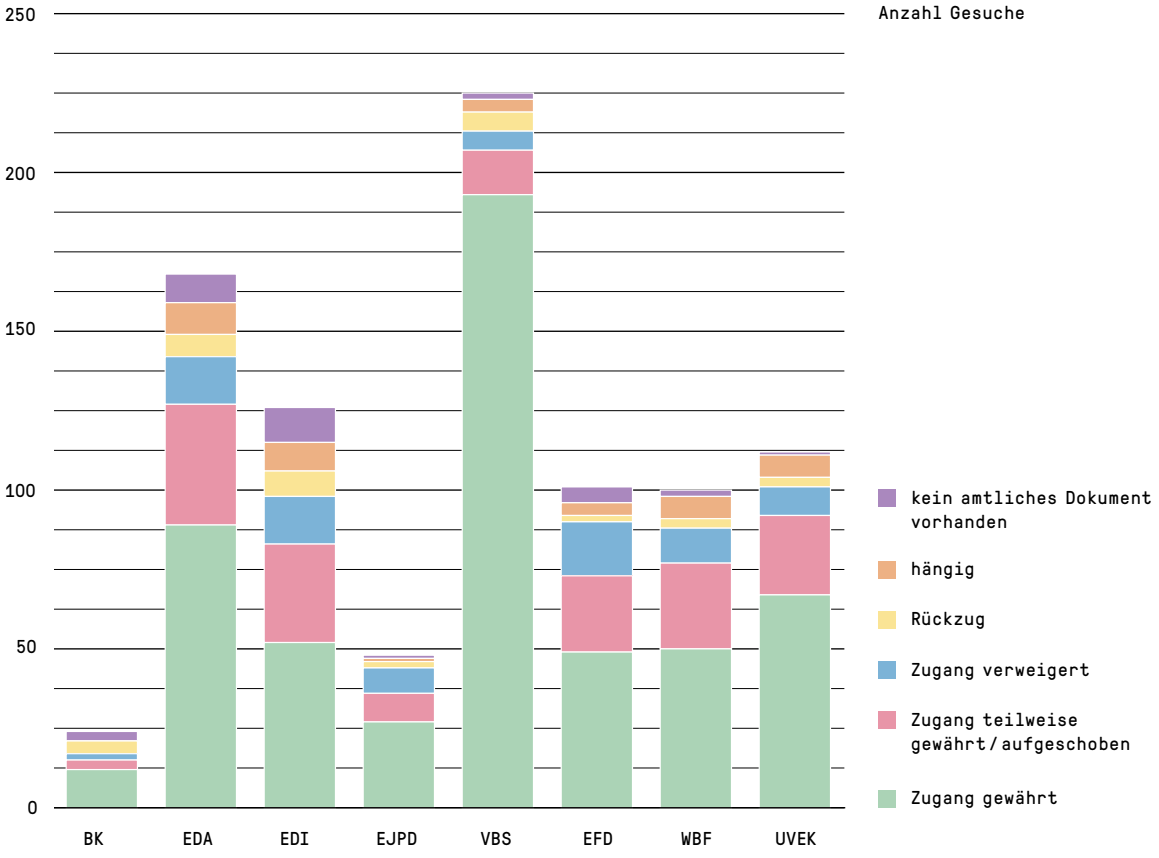
	Betroffener Fachbereich	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt/aufgeschoben	Zugangsgesuch zurückgezogen	Zugangsgesuch hängig	Kein amtliches Dokument vorhanden
Eidg.Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK	GS	**10**	8	1	0	0	1	0
	BAV	**11**	8	0	3	0	0	0
	BAZL	**15**	7	2	2	0	3	1
	BFE	**12**	6	0	4	1	1	0
	ASTRA	**10**	9	0	0	0	1	0
	BAKOM	**4**	3	0	0	0	1	0
	BAFU	**35**	19	3	12	1	0	0
	ARE	**0**	0	0	0	0	0	0
	ComCom	**1**	1	0	0	0	0	0
	ENSI	**10**	3	2	4	1	0	0
	PostCom	**1**	1	0	0	0	0	0
	UBI	**3**	2	1	0	0	0	0
	Total	**112**	**67**	**9**	**25**	**3**	**7**	**1**
Bundesanwaltschaft BA	BA	**10**	3	1	0	3	1	2
	Total	**10**	**3**	**1**	**0**	**3**	**1**	**2**
Parlamentsdienste PD	PD	**1**	0	1	0	0	0	0
	Total	**1**	**0**	**1**	**0**	**0**	**0**	**0**

Anzahl Schlichtungsgesuche nach Kategorien der Antragssteller

Kategorie Antragsteller	2019
Medien	**34**
Privatpersonen (bzw. keine genaue Zuordnung möglich)	**40**
Interessenvertreter (Verbände, Organisationen, Vereine usw.)	**7**
Rechtsanwälte	**5**
Unternehmen	**47**
Total	**133**

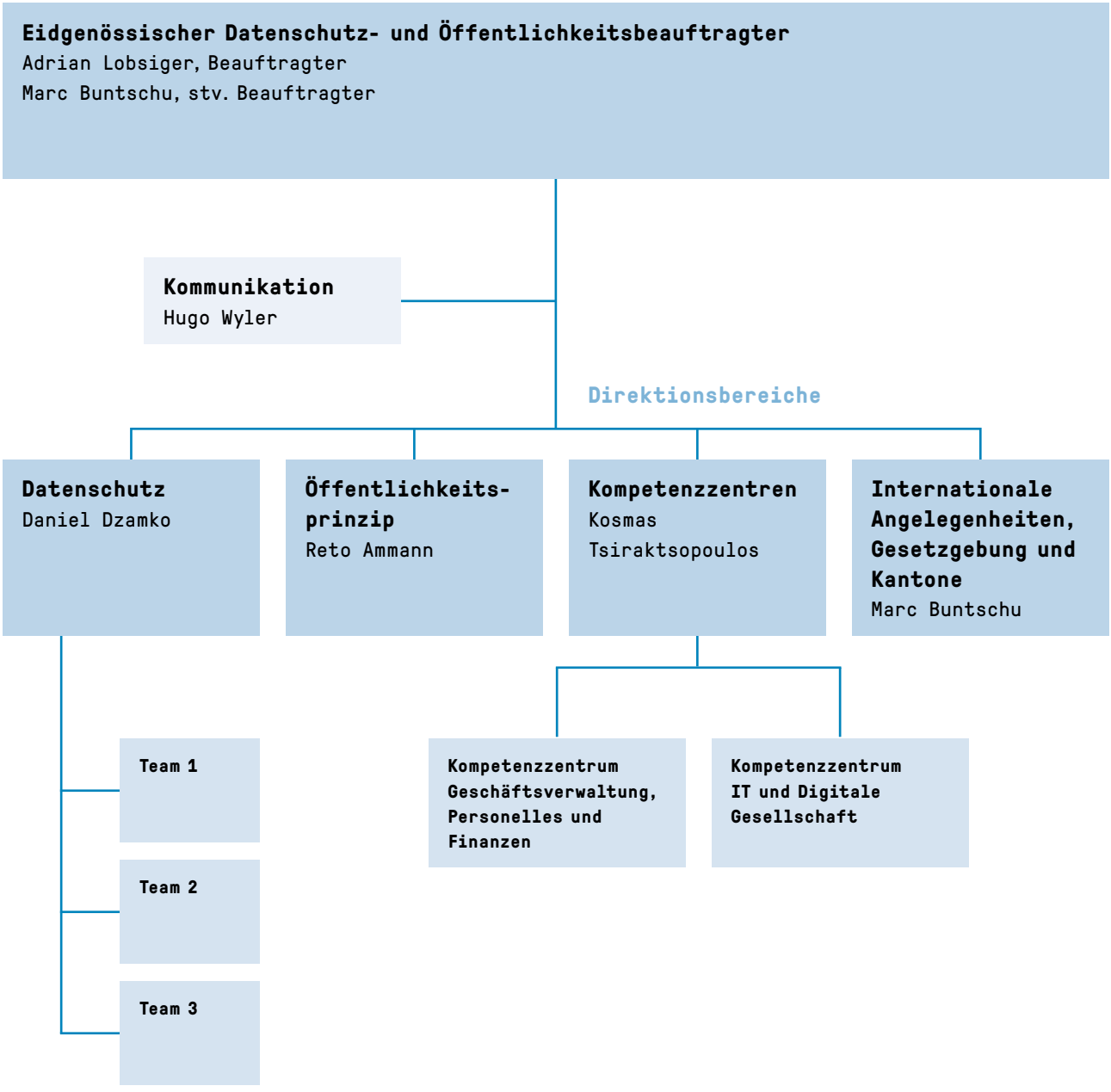
Zugangsgesuche der gesamten Bundesverwaltung vom 1. Januar bis 31. Dezember 2019





3.4 Organisation EDÖB (Stand 31. März 2020)

Organigramm



Mitarbeiter und Mitarbeiterinnen des EDÖB

Anzahl Mitarbeitende	37		
FTE	30.8		
nach Geschlecht	Frauen	19	51%
	Männer	18	49%
nach Beschäftigungsgrad	1-89%	25	68%
	90-100%	12	32%
nach Sprache	Deutsch	29	78%
	Französisch	7	19%
	Italienisch	1	3%
nach Alter	20-49 Jahre	22	59%
	50-65 Jahre	15	41%
Kaderpositionen	Frauen	3	33%
	Männer	6	67%

Abkürzungsverzeichnis

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

AFAPDP Französischsprachige Vereinigung der Datenschutzbehörden

AIA Internationaler automatischer Informationsaustausch

ALBA Automatischer Austausch länderbezogener Berichte

ASTRA Bundesamt für Strassen

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

BGÖ Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsgesetz)

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

DoC Department of Commerce (US-Handelsministerium)

DSG Bundesgesetz über den Datenschutz (Datenschutzgesetz)

DSGVO Datenschutzgrundverordnung der EU

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

EIDCOM Kommission für die Aufsicht und Kontrolle über die Anbieter der E-ID

EPD Elektronisches Patientendossier

EuGH Gerichtshof der Europäischen Union

Eurodac Biometrische Datenbank der EU im Asylwesen

fedpol Bundesamt für Polizei

FTC Federal Trade Commission; US-Behörde für Konsumentenschutz

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

Konvention 108+ Modernisierte Datenschutzkonvention des Europarats (auch Übereinkommen 108+)

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

PNR Passenger Name Record (Fluggastdatensatz)

Privatim Konferenz der Schweizer Datenschutz-Beauftragten (kantonale Datenschutzbehörden)

RIPOL Automatisiertes Fahndungssystem der Polizei

SBFI Staatssekretariat für Bildung, Forschung und Innovation

SDSG Bundesgesetz über den Datenschutz im Rahmen der Anwendung des Schengen-Besitzstands in Strafsachen [SR 235.3]

SEM Staatssekretariat für Migration

Seco Staatssekretariat für Wirtschaft

SIF Staatssekretariat für internationale Finanzfragen

SIRENE Supplementary Information Request at the National Entry (Nationale Kontaktstelle für den Austausch zusätzlicher Informationen)

SIS Schengener Informationssystem

SIS II Schengener Informationssystem der zweiten Generation

SPK Staatspolitische Kommission (für DSG-Beratung zuständig)

T-PD Beratender Ausschuss zum Übereinkommen 108 des Europarats

VBGÖ Verordnung zum BGÖ

VIS Visa-Informationssystem

ZEMIS Zentrales Migrationsinformationssystem

Abbildungsverzeichnis

Grafiken

Tabellen

Die Bilder in diesem Bericht sind als vom Inhalt losgelöste Bildstrecke konzipiert und vermitteln unsere alltägliche Mobilitätswelt, die auch zahlreiche Datenschutzfragen aufwirft. Einzelne Bildteile sind gepixelt dargestellt, um auf die Problematik der Identifizierung aufmerksam und gleichzeitig Personen und Firmen unkenntlich zu machen. Die Aufnahmen erstellte der Fotograf Ben Zurbriggen aus Biel.

Kennzahlen

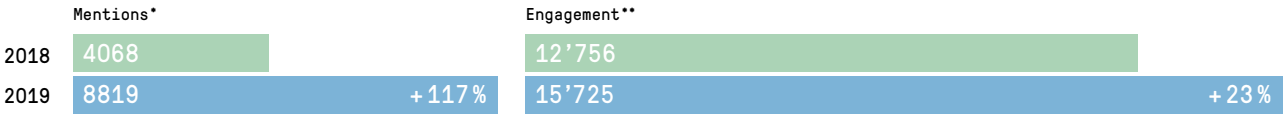
Leistungen Datenschutz

49,8 %	16,7 %	24,2 %	9,3 %
Beratung	Aufsicht	Information	Gesetzgebung

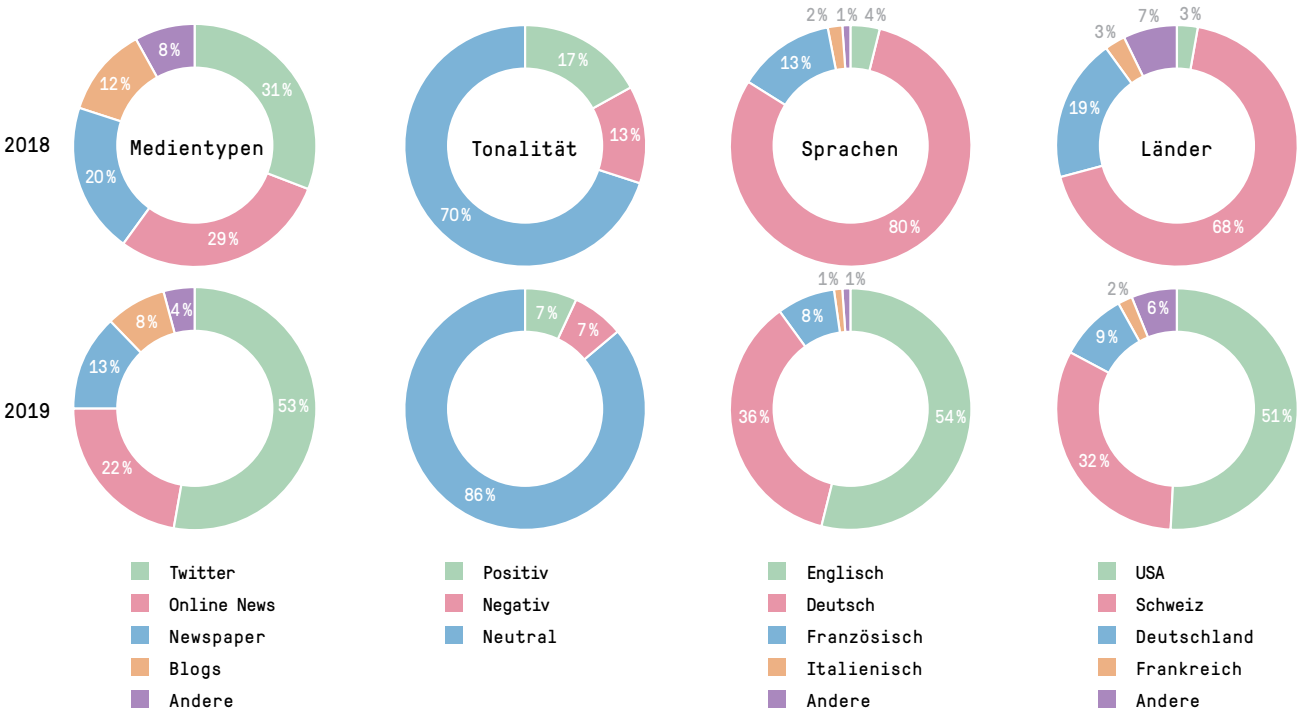
Zugangsgesuche Öffentlichkeitsprinzip (BGÖ)

59 %	19 %	9 %	4 %	5 %	4 %
gewährt	teilweise gewährt / aufgeschoben	verweigert	Rückzug	hängig	kein amtliches Dokument vorhanden

Mediale Resonanz des Beauftragten im Social Web

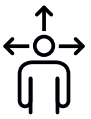


* Anzahl aller Erwähnungen des EDÖB (sog. Mentions auf Blogs, Twitter, Onlinenews, etc.)
** Anzahl aller Interaktionen (Likes, Retweets, etc.)



Anliegen des Datenschutzes

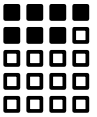
Faire Information
Unternehmen und Bundesorgane informieren transparent über ihre Datenbearbeitung: verständlich und vollständig.



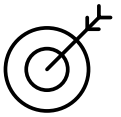
Wahlmöglichkeit
Betroffene geben ihre Einwilligung informiert und erhalten eine echte Wahlfreiheit.

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.

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. 410.027.D

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

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
Feldeggweg 1
CH-3003 Bern

E-Mail: info@edoeb.admin.ch
Website: www.derbeauftragte.ch
@derBeauftragte
Telefon: +41 (0)58 462 43 95 (Mo – Fr, 10 – 12 Uhr)
Telefax: +41 (0)58 465 99 96