28. Tätigkeitsbericht 2020/21

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Tätigkeitsbericht 2020/2021
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 2020 und 31. März 2021 ab.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Vorwort

Die Berichtsperiode war geprägt von einer anhaltenden Pandemie und den Massnahmen, die der Bundesrat und seine Verwaltung zum Schutz der Bevölkerung und zur Stützung der Wirtschaft getroffen haben.

Vor diesem Hintergrund wird es nicht erstaunen, dass sich die Aufsichtstätigkeit unserer Datenschutzbehörde auf die digitalen Stützen der Pandemiebekämpfung wie die «SwissCovid App» oder den Impf-, Test- und Genesungsnachweis konzentrierte. Auch beim Vollzug des Öffentlichkeitsgesetzes war unser Arbeitsalltag von COVID-19 geprägt, indem ein hoher Anteil der eingegangenen Schlichtungsgesuche den Zugang zu amtlichen Dokumenten wie etwa über die Beschaffung von Masken oder Impfstoffen betrafen.

Während der Staat bei der Bekämpfung der zähen Pandemie mit einer hohen Kadenz von Massnahmen in die Privatsphäre und informationelle Selbstbestimmung der Bevölkerung eingriff, pochte unsere Behörde auf die Transparenz des behördlichen Handelns. Weil die Verwaltung bei der Bewältigung von Krisen Prioritäten setzen muss, sind wir dabei pragmatisch vorgegangen. Etwa indem wir gegenüber Medienschaffenden für die nachträgliche Dokumentierung der Tätigkeit des Bundesamtes für Gesundheit für Geduld warben.

Für eine Bilanzierung der Schäden dieser freiheitszehrenden Pandemie ist es zu früh. Eines aber steht fest: Auch unsere Behörde hat ihre Lehren aus den digitalen Pannen gezogen, die in dieser Krise für Staunen und Empörung sorgten. Kritik an Amtsstellen und Führungspersonen sollten indessen nicht über die Defizite der asynchronen Digitalisierung unseres Landes hinwegtäuschen. Allen voran das Fehlen des Basisdienstes einer amtlich bestätigten elektronischen Identität, die sich gerade für die zeitgemässe und datenschutzkonforme Bewirtschaftung von Gesundheitsdaten als unverzichtbar erweist.

Adrian Lobsiger
Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter

Bern, den 31. März 2021

Datenschutz

Öffentlichkeitsprinzip

Der EDÖB

Texte und Bilder mit Coronabezug

Aktuelle Herausforderungen

I Digitalisierung

Die trotz verfügbaren Impfstoffen anhaltende Corona-Krise und die von ihr beschleunigte Digitalisierung von Arbeit und Konsum haben den Umgang der Schweizer Bevölkerung mit Informations- und Kommunikationstechnologien (IKT) auch in der aktuellen Berichtsperiode geprägt.

Technologie und Wirtschaft

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

Die digitale Realität basiert auf dem lichtschnellen Internet-Transport von Signalen, welche Milliarden von portablen Geräten, sog. «Smart Devices», in Schriften, Bilder, Töne oder Vibrationen verwandeln und sinnlich wahrnehmbar machen. Die jederzeitige Verfügbarkeit und breite Streuung von Informationen befriedigen Neugier, Spieltrieb und Wissensdrang unserer Gesellschaft.

Beides wird den Menschen aber schnell lästig, wenn Sondernutzungsansprüche an Daten oder der Intimsphärenschutz ins Spiel kommen. Private Individuen und Unternehmen pflegen deshalb einen Teil ihrer Daten abzuschotten und zu verschlüsseln, was wiederum der Eingriffsverwaltung und Polizei ein Dorn im Auge ist. Auch sehen sich die Besitzer von Smart Devices zunehmend mit der Forderung privater und behördlicher Akteure konfrontiert, ihr Gerät für automatische Datenabgleiche – sog. «Scans» – vorzuweisen, was beim Gedanken daran, dass sich dort umfangreiche Spuren ihrer digitalen Lebensführung befinden, Unbehagen auslösen kann. Es ist deshalb nicht jede oder jeder Einzelne willens, ein mit einem bestimmten Programm bestücktes Smart Device vorzuzeigen. Auch gibt es Menschen, die dazu aufgrund ihres Alters, ihrer Gesundheit oder wegen Behinderungen gar nicht in der Lage sind.

In der aktuellen Phase der Pandemiebekämpfung wird absehbar, dass der Druck auf all diese Personen zunehmen wird. Mit Blick auf die Wiedereröffnung von Betrieben und die Aufhebung von Veranstaltungsverboten wird absehbar, dass der Zugang zu gewissen Gütern und Leistungen von Nachweisen von Covid-Testresultaten oder Covid-Impfungen abhängig gemacht werden dürfte. Um zu verhindern, dass die Bevölkerung in eine Smartphone-Tragpflicht geschubst wird, fordert der EDÖB, dass ihr bei der Erhebung dieser Gesundheitsdaten nebst digitalen auch alternative Erhebungsmethoden zu zumutbaren Konditionen angeboten werden. Letztere sind wichtig, weil davon auszugehen ist, dass die systematischen Personendatenbearbeitungen im Kontext der Pandemie die informationelle Selbstbestimmung der Bevölkerung über die aktuelle Krise hinaus prägen werden. Angesichts der hohen Verbreitung von Smart Devices ist absehbar, dass die Krise zum Trittbrett behördlicher und kommerzieller Interessen werden kann, welche die jederzeitige Zugänglichkeit dieser Geräte als mobile Identifikations- und Dokumentationsmittel nahelegen. Um zu verhindern, dass Smart Devices zu digitalen Fussfesseln degenerieren, hat der Beauftragte sowohl bezüglich der Erhebung von Kontaktdaten für das Contact Tracing als auch der Nachweise von Testresultaten und Impfungen öffentlich gefordert, auch herkömmliche Informationsträger wie Papier zuzulassen (s. Mitteilungen zu Gästelisten sowie Erhebung von Gesundheitsdaten durch Private). Entsprechende Überlegungen dürften denn auch für den Bundesgesetzgeber ausschlaggebend gewesen sein, als er im Frühsommer 2020 im Epidemiengesetz den Grundsatz verankerte, dass niemand eine Leistung davon abhängig machen darf, ob jemand die Swiss Covid App verwendet oder nicht.

Die weitreichenden Auswirkungen der fortschreitenden Automatisierung bei der Bearbeitung grosser Datenmengen haben sich im Berichtsjahr auch bei der Durchführung von Wahlen und Abstimmungen eindrücklich gezeigt. Wenn heute zur Auswertung grosser Mengen von Voten maschinelle und digitale Technik eingesetzt wird, sorgen sich die Stimmenden vor allem anderen um die Transparenz und Verlässlichkeit ebendieser Tech-

nik, womit typische Fragestellungen des Datenschutzes angesprochen sind. Das verbreitet vorhandene Misstrauen gegenüber automatisierten Vorgängen hat denn auch zu den Wirren im Anschluss an die letzten US-Präsidentschaftswahlen beigetragen. Indem die damaligen Anwälte des Weissen Hauses mit Vorliebe abstrakte, technische Aspekte der Datenübermittlung, -zählung und -auswertung aufs Korn nahmen und mit einer systemischen Generalkritik diskreditierten, verstärkten sie die Verunsicherung einer Öffentlichkeit, die in den Foren des Internets einem Sperrfeuer von Glaubensbotschaften über gezinkte Algorithmen und andere Machenschaften ausgesetzt war. Vor diesem Hintergrund ist davon auszugehen, dass mit der fortschreitenden Automatisierung von Wahlen und Abstimmungen jene Arbeitsinstrumente des modernen Datenschutzrechts an Bedeutung gewinnen werden, die bei automatisierten Vorgängen, die zu Entscheidungen führen, ein Minimum an menschlichem Zutun verlangen.

Gesellschaft und Datenpolitik

Am 7. März 2021 hat das Schweizer Volk das Bundesgesetz über elektronische Identifizierungsdienste (E-ID) deutlich abgelehnt. Während Bundesrat und Parlament bei der Bevölkerung vergeblich um Vertrauen in eine private Herausgeberschaft der E-ID warben, setzte sich das Referendumskomitee mit seinem zentralen Argument durch, deren Ausgabe sei ausschliesslich in behördliche Verantwortung zu legen. Wenn sich das Volk dem Staat im Zusammenhang mit einem digitalen Schlüsselprojekt für mehr staatliche Führung ausspricht, dürfte dies auf die berechtigte Erwartung zurückzuführen sein, dass sich staatliches Tätigwerden und die daraus abzuleitende Bearbeitung von Personendaten auf das beschränkt, was im Gesetz steht, und sich die Behörden selbstbeflissen am Legalitätsprinzip orientieren.

Diese Erwartungen der Bevölkerung stehen in einem gewissen Kontrast zu den Erfahrungen des EDÖB. Im Zuge unserer Beratungs- und Aufsichtstätigkeit stellen wir fest, dass sich die mit der Herausforderung der digitalen Transformation konfrontierte Bundesverwaltung mit dem Legalitätsprinzip zunehmend schwertut und die Anforderungen, welche die bundesgerichtliche Praxis an die Bestimmtheit gesetzlicher Grundlagen zur Bearbeitung von Personendaten stellt, in Zweifel zieht: So sei es nicht länger vertretbar, die Inhalte, Kategorien, Zwecke sowie die Intensität und Dauer behördlicher Datenbearbeitungen gesetzlich zu verankern, weil dies angeblich den Erhalt nicht mehr zeitgemässer «Datensilos» und «Medienbrüche» fördere, die die Verwaltung daran hinderten, sich flexibel zu vernetzen und effizient zu arbeiten.

Dem ist entgegenzuhalten, dass der Beauftragte die Digitalisierung der Bundesverwaltung ebenso wenig in Frage stellt, wie deren Bedürfnis nach zeitgemässen Rechtsgrundlagen, welche die organisatorische und technologische Gestaltungsfreiheit der Ämter nicht unnötig einengen. Mit einer lösungsorientierten Beratungstätigkeit zeigt der EDÖB auf, dass generell-abstrakt und technologieneutral formulierte Vorgaben im Gesetz der digitalen Transformation keineswegs im Wege stehen. Auch unterstützt er Bestrebungen der Verwaltung, historisch gewachsene Systemstrukturen zu vereinfachen.

Trotz dieses Bekenntnisses zur digitalen Transformation kann die Datenschutzaufsicht des Bundes die Verwaltung nicht davon dispensieren, Zweck, Umfang und Intensität digitaler Bearbeitungen von Personendaten von einem Auftrag der politischen Organe abzuleiten, der im Gesetz bürgerverständlich verankert ist. Auch

«Die Bevölkerung soll nicht in eine Smartphone-Tragpflicht geschubst werden.»

ist es unabdingbar, dass der demokratisch legitimierte Gesetzgeber bei der Regelung der behördlichen Datenbearbeitung politisch und staatsrechtlich gebotene Zuständigkeitsgrenzen zieht, indem er Verantwortlichkeiten zuweist, den direkten Zugriff auf Personendaten eingrenzt und den Austausch von Informationen über den Weg der Amtshilfe regelt. Dass die digitale Transformation der Verwaltung ohne Verwässerung des Legalitätsprinzips umzusetzen ist, geht im Übrigen auch aus dem neuen Datenschutzgesetz hervor, in welchem der Gesetzgeber von 2020 das bisherige Versprechen bekräftigte, dass Bundesorgane nur dann sensible Bürgerdaten bearbeiten, wenn dies ein dem Referendum unterliegendes Gesetz vorsieht und erkennbar macht, zu welchen Zwecken und in welchem Umfang welche Arten und Inhalte von Daten mit welcher Intensität bearbeitet werden.

Einen Austausch über die Anforderungen des Legalitätsprinzips führte der EDÖB in der Berichtsperiode u.a. mit der Eidgenössischen Zollverwaltung. Es ging dabei um die Gestaltungspielräume des zukünftigen Bundesamtes für Zoll und Grenzsicherheit, dessen Personal grosse Mengen sensibler Personendaten bearbeiten wird und wie die Mitarbeitenden des Bundesamtes für Polizei oder des Nachrichtendienstes des Bundes bewaffnet und mit polizeilichen Befugnissen ausgestattet werden soll.

Die Bearbeitung von Personendaten durch diese Sicherheitsbehörden des Bundes ist mit hohen Risiken für die Privatsphäre und informationelle Selbstbestimmung der Bevölkerung verbunden, weil diese bei der Beschaffung eines Teils ihrer Informationen verdeckt vorgehen und betroffene Personen je nach Ergebnis der Auswertung der Daten mit einschneidenden Zwangsmassnahmen belegen. Vor diesem Hintergrund darf die Datenschutzaufsicht des Bundes bei der digitalen Transformation dieser Ämter hinsichtlich der Beachtung der bundesgerichtlichen Anforderungen an die Bestimmtheit der gesetzlichen Regelung polizeibehördlicher Personendatenbearbeitungen keine Abstriche tolerieren. Nur hinreichend bestimmte Gesetze können verhindern, dass es mit der fortschreitenden digitalen Transformation der Sicherheitsbehörden des Bundes und der kantonalen Polizeikorps zu einer Verwischung von Zuständigkeiten kommt. Würde die digitale Verknüpfung der Personendaten, die im föderalistischen Gefüge der Sicherheitsbehörden zur Erfüllung so unterschiedlicher Zwecke wie der sicherheitspolizeilichen Gefahrenabwehr, der kriminalpolizeilichen Strafverfolgung, des nachrichtendienstlichen Staatsschutzes sowie zum Vollzug zahlreicher Spezialgesetze bearbeitet werden, dem Belieben der Behörden überlassen, führte dies zu einer intransparenten Konzentration von Polizeimacht, die mit der Kompetenzordnung der Bundesverfassung nicht zu vereinbaren wäre.

Die Bearbeitung der Polizeidaten des Bundes vom Gesetz auf aufgabenbezogene Kategorien zurückzubinden, ist umso wichtiger, als sich die Organisation der Sicherheitsbehörden auf Stufe des Bundes in ihrer historisch geprägten Komplexität in eigenartiger Weise von den Verhältnissen in den Kantonen abhebt. Während die verdeckt und zwangsbewehrt erfolgenden Erhebungen von Personendaten dort durch ein einziges Polizeikorps durchgeführt werden, dessen Aufgaben und Befugnisse im kantonalen Polizeigesetz nachgeschlagen werden können, verteilt die Eidgenossenschaft ihre Polizeimacht wie erwähnt auf eine Vielzahl von bewaffneten Verbänden, die auf der Grundlage unterschied-

«Die Sicherheitsbehörden des Bundes tun sich zunehmend schwer mit dem Legalitätsprinzip.»

lichster Bundesgesetze Personendaten bearbeiten. Dass das Fehlen eines mit den kantonalen Polizeigesetzen vergleichbaren Erlasses und die schwer überblickbare Vielzahl von bundesrechtlichen Spezialerlassen die Transparenz der Personendatenbearbeitung durch die Bundessicherheitsbehörden in einer mit der Datenschutzgesetzgebung schwer vertretbaren Weise mindert, beanstandet der Beauftragte seit vielen Jahren vergeblich in seinen Tätigkeitsberichten. Im Kontext mit der digitalen Transformation hat diese Rechtszersplitterung inzwischen dazu geführt, dass es für diese Behörden immer anspruchsvoller wird, ihre vielschichtigen Datenbearbeitungen zu überblicken. Der Beauftragte sieht in diesem Umstand eine weitere Erklärung dafür, weshalb sich gerade die Sicherheitsbehörden des Bundes zunehmend schwer tun mit der Handhabung des Legalitätsprinzips.

Gesetzgebung

Die eidgenössischen Räte haben ihre langwierigen Arbeiten zur Totalrevision der Datenschutzgesetzgebung des Bundes mit der Schaffung des totalrevidierten Bundesgesetzes über den Datenschutz vom 25. September 2020 zum Abschluss gebracht (s. Schwerpunkt 1).

II Beratungs-, Kontroll- und Schlichtungstätigkeit

Damit der EDÖB als Aufsichtsbehörde sicherstellen kann, dass Personendaten nicht mit der technisch machbaren, sondern rechtlich zulässigen Intensität bearbeitet werden, verlangt er von den Verantwortlichen digitaler Applikationen, dass sie hohe datenschutzrechtliche Risiken bereits im Planungs- und Projektstadium minimieren und gegenüber der betrieblichen und behördlichen Datenschutzaufsicht dokumentieren. Mit dieser Ausrichtung haben wir die aufsichtsrechtliche Beratung einer Vielzahl von Big Data Projekten von Bundesbehörden und privaten Unternehmen fortgesetzt und den selbstverantwortlichen Einsatz moderner Arbeitsinstrumente wie der Datenschutzfolgenabschätzung sowie betrieblicher Datenschutzverantwortlicher gefördert.

Den gewichtigsten Schwerpunkt hat der EDÖB in der aktuellen Berichtsperiode bei der aufsichtsrechtlichen Begleitung und Kontrolle der zahlreichen digitalen Projekte im Zusammenhang mit der Bekämpfung der aktuellen Pandemie gesetzt, welche im vorliegenden Jahresbericht mit gelber Farbe gekennzeichnet sind. Die Pandemie hat den EDÖB auch in seiner Eigenschaft als Öffentlichkeitsbeauftragten herausgefordert. So sah er sich mit einer Vielzahl von Schlichtungsanträgen konfrontiert, die sich u.a. auf amtliche Dokumente zur Beschaffung von Masken oder Impfstoffen bezogen und infolge der allgemeinen Verpflichtung zu Home-Office grösstenteils durch den arbeitsintensiven Erlass schriftlicher Empfehlungen abgeschlossen werden mussten.

Sechs von insgesamt 15 Grossprojekten, die der EDÖB aufgrund seiner gesetzlichen Beratungspflichten begleitete, standen im Zusammenhang mit der vom Bundesrat angeordneten digitalen Transformation der Bundesverwaltung, welche den von Politik und Medien vorab im Zusammenhang mit der Pandemiebekämpfung angemahnten Digitalisierungsrückstand aufzuholen sucht. Nebst den erwähnten Projekten des Bundesamtes für Gesundheit begleitete der EDÖB denn auch Digitalisierungsvorhaben zahlreicher weiterer Bundesorgane mit dem erwähnten Schwerpunkt bei den Sicherheitsbehörden (s. oben sowie Kap. 1.2 und 3.1).

Nachdem die Aufwendungen für die Kontrollaufgaben in der Periode 2015/16 deutlich absanken, konnten diese in den letzten Jahren leicht angehoben und wegen der anhaltend knappen Mittelausstattung nur auf tiefem Niveau stabilisiert werden. Auch in der aktuellen Berichtsperiode vermochte der EDÖB die berechtigten Erwartungen der Öffentlichkeit nicht im gewünschten Mass zu erfüllen. Obwohl der EDÖB eine enge Zusammenarbeit mit dem nationalen Zentrum für Cybersicherheit sucht, fehlt es ihm an Mitteln (s. Kap. 3.1), um systematisch Stichproben und Kontrollen der technischen Sicherheit durchzuführen, wie sie gerade bei sensiblen Datenhaltungen von Gesundheitsdaten nützlich wären. Erinnert sei in diesem Kontext an den Fall der Stiftung «meineimpfungen».

III Nationale und internationale Kooperation

Nationale Kooperation

Im Zuge der Bekämpfung der aktuellen Pandemie stellten sich sowohl beim Contact Tracing wie auch bei der Bearbeitung von Personendaten im Zusammenhang mit COVID-19 Impfungen und Tests Abgrenzungsfragen zwischen eidgenössischen und kantonalen Zuständigkeiten. Die eingespielten Kontakte zwischen den kantonalen Datenschutzbeauftragten und dem EDÖB gewährleisteten, dass stets Lösungen für ein abgestimmtes und pragmatisches Vorgehen gefunden werden konnten.

Internationale Kooperation

Die Pandemiebekämpfung und der damit zusammenhängende Umgang mit Gesundheitsdaten werfen für den Datenschutz in vielen betroffenen Staaten vergleichbare Fragestellungen auf, weshalb der EDÖB die internationalen Entwicklungen aufmerksam verfolgte und dafür auch seine Kontakte zu seinen ausländischen Partnerbehörden nutzte.

Europarat

Dem EDÖB ist es ein Anliegen, sich aktiv beim Europarat einzubringen. So nahm er weiterhin an den Sitzungen des beratenden Ausschusses für das Übereinkommen zum Schutz des Menschen bei der Verarbeitung personenbezogener Daten (Übereinkommen 108) teil. Gleichzeitig wurde eine Vertreterin des EDÖB in das Büro des beratenden Ausschusses für das Übereinkommen 108 gewählt, das die Arbeiten des Ausschusses zwischen den Plenarsitzungen leitet.

Evaluation des Datenschutzniveaus

Der für Ende Mai 2020 erwartete Bericht der Europäischen Kommission zur Angemessenheit des Datenschutzniveaus der Schweiz verzögerte sich, wird aber noch vor dem Sommer 2021 erwartet.

Mit dem aus der EU ausgetretenen Vereinigte Königreich konnte die Schweiz die gegenseitigen Anerkennungen der Angemessenheit des Datenschutzniveaus hingegen noch in der Berichtsperiode zu einem erfolgreichen Abschluss bringen.

Wegfall des Swiss-US Privacy Shield als angemessenes Datenschutzniveau

Der Gerichtshof der Europäischen Union (EuGH) fällte seinen mit Spannung erwarteten Entscheid betreffend die Übermittlung von Daten von der EU in die USA (Schrems II) am 16. Juli 2020. Dabei erklärte der EuGH den Angemessenheitsbeschluss 2016/1250 der EU-Kommission betreffend die unter dem EU-US Privacy Shield Regime zertifizierten US-Unternehmen für ungültig.

Urteile des EuGH haben keine Geltung für die Schweiz. Vor dem Hintergrund seiner periodischen Evaluationen des CH-US Privacy Shield Regimes und der Angemessenheitsanerkennungen zwischen der Schweiz und der EU stellte der EDÖB dennoch fest, dass dieses Regime den Betroffenen in der Schweiz kein adäquates Schutzniveau mehr bietet. Er forderte deshalb Schweizer Unternehmen auf, die Übermittlung von Daten in die USA auf der Grundlage von vertraglichen Garantien und projektbezogenen Risikofolgenbeurteilungen vorzunehmen.

Datenschutz

1.1 Digitalisierung und Grundrechte

Datenschutzfolgenabschätzung betreffend SwissID

Die SwissSign Group AG hat dem EDÖB im Berichtsjahr ihre Datenschutzfolgenabschätzung betreffend die SwissID zur Kenntnisnahme zugestellt.
Aufgrund der systemrelevanten Bedeutung der «SwissID» der SwissSign Group AG hielt der EDÖB in der Vergangenheit regelmässige Sitzungen mit den Verantwortlichen des Unternehmens ab und hat in diesem Rahmen unter anderem darauf hingewirkt, dass für reine Single-Sign-On-Dienste der «SwissID» eine anonyme Anmeldung möglich sein muss. Die SwissSign Group AG hat diese Forderung in ihre Datenschutzpolitik übernommen. Die entsprechenden Anpassungen der Allgemeinen Geschäftsbedingungen sollen bald folgen.

Nachdem die SwissSign Group AG einen externen Datenschutzberater mit der Erstellung einer Datenschutzfolgenabschätzung beauftragt hat, wurde das Dokument dem EDÖB im Berichtsjahr zugestellt und durch diesen analysiert. Der EDÖB stellte fest, dass die Prozesse der Bearbeitung von Personendaten darin ausführlich beschrieben, die Risiken der betroffenen Massnahmen betreffend die Grundrechte bewertet und Massnahmen zum Schutz der Persönlichkeit aufgeführt werden.

Der EDÖB nahm zur Kenntnis, dass die Datenschutzfolgenabschätzung nach Einschätzung des Verantwortlichen als abgeschlossen und die Datenbearbeitung im Zusammenhang mit der «SwissID» angesichts der in beschriebenen Risiken und Massnahmen als zulässig erachtet wird.

Projekt der Schweizer Medienverlage für ein gemeinsames Login auf Online-Portalen

Die Schweizer Digital-Allianz treibt ihre Arbeiten zur Schaffung einer einheitlichen SSO-Lösung für Online-Portale der Medienverlage voran. Der EDÖB hat im Rahmen eines Austausches Verbesserungsmöglichkeiten aufgezeigt.
Mit ihrem SSO-Projekt (Single-Sign-On) möchte die Schweizer Digital-Allianz, dass Nutzer künftig mit einem einzigen, gemeinsamen Login auf diverse Webangebote von Schweizer Medienhäusern zugreifen können. Die Allianz, ein Zusammenschluss mehrerer Schweizer Medienunternehmen, hat ihr Projekt zur Schaffung des zentralen SSO weiterentwickelt und im Frühjahr 2021 eine Pilotphase gestartet. Im Rahmen vorgängiger Projektpräsentationen und dem dazu geführten Austausch haben wir der Digital-Allianz unseren Standpunkt zu den für den Datenschutz wesentlichen Aspekten des Projektes mitgeteilt und auf Verbesserungsmöglichkeiten hingewiesen.

Das Projekt läuft nach Abschluss des Berichtsjahres weiter. Wir werden auch bei den noch folgenden Arbeiten auf eine, dem Persönlichkeitsschutz optimal Rechnung tragende Ausgestaltung der SSO-Lösung hinwirken.

Cloud-Initiativen zur Umsetzung der IKT-Strategie des Bundes.

Der EDÖB begleitete die Erarbeitung von strategischen Zielen und Leitplanken für die digitale Transformation in der Bundesverwaltung. Der Aufbau der dazu notwendigen IT-Infrastrukturen umfasst dabei auch die Gewährleistung der sicheren Nutzung von öffentlichen Cloud-Diensten (Public Clouds). Dies in Ergänzung zur bereits vorhandenen Option, Anwendungen und Daten in den eigenen Rechenzentren der Bundesverwaltung (Private Clouds) betreiben, respektive bearbeiten zu können. Wir fordern, dass datenschutzrechtliche Anforderungen bereits bei der Ausschreibung berücksichtigt werden.

Die Digitalisierung erfordert die Verwendung einer Vielzahl von Anwendungen und Diensten, welche eine hohe Agilität, Flexibilität und Ausbaufähigkeit aufweisen müssen. Um diesen Anforderungen gerecht zu werden, bietet der Einsatz, sowohl von öffentlichen als auch von privaten Cloud-Lösungen einen wichtigen Beitrag, indem diese die benötigten Dienste und Werkzeuge in Echtzeit und als Self-Service-Dienst für den Selbstbezug von Komponenten bereitstellen (s. für Begriffserklärungen die separate Box). Die Bundesverwaltung nutzt bereits heute in beschränktem Umfang einfach erweiterbare Cloud-Dienste in den verschiedensten Ausprägungen. Eine Umfrage bei den Departementen und der Bundeskanzlei im vierten Quartal 2019 hat gezeigt, dass gerade der Bedarf an öffentlichen Cloud-Diensten in Zukunft zunehmen wird.

Die Verwaltungseinheiten der zentralen Bundesverwaltung können, gerade durch die Nutzung dieser Public Clouds, effizient und zeitnah auf innovative und relativ kostengünstige Lösungen sowie neueste Technologien zugreifen. Dies eröffnet neue Möglichkeiten, digitale Verwaltungsleistungen rasch und agil bereitzustellen. Zumindest in Bereichen ohne erhöhte Sicherheitsanforderungen können

dadurch kostspielige IKT-Betriebsleistungen optimiert und ausgelagert werden. Aus diesem Grund bestand innerhalb der Bundesverwaltung ein Handlungsbedarf, zusätzlich zu den bereits vorhandenen Private-Cloud-Lösungen, eine strategische Option zur Nutzung von Public-Cloud-Diensten zu schaffen. Zusätzlich sollte eine vertiefte Abklärung zu Bedarf, Ausgestaltung, Notwendigkeit und Machbarkeit einer öffentlichen, aber rein schweizerischen Cloud- und Dateninfrastruktur «Swiss Cloud» durchgeführt werden.

Aber gerade die Nutzung von öffentlichen Cloud-Diensten hat zur Folge, dass eine grössere Abhängigkeit von den meist weltweit tätigen Anbietern entsteht. Dies betrifft sowohl die technologische Abhängigkeit als auch die Verfügbarkeit von Daten und Anwendungen. Dabei stellt sich zwangsläufig die Frage, wie die Souveränität über die eigenen Daten und der Schutz vor unerwünschtem Datenabfluss sicherzustellen ist.

Um dieser Fragestellung Rechnung zu tragen, wirkte der EDÖB mit zahlreichen Ergänzungen in den Kriterien für die Beschaffung von Public-Clouds drauf hin, dass der Datenschutz und die Datensicherheit bereits durch die Anbieter über die gesamte Verarbeitungskette gewährleistet wird. Auch brachte er sich massgeblich bei der Erarbeitung von Vorgaben zur Zulässigkeit dieser Cloud-Dienste aus Informationssicherheits- und Datenschutzsicht ein. Aufgrund der Tragweite dieses Projekts erachtete es der EDÖB zudem als unabdingbar, bereits in den Offerten spezifische Datenschutz-Zertifizierungen von den Anbietern einzufordern.

Es zeigt sich, dass datenschutzrechtliche Überlegungen bereits in einer sehr frühen Phase von Projekten mit Personendatenbearbeitungen einzubeziehen sind. Der EDÖB wird die Cloud-Initiativen weiter begleiten und die Umsetzung der geforderten Kriterien und Vorgaben überprüfen.

Cloud-Dienste

Während früher fast jedes Unternehmen über ein eigenes Rechenzentrum verfügte, werden heute vielfach Cloud-Dienste verwendet. Unter einer Cloud bzw. Cloud-Computing ist die internetbasierte Bereitstellung von Speicherplatz, Rechenleistung oder Anwendungssoftware als Dienstleistung zu verstehen. Eine Cloud ist also eine Online-IT-Infrastruktur, in welche Daten oder ganze Systemumgebungen ausgelagert werden. Dabei werden Cloud-Lösungen nach Verwendungszweck und gewünschter Integrationstiefe unterschieden.

Zu den grossen Vorteilen einer Cloud zählen:

- Hohe Skalierbarkeit, also die Möglichkeit, Speicherkapazität und Rechenleistung je nach Bedarf einfach erhöhen und verringern zu können
- Hohe Verfügbarkeit und Sicherheit durch Verwendung modernster Technologien
- Investitionssicherheit, da die Umgebung vom jeweiligen Anbieter gewartet wird und grosse Investitionen in eine eigene Serverinfrastruktur wegfallen

Verwendungszweck der Cloud

Für Cloud-Services gibt es verschiedene Arten der Bereitstellung, welche sich von den jeweiligen Anforderungen der Benutzer ableiten lassen. Die wichtigsten:

- Private Cloud: Sie wird meist im eigenen Rechenzentrum des Unternehmens aufgebaut und nur von einer Firma genutzt. Üblicherweise wird sie vom Unternehmen selbst oder gegebenenfalls von einem externen Anbieter betrieben und ist nur für klar bestimmte Personengruppen zugänglich. Die private Cloud wird strengen Anforderungen an Datensicherheit und Datenschutz gerecht und eignet sich daher speziell für sensible Daten wie beispielsweise vertrauliche Personalinformationen oder vertrauliche Firmendaten.
- Öffentliche Cloud («public cloud»): Sie ist ein Angebot eines frei zugänglichen Anbieters, der seine Dienste offen über das Internet für jedermann zugänglich macht. Dabei teilen sich alle Benutzer die gleiche Infrastruktur. Bekannte Online-Speicher wie etwa Dropbox oder Google Drive, aber auch Mailanbieter wie Gmail oder Hotmail, bauen typischerweise auf einer solchen öffentlichen Cloud auf.
- Hybride Cloud: Bei dieser handelt es sich um eine Mischlösung aus einer privaten und einer öffentlichen Cloud. Der Benutzer bezieht dabei eine «public cloud», und darin integriert ist eine private Umgebung für sensible Daten und Anwendungen. Diese Mischform ist beliebt, wenn es darum geht, hoch sensible Daten in einer privaten Cloud zu lagern, während weniger sensible Daten einfacher und günstiger ausgelagert werden können.
- Multi Cloud: In dieser sind mehrere Cloud-Dienste verbunden, womit die Lösungen verschiedener Cloud-Anbieter parallel genutzt werden können. Sie bietet weitaus mehr Möglichkeiten als die hybride Form.

Integrationstiefe der Cloud

Beim Cloud-Computing lassen sich generell drei sogenannte Cloud-Service-Ebenen unterscheiden, welche aufeinander aufbauen. Beginnend bei der Infrastruktur über die Plattform bis hin zur Software, stellen diese Service-Ebenen drei übereinanderliegende Schichten dar und bilden gleichzeitig die Cloud-Architektur ab.

- Infrastrukturebene (Infrastructure-as-a-Service): Dabei werden Ressourcen wie Rechenleistung, Speicher- oder Netzwerkkapazitäten aus der Cloud bezogen. Werden zuvor lokale Server in die Cloud verschoben, ersetzt nun die Cloud die Hardware vor Ort, während die Betreuung des Betriebssystems und der Anwendungen im Unternehmen bestehen bleiben.
- Plattformebene (Plattform-as-a-Service): Dabei werden zusätzlich das Betriebssystem und die systemnahen Anwendungen wie Backup-, Antivirus- und Wartungsanwendungen usw. aus der Cloud bezogen. Anstatt Software auf einer eigenen Umgebung zu entwickeln, können Unternehmen komplette Entwicklungs- und Bereitstellungsumgebungen in der Cloud nutzen.
- Softwarebene (Software-as-a-Service): Dem Benutzer wird eine Cloud-Anwendung mit all ihren zugrundeliegenden IT-Infrastrukturen und -Plattformen zur Verfügung gestellt. Er bezieht beim Anbieter somit sämtliche IT-Komponenten.

Der Einstieg der Bundesverwaltung in die Cloud muss datenschutzkonform erfolgen

Die «Cloud-Strategie der Bundesverwaltung» soll den Weg für eine cloudbasierte Digitalisierung der Bundesverwaltung ebnen. Der EDÖB nahm zum Strategiepapier Stellung und konnte seine wichtigsten Anliegen aus Sicht des Datenschutzes erfolgreich einbringen.

Das Informatiksteuerungsorgan des Bundes (ISB) wurde durch den Bundesrat beauftragt, ein Strategiedokument zu erarbeiten, welches die Cloud-Vision des Bundes konkretisiert und verbindliche Leitlinien und Grundsätze für die Beschaffung von Cloud-Anwendungen durch die einzelnen Verwaltungseinheiten vorschreibt. Der EDÖB erhielt eine vorläufige Version des Strategiedokumentes zur Vorkonsultation und ortete an verschiedene Stellen Verbesserungspotenzial. Insbesondere stellte der EDÖB fest, dass das Dokument einen starken Fokus auf die Anforderungen an die Informationssicherheit legte, weitere rechtliche Aspekte des Datenschutzes dagegen nur oberflächlich behandelte.

Dementsprechend haben wir Ergänzungen vorgeschlagen, um die datenschutzrechtlichen Anforderungen an eine Auslagerung von Datenbearbeitungen in eine Cloud im Strategiedokument zu verankern. Unsere Ergänzungsvorschläge zielten insbesondere darauf ab, dass die zusätzlichen Risiken einer Auslagerung von Datenbearbeitungen an ausländische Public-Cloud-Anbieter aus einem Land ohne angemessenes Datenschutzniveau berücksichtigt werden.

In diesem Sinne haben wir vorgeschlagen, dass das Dokument vorsieht, dass für die Beurteilung, ob und mit welchen Massnahmen die Datenbearbeitung mittels Cloud-Anwendungen zulässig ist, eine Datenschutz-Folgenabschätzung vorzunehmen ist, wenn Personendaten in der Cloud bearbeitet werden. Dieser Mechanismus soll es

ermöglichen, die Rechtskonformität der Cloud-Anwendung zu prüfen, wobei als Kriterien der Standort der Server, das im fraglichen Land geltende Recht und die vorgesehenen technischen und organisatorischen Massnahmen herangezogen werden sollten. Unsere Bemerkungen und Änderungsvorschläge wurden in die finale Fassung des Dokuments eingearbeitet.

Die Bundesverwaltung und auch private Nutzer von Public-Cloud-Lösungen müssen sich immer häufiger mit dieser Fragestellung befassen, seitdem das Privacy Shield Framework re-evaluiert wurde (s. Schwerpunkt II) und man nicht ohne Weiteres davon ausgehen kann, dass die Standardvertragsklauseln ein angemessenes Datenschutzniveau in den USA gewährleisten. Dies weil viele Anbieter in den USA ansässig sind.

CORONA

Zugang des BAG zu Mobilitätsdaten der Swisscom

Nachdem der Bundesrat am 21.03.2020 Ansammlungen von mehr als fünf Personen im öffentlichen Raum verboten hatte, prüfte das BAG anhand von Informationen der Swisscom, ob diese Massnahme zum Schutz vor Infektionen mit dem Coronavirus eingehalten wird. Der EDÖB kam zum Schluss, dass die Swisscom dem BAG ausschliesslich Zugang zu anonymisierten Daten gewährt hat.

Die Swisscom bearbeitet mit der Mobility Insights Plattform (MIP) anonymisierte Gruppenstatistiken anhand aggregierter Mobilitätsdaten zur Auswertung von Mobilitätsverhalten auf dem Gebiet der Schweiz. Nachdem bekannt wurde, dass dem BAG im Rahmen der Pandemiebekämpfung Zugang zu diesen Daten gewährt werden soll, um eine Übersicht darüber zu verschaffen, ob es in der Schweiz noch grössere Menschenansammlungen gibt, hat der EDÖB dazu Vorabklärungen eingeleitet, in deren Rahmen er auch einen Augenschein beim BAG durchgeführt hat.

Die mit einer mindesten achtstündigen Verzögerung zugänglich gemachten visualisierten Auswertungen zeigen den zeitlichen Verlauf der Aufenthalte von Handybesitzern in 100 mal 100 Meter grossen Gebieten, wenn mehr als 20 Mobilfunkgeräte von Abonnenten der Swisscom in einem solchen Gebiet vorhanden sind. Die Standortdaten werden dabei frühestmöglich anonymisiert und aggregiert, und dem BAG werden zu keinem Zeitpunkt die der Visualisierung zugrundeliegenden Klardaten angezeigt. Die dem BAG zugänglichen Visualisierungen lassen keine Rückschlüsse auf bestimmte Personen zu und sind damit anonym. Dementsprechend gelangte der EDÖB in seiner Kurzauswertung vom 03.04.2020 zum Schluss, dass die Datenbearbeitung durch die Swisscom und die Weitergaben von anonymen Daten an das BAG datenschutzrechtlich erlaubt sind (s. Mitteilung «Zugang des BAG zu visualisierten Daten der Swisscom grundsätzlich erlaubt»).

Aufgrund dieser Informationen konnte der EDÖB auf die Eröffnung einer formellen Sachverhaltsabklärung verzichten. Der EDÖB war indessen der Auffassung, dass die der Öffentlichkeit zugänglichen Informationen zur Zusammenarbeit zwischen dem BAG und der Swisscom und den damit verbundenen Datenbearbeitungen spärlich und nicht ohne Weiteres auffindbar waren. Er hat die Swisscom daher dazu aufgefordert, die Öffentlichkeit mit detaillierteren Informationen zum Datenbearbeitungsvorgang zu bedienen. Die Swisscom ist dieser Aufforderung nachgekommen und hat FAQs betreffend die Nutzung der Mobility Insights Plattform von Swisscom durch das Bundesamt für Gesundheit (BAG) erstellt.

Programm Nationale Datenbewirtschaftung

Die Datenbewirtschaftung der öffentlichen Hand soll durch die Mehrfachnutzung von Daten einfacher und effizienter werden. Mit diesem Ziel hat der Bundesrat im Rahmen des Programms Nationale Datenbewirtschaftung mehrere Pilotprojekte lanciert. Der EDÖB steht im Austausch mit dem dafür verantwortlichen Bundesamt für Statistik und wirkt auf eine datenschutzkonforme Umsetzung hin.

Die Zielsetzung des Programms Nationale Datenbewirtschaftung (NaDB) ist, dass Personen und Unternehmen den Behörden bestimmte Angaben nur noch einmal melden müssen («Once-Only»-Prinzip) und dadurch entlastet werden sollen. Durch eine Mehrfachverwendung von Daten soll zudem der administrative Aufwand in der öffentlichen Verwaltung reduziert werden. Um dies zu erreichen, wird ein erleichterter Datenaustausch zwischen den Behörden angestrebt.

Der EDÖB hat zunächst im Rahmen einer Ämterkonsultation zu Berichten von vier Pilotprojekten zu den Themen Qualitätssicherung der Unternehmensdaten, Lohnstatistiken, Steuerdaten sowie Prozessen, Rollen und Verantwortlichkeiten Stellung genommen. Dabei betonte er, dass dem Datenschutz bei der mit dem Programm angestrebten Mehrfachnutzung von Informationen eine entscheidende Bedeutung zukommt. Die Mehrfachnutzung birgt aus seiner Sicht erhebliche datenschutzrechtliche Risiken. So ist insbesondere sicherzustellen, dass das «Once-Only»-Prinzip nicht dazu führt, den Kreis von Zugriffsberechtigten zu erweitern. Weiter muss zwingend geregelt werden, wer welche Daten zu welchem Zweck bearbeiten darf. Zudem ist klar zwischen Datenbearbeitungen zu statistischen Zwecken und solchen zu anderen Zwecken zu unterscheiden. Darüber hinaus muss transparent ersichtlich sein, wie die Datenerhebung, die weitere Datenbearbeitung und die Zugriffsmöglichkeiten geregelt sind.

Im Nachgang zu dieser Ämterkonsultation fand ein Austausch zwischen dem Bundesamt für Statistik, das mit der Umsetzung betraut ist, und dem EDÖB statt, an welchem diese Aspekte nochmals erörtert werden konnten. Der Beauftragte wird die Umsetzung des Programms NaDB weiter beratend begleiten und den verantwortlichen Stellen als Ansprechperson zur Verfügung stehen.

CORONA

Merkblatt betreffend die datenschutzkonforme Verwendung von Audio- und Videokonferenzlösungen

Aufgrund der Pandemie haben sich Anwendungen für Audio- und Videokonferenzen in sehr kurzer Zeit durchgesetzt. Die riesige Menge an Nutzerinnen und Nutzer hat diese digitalen Plattformen für Angriffe interessant gemacht. Bei der Wahl der Software ist es deshalb wichtig, Informationssicherheit und Datenschutz im Auge zu behalten. Nicht nur werden teilweise Personendaten missbräuchlich weiterverarbeitet, sondern auch ist deren Sicherheit nicht immer erkenntlich oder die Plattformen weisen sogar bekannte Schwachstellen auf.

Das Merkblatt des EDÖB (s. MItteilung «Massnahmen für eine sichere Nutzung von Audio- und Videokonferenzlösungen») richtet sich an alle Nutzergruppen – sowohl im privaten wie im geschäftlichen Umfeld und hilft ihnen, ihre Personendaten zu schützen und unerwünschte Effekte zu verhindern. Darin empfiehlt der EDÖB einerseits Schutzmassnahmen bei der Verwendung, wie beispielsweise dem Umgang mit Meeting-ID und -Passwort, dem Kameragebrauch oder der Bildschirmpräsentation. Andererseits gibt das Merkblatt Hinweise für eine Evaluation und Einführung einer Audio- und Videokonferenzlösung. So ist es etwa ratsam, den Umgang mit Metadaten, die Verschlüsselung oder die Sicherheit des Providers zu prüfen. Vor der Implementierung im Unternehmen sollten ausserdem in einem Reglement die Nutzungsbestimmungen geklärt werden. Das Unternehmen ist darüber hinaus verpflichtet, die Mitarbeitenden über eine allfällige Aufzeichnung oder Überwachung transparent zu informieren.

Da die Versuchung besteht, die während der Pandemie adhoc genutzten Lösungen auch gleich in die bestehende IKT-Infrastruktur einzugliedern, empfiehlt der Beauftragte, die Beschaffung solcher Lösungen über ordentliche Projekte oder die IT-Verantwortlichen abzuwickeln, damit die Compliance sichergestellt werden kann. Die eingesetzte Audio- und Videokonferenzlösung soll über Sicherheitseinstellungen verfügen, welche höhere Datenschutzstandards erlaubt – insbesondere im Hinblick auf Geschäfts- und Berufsgeheimnisse.

Datenbearbeitungen von Dating-Apps

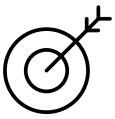
Der EDÖB hat bei einem Schweizer Anbieter von Dating-Apps ein Verfahren eröffnet, um seine Bearbeitungsmethoden und seinen Umgang mit Löschungsbegehren zu überprüfen.

Nach Angaben des Bundesamts für Statistik spielen Dating-Apps und -Webseiten bei der Partnersuche eine zunehmend bedeutsame Rolle in der Schweiz: Fast zwanzig Prozent der Paare, die in den letzten fünf Jahren in eine Beziehung getreten sind, haben sich online über eine Partnerbörse, eine Dating-App oder ein soziales Netzwerk[1] kennengelernt. Dating-Apps und -Webseiten zeichnen sich dadurch aus, dass sie geeignete Partner basierend auf den Personendaten der Kundinnen und Kunden vermitteln, die sie mithilfe eines Algorithmus teil- oder vollautomatisch bearbeiten.

Um die Erfolgschancen der Partnervermittlung zu erhöhen, werden die Nutzer animiert, teilweise sehr sensible Informationen über sich preiszugeben. So z.B. Daten über Weltanschauungen, Religion, Alkoholkonsum. Die Bearbeitung dieser Personendaten birgt somit hohe Risiken, weil daraus Rückschlüsse auf wesentliche Aspekte der Persönlichkeit der Nutzer gezogen werden können.

[1] Bundesamt für Statistik (Hg.): Erhebung zu Familien und Generationen 2018. Erste Ergebnisse. Neuchâtel 2019, S. 9. https://www.bfs.admin.ch/bfs/de/home/statistiken/bevoelkerung/erhebungen/efg.assetdetail.10467788.html (Abgerufen: 14.04.2020)

Im Frühjahr 2021 hat der EDÖB eine Sachverhaltsabklärung bei einem in der Schweiz ansässigen Anbieter einer solchen Dating-App eröffnet. Anlass dafür waren Meldungen von Personen, die uns darauf aufmerksam machten, dass sie keine Möglichkeit hätten, ihr Konto über die App zu löschen, und dass an den Betreiber der App gerichtete Löschungsbegehren nicht bearbeitet würden. Nebst der Klärung dieses Punktes zielt unsere Sachverhaltsabklärung auch darauf ab, die Einhaltung weiterer datenschutzrechtlicher Vorgaben durch diesen Anbieter zu überprüfen. Dies insbesondere im Hinblick auf die Anforderungen an die Transparenz und Sicherheit der Bearbeitung sowie die allfällige Weitergabe von Personendaten an Dritte.



EEDÖB plant neue Meldeportale

Der EDÖB bereitet die Einführung von zwei Online-Meldeportalen für die vom neuen DSG vorgesehenen Meldungen von Datenverlusten und Bekanntgaben von Datenschutzberaterinnen und -beratern vor.

Das revidierte Datenschutzgesetz legt neue Meldepflichten für Datenverantwortliche gegenüber dem EDÖB fest. Diese umfassen die Registrierung von Datenbearbeitungen durch Bundesorgane, die Bekanntgabe von Datenschutzberaterinnen und -beratern sowie die Meldung von Verletzungen der Datensicherheit. Der EDÖB ist bestrebt, den Aufwand möglichst tief zu halten, indem diese Meldungen einfach und sicher online getätigt werden können.

Erstens bedarf es einer Anpassung des Registers der beim EDÖB gemeldeten Datensammlungen, da künftig nur noch Bundesorgane verpflichtet sind, ihre Verzeichnisse der Bearbeitungstätigkeiten an den Beauftragten zu melden. Das Melde- und Suchportal www.datareg.admin.ch wird entsprechend erneuert und für die neuen Vorgaben ausgelegt.

Zusätzlich soll die Einführung von zwei neuen Meldeportalen erfolgen. In einem ersten Webportal sollen künftig die von den Verantwortlichen benannten Datenschutzberaterinnen und -berater strukturiert und effizient erfasst werden. Das Portal eignet sich dabei die Prinzipien eines Self-Service-Kiosks an, in welchem die Verantwortlichen die Kontaktdaten der Datenschutzberaterinnen und -berater selbstständig erfassen, mutieren und löschen. Im zweiten Portal sind die Meldungen von Verletzungen der Datensicherheit zu erfassen, die ein hohes Risiko für die Betroffenen nach sich ziehen. Der Beauftragte rechnet mit einer grösseren Anzahl an Meldungen. Auch dieses Portal soll eine strukturierte und einfache Erfassung ermöglichen und zudem eine Ressourcen schonende Automatisierung bei der Datenauswertung sicherstellen. Es soll zeitnahe Reaktionen auf die gemeldeten Ereignisse gewährleisten.

Das neue Datenschutzgesetz aus Sicht des EDÖB

Bis zum Inkrafttreten des neuen DSG (s. Box) werden Privatwirtschaft und Bundesbehörden ihre Bearbeitung von Personendaten an die neuen Bestimmungen anpassen müssen. Der Beauftragte hat am 5. März 2021 hierzu die aus seiner Sicht wesentlichsten Neuerungen festgehalten und publiziert (s. Mitteilung «Das neue Datenschutzgesetz aus Sicht des EDÖB»). Er empfiehlt verschiedene Punkte zur Beachtung.

Nur noch Daten von natürlichen Personen

Das revidierte DSG bezweckt analog der DSGVO ausschliesslich den Schutz der Persönlichkeit von natürlichen Personen, über welche Personendaten bearbeitet werden – und nicht mehr wie bisher auch die Daten von juristischen Personen.

Besonders schützenswerte Personendaten

Die bisherige Definition der besonders schützenswerten Personendaten wird um genetische und, sofern diese eine natürliche Person eindeutig identifizieren, biometrische Daten erweitert.

Privacy by Design und by Default

Im revidierten DSG sind neu die Grundsätze «Privacy by Design» (Datenschutz durch Technik) und «Privacy by Default» (Datenschutz durch datenschutzfreundliche Voreinstellungen) verankert. Sie verpflichten Behörden und Unternehmen, die Bearbeitungsgrundsätze des DSG bereits ab der Planung entsprechender Vorhaben umzusetzen. Die Applikationen sind u.a. so auszugestalten, dass die Daten standardmässig anonymisiert oder gelöscht werden. Datenschutzfreundliche Voreinstellungen schützen die Nutzer von privaten Online-Angeboten, die sich weder mit Nutzungsbedingungen noch den daraus abzuleitenden Widerspruchsrechten auseinandergesetzt haben, indem nur die für den Verwendungszweck unbedingt nötigen Daten bearbeitet werden, solange sie nicht aktiv werden und weitergehende Bearbeitungen autorisieren.

Datenschutz-Folgenabschätzung

Datenschutz-Folgenabschätzungen sind im Schweizer Datenschutzrecht nicht neu – Bundesorgane sind bereits heute dazu verpflichtet. Wenn eine beabsichtigte Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann, müssen gemäss Art. 22 revDSG neu auch private Verantwortliche vorgängig eine Datenschutz-Folgenabschätzung erstellen. Das hohe Risiko ergibt sich – insbesondere bei Verwendung neuer Technologien – aus der Art, dem Umfang, den Umständen und dem Zweck der Bearbeitung. Insbesondere liegt ein hohes Risiko dann vor, wenn ein Profiling mit hohem Risiko oder umfangreiche Bearbeitungen besonders schützenswerter Personendaten geplant sind. Ist aus einer Datenschutz-Folgenabschätzung erkennbar, dass die geplante Bearbeitung trotz der vom Verantwortlichen vorgesehenen Massnahmen noch ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen zur Folge hätte, muss dieser nach Art. 23 revDSG vorgängig die Stellungnahme des EDÖB einholen. Hat der EDÖB Einwände gegen die Folgenabschätzung selber, wird er dem Verantwortlichen entsprechende Präzisierungen oder Ergänzungen nahelegen.

Verhaltenskodizes

In Art. 11 hat das neue DSG für Berufs-, Branchen- und Wirtschaftsverbände Anreize gesetzt, eigene Verhaltenskodizes zu entwickeln und diese dem EDÖB zur Stellungnahme vorzulegen. Dessen Stellungnahmen werden veröffentlicht. Sie können Einwände enthalten und entsprechende Änderungen oder Präzisierungen empfehlen. Positive Stellungnahmen des EDÖB begründen die gesetzliche Vermutung, dass das im Verhaltenskodex festgehaltene Verhalten datenschutzrechtskonform ist. Allgemein gehaltene Kodizes vermögen indessen nicht vor beliebigen Risiken zu dispensieren, die der Text nicht näher bezeichnet.

Zertifizierungen

Gemäss Art. 13 revDSG können nebst den Betreibern von Datenbearbeitungssystemen oder -programmen neu auch deren Hersteller ihre Systeme, Produkte und Dienstleistungen zertifizieren lassen. Mittels Zertifizierung können Unternehmen z.B. nachweisen, dass sie dem Grundsatz von Privacy by Default gerecht werden und über ein angemessenes Datenschutzmanagementsystem verfügen.

Verzeichnis der Bearbeitungstätigkeiten

Neu müssen nach Art. 12 revDSG die Verantwortlichen sowie die Auftragsbearbeiter je ein Verzeichnis sämtlicher Datenbearbeitungen führen. Die entsprechenden Mindestangaben gibt das neue DSG vor. Das Verzeichnis muss stets à jour gehalten werden. Der Bundesrat wird in der Verordnung Ausnahmen für Unternehmen vorsehen, die weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigten und deren Datenbearbeitung ein geringes Risiko von Verletzungen der Persönlichkeit von betroffenen Personen mit sich bringt.

Bekanntgabe von Personendaten ins Ausland

Das revidierte DSG hält in Art. 16 fest, dass Daten ins Ausland bekanntgegeben werden dürfen, wenn neu der Bundesrat festgestellt hat, dass die Gesetzgebung des


ABHOLEN / PICK UP

Drittstaates einen angemessenen Schutz gewährleistet. Er wird zu diesem Zweck eine Liste publizieren, die nach dem bisherigen Recht vom EDÖB geführt wurde. Figuriert der betreffende Exportstaat nicht auf der Liste des Bundesrates, dürfen Daten wie nach bisherigem Recht trotzdem dorthin geleitet werden, wenn ein geeigneter Datenschutz auf andere Weise gewährleistet wird.

Ist eine Bekanntgabe ins Ausland geplant – wozu auch die Speicherung auf ausländischen Systemen (Cloud) gehört – sind die Länder anzugeben, gleichgültig, ob diese einen angemessenen Datenschutz bieten. Hier geht das DSG weiter als die DSGVO.

Ausgebaute Informationspflichten

In Erfüllung des Revisionsziels der Transparenz baut Art. 19 revDSG die Informationspflicht für Unternehmen aus. Neu gilt, dass ein privater Verantwortlicher bei grundsätzlich jeder beabsichtigten Beschaffung von Personendaten die betroffene Person vorgängig angemessen informieren muss, selbst wenn die Daten nicht direkt bei ihr beschafft werden. Im aktuellen DSG ist diese Informationspflicht bisher nur bei besonders schützenswerten Personendaten und Persönlichkeitsprofilen vorgeschrieben. Unternehmen werden somit ihre Datenschutzerklärungen entsprechend überprüfen und nachführen müssen. Führen Bearbeitungen zu automatisierten Einzelentscheidungen, haben die Verantwortlichen nach Art. 21 revDSG neue Informationspflichten gegenüber der beschwerten Person wahrzunehmen und dieser die ihr zustehenden Anhörungs- und Überprüfungsrechte zu gewähren.

Auskunftsrecht der betroffenen Personen

Das Recht einer betroffenen Person, Auskunft darüber zu verlangen, ob Personendaten über sie bearbeitet werden, wurde im neuen DSG ausgebaut. Art. 25 revDSG enthält eine erweiterte Liste an Mindestinformationen, die vom Verantwortlichen herausgegeben werden müssen, beispielsweise die Aufbewahrungsdauer der über sie bearbeiteten Personendaten.

Meldepflicht bei Verletzungen der Datensicherheit

Gemäss Art. 24 revDSG muss der Verantwortliche dem EDÖB neu Verletzungen der Datensicherheit melden, die für die Betroffenen zu einem hohen Beeinträchtigungsrisiko ihrer Persönlichkeit oder ihrer Grundrechte führen. Dabei hat die Meldung an den EDÖB so rasch wie möglich zu erfolgen. Vorher wird der Verantwortliche eine Prognose zu den möglichen Auswirkungen der Verletzung stellen und eine erste Beurteilung darüber vorzunehmen, ob die betroffenen Personen über das Ereignis zu informieren sind und auf welche Weise dies geschehen könnte.

Recht auf Datenportabilität

Mit dem Recht auf Datenherausgabe und -übertragung gemäss Art. 28 revDSG hat eine betroffene Person neu die Möglichkeit, ihre Personendaten, welche sie einem privaten Verantwortlichen bekanntgegeben hat, in einem gängigen elektronischen Format heraus zu verlangen oder einem Dritten übertragen zu lassen. Das Recht kann kostenlos geltend gemacht werden, ausser wenn die Herausgabe oder Übertragung mit einem unverhältnismässigen Aufwand verbunden ist.

Gestärkte Aufsichtsbefugnisse

Mit dem revidierten DSG wird der Beauftragte prinzipiell alle Verstösse untersuchen müssen. Neu kann er gegen unzureichende Datenbearbeitungen Verfügungen erlassen und muss in bestimmten Fällen zwingend konsultiert werden. Künftig sind Bussen bis zu CHF 250'000 möglich.

Untersuchung aller Verstösse gegen Datenschutzvorschriften

Der EDÖB wird in Zukunft alle Verstösse gegen das neue DSG durch Bundesorgane oder private Personen von Amtes wegen zu untersuchen haben (Art. 49 Abs. 1 revDSG). Im aktuellen DSG gilt noch die Einschränkung, wonach der EDÖB gegen Private nur dann von sich aus eine Untersuchung inklusive Sachverhaltsabklärungen durchführt, wenn die Bearbeitungsmethode geeignet ist, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen. Diese, als «Systemfehler» bezeichnete Interventionsschwelle fällt inskünftig weg. Bei Verletzungen der Datenschutzvorschriften von geringfügiger Bedeutung kann jedoch auch nach neuem Recht von der Eröffnung einer Untersuchung abgesehen werden (Art. 49 Abs. 2 revDSG). Auch kann der EDÖB wie bis anhin von der Eröffnung formeller Schritte absehen, wenn sich nach einer ersten Kontaktnahme mit dem oder der Bearbeitungsverantwortlichen zeigt, dass dieser Mängel, auf die

er aufmerksam gemacht wurde, anerkennt und innert nützlicher Zeit behebt. Aufgrund seiner beschränkten Ressourcen ist davon auszugehen, dass der EDÖB bei der Behandlung von Anzeigen auch nach Inkrafttreten des neuen Gesetzes nach Massgabe des Opportunitätsprinzips Prioritäten setzen wird.

Verfügungen

Nach Art. 51 Abs. 1 revDSG kann der EDÖB neu Verfahren nach dem Verwaltungsverfahrensgesetz durchführen und gegenüber Bundesorganen oder privaten Bearbeitungsverantwortlichen formell verfügen, eine Datenbearbeitung ganz oder teilweise anzupassen, zu unterbrechen oder gar einzustellen sowie Personendaten löschen oder vernichten zu lassen. So kann der EDÖB zum Beispiel verfügen, dass ein Unternehmen betroffene Personen über eine gemeldete Verletzung der Datensicherheit informieren muss. Bisher hatte der EDÖB lediglich die Kompetenz, Empfehlungen auszusprechen und bei deren Nichtverfolgung mit Klage an das Bundesverwaltungsgericht zu gelangen.

Konsultationen

Der EDÖB ist weder eine Genehmigungsbehörde noch eine Zulassungsstelle für Applikationen, Produkte, Regulierungen und Projekte. Das neue Gesetz sieht indessen an verschiedener Stelle vor, dass die Verantwortlichen den EDÖB vor dem definitiven Abschluss entsprechender Arbeiten und der Realisierung ihrer Vorhaben konsultieren müssen. So sind ihm Verhaltenskodizes und bei hohen Restrisiken auch Datenschutz-Folgenabschätzungen zur Stellungnahme vorzulegen.

Spontane Stellungnahmen und Information der Öffentlichkeit

Abgesehen von den Stellungnahmen im Rahmen formeller Konsultationen steht es dem EDÖB weiterhin frei, sich spontan zu neuen Technologien, Phänomenen der Digitalisierung oder zu Bearbeitungspraktiken gewisser Branchen zu äussern und seine Meinungsäusserungen und Einschätzungen zu publizieren. In Fällen von allgemeinem Interesse informiert der EDÖB die Öffentlichkeit zudem - wie nach bisherigem Recht - über seine Feststellungen und Massnahmen (auch im Rahmen formeller Untersuchungen).

Gebühren

Art. 59 revDSG regelt, für welche Leistungen der EDÖB von privaten Personen zukünftig Gebühren erheben wird. So fällt eine Gebühr an für Stellungnahmen zu einem Verhaltenskodex oder zu einer Datenschutz-Folgenabschätzung oder für die Genehmigung von Standarddatenschutzklauseln und verbindlichen unternehmensinternen Datenschutzvorschriften. Aber auch für allgemeine Beratungsdienstleistungen gegenüber Privaten wird der EDÖB zukünftig Gebühren erheben.

Sanktionen

Im neuen DSG werden Bussen für private Personen bis zu CHF 250'000 angedroht (Art. 60 revDSG). Strafbar sind vorsätzliches Handeln und Unterlassen, nicht jedoch Fahrlässigkeit. Nur auf Antrag bestraft werden die Missachtung von Informations-, Auskunfts- und Meldepflichten sowie die Verletzung von Sorgfaltspflichten und der beruflichen Schweigepflicht. Von Amtes wegen verfolgt wird hingegen die Missachtung von Verfügungen des EDÖB. Gebüsst wird grundsätzlich die verantwortliche natürliche Person. Neu kann aber auch das Unternehmen selbst bis zu CHF 50'000 gebüsst werden, wenn die Ermittlung der strafbaren natürlichen Person innerhalb des Unternehmens oder der Organisation einen unverhältnismässigen Untersuchungsaufwand mit sich ziehen würde.

Dem EDÖB kommen auch nach neuem Recht keine Sanktionsbefugnisse zu. Die fehlbaren Personen werden durch die kantonalen Strafverfolgungsbehörden gebüsst. Der EDÖB kann zwar Anzeige erstatten und im Verfahren die Rechte einer Privatklägerschaft wahrnehmen (Art. 65 Abs. 2 revDSG), ein Strafantragsrecht steht ihm aber nicht zu.

Ein langer Weg bis ans Ziel

In der Herbstsession 2020 hat das Eidgenössische Parlament das totalrevidierte Bundesgesetz über den Datenschutz sowie weitere, geänderte Erlasse zum Datenschutz verabschiedet. Der Bundesrat wird das neue DSG mit den dazugehörigen Vollzugsverordnungen voraussichtlich im zweiten Semester des Jahres 2022 in Kraft setzen.

Vorgeschichte

Das erste Bundesgesetz über den Datenschutz vom 19. Juni 1992 trat Mitte 1993 in Kraft. Nach einer Teilrevision im Jahr 2008, deren Ziel es war, die Bevölkerung besser über die Bearbeitung ihrer Daten zu informieren, sollte sich bald zeigen, dass die rasante, technologische Entwicklung weitere Anpassungen notwendig machte. Um der Bevölkerung in ihrem heutigen Alltag, der von Cloud-Computing, Big Data und sozialen Netzwerken geprägt ist, einen zeitgemässen Datenschutz zu garantieren, wurde eine umfassende Erneuerung des DSG unausweichlich.
Im Herbst 2017 verabschiedete der Bundesrat den Entwurf zu einer Totalrevision, den er an die Eidgenössischen Räte überwies.

Ziele der Revision

Nebst der Stärkung der Rechte der betroffenen Personen hob der Bundesrat in seiner Botschaft den sog. risikobasierten Ansatz als Leitlinien der Revision hervor: Staat und Unternehmen sollen die Risiken für die Privatsphäre und informationelle Selbstbestimmung frühzeitig erheben und die Anforderungen des Datenschutzes bereits im Planungsstadium ihrer digitalen Projekte miteinbeziehen. Hohe Risiken und die zu deren Beseitigung oder Minderung getroffenen organisatorischen und technischen Massnahmen sind zu dokumentieren. Sodann sollte das revidierte DSG die Selbstregulierung fördern, indem die Mitglieder von Branchen, die einen verbindlichen Verhaltenskodex erlassen, von gewissen Pflichten entbunden werden. Und nicht zuletzt sollte es die Aufsichtsbefugnisse des EDÖB stärken.

Etappierte Beratung

Anfang 2018 beschloss das Parlament, die Revision in zwei Etappen aufzuteilen: Zwecks Beachtung staatsvertraglicher Umsetzungsfristen wurden in einer ersten Etappe vorab die Bestimmungen zu Datenbearbeitungen angepasst, die für Bundesorgane wie das fedpol gelten. Diese Arbeiten mündeten im sog. Schengen-DSG, welches am 1. März 2019 in Kraft trat (s. 27. TB, Kap. 1.2).

Erst in einer zweiten Etappe erfolgte die Totalrevision des DSG als Ganzes. In der Herbstsession 2019 nahm sich der Nationalrat der Totalrevision als Erstrat an, welche die Eidgenössischen Räte am 25. September 2020 nach Bereinigung aller Differenzen verabschiedet haben. Bei der Ausgestaltung des neuen DSG berücksichtigten Bundesrat und Parlament die von der Schweiz unterzeichnete Erweiterung der Europaratskonvention 108[1] sowie die Datenschutzgrundverordnung der Europäischen Union (DSGVO)[2]. Aufgrund ihres extraterritorialen Anwendungsbereichs wird Letztere seit ihrer Inkraftsetzung im Mai 2018 bereits von weiten Teilen der Schweizer Wirtschaft angewandt. Trotz dieser Anlehnung an das europäische Recht entspricht das neue DSG der schweizerischen Rechtstradition, indem es einen hohen Abstraktionsgrad ausweist und technologieneutral formuliert ist. Von der DSGVO hebt es sich nicht nur aufgrund seiner Kürze, sondern auch einer teilweise unterschiedlichen Terminologie ab.

Allgemein wird davon ausgegangen, dass die Schweiz und die EU nach der Erneuerung ihrer Datenschutzgesetzgebungen gegenseitig die Gleichwertigkeit ihrer Datenschutzniveaus anerkennen werden, so dass der formlose Austausch von Personendaten über die Landesgrenzen weiterhin möglich bleibt. Die Erneuerung des aus dem Jahre 2000 stammenden Anerkennungsbeschlusses der EU gegenüber der Schweiz stand bei Redaktionsschluss des aktuellen Tätigkeitsberichts noch aus.

---

[1] Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, abgeschlossen in Strassburg am 28. Januar 1981, von der Bundesversammlung genehmigt am 5. Juni 1997. Die Erweiterung der Konvention wurde im Sommer 2020 von den Eidgenössischen Räten genehmigt. Der Bundesrat wird sie erst nach Inkrafttreten des neuen DSG ratifizieren können.

[2] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

1.2 Justiz, Polizei, Sicherheit

Auskunftsgesuche beim Nachrichtendienst des Bundes (NDB)

Nachdem der NDB im Jahr 2019 mit einer ungewöhnlich hohen Anzahl von Auskunftsgesuchen konfrontiert war, die er zunächst nur mit grosser Verzögerung behandeln konnte, ergriff er besondere Massnahmen zum Abbau dieser Pendenzen, welche der EDÖB aufsichtsrechtlich begleitete.

Ende 2019 berichteten verschiedene Medien darüber, dass der NDB viel mehr Gesuche über Verzeichnungen in seinen Informationssystemen als sonst üblich erhalte. Auslöser waren unter anderem frühere Medienberichte, die mit einer «Bespitzelung» verschiedener Politikerinnen und Politiker titelten. Diesbezüglich führte einerseits die Geschäftsprüfungsdelegation der beiden Räte (GPDel) Abklärungen durch. Andererseits prüfte die unabhängige Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten (AB-ND) die Führung von Dossiers über Politikerinnen und Politiker im Geschäftsverwaltungssystem des NDB.

Nachdem der EDÖB aufgrund von Bürgerbeschwerden darauf aufmerksam wurde, dass der NDB bei der Behandlung der Auskunftsgesuche sehr lange Bearbeitungszeiten aufwies, wurde er bei diesem vorstellig. Der NDB hielt gegenüber dem EDÖB fest, dass er seit 2019 rund zehnmal mehr Auskunftsgesuche als üblich erhalten habe. So seien innerhalb von etwas mehr als einem Jahr über tausend Gesuche eingetroffen. Der NDB werde alles daran setzen, um die hängigen Gesuche innert Wochen zu behandeln. Inzwischen habe er eine Arbeitsgruppe gebildet, um die Arbeitsabläufe so anzupassen, dass die zahlreichen hängigen Gesuche ohne Qualitätseinbusse abgebaut werden könnten.

Im Juni 2020 teilte der NDB dem EDÖB mit, dass u.a. dank den für den Pendenzenabbau zusätzliche verfügbar gemachten Ressourcen die neu eintreffenden Auskunftsgesuche seit Mai 2020 fristgerecht beantwortet werden konnten. Der NDB hielt weiter fest, dass noch rund 50 Auskunftsgesuche älteren Datums pendent seien, die regelmässig abgebaut wurden.

Botschaft zur Revision des DNA-Profil-Gesetzes wurde verabschiedet

Mit der Revision des DNA-Profil-Gesetzes will der Bundesrat den Behörden ermöglichen, bei Strafermittlungen mehr Informationen aus einer DNA-Spur herauszulesen. Der Forderung des EDÖB nach einem strengen Gesetzesrahmen wurde nachgekommen.

Der Bundesrat hat die Botschaft zur Revision des DNA-Profil-Gesetzes am 4. Dezember 2020 verabschiedet. Mit der Revision will der Bundesrat den Behörden ermöglichen, bei Strafermittlungen mehr Informationen aus einer DNA-Spur herauszulesen. Die Sicherheitspolitische Kommission des Nationalrates (SiK-N) hat am 26. Januar 2021 nach ausführlichen Anhörungen ohne Gegenstimmen entschieden, auf die Vorlage einzutreten. Sie ist der Ansicht, dass dadurch den Ermittlungsbehörden griffige Methoden gereicht werden, um Ermittlungsarbeiten rascher und fokussierter zu gestalten. Die Kommission betont, dass die Verhältnismässigkeit der Vorlage gegeben sei, da die Analyseergebnisse der Phänotypisierung nur zur Aufklärung von Straftatbeständen zur Anwendung komme, die eine maximale Freiheitsstrafe von mehr als drei Jahren vorsehen. In der aktuellen Praxis darf in bestimmten Fällen aus einer DNA-Spur nur das Geschlecht bestimmt werden. Mit der Vorlage sollen neu auch die Wahrscheinlichkeiten von Augen-, Haar- und Hautfarbe, die

mögliche biogeografische Herkunft sowie das Alter eruiert werden dürfen. Wie vom EDÖB gefordert, wird gesetzlich abschliessend festgelegt, welche Merkmale untersucht werden dürfen.

Der EDÖB hatte zum Änderungsentwurf des EJPD Stellung genommen und einen strengen Gesetzesrahmen gefordert (betreffend erste Ämterkonsultation vgl. 27. TB, Kap. 1.2). Er vertrat im Konsultationsverfahren – wie bereits im Zusammenhang mit dem Vorentwurf – den Standpunkt, dass die Phänotypisierung und der Suchlauf nach Verwandtschaftsbezug durch das Zwangsmassnahmengericht anzuordnen sind. Es handelt sich dabei um Instrumente, die mit erheblichen Grundrechtseingriffen verbunden sind und die nur zur Aufklärung schwerer Verbrechen gegen die körperliche Unversehrtheit, die Freiheit oder die sexuelle Integrität eingesetzt werden dürften. Er begrüsst den Umstand, dass diese Forderung – trotz der ursprünglichen Ablehnung durch das EJPD – berücksichtigt wurde.

Gesetzgebungsvorlage zur Überprüfung von Mobiltelefonen im Asylverfahren

Das mit der parlamentarischen Initiative 17.423 angestossene Gesetzgebungsvorhaben will dem Staatssekretariat für Migration (SEM) weitergehende Kompetenzen zur Überprüfung von mobilen Datenträgern bei der Identitätsabklärung im Asyl- und Wegweisungsverfahren einräumen. Der Beauftragte hat diesbezüglich bereits früh grundlegende Bedenken geäussert. Er begrüsst die zwischenzeitlich gemachten Verbesserungen, hält aber dennoch an seiner grundsätzlichen Ablehnung der Vorlage fest.

Die von Nationalrat Rutz am 17. März 2017 eingereichte parlamentarische Initiative 17.423 fordert eine Änderung der rechtlichen Grundlagen, die es dem SEM erlauben, mobile Datenträger von Asylsuchenden auszuwerten. Die staatspolitischen Kommissionen beider Räte haben der Initiative Folge gegeben. Gestützt darauf wurde die Änderung des Asylgesetzes sowie des Ausländer- und Integrationsgesetzes ausgearbeitet, welche dem SEM weitergehende Kompetenzen zur Überprüfung von mobilen Datenträgern bei der Identitätsabklärung im Asyl- und Wegweisungsverfahren gewährt.

Der EDÖB hat in den Konsultationsverfahren zur Vorlage Stellung genommen und grundlegende Bedenken geäussert (s. Bericht vom 4.6.2020). So wies er darauf hin, dass es sich bei der Auswertung elektronischer Datenträger um einen massiven Eingriff in die Privatsphäre vieler Menschen handelt, der sich auf genügende formelle Rechtsgrundlagen stützen muss. Der EDÖB äusserte zudem Zweifel darüber, ob die vorgeschlagenen Massnahmen die gewünschte Wirkung erzielen können und ob die vorgeschlagene Regelung im Lichte der verfassungsrechtlichen Grundsätze der Gleichheit und Verhältnismässigkeit grundrechtskonform umgesetzt werden kann, zumal das administrative Asyl- bzw. Wegweisungsverfahren anders als das Strafprozessrecht keine eigentlichen verfahrensrechtlichen Garantien für die Beschlagnahme und Auswertung elektronischer Datenträger kennt. Ebenso wenig dürfe die Massnahme zu einem indirekten Zwang führen, Smart Devices auf sich zu tragen und jederzeit verfügbar zu machen.

Die betroffenen Behörden, darunter insbesondere das SEM, haben die Kritik konstruktiv aufgenommen und sind in weiten Teilen auf die Forderungen des EDÖB eingegangen. So wurde vom zwangsweisen Einzug elektronischer Datenträger abgesehen und eine formell-gesetzliche Grundlage für die Massnahme geschaffen. Wie vom Beauftragten gefordert, wird nun ausdrücklich geregelt, dass es sich bei der Auswertung mobiler Datenträger zur Identitätsabklärung um eine subsidiäre Massnahme handelt, welche in jedem Fall verhältnismässig zu erfolgen hat, und dass die Weigerung einer asylsuchenden Person nur bei der Glaubwürdigkeitsprüfung berücksichtigt werden darf. Den betroffenen Personen kommen Anwesenheits- und Informationsrechte zu. Die Position von Drittpersonen, deren Personendaten bei der Auswertung mitbetroffen sind, konnte ebenfalls gestärkt werden. Schliesslich begrüsst der Beauftragte, dass seinen grundsätzlichen Bedenken

gegenüber der Geeignetheit und Wirksamkeit der vorgesehenen Massnahme durch eine Evaluationspflicht Rechnung getragen werden soll.

Für den Beauftragten ist allerdings weiterhin nicht erkennbar, wie der Grundsatz der Subsidiarität und der Verhältnismässigkeit in der Praxis umgesetzt werden soll. Laut dem erläuternden Bericht zur Änderung der rechtlichen Grundlagen sollen andere Massnahmen zur Identitätsabklärung namentlich dann zum Zuge kommen, wenn sie im Vergleich zur elektronischen Datenauswertung mit einem geringeren Aufwand möglich sind. Für die Beurteilung der Verhältnismässigkeit einer Massnahme dürfte damit letztlich ausschlaggebend sein, welches Auswertungsverfahren den geringsten Aufwand bereitet. Dabei ist zu bedenken, dass gemäss Gesetzesvorlage die Auswertung von Personendaten durch den Einsatz einer entsprechenden Software automatisiert erfolgen kann. In der Folge könnte die Auswertung elektronischer Datenträger regelmässig, wenn nicht gar standardmässig, erfolgen. Die Effizienz darf jedoch nicht über die Wahrung fundamentaler Freiheitsrechte gestellt werden. Der Beauftragte muss daher an seiner grundsätzlichen Ablehnung der Vorlage festhalten. Er gibt dabei über den Kontext des Asylrechts hinaus zu bedenken, dass freiheitseinschränkende Massnahmen oft zunächst gegenüber Minderheiten eingeführt werden, bevor sie schrittweise in anderen Zusammenhängen auf breite Bevölkerungskreise ausgeweitet werden.

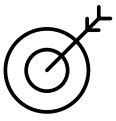
Intervention des EDÖB bei der Eidgenössischen Zollverwaltung: Ungenügende Regelung der Datenbearbeitung in neuem Zollpolizeigesetz

Die Eidgenössische Zollverwaltung erarbeitet eine Gesetzesrevision mit dem Ziel, den rechtlichen Rahmen für den Einsatz zukunftsorientierter digitaler Technologien zu legen und gleichzeitig die notwendige organisatorische Flexibilität zu schaffen, um in Zukunft noch rascher und wirksamer auf veränderte Lagen reagieren zu können. Der Beauftragte begrüsst diese Bestrebungen. Er kritisiert jedoch die unzureichende Ausgestaltung der Datenbearbeitungsregeln in diesem Grossprojekt.

Unter der Kurzbezeichnung «BAZG-Vollzugsaufgabengesetz» (BAZG-VG) hat der Bundesrat am 11. September 2020 die Vernehmlassung über ein Gesetzespaket eröffnet, mit dem er die rechtliche Grundlage für das Digitalisierungs- und Transformationsprogramm (DaziT) der Eidgenössischen Zollverwaltung schaffen will. Dabei handelt es sich um ein finanziell bedeutsames und datenschutzsensibles Grossvorhaben. Die Zollverwaltung und das dort integrierte Grenzwachtkorps sollen in ein neu zu schaffendes Zollpolizeiamt, das «Bundesamt für Zoll und Grenzsicherheit (BAZG)», überführt werden. Dessen gesamte Belegschaft soll mit Polizeibefugnissen und damit zwangsbewehrten Datenbeschaffungskompetenzen ausgestattet werden.

Der EDÖB hat die Eidgenössische Zollverwaltung in der zweiten Ämterkonsultation (betreffend erste Ämterkonsultation vgl. 27. TB, Kap. 2.4), welche vom 5. bis zum 25. März 2020 stattfand, vergeblich darauf hingewiesen, dass die vorgesehenen Bestimmungen zur Personendatenbearbeitung aus seiner Sicht gewichtige Mängel aufwiesen. Diese liessen insbesondere die vom Datenschutzgesetz verlangte Bestimmtheit vermissen, welche es der Bevölkerung ermöglichen würde, die in deren Privatsphäre und Selbstbestimmung eingreifenden staatlichen Datenbearbeitungen sowie die ihr dagegen zur Verfügung stehenden Schutzrechte einzuschätzen.

Der Beauftragte hat den Bundesrat dahingehend beraten, dass sich Regierung und Parlament als politische Organe des Bundes vorbehalten mögen, die wesentlichen Grundzüge der neu in einem einzigen System der Zollpolizei vorzunehmenden Datenbearbeitungen und die Schnittstellen zu diesem System zu regeln.



Vor dem Hintergrund dieser Hinweise hat der Bundesrat die Verwaltung angewiesen, die Datenbearbeitungsbestimmungen zu überarbeiten, was in den Vernehmlassungsunterlagen angedeutet wurde. Der Beauftragte begrüsst dies. Er steht im intensiven Austausch mit der Eidgenössischen Zollverwaltung und dem Bundesamt für Justiz, um anhand konkreter Anregungen eine Bereinigung der festgestellten Mängel zu bewirken.

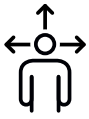
1.3 Steuer- und Finanzwesen

Der EDÖB setzt sich vor Bundesgericht für das Recht auf Information in der internationalen Steueramtshilfe ein

Das Bundesverwaltungsgericht hiess im 2019 eine Beschwerde des EDÖB zum Recht auf Information in der internationalen Steueramtshilfe gut. Im anschliessenden Beschwerdeverfahren vor Bundesgericht hat sich der Beauftragte erneut für das Recht auf Information eingesetzt. Der Entscheid des Bundesgerichts steht noch aus.

In der internationalen Steueramtshilfe knüpft das Recht, über ein laufendes Amtshilfeverfahren informiert zu werden, an die Beschwerdeberechtigung einer Person an (vgl. Art. 14 Steueramtshilfegesetz). 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 der Übermittlung zu informieren hat (s. 25. TB, Kap. 1.9.2). Dem lag die Auffassung des EDÖB zugrunde, dass Drittpersonen legitimiert sind, sich gegen eine unrechtmässige Übermittlung ihrer Daten mittels Beschwerde zur Wehr zu setzen. 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 begrüsste das Urteil, da es die Grundrechte der Bankmitarbeitenden und weiterer Drittpersonen schützt.



Die ESTV erhob beim Bundesgericht Beschwerde. Die von der ESTV beantragte Sistierung des Verfahrens hob das Bundesgericht auf, nachdem es am 13. Juli 2020 in einer anderen Angelegenheit mit ähnlicher Fragestellung ein Grundsatzurteil (BGE 146 I 172) gefällt hatte. In jenem Urteil schränkte das Bundesgericht das Recht auf Information stark ein: Es führte aus, dass Drittpersonen, deren Daten von der ESTV ungeschwärzt an die ersuchende ausländische Behörde übermitteln werden sollen, lediglich ausnahmsweise, nämlich aufgrund besonderer Umstände, legitimiert sind, sich dagegen mittels einer Beschwerde zu wehren. Sodann muss die ESTV nicht sämtliche beschwerdelegitimierten Drittpersonen von Amtes wegen vorgängig der Datenübermittlung informieren, sondern lediglich solche, deren Beschwerdeberechtigung aufgrund der Akten geradezu offensichtlich ist.

Unter Berücksichtigung dieser neuesten Rechtsprechung anerkannte der EDÖB vor Bundesgericht, dass Drittpersonen in der internationalen Steueramtshilfe nicht generell, sondern nur ausnahmsweise beschwerdelegitimiert sind. Er hielt jedoch an der vom Bundesverwaltungsgericht bestätigten Auffassung fest, dass sämtliche Drittpersonen im Grundsatz von Amtes wegen vorgängig der Übermittlung ihrer Daten informiert werden müssen. Nur so können tatsächlich alle Drittpersonen, die im Sinne der bundesgerichtlichen Rechtsprechung beschwerdelegitimiert sind, von ihrem Beschwerderecht Gebrauch machen und sich gegen eine bevorstehende Datenübermittlung zur Wehr setzen. Der EDÖB hat vor Bundesgericht sodann erneut skizziert, wie sich eine grundsätzliche Informationsverpflichtung der ESTV umsetzen liesse, ohne dass dieser daraus ein unverhältnismässiger Aufwand entsteht und die internationale Steueramtshilfe übermässig verzögert oder behindert wird. Der Entscheid in dieser Angelegenheit steht zurzeit noch aus.


Restaurants

1.4 Handel und Wirtschaft

Abklärungen 5G Implementierungen von Sunrise und Swisscom

Der EDÖB konnte zwei unabhängig voneinander geführte Sachverhaltsabklärungen bei den Firmen Sunrise und Swisscom zur Implementierung der neuen Mobilfunkstandards der 5. Generation (5G) abschliessen. Beide Anbieter zeigten auf, dass der Datenschutz und die technische Sicherheit einen hohen Stellenwert geniessen.

Der neue Fernmeldestandard 5G soll gemäss den technischen Spezifikationen nebst einer höheren Datengeschwindigkeit (sog. Datendurchsatzrate) auch eine erhöhte Sicherheit bieten. Aufgrund der Aktualität und Tragweite dieser Umstellung hat der EDÖB im Jahr 2019 zwei formelle Sachverhaltsabklärungen bei den Anbietern Swisscom und Sunrise eröffnet, als diese die 5G-Einführung planten. Beide Anbieter haben dem EDÖB Einblick in die Konzeption und den Stand der Implementierung gegeben und umfangreiche Dokumentationen zugestellt. Nebst einer Vielzahl von technischen Fragen waren für den Beauftragten folgende Aspekte von besonderer Bedeutung: Einerseits war bereits 2018 diversen Medienberichten zu entnehmen, dass bei der Implementierung des 5G-Standards empfindliche Schwachstellen auftreten können und Sicherheitslücken bekannt seien. Andererseits bestanden Sicherheitsbedenken bezüglich der verwendeten Ausrüster, insbesondere Huawei. Der EDÖB verlangte deshalb von den kontrollierten Unternehmen eine Stellungnahme, wie sie den bekannten Schwachstellen begegnen und ob Abhängigkeiten zu einzelnen Lieferanten - namentlich zu Huawei - bestehen, welche die Verfügbarkeit (beispielsweise aufgrund von US-Handelssanktionen), die Vertraulichkeit oder die Datensicherheit beeinträchtigen.

Der Anbieter Sunrise zeigte auf, dass er sich konsequent mit internationalen Gremien und Arbeitsgruppen der Telekommunikationsbranche austauscht und dass er seine Implementierung zusätzlich durch eine unabhängige externe Firma untersuchen liess. Insbesondere die dort identifizierten Massnahmen zur Verbesserung sind aus Sicht des EDÖB für die Erzielung einer ausreichenden Sicherheit und eines angemessenen Datenschutzniveaus von grossem Wert. Er hat Sunrise deshalb die abschliessende Umsetzung dieser Massnahmen empfohlen. Bezüglich ihres 5G-Partners und Ausrüsters Huawei hat Sunrise Risikoanalysen durchgeführt. Dabei wurden Risiken in den Bereichen Verfügbarkeit, Zusammenarbeit und Spionage identifiziert. Für diese anbieterspezifischen Risiken hat Sunrise Massnahmen definiert und umgesetzt.

Wie bei Sunrise fand der EDÖB auch bei der Swisscom keine Anhaltspunkte, wonach die Umsetzung mit Fokus auf die Datensicherheit und den Datenschutz nicht angemessen wäre. Bezüglich der Datensicherheit von 5G hat die Swisscom interne Security Assessments durchgeführt. Wie Sunrise steht auch Swisscom im Austausch mit diversen internationalen Gremien und Arbeitsgruppen und orientiert sich an deren bewährten Ansätzen für einen sicheren Betrieb. Swisscom benennt ihren langjährigen Partner Ericsson als Hauptausrüster für die 5G-Technologie und erklärt, dass es sich bei den von Huawei gelieferten und im Antennenbau eingesetzten Komponenten lediglich um passive Elemente ohne Elektronik handelt, die nur für das Empfangen und Senden der Wellensignale verwendet werden.

Der EDÖB kommt zum Schluss, dass die Datensicherheit von den kontrollierten Unternehmen angemessen berücksichtigt wurde und die Datenschutzüberlegungen bei der Einführung einen hohen Stellenwert geniessen. Bei einer vollständigen Adaption des 5G-Standards sind gegenüber 4G Vorteile bezüglich der Informationssicherheit ersichtlich.

Fehlerhafte Datenbankeinträge bei Inkassounternehmen

Der EDÖB hat die Sachverhaltsabklärung betreffend mögliche fehlerhafte Datenbankeinträge bei einem der führenden Inkassounternehmen fortgesetzt und den Untersuchungsgegenstand erweitert.

Im Februar 2020 hatte der Beauftragte bei dem Unternehmen eine Sachverhaltsabklärung wegen angeblich fehlerhaften Datenbankeinträgen und daraus folgenden Verwechslungen von Personen mit gleichen oder ähnlichen Namen und Adressen sowie möglicherweise vorhandenen Schwierigkeiten bei der Korrektur von solchen Fehleinträgen eröffnet (s. 27. TB, Kap. 1.4).

Im Berichtsjahr zeigte sich anhand von Bürger- und Medienanfragen, dass auch sogenannte «negative Haushaltstreffer» datenschutzrechtliche Fragen aufwerfen. Der EDÖB entschied sich deshalb, die laufende Sachverhaltsabklärung um diesen Punkt zu erweitern. Von negativen Haushaltstreffern spricht man, wenn im Rahmen von Bonitätsauskünften negative Bonitätsinformationen über andere Personen im selben Haushalt bekannt gegeben werden. So kann es passieren, dass Kundinnen und Kunden in Online-Shops trotz einwandfreier Bonität Waren nicht auf Rechnung bestellen können, wenn in ihrem Haushalt eine Person mit negativer Bonität wohnhaft ist. Diese rechtlichen Abklärungen waren am Ende des Berichtsjahres noch im Gang.

Kreditfähigkeitsprüfung bei Autoleasing

Um einen Leasingvertrag abschliessen zu können, müssen Kundinnen und Kunden ihr Einverständnis geben, dass ihre Kreditfähigkeit durch den Leasinganbieter geprüft wird. Dazu kann dieser auch Auskünfte bei Dritten einholen. Der EDÖB nimmt erste Abklärungen zu diesen Datenbearbeitungen vor.

Bevor Konsumentinnen und Konsumenten einen Leasingvertrag für ein Auto abschliessen können, muss der Leasinganbieter deren Zahlungsfähigkeit überprüfen. Er muss zu diesem Zweck gewisse Informationen über die potenziellen Leasingnehmenden einholen, die Auskunft über deren wirtschaftliche Verhältnisse geben. Fällt diese Kreditfähigkeitsprüfung negativ aus, darf der Leasingvertrag nicht abgeschlossen werden. Dies ist im Konsumkreditgesetz so vorgesehen. Ziel ist es, eine Überschuldung der Konsumentinnen und Konsumenten zu vermeiden. Diese Datenbearbeitungen unterliegen den Bestimmungen des DSG und dürfen die Persönlichkeit der Leasingnehmenden und allfälliger Dritter nicht widerrechtlich verletzen. Insbesondere dürfen nur diejenigen Informationen bearbeitet werden, die erforderlich sind, um die Kreditfähigkeit feststellen zu können.

Durch Bürgeranfragen erhielt der EDÖB Kenntnis davon, dass sich ein Leasinganbieter von Leasingantragstellenden deren Einverständnis geben lässt, zwecks Prüfung der Zahlungsfähigkeit zahlreiche Auskünfte bei Dritten einholen zu dürfen. Zustimmen muss man auch dem Einholen von Auskünften über dritte Personen wie Ehepartner oder Familienmitglieder. Für den EDÖB stellte sich die Frage, ob sich diese Datenbearbeitungen auf ein datenschutzrechtlich erlaubtes Mass beschränken und ob die Erkennbarkeit der Datenbearbeitung für die Betroffenen gewährleistet ist. Der Beauftragte hat den Leasinganbieter deshalb um Stellungnahme zu verschiedenen Fragen gebeten. Anhand der Antworten wird er prüfen, ob er eine Abklärung vornehmen und gegebenenfalls Massnahmen empfehlen soll.

Migros Sachverhaltsabklärung Videoüberwachung

Im Berichtsjahr hat der EDÖB im Rahmen einer Sachverhaltsabklärung das neue Videoüberwachungssystem der Migros beurteilt. Das Unternehmen legte dar, dass weder Gesichtserkennung noch automatisierte Auswertungen von Verhaltensmustern oder ähnliche Analysen erfolgen. Der EDÖB hat keine Empfehlungen erlassen, jedoch Verbesserungen bezüglich der Information der Kundinnen und Kunden über das System verlangt.

Videoüberwachungssysteme können für Unternehmen ein Mittel sein, um ihre berechtigten Interessen, wie zum Beispiel der Schutz von Eigentum, zu wahren. Auf der anderen Seite wächst in der Öffentlichkeit das Unbehagen gegenüber solchen Vorhaben nicht zuletzt wegen neuen technischen Möglichkeiten der Identifizierung und Analyse.

Auch das neue System der Migros wurde in den Medien kritisiert und sorgte für einige Verunsicherung. Um sich Klarheit über die Funktionen der neuen Videoüberwachung der Migros zu verschaffen, hat sich der EDÖB das System und die vom Unternehmen getroffenen Massnahmen zum Schutz der Persönlichkeitsrechte im Rahmen seiner Aufsichtstätigkeit beschreiben und dokumentieren lassen.

Nach Auswertung der Stellungnahme der Migros und den eingereichten Unterlagen konnte der EDÖB zunächst feststellen, dass sich das neue Videoüberwachungssystem auf reaktive Funktionen beschränkt: In einem konkreten Verdachtsfall kann der Sicherheitsverantwortliche einer Migros-Filiale durch manuelle Auswahl eines Standbilds bestimmte Parameter einer verdächtigen Person erfassen (Haarfarbe, Geschlecht und Grösse). Das System sucht in den aufgezeichneten Videoaufnahmen und innerhalb eines definierten Zeitraumes nach derselben Kombination von Parametern. Das Bildmaterial wird dem Sicherheitspersonal der betreffenden Migros-Filiale angezeigt und soll so bei der Ermittlung von deliktischen Handlungen helfen.

Die Migros hielt fest, dass weder eine Gesichtserkennung noch eine automatisierte Auswertung von Verhaltensmustern oder ähnliche Analysen erfolgen. Die Identifikation von Personen, welche mit dem Videoüberwachungssystem aufgenommen wurden, ist nur in begründeten Einzelfällen ausserhalb des Systems möglich und folgt einem vom Unternehmen festgelegten Verfahren.

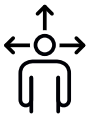
Da sich das neue Videoüberwachungssystem angesichts seiner eingeschränkten Funktionen folglich nicht wesentlich von bisherigen Systemen unterscheidet, kann der EDÖB von datenschutzrechtlichen Empfehlungen absehen. Des Weiteren erscheinen die von der Migros dargelegten technischen und organisatorischen Massnahmen und Prozesse geeignet, die Sicherheit der bearbeiteten Personendaten im Zusammenhang mit dem Videoüberwachungssystem zu gewährleisten.

Der EDÖB hat jedoch Verbesserungen in Bezug auf die Informationen über das neue System in den Datenschutzbestimmungen und auf der Webseite der Migros verlangt, da diese zu allgemein formuliert sind und das neue System und seine Funktionen nicht erklären. Zudem verlangte er von der Migros, dass sie ihn über zukünftige Vorhaben oder allfällige Funktionserweiterungen im Bereich Videoüberwachung rechtzeitig und vorgängig informiert. Eine Antwort der Migros war im Zeitpunkt des Redaktionsschlusses dieses Berichts noch ausstehend.

Bearbeitung von Kundendaten durch Onlineshops

Wir haben bei einem Onlineshop ein Verfahren eröffnet, um die bei ihm anfallenden Bearbeitungen von Kundendaten auf ihre Datenschutzkonformität hin zu überprüfen. Ausserdem stellt sich die Frage, ob die Datenbearbeitungen gegen den ausdrücklichen Willen der Nutzer erfolgen dürfen.

Sei es wegen der Schliessung von Ladengeschäften während des Lockdowns oder wegen der mit einem Geschäftsbesuch verbundenen Risiken – die Corona-Pandemie hat viele Personen dazu veranlasst, ihre Einkäufe online zu erledigen. Für manche Personen sind Onlineshops sogar die einzige Möglichkeit geworden, um bestimmte Waren zu beschaffen. Aufgrund von Bürgeranfragen wurden wir darauf aufmerksam gemacht, dass man bei einem der grössten Schweizer Onlinehändler ein Kundenkonto erstellen und mithin sämtlichen in der Datenschutzerklärung umschriebenen Datenbearbeitungen zustimmen musste, um eine Bestellung tätigen zu können.



Unter anderem bedeutete dies, dass die Kundinnen und Kunden der Aufzeichnung und der Auswertung ihres Kaufverhaltens in individualisierter und personenbezogener Form, der Verknüpfung mit weiteren Personendaten (z.B. mit in der Vergangenheit von diesem oder anderen Unternehmen des Konzerns oder von Dritten bereits gesammelten oder öffentlich erhältlichen Personendaten) sowie der Weitergabe von Personendaten an andere Unternehmen des Konzerns zustimmen mussten. Später beim Kundendienst eingereichte Widerspruchsbegehren konnten diese Datenbearbeitungen nicht verhindern. Der Betreiber des Onlineshops lehnte diese mit der Begründung ab, dass die Datenschutzerklärung für die gesamte Kundschaft ausnahmslos und gleichermassen gelte und diese Bearbeitungen keine Optionen für die Kundinnen und Kunden seien.

Im Frühjahr 2020 haben wir den Betreiber des Onlineshops im Sinne einer Vorabklärung angeschrieben, um uns einerseits einen Überblick über seine Bearbeitungsmethoden zu verschaffen und andererseits die Widerspruchsmöglichkeiten der Kundinnen und Kunden zu klären. Nach Auswertung der Antwort des Betreibers haben wir in der Folge eine Sachverhaltsabklärung eröffnet. Unser Fokus liegt dabei nebst der Analyse der Datenschutzkonformität der vom Betreiber des Onlineshops und weiteren Unternehmen des Konzerns durchgeführten Datenbearbeitung auf der Frage, ob diese Datenbearbeitungen gegen den ausdrücklichen Willen der Nutzer erfolgen dürfen.

Verwendung der Daten von ricardo.ch innerhalb der TX Group

Im Rahmen des laufenden Verfahrens zur Abklärung des Sachverhalts hat der EDÖB die rechtliche Prüfung der Verwendung der auf der Plattform ricardo.ch erhobenen Daten durch die TX Group vorgenommen. Wir sind zum Schluss gekommen, dass die Datenbearbeitungen, welche zum Zweck der gezielten Werbung durchgeführt werden, durch eine Einwilligung der Nutzerinnen und Nutzer gerechtfertigt werden müssen. Ferner sind wir der Auffassung, dass die Information an die Nutzergruppe derzeit ungenügend und dass die Datenschutzerklärung verbesserungsbedürftig ist.

Wie aus unseren vorangehenden Tätigkeitsberichten zu entnehmen ist, eröffnete der EDÖB eine Sachverhaltsabklärung gegen Ricardo bezüglich der Verwendung der bei der Online-Auktionsplattform ricardo.ch gesammelten Daten und dehnte diese auf die Tamedia/TX Group. Unsere in diesem Zusammenhang durchgeführte Sachverhaltsfeststellung konnte im März 2020 abgeschlossen werden. Diese Feststellung beruht namentlich auf der neuen Datenschutzerklärung von ricardo.ch, die von den Unternehmen der TX Group standardmässig eingesetzt wird, sowie auf den Antworten von ricardo.ch und TX Group betreffend den konzerninternen Umgang mit Daten. Unsere rechtliche Beurteilung aus Sicht des Datenschutzgesetzes DSG wird in einem Schlussbericht dargelegt.

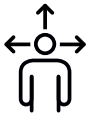
Die Datenschutzerklärung von Ricardo sieht namentlich die Möglichkeit vor, den Unternehmen der

TX Group oder deren Partnern personenbezogene Daten, die auf der Plattform ricardo.ch gesammelt werden, «zur Personalisierung und zu Marketingzwecken» zu übermitteln. Dazu gehört, dass das Online-Verhalten der Nutzerinnen und Nutzer anhand von Analysetools mitverfolgt und analysiert werden kann. Eine solche Datenbearbeitung erfolge «vor allem mit pseudonymisierten oder anonymisierten Daten». Zweck der Datenbearbeitung ist das Adressieren oder Anzeigen von «anonymer Werbung» auf Portalen der TX Group sowie die Verbesserung der Sicherheit.

Unsere Sachverhaltsfeststellung konnte aufzeigen, dass die TX Group (ehemals Tamedia AG) bestimmte Daten der Nutzerinnen und Nutzer der Plattform ricardo.ch für Marketingzwecke bearbeitet und analysiert. Die Datenbank des Konzerns lässt sich anhand von Daten speisen, die auf verschiedenen Portalen der TX Group erhoben und in eine aggregierte Form gebracht werden. Zweck der Analyse und der Verknüpfung dieser aus unterschiedlichen Quellen stammenden Daten ist es, gezielte Werbung an die Nutzerinnen und Nutzer von Dienstleistungen der TX Group oder ihrer Partnerfirmen zu adressieren, wobei eine Segmentierung nach sozio-demografischen Merkmalen (anhand der von der Nutzerin bei der Registrierung gemachten Angaben) und nach mutmasslichen Interessensgebieten erfolgt, welche aus dem Online-Verhalten der Nutzer auf anderen Portalen der TX Group oder ihrer Partnersites hergeleitet werden. Möglich wird die Verknüpfung der Daten innerhalb der TX Group durch pseudonyme Identifikatoren, die unter anderem ausgehend von Email-Adressen erzeugt werden.

Unsere rechtliche Prüfung des Sachverhalts führte unter anderem zu folgenden Feststellungen:

- Die Bearbeitung der Daten, insbesondere die von der TX Group vorgenommene Datenverknüpfung und die Nutzersegmentierung, entspricht einer Bearbeitung von Personendaten, die dem Datenschutzgesetz untersteht. Die Zusammenstellung von Daten, die aus dem Profiling hervorgehen, kann zudem im vorliegenden Fall ein Persönlichkeitsprofil im Sinne des DSG darstellen, so dass die erhöhten datenschutzrechtlichen Anforderungen hier zum Tragen kommen.



- Ein derartiges Profiling zum Zweck der gezielten Werbung setzt nach Auffassung des Beauftragten die Einwilligung der betroffenen Personen voraus, welche ausserdem ausdrücklich erfolgen muss. Denn die vorliegenden berechtigten Interessen der TX Group überwiegen im konkreten Fall das Recht auf informationelle Selbstbestimmung der Nutzerinnen und Nutzer der Plattform ricardo.ch nicht.
- Die Datenschutzerklärung und die diesbezügliche Kommunikation von ricardo.ch/TX Group sind im Sinne des Grundsatzes der Transparenz zu verbessern. Insbesondere müssen die Nutzer eindeutig nachvollziehen können, welche Datenbearbeitungen von Ricardo einerseits und von der TX-Gruppe andererseits durchgeführt werden, welche Zwecke damit verfolgt werden, und ob es Möglichkeiten gibt, dagegen Einspruch zu erheben. Gegebenenfalls müssen die Widerspruchsmöglichkeiten effektiv durchgesetzt werden können.

Der EDÖB arbeitet an der Prüfung des weiteren Vorgehens.

Revision der Energieverordnung

Der EDÖB fordert im Rahmen der Revision der Stromversorgungsverordnung (StromVV) im Interesse der Betroffenen eine höchstens zweijährige Frist für die Aufbewahrung von Messdaten durch die Netzbetreiber. Das UVEK lehnt diese Forderung ab – u.a. mit Verweis auf die bereits bestehenden fünfjährigen Fristen in der StromVV. Eine entsprechende Differenz wurde ausgewiesen.

Im Rahmen einer Ämterkonsultation im Bereich der Revision der Energieverordnung erachtete der EDÖB die darin festgelegte Aufbewahrungsfrist der Lastgangwerte von fünf Jahren aus zeitlicher Hinsicht als nicht verhältnismässig. Der EDÖB ist der Ansicht, dass es sich hier um eine Vorratsdatenspeicherung handelt, welche alle Strombezüger in der Schweiz betrifft. Für den Zweck der Stromverbrauchsoptimierung sollen die Lastgangprofile fünf Jahre gespeichert werden, obschon davon ausgegangen werden muss, dass die Mehrheit der Betroffenen diese nie auswerten wird. Auch für die Zwecke des Bilanz-Netzmanagements und der Abrechnung sind mildere Mittel möglich, um die verfolgten Zwecke zu erreichen, wie z.B. eine Aggregierung gemäss den Tarifpositionen (z.B. Hoch-/Niedertarif) für die Rechnungsstellung, wodurch das Lastgangprofil an sich nicht mehr abrechnungsrelevant wäre. Gemäss der StromVV werden die Personendaten und Persönlichkeitsprofile nach zwölf Monaten vernichtet, sofern sie nicht abrechnungsrelevant oder anonymisiert sind.

Die lange Aufbewahrung von fünf Jahren erweist sich insbesondere deshalb als problematisch, weil es sich bei den Lastgangprofilen um Persönlichkeitsprofile resp. nach dem revidierten DSG um ein Profiling handelt, bei denen erhöhte datenschutzrechtliche Anforderungen gelten.

Der EDÖB vertritt daher die Auffassung, dass die Personendaten nach zwölf Monaten, oder aber aus Praktikabilitätsgründen spätestens nach zwei Jahren, zu löschen sind, wenn nicht eine explizite Einwilligung der Betroffenen für eine längere Aufbewahrungsdauer vorliegt, z.B. zwecks Auskunft über die Daten des Lastgangprofils für Effizienzlösungen. Die entsprechende Bestimmung sollte dahingehend abgeändert werden, dass die Aufbewahrungsdauer für Lastgangprofile wie bisher zwölf Monate beträgt und die Kunden mit einer expliziten Einwilligung eine darüber hinausgehende Aufbewahrungsdauer bis maximal fünf Jahre beantragen können.

1.5 Gesundheit

Anforderungen an Cloud-Lösungen für die Bearbeitung von Patientendaten

Im Gesundheitsbereich werden zunehmend Cloud-Lösungen für die Bearbeitung von Patientendaten genutzt. Der EDÖB hat im Rahmen seiner Beratungstätigkeit auf die Punkte hingewiesen, die von Gesundheitsfachpersonen bei der Auswahl einer Cloud-Lösung zu beachten sind.

Der EDÖB wurde im Berichtsjahr wiederholt von Ärzten, Psychologen und weiteren im Gesundheitsbereich tätigen Personen bezüglich der Verwendung von Cloud-Lösungen für die Bearbeitung von Patientendaten kontaktiert. Dabei ging es um die Bearbeitung resp. Speicherung von Gesundheitsdaten in einem von einem externen Anbieter (sog. Cloud-Provider) betriebenen Rechenzentrum. Die Anfragen betrafen insbesondere die Aufbewahrung und Weitergabe, bzw. die Löschung von Patientendaten (z.B. nach dem Tod eines Patienten oder nach Auflösung einer Arztpraxis).

Der EDÖB weist im Rahmen seiner Beratungstätigkeit zunächst darauf hin, dass der Arzt auch bei der Verwendung einer Cloud-Lösung für die Sicherheit der Daten verantwortlich bleibt, selbst wenn er fortan nur noch eine begrenzte Kontrolle über die Datensicherheit hat. Daher muss er den Cloud-Provider sorgfältig auswählen und auf folgende Punkte achten:

- Die Daten sollten in der Schweiz verbleiben;
- Der Vertrag mit dem Cloud-Provider sollte den Anforderungen aus dem Arztgeheimnis genügen;
- Alle Personen mit Zugriff auf die Patientendaten müssen der ärztlichen Schweigepflicht unterstehen;
- Die Löschung der Patientendaten sollte jederzeit möglich sein;
- Eine Liste aller Personen, die Zugriff auf die Daten haben, sollte jederzeit eingefordert werden können;
- Die Datensicherheit sollte regelmässig überprüft werden, und die dazugehörigen Audits sollten verfügbar sein;
- Der Ansprechpartner in Sachen Datenschutz sollte dem Arzt bekannt sein;
- Ein Backup sollte täglich erstellt werden können;
- Alle Verbindungen müssen verschlüsselt werden, und eine 2-Faktoren-Authentifizierung sollte die Zugriffe auf die Daten auf die berechtigen Personen beschränken.

Abschliessend lässt sich deshalb festhalten, dass der EDÖB von der Verwendung von gängigen unentgeltlichen Cloud-Lösungen für den Austausch bzw. für die Aufbewahrung von Patientendaten abrät, da diese die obengenannten Bedingungen in der Regel nicht erfüllen.

CORONA

Sachverhaltsabklärung in Sachen meineimpfungen.ch

Bereits Jahre vor der Pandemie wurde die von einer Stiftung betriebene elektronische Impfplattform meineimpfungen.ch ins Leben gerufen und unter anderem vom Bundesamt für Gesundheit (BAG) finanziell unterstützt. Die Plattform war als elektronische Alternative des gängigen Impfbüchleins angedacht.

Im Kontext der COVID-19-Pandemie erhielt die Plattform einen erheblichen Zuwachs an Nutzerinnen und Nutzern. Dies mitunter aufgrund bereitgestellter Schnittstellen zu der vom BAG propagierten Applikation für die Anmeldung der Impfwilligen. Die Stiftung entwickelte und betrieb zudem im Auftrag des BAG ein spezifisches Modul für die Dokumentation der COVID-19-Impfung (myCOVIDvac).

Ende März 2021 wurde der Beauftragte mit den Ergebnissen einer journalistischen Recherche konfrontiert, welche auf mögliche schwerwiegende Sicherheits- und Datenschutzmängel bei der Plattform meineimpfungen.ch hinwies. Nach Rücksprache mit dem Nationalen Zentrum für Cybersicherheit (NCSC) hat der Beauftragte innert Tagesfrist eine formelle Sachverhaltsabklärung eröffnet und der Stiftung die sofortige Einstellung des Betriebs empfohlen. Bei Abschluss des Geschäftsjahres war das Verfahren noch pendent und eine Wiederaufnahme des Betriebs der Plattform noch nicht absehbar.

Weiter hat der EDÖB in Absprache mit den Datenschutzbehörden der Kantone darauf hingewirkt, dass weitere Plattformen, die Private im Kontext mit der Pandemiebekämpfung im Auftrag oder mit Empfehlung der Gesundheitsbehörden von Bund und Kantonen betreiben, näher überprüft werden.

CORONA

Datenschutzrechtliche Herausforderungen mit Blick auf mögliche Erleichterungen für geimpfte Personen

Mit dem Verfügbarwerden von Impfungen gegen das COVID-19-Virus setzte eine öffentliche Diskussion über die Aufhebung von Verboten und die Freiheit einschränkenden Massnahmen zu Gunsten von Geimpften ein. Der EDÖB sprach sich seit Dezember 2020 öffentlich dafür aus, dass die mit Erleichterungen für Geimpfte einhergehende Bearbeitung von Gesundheitsdaten durch Staat und Wirtschaft nach klaren Vorgaben des öffentlichen Rechts erfolgen muss und nicht zu einer faktischen Smartphone-Tragpflicht führen darf.

Mit der Perspektive auf eine Impfung gegen das COVID-19-Virus setzte in der zweiten Welle der Pandemie eine öffentliche Diskussion über die Aufhebung von Verboten und die Freiheit einschränkenden Massnahmen zu Gunsten von Geimpften ein. Wie diese aus rechtlicher Sicht umzusetzen wäre, haben die Staatspolitischen Kommissionen beider Räte unter Anhörung des Beauftragen erörtert (siehe dazu die Medienmitteilung SPK-S vom 23.02.2021).

Der Staat und Private, die staatliche Aufgaben erfüllen, dürfen Differenzierungen aufgrund des Impfstatus nur gestützt auf eine entsprechende gesetzliche Grundlage vornehmen. Demgegenüber sind unter Privaten solche Differenzierungen vor dem Hintergrund der Vertragsfreiheit grundsätzlich auch ohne explizite Rechtsgrundlage möglich.

Machen Private den Zugang zu Gütern oder Leistungen vom Impfstatus ihrer Kundschaft oder Gäste abhängig, bearbeiten sie dabei regelmässig Gesundheitsdaten ihrer Mitbürgerinnen und Mitbürger, was je nach Umständen, zu Persönlichkeitsverletzungen führen kann. Der

Beauftragte stellte sich deshalb bereits zu Beginn der öffentlichen Diskussion wie auch in den erwähnten Anhörungen auf den Standpunkt, dass für diesen Fall gesetzliche Vorgaben geschaffen werden sollten. Er wies zudem auf die datenschutzrechtlichen Anforderungen hin, deren Erfüllung Private sicherzustellen haben, sofern sie den Zugang zu Gütern oder Leistungen von der Offenlegung eines Testresultats oder eines Impfnachweises abhängig machen wollen (siehe dazu unsere Kurzmitteilung vom 22.01.2021).

So muss die Beschaffung und Weiterbearbeitung der Personendaten im Sinne der Verhältnismässigkeit geeignet sein, den verfolgten Zweck, d.h. den Schutz vor Übertragung und Erkrankung, zu erfüllen. Sodann ist auf die Einforderung von Gesundheitsdaten als Voraussetzung für den Zugang zu Gütern oder Leistungen abzusehen, wenn deren Verzicht den Betroffenen nicht zugemutet werden kann. Mit Blick auf die Art der Bearbeitung betonte der EDÖB schliesslich, dass Personen, die nicht in der Lage oder nicht willens sind, einen Impfnachweis auf dem Smartphone vorzuzeigen, zumutbare Alternativen zur digitalen Bearbeitung der erwähnten Personendaten unter vergleichbaren Bedingungen anzubieten sind.

Dieser letzte Aspekt ist für den Beauftragten von besonderer Bedeutung, weil davon auszugehen ist, dass die systematische Personendatenbearbeitung durch Private im Kontext der Pandemie die informationelle Selbstbestimmung der Bevölkerung über die aktuelle Situation hinaus prägen wird.

CORONA

Datenschutzkonforme Umsetzung des COVID-19-Zertifikats

Angesichts des Bedürfnisses, für Auslandreisen eine erfolgte COVID-19-Impfung, eine durchgemachte Erkrankung oder ein negatives Testresultat nachweisen zu können, hat das Bundesparlament im März 2021 eine Gesetzesbestimmung für ein einheitliches, fälschungssicheres und international anerkanntes COVID-19-Zertifikat geschaffen. Der Beauftragte begleitet die Umsetzungsarbeiten des Bundesamtes für Gesundheit (BAG) im Rahmen seiner aufsichtsrechtlichen Beratungspflicht.

Im Verlauf der zweiten Welle der Pandemie zeichnete sich das Bedürfnis ab, vorab für den internationalen Personenverkehr, eventuell aber auch weitere Verwendungsmöglichkeiten, für geimpfte, genesene oder negativ auf das Coronavirus getestete Personen die entsprechenden Bescheinigungen in zuverlässiger Art und Weise vorbringen zu können. Spezifische gesetzliche Regelungen über Form und Inhalt eines Impfausweises bestanden bis dahin in der Schweiz keine. So wurden auch die Nachweise über eine erfolgte COVID-19-Impfung oder ein Testresultat in Papierform, per SMS, E-Mail oder als (verifizierbarer) Eintrag auf einer einschlägigen Plattform angeboten. Die vielfältigen Möglichkeiten wurden jedoch nicht alle den datenschutzrechtlichen Anforderungen gerecht, was den EDÖB zu aufsichtsrechtlichen Interventionen veranlasste (s. Box zu «meineimpfungen.ch»).

Im März 2021 hat der Bundesgesetzgeber mit dem neuen Artikel 6a des COVID-19-Gesetzes ein einheitliches und international anerkanntes COVID-19-Zertifikat eingeführt. In dieser Bestimmung werden die Voraussetzungen für die Impf-, Test- und Genesungsnachweise festgehalten. Demnach muss ein entsprechender Nachweis persönlich, fälschungssicher, unter Einhaltung des Datenschutzes überprüfbar und so ausgestaltet sein, dass nur eine dezentrale oder lokale Überprüfung der Authentizität und Gültigkeit von Nachweisen möglich ist. Sodann soll der Nachweis möglichst für die Ein- und Ausreise in andere Länder verwendet werden können. In der Vorgabe des Gesetzgebers, wonach das Zertifikat künftig nicht nur digital, sondern auch auf Papier nutzbar sein soll, findet auch die Forderung des Beauftragten Niederschlag, dass das elektronisch verfügbare Zertifikat nicht zu einer faktischen Smartphone-Tragpflicht führen darf.

Weiter sieht die Bestimmung vor, dass der Bund den Kantonen und Dritten ein System für die Erteilung von Nachweisen zur Verfügung stellen kann. Zur Entwicklung eines solchen Systems hat das BAG am 29. März 2021 eine Projektgruppe eingesetzt, die der EDÖB in Ausübung seiner aufsichtsrechtlichen Beratungspflicht begleitet. Seine Forderungen zur datenschutzrechtlichen Ausgestaltung decken sich im Wesentlichen mit der Haltung des Europäischen Datenschutzausschusses (EDSA) und des Europäischen Datenschutzbeauftragten (EDSB) zum «Digitalen Grünen Pass», der im EU-Raum für den grenzüberschreitenden Verkehr eingeführt werden soll. Darüber hinaus hat der EDÖB gegenüber der Projektgruppe datenschutzrechtliche Vorgaben für eine datensparsame Ausgestaltung der Zertifikate für allfällige weitere Verwendungszwecke im Inland formuliert. Für solche weiteren Verwendungszwecke sollen gemäss der vom Beauftragten vertretenen Meinung öffentlich-rechtliche Grundlagen geschaffen werden, die sich nicht nur an Behörden, sondern auch Private richten (s. vorangehenden Text).

Elektronisches Patientendossier – Erste Stammgemeinschaften zertifiziert

In allen Regionen der Schweiz steht das elektronische Patientendossier (EPD) in den Startlöchern. Der EDÖB hat hierbei die Entwicklung der Zertifizierungsverfahren verfolgt. Sodann hat er Kontakt mit neuen Stammgemeinschaften aufgenommen und bei bereits bestehenden Kontakten den Austausch intensiviert. Inzwischen wurden die ersten Stammgemeinschaften zertifiziert.

Das EPD ist ein virtueller Sammelort von Links, mit welchem Privatpersonen über ihre persönlichen Gesundheitsdaten, wie beispielsweise Arztberichte oder Rezepte, digital verfügen können. Diese Gesundheitsdaten sind besonders schützenswerte Personendaten, deren Bearbeitung eine ausdrückliche Einwilligung der Betroffenen voraussetzt. Dies bedingt wiederum eine angemessen klare und vollständige Information der Patientinnen und Patienten. Für den EDÖB ist die saubere Umsetzung dieses Aspekts von besonderer Bedeutung. So konnte er im Berichtsjahr bereits entsprechende Dokumente von Stammgemeinschaften sichten.

Das am 15. April 2017 in Kraft getretene Bundesgesetz über das elektronische Patientendossier (EPDG) sieht vor, dass Patientinnen und Patienten sämtliche Zugriffsrechte zu jedem einzelnen Dokument selbst verwalten können. Richtig umgesetzt werden müssen somit Vertraulichkeitsstufen für jedes Dokument, die Zuweisung von Benutzerrollen an einzelne Gesundheitsfachpersonen, Stellvertretungsregelungen und die Einstellung, dass ein Zugriff in Notfallsituationen nur mit vorgängiger Berechtigung der behandelnden Gesundheitsfachperson möglich sein soll. Der EDÖB hat auch darauf ein Augenmerk gesetzt und wird die Regelung der Zugriffsrechte insbesondere nach den abgeschlossenen Zertifizierungsverfahren der Stammgemeinschaften weiter beobachten, sodass Patientinnen und Patienten auch nach Erteilung ihrer Einwilligung die Kontrolle über die Daten behalten. Der EDÖB steht sodann auch weiterhin im Austausch mit dem BAG, den Anbietern der technischen Infrastruktur und kantonalen Datenschutzbehörden. U.a. ermöglicht dieser Kontakt, Kompetenzfragen zu klären, die sich daraus ergeben, dass gewisse medizinische Leistungserbringer wie Spitäler der kantonalen Datenschutzaufsicht unterstehen, während der EDÖB die Ärztinnen und Stammgemeinschaften beaufsichtigt.

Geplant war, dass die Stammgemeinschaften im April 2020 ihren Betrieb aufnehmen. Jedoch hat sich der geplante Starttermin aufgrund länger andauernder Zertifizierungsverfahren verzögert. Mitte November 2020 wurde mit «eHealth Aargau (SteHAG)» die erste Stammgemeinschaft gemäss EPDG zertifiziert. Mit der Stammgemeinschaft Südost des Vereins «eSANITA» konnte Ende Dezember 2020 ein zweiter EPD-Anbieter die Zertifizierung abschliessen. Der EDÖB hat die beiden Gemeinschaften aufgefordert darzulegen, welche wesentlichen Datenschutzrisiken sie im Zusammenhang mit dem EPD bislang identifiziert haben, mit welchen Massnahmen sie diesen Herausforderungen begegnen und wie sie diesbezüglich ihre datenschutzrechtliche Verantwortung wahrnehmen.

Wichtigster Ansprechpartner für den Beauftragten werden die Datenschutz- und Datensicherheitsverantwortlichen sein, welche die Stammgemeinschaften gestützt auf die EPDV einsetzen müssen.

CORONA

Proximity Tracing-App des Bundes (SwissCovid-App)

Bereits zu Beginn der Corona-Pandemie wurde der EDÖB von den Entwicklern des Proximity Tracing-Systems, das später zur SwissCovid-App des Bundes führte, um eine beratende Mitwirkung an ihren Arbeiten angegangen. Das System ermittelt via Bluetooth-Funktechnik epidemiologisch relevante Kontakte zwischen Mobiltelefonen und zeichnet sie lokal auf. Der EDÖB hat die Entwicklung der SwissCovid-App zunächst in technischer Hinsicht und später auch mit Blick auf die Gesetzgebung eng begleitet.

Am 21. März 2020, wenige Tage nachdem in der Schweiz die ausserordentliche Lage im Sinne des Epidemiengesetzes (EpG) ausgerufen worden war, wurde der EDÖB von den Entwicklern einer «Covid Proximity Tracing-App» kontaktiert und um eine datenschutzrechtliche Beurteilung gebeten. Die Projektverantwortlichen aus dem Umfeld der École polytechnique fédérale de Lausanne (EPFL) und aus der Privatwirtschaft bezweckten mit der Applikation die Alarmierung von Personen, welche die Covid-App dokumentiert. Dies erlaubte es unseren Spezialisten, die Applikation und deren Systemarchitektur unter Einschluss der Umsetzung im Backend-Server technisch zu überprüfen. Im Mai stellte der EDÖB u.a. gestützt auf eine Datenschutz-Folgenabschätzung fest, dass die datenschutzrechtlichen Voraussetzungen für die Durchführung eines Pilotbetriebs gegeben waren (s. Stellungnahme des EDÖB vom 13. Mai 2020).

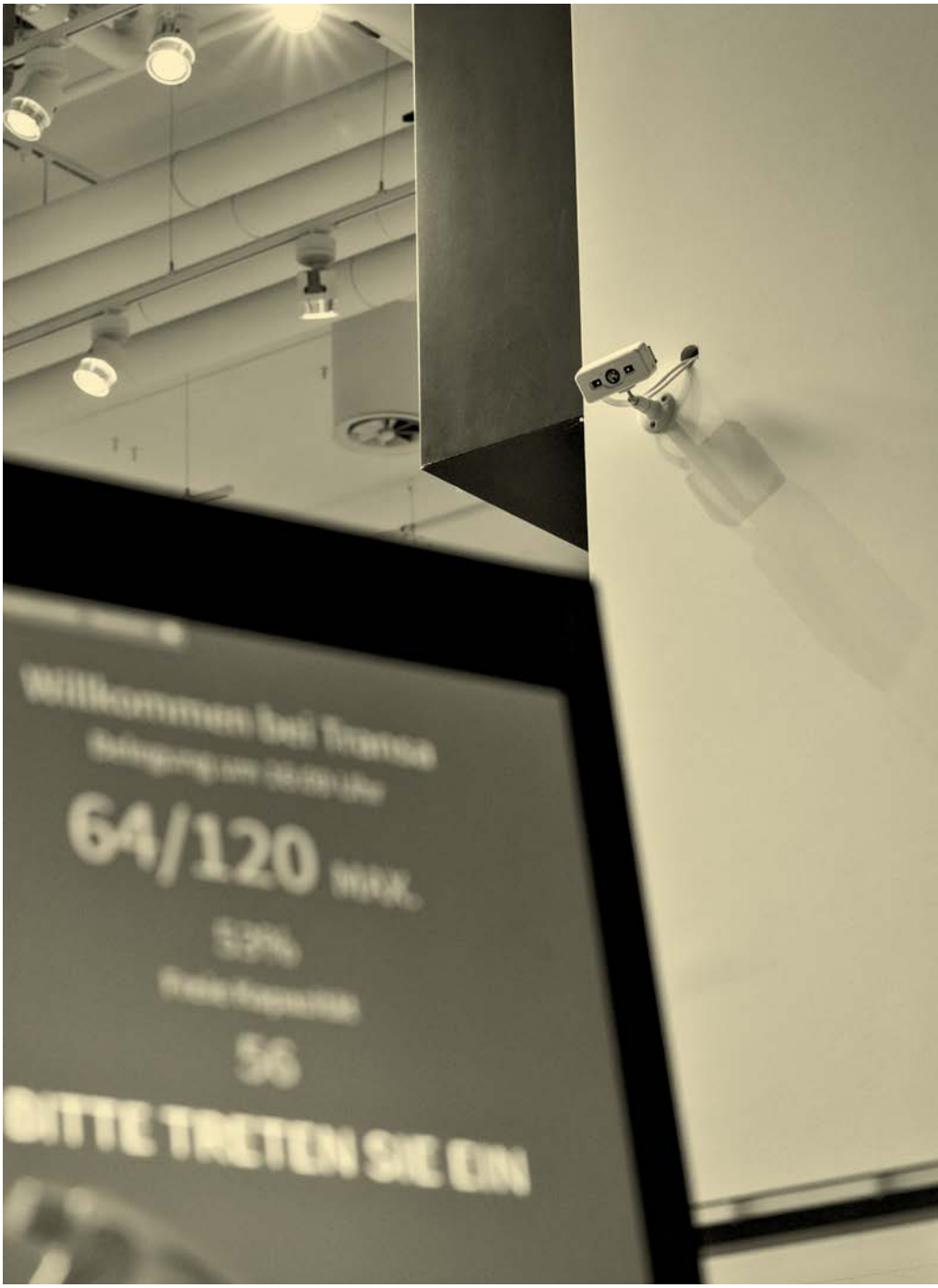
Nach Würdigung eines im Juni veröffentlichten Berichts des Nationalen Zentrums für Cybersicherheit (NCSC) bekräftige der EDÖB diese Einschätzung. Er unterstrich, dass die von datenschutzaffinen Kreisen und Medienberichten kritisierte Nutzung der Programmierschnittstellen (sog. API-Schnittstellen, application programming interface) von Google und Apple für die SwissCovid-App im Vergleich mit der übrigen Alltagsnutzung dieser Schnittstellen durch die Bevölkerung keine signifikant höheren Risiken mit sich bringt.

Nachdem der Beauftragte gegenüber der Verwaltung vergeblich forderte, für die Applikation nach Massgabe von Art. 17 DSG die Schaffung einer hinreichend konkreten Rechtsgrundlage im Epidemiengesetz einzuleiten, konnte er die zuständigen parlamentarischen Kommissionen dahingehend beraten, eine solche zu schaffen.

Deren Verankerung erfolgte über die dringliche Einführung eines neuen Artikels 60a im Epidemiengesetz per 25. Juni 2020.

Gemäss dieser Bestimmung ist die Verwendung der SwissCovid-App freiwillig. Einerseits war sich der Gesetzgeber bewusst, dass ein Obligatorium politisch schwer vermittelbar und – angesichts der Möglichkeit, die Bluetooth-Funktion jederzeit zu deaktivieren – auch kaum durchsetzbar gewesen wäre. Andererseits hat das Parlament ein Zeichen gegen die Schaffung einer faktischen Smartphone-Tragpflicht gesetzt, indem es Behörden, Unternehmen und Einzelpersonen verboten hat, jemanden aufgrund der Verwendung oder Nichtverwendung der App zu bevorzugen oder zu benachteiligen.

Am 25. Juni 2020 wurde die SwissCovid-App in den App-Stores von Apple und Google lanciert. Während Teile der Bevölkerung der Applikation auch Monate später ein erhebliches Misstrauen hinsichtlich ihrer Datenschutzkonformität entgegenbringen, erheben andere Stimmen den Vorwurf, der Gesetzgeber habe deren Wirksamkeit durch die Berücksichtigung des Datenschutzes zu sehr eingeschränkt. Im Spannungsfeld dieser gegensätzlichen Haltungen vermochte das BAG die Verbreitung der Applikation bisher nicht über die zwar beachtliche – optimistische Erwartungen indessen verfehlende – Grössenordnung von rund drei Millionen Downloads und 1,7 Millionen aktive Nutzende zu steigern.



CORONA

Der gesetzliche Rahmen der Kontaktdatenerfassung

Mit seinen Interventionen hat der EDÖB dazu beigetragen, dass die Erhebung von Kontaktdaten zur Rückverfolgung von Ansteckungen mit COVID-19, das sogenannte Contact Tracing, auf hinreichend bestimmte Rechtsgrundlagen gestellt wurde und dabei die Grundsätze des Datenschutzgesetzes eingehalten werden.

Als es am 11. Mai 2020 zur Wiedereröffnung der Restaurants, Bars, Diskotheken, Fitnesszentren und weiterer öffentlich zugänglicher Einrichtungen kam, haben viele Betriebe im Rahmen der vom Bundesrat angeordneten Schutzkonzepte die Erhebung von Kontaktdaten zur Rückverfolgung von Ansteckungen vorgesehen. Da für die Erhebung und Weiterbearbeitung dieser Daten zunächst keine gesetzliche Grundlage bestand, hat sich der EDÖB öffentlich dafür ausgesprochen, dass diese vorderhand nur freiwillig erfolgen durften (s. Mitteilung «Corona-Schutzkonzepte»).

Mit seiner Intervention konnte der EDÖB dazu beitragen, dass der Bundesrat das per 22. Juni 2020 eingeführte Kontaktdaten-Obligatorium auf eine hinreichend bestimmte Rechtsgrundlage stellte. Mit der COVID-19-Verordnung besondere Lage hat er den Verwendungszweck der gesammelten Daten eingegrenzt (Übermittlung an die zuständige kantonale Behörde zum Zweck des Contact Tracing im Falle einer Infektion), die Anforderungen an die Aufbewahrung (Wahrung der Vertraulichkeit) und die automatische Löschung nach 14 Tagen geregelt sowie die auf Bundesebene zu erfassenden Datenkategorien festgelegt (Name, Vorname, Wohnort und Telefonnummer).

Um die Effizienz der Kontaktrückverfolgung zu verbessern, haben einige Kantone die Betreiber der Gaststätten angewiesen, für die Kontaktdatenerhebung eine bestimmte Applikation zu verwenden. Abgesehen vom Hinweis auf das Erfordernis einer klaren (kantonal-)rechtlichen Grundlage hat der EDÖB betont, dass die entsprechenden Applikationen eine erkennbare, zweckgebundene und sichere Datenbearbeitung gewährleisten müssen. Auch hat er wiederholt darauf hingewiesen, dass Private ihren Kunden keine faktische Smartphone-Tragpflicht auferlegen dürfen. Zum einen gibt es Leute, die nicht willens sind, ein mit einem bestimmten Programm bestücktes Smart Device vorzuzeigen, weil sie sich vor einem Zugriff auf die dort vorhandenen Daten ihrer digitalen Lebensführung fürchten und zum anderen gibt es Personen, die dazu aufgrund ihres Alters, ihrer Gesundheit oder wegen Behinderungen gar nicht in der Lage sind. Diesen Menschen haben die privaten Betriebe nebst digitalen auch alternative Erhebungsmethoden wie das Ausfüllen von Papierformularen zu zumutbaren Konditionen zur Verfügung zu stellen.

Seit dem Sommer 2020 haben sich schliesslich Hinweise auf Probleme juristischer und technischer Natur bei der Verwendung bestimmter Applikationen für die Kontaktdatenerfassung gehäuft. Dies hat den EDÖB veranlasst, in Bezug auf eine in Teilen der Schweiz stark verbreitete App eine Sachverhaltsabklärung einzuleiten. Der EDÖB ist bestrebt, die Untersuchung vor der nächsten Wiedereröffnung der Gastronomie abzuschliessen, was angesichts der Formalitäten des Verfahrens eine grosse Herausforderung darstellt.

1.6 Arbeit

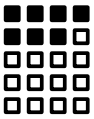
Zulässigkeit von Background Checks im Bewerbungsverfahren

Vermehrt bieten insbesondere ausländische Firmen interessierten Schweizer Arbeitgebern die Möglichkeit, Datenbanken nach Informationen über Stellenbewerberinnen und -bewerber zu durchforsten und anschliessend eine Anstellungsempfehlung abzugeben. Der EDÖB wurde mehrfach mit Blick auf die Zulässigkeit von sogenannten Background Checks kontaktiert.

Gemäss Art. 328b OR darf der Arbeitgeber nur diejenigen Daten bearbeiten, die für das vorliegende Bewerbungsverfahren notwendig sind. Dabei muss er stets auch die Datenbearbeitungsgrundsätze des DSG, insbesondere das Verhältnismässigkeitsprinzip und das Transparenzgebot, beachten.

Das Verhältnismässigkeitsprinzip verlangt, dass das Durchforsten von Datenbanken und die anschliessende Auswertung der eingesehenen Daten geeignet, notwendig und zumutbar sind, um die Qualifikation der Kandidatinnen und Kandidaten zu überprüfen. Eine mehr oder weniger ausgedehnte Personensicherheitsprüfung kann in Bereichen, in denen die Arbeitnehmenden Zugang zu sensiblen Informationen haben, geeignet, notwendig und zumutbar sein, um gewisse Risiken einzudämmen, so z.B. im Banken- oder Sicherheitssektor. Wo hingegen keine besonderen Risiken vorliegen, wie dies unter Vorbehalt besonderer Umstände beispielsweise bei Lehrpersonen der Fall sein dürfte, erscheint eine umfassende Sicherheitsprüfung als unverhältnismässig.

Unabhängig von der Frage der Verhältnismässigkeit ist der Arbeitgeber aufgrund des Transparenzgebots verpflichtet, die betroffene Person über den Background Check und die dabei



erfolgenden Datenbearbeitungen und Auswertungen zu informieren. Erst dies stellt sicher, dass die betroffene Person die Rechtmässigkeit der Datenbearbeitung und Richtigkeit der Daten überprüfen bzw. ihre Rechte geltend machen kann. Im Lichte des Transparenzgebots unzulässig sind somit heimlich durchgeführte Background Checks, die den betroffenen Personen nicht offengelegt werden.

CORONA

Datenschutzrechtliche Aspekte im Homeoffice

Im Berichtsjahr wurde für zahlreiche Angestellte die Verlegung des Arbeitsplatzes in die eigenen vier Wände angeordnet. Entsprechend beschäftigte sich der EDÖB vermehrt mit Fragen rund um die Verwendung verschiedener Videokonferenzlösungen, die Überwachung vom Mitarbeitenden sowie Zugriffe auf Schweizer Firmenserver aus dem Ausland.

Die Frage, unter welchen Voraussetzungen Homeoffice für Angestellte eingeführt werden kann, beantwortet sich nach Massgabe des Arbeitsrechts. Aus datenschutzrechtlicher Perspektive ergeben sich aus dieser Konstellation allerdings einige nicht unerhebliche Fragestellungen, etwa im Zusammenhang mit dem Einsatz digitaler Kommunikationsmittel für Telefon- und Videokonferenzen (s. Kap. 1.1, Box zu entsprechendem Leitfaden) oder mit der Verwendung von Plattformen für den Datenaustausch. Selbst wenn sich die Pflichten der Arbeitnehmenden punktuell verschieben können, bleibt der Arbeitgeber auch in Krisenzeiten für die Informationssicherheit und den Datenschutz verantwortlich und somit an die Datenbearbeitungsgrundsätze des DSG gebunden. Im Sinne dieser Ausführungen obliegt es deshalb dem Arbeitgeber, eine Software auszuwählen, welche die Sicherheit der bearbeiteten Personendaten in hinreichender Weise gewährleistet. Unter dem Titel «Massnahmen für eine sichere Nutzung von Audio- und Videokonferenzlösungen» hat der EDÖB auf seiner Webseite einen Leitfaden publiziert, der die wichtigsten datenschutzrechtlichen Vorgaben zusammenfasst, die bei der Auswahl der entsprechenden Plattformen beachtet werden müssen.

Mehrere Anfragen aus der Bevölkerung bezogen sich auf die Befürchtung, im Homeoffice einer permanenten Überwachung durch den Arbeitgeber ausgesetzt zu sein. Der EDÖB ist sich bewusst, dass je nach verwendeter IT-Lösung das Verhalten der Arbeitnehmenden im Homeoffice auf einfache Art und Weise permanent überwacht werden könnte – was jedoch im Lichte des DSG unzulässig und auch gestützt auf Normen des Arbeitsgesetzes ausdrücklich untersagt ist.

Schliesslich sah sich der EDÖB mehrmals mit der Frage konfrontiert, ob es sich um eine Datenbekanntgabe ins Ausland handelt, wenn Arbeitnehmende im Homeoffice im Ausland arbeiten – sei dies in einer Ferienresidenz oder im Falle von Grenzgängern, im eigenen Zuhause – und von dort auf den Firmenserver in der Schweiz zugreifen. Solange jedoch der Arbeitnehmende aus seinem Homeoffice im Ausland per Virtual Private Network (VPN) auf den Firmenserver zugreift und Personendaten nur in dem Umfang bearbeitet, wie er es normalerweise auch in den Büroräumlichkeiten des Unternehmens tun würde und insbesondere die Personendaten niemandem im Ausland zugänglich macht, handelt es sich nach Ansicht des EDÖB nicht um eine grenzüberschreitende Datenbekanntgabe im Sinne des DSG. Unabhängig davon, ob sich Mitarbeitende im Homeoffice im Ausland oder in der Schweiz befinden, muss die Vertraulichkeit von Personendaten in jedem Fall gewährleistet sein.

CORONA

Datenschutzrechtliche Vorgaben zur Früherkennung von Corona im Arbeitsbereich

Die Corona-Pandemie warf mit Blick auf die Arbeitsverhältnisse diverse Fragen zur Datenschutzkonformität auf, so etwa bezüglich der Zulässigkeit von Temperaturmessungen am Arbeitsplatz oder der internen Kommunikation über festgestellte Ansteckungen. Regelmässig stellte sich dabei die Frage, ob die entsprechenden Massnahmen verhältnismässig sind.

Der Arbeitgeber darf im Rahmen des Arbeitsverhältnisses nur diejenigen Daten über die Arbeitnehmenden bearbeiten, die für die Durchführung des Arbeitsverhältnisses notwendig sind. Der Verhältnismässigkeitsgrundsatz gemäss DSG muss dabei stets berücksichtigt werden. So muss jede Datenbearbeitung geeignet, notwendig und zumutbar sein, um das angestrebte Ziel – in diesem Fall die Vermeidung von Infektionen am Arbeitsplatz – zu erreichen.

Mit Blick auf Temperaturmessungen am Arbeitsplatz stellte sich die Frage, ob diese Massnahme tatsächlich geeignet ist, um die Ansteckungen zu begrenzen. Einerseits kann eine erhöhte Temperatur ein Symptom einer anderen Krankheit sein, andererseits kann die Körpertemperatur durch die Einnahme von Medikamenten auf einfache Art und Weise künstlich gesenkt werden. Ferner weisen nicht alle Virusträger Fiebersymptome auf. So erscheint die flächendeckende Temperaturmessung nur bedingt geeignet, um Ansteckungen am Arbeitsplatz zu verhindern. Der Arbeitgeber musste sich alsdann fragen, ob es nicht andere Massnahmen gibt, die weniger einschneidend sind und die zum gleichen Ziel führen könnten. Der EDÖB hat in diesen Fällen jeweils vorgeschlagen, die Mitarbeitenden zu verpflichten, sich beim Auftreten der für eine Corona-Infektion typischen Symptome sofort bei einer Vertrauensperson im Betrieb zu melden. Der EDÖB hat sich bei der Beurteilung dieser Fragestellung auch an den Empfehlungen der Swiss National COVID-19 Science Task Force orientiert, die von Temperaturmessungen als isolierte, präventive Massnahme ausdrücklich abgeraten hat.

Regelmässig wurde auch die Frage aufgeworfen, wie ein Arbeitgeber einen Ansteckungsfall der übrigen Belegschaft mitteilen soll bzw. darf – dies mit dem Ziel, dass sich diejenigen Mitarbeitenden, die mit der infizierten Person Kontakt hatten, in Quarantäne begeben können. Der Arbeitgeber hat gegenüber den Arbeitnehmenden eine Fürsorgepflicht, welche die Bearbeitung dieser Information gebietet, auch wenn die Kontaktrückverfolgung grundsätzlich den zuständigen kantonalen Behörden (Kantonsarzt) obliegt und nicht den jeweiligen Arbeitgebern.

1.7 Versicherungen

Einführung des Hinweis- und Informationssystems HIS in der schweizerischen Versicherungswirtschaft

Der EDÖB hat den Schweizerischen Versicherungsverband im Hinblick auf die Einführung des Hinweis- und Informationssystems HIS beraten, einer Datenbank für teilnehmende Versicherungsgesellschaften zur Verhinderung von Versicherungsmissbrauch. Der EDÖB hat betont, dass sämtliche Datenbearbeitungen im Zusammenhang mit dem Betrieb des HIS dem datenschutzrechtlichen Grundsatz der Verhältnismässigkeit genügen müssen. Die Beratung des EDÖB zum HIS wurde bereits im Berichtsjahr 2017/2018 initiiert (s. 25. TB, Kap. 1.6.2) und nun fortgesetzt.

Die dem HIS angeschlossenen schweizerischen Versicherungsgesellschaften melden darin Personen, bei denen anlässlich der Schadenerledigung eine reglementarisch definierte Unregelmässigkeit – zum Beispiel eine Anzeigepflichtverletzung nach Art. 6 des Versicherungsvertragsgesetzes (VVG) – festgestellt worden ist. In zukünftigen Schadenfällen erscheint bei einer Abfrage der betreffenden Person im System ein entsprechender Hinweis auf diese Unregelmässigkeit, so dass die Versicherungsgesellschaft ihre Leistungspflicht im neuen Schadenfall vertieft prüfen kann. Die Meldegründe sind versicherungsvertrags- oder haftpflichtrechtlicher, nicht jedoch strafrechtlicher Natur. Ob eine Person im HIS gemeldet ist, kann eine Versicherungsgesellschaft nur abfragen, wenn die Person in einem neuen Schadenfall beteiligt ist, nicht aber ausserhalb eines Schadenbearbeitungsprozesses, namentlich vor einem Vertragsabschluss mit der betreffenden Person. Im HIS eingetragen werden nicht nur die versicherte Person, sondern auch allenfalls beteiligte andere Personen wie «Anstifter» oder «Gehilfen».

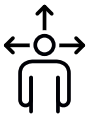
Der EDÖB hat im Rahmen seiner Beratung insbesondere betont, dass sämtliche Datenbearbeitungen im Zusammenhang mit dem HIS dem datenschutzrechtlichen Grundsatz der Verhältnismässigkeit zu genügen haben. So muss ein Eintrag in das HIS geeignet und erforderlich sein, um Versicherungsmissbrauch zu verhindern und aufzudecken, und die damit einhergehende Beeinträchtigung der Privatsphäre muss der betroffenen Person auch zugemutet werden können. Die Gründe für eine Meldung sind eng zu halten und reglementarisch klar zu definieren, und sie müssen transparent gemacht werden. Eine Meldung darf es der Versicherungsgesellschaft zwar ermöglichen, in einem neuen Schadenfall das Leistungsbegehren der versicherten Person vertieft zu prüfen, sie darf jedoch nicht zu einer Vorverurteilung dieser Person führen. Sodann müssen Vorkehrungen getroffen worden sein, um die Richtigkeit der Personendaten sicherzustellen. Versicherungsgesellschaften, die sich nicht an das Reglement halten und mehrfach ungerechtfertigte Eintragungen vornehmen, sollten eruiert und sanktioniert werden können.

Die Anregungen des EDÖB wurden mehrheitlich umgesetzt. Namentlich wurden die Gründe für eine Meldung im HIS weiter präzisiert. Letztlich wird sich in der Praxis weisen müssen, inwieweit das HIS zur Verhinderung von Versicherungsmissbrauch beitragen kann, wie gut sich die Versicherungsgesellschaften an die reglementarischen Vorgaben halten und ob aus datenschutzrechtlicher Sicht künftig allenfalls Anpassungen notwendig werden.

Weitergabe von Mitgliederdaten an Sponsoren

Der EDÖB fordert das Vorliegen einer gültigen Einwilligung für die rechtmässige Datenweitergabe an Sponsoren. Vereinsmitglieder müssen der Datenweitergabe widersprechen können, ohne dadurch einen unverhältnismässigen Nachteil zu erleiden.

Im Berichtsjahr erhielt der EDÖB verschiedene Anfragen betreffend die Weitergabe von Adressdaten von Vereinsmitgliedern an Sponsoren für Werbezwecke. Es stellte sich die Frage, ob es zulässig ist, einen höheren Mitgliederbeitrag von denjenigen Mitgliedern zu erheben, die der Weitergabe ihrer Daten widersprochen haben.



Wir haben die betroffenen Personen und Vereine darauf hingewiesen, dass von einem unverhältnismässigen Nachteil auszugehen ist, wenn die Erhöhung des Beitrags so hoch ist, dass sich die betroffenen Personen praktisch gezwungen fühlen, der Datenbekanntgabe zuzustimmen.

Bereits früher wies der EDÖB Sportverbände und Sponsoren auf ihre Verantwortung für die Rechtmässigkeit der durch sie durchgeführten Datenbearbeitungen hin (vgl. 22. Tätigkeitsbericht 2014/2015, Ziff. 1.8.5). Vereine dürfen ohne die gültige Einwilligung der betroffenen Personen keine Daten an Sponsoren weitergeben. Damit eine Datenweitergabe rechtmässig erfolgen kann, müssen alle betroffenen Personen angemessen und vorgängig über die beabsichtigte Datenweitergabe (d.h. welche Daten an welche Empfänger für welchen Zweck weitergegeben werden sollen) informiert werden und dem zustimmen können. Wenn die Zustimmung in Form eines Opt-out erfolgt, ist es unerlässlich, dass die Mitglieder eine einfache Möglichkeit haben, der Weitergabe ihrer Daten zu widersprechen, ohne dadurch einen unverhältnismässigen Nachteil zu erleiden. Sponsoren müssen wiederum vertraglich sicherstellen, dass sie nur die Adressdaten von Vereinsmitgliedern bearbeiten, welche ihnen gestützt auf eine wirksame Einwilligung weitergegeben worden sind.

Systematische Verwendung der AHV-Nummer durch die Behörden: Das Parlament sagt Ja zur Gesetzesänderung

Am 18. Dezember 2020 stimmte das Parlament der Änderung des Bundesgesetzes über die Alters- und Hinterbliebenenversicherung zu. Sie ermächtigt einen breiten Kreis von berechtigten Behörden, Organisationen und Personen zur systematischen Verwendung der 13-stelligen AHV-Nummer AHVN13 als eindeutigen Identifikator ausserhalb des Sozialversicherungsbereichs. Der EDÖB konnte für umfangreiche Garantien im Bereich des Datenschutzes sorgen.

Am 1. Februar 2017 gab der Bundesrat dem Eidgenössischen Departement des Innern (EDI) den Auftrag, eine Konsultation zur systematischen Verwendung der AHV-Nummer durch die Behörden von Bund, Kantonen und Gemeinden durchzuführen. Eine interne Arbeitsgruppe, zu der wir nicht eingeladen worden waren, sah zum damaligen Zeitpunkt keine besonderen Gefahren für den Datenschutz. Dies obgleich sich sowohl der EDÖB als auch die kantonalen Beauftragten aus Datenschutzgründen bereits gegen den Grundsatz der systematischen Verwendung der AHVN13 ausgesprochen hatten.

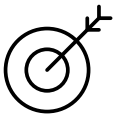
Gemeinsam mit dem Bundesamt für Justiz (BJ) gab der EDÖB deshalb bei Prof. David Basin, ordentlicher Professor für Informationssicherheit an der ETH Zürich, eine Risikofolgenabschätzung zur systematischen Verwendung der AHV-Nummer in Auftrag. Das Gutachten vom 27. September 2017 kam zum Schluss, dass die systematische Verwendung der AHVN13 nicht unerhebliche Risiken für den Datenschutz mit sich bringt (s. 25. TB, Kap. 1.1.2). Der Experte empfahl die Verwendung von sektorspezifischen Nummern, hielt allerdings auch fest, dass die angestrebte Datenschutzwirkung durch diese alleinige Massnahme nicht zu erzielen sei und weitere, aufwändige Massnahmen wie etwa die Neustrukturierung der Datenbankarchitekturen nötig wären.

Im Anschluss an dieses Gutachten forderte die Kommission für Rechtsfragen des Nationalrats in einem Postulat vom 20. Oktober 2017 (17.3968) den Bundesrat auf, in einem Konzept darzulegen, wie den Risiken begegnet werden kann, die mit der Verwendung der AHVN13 als einziger Personenidentifikationsnummer verbunden sind. Zudem sei unter Berücksichtigung der Beurteilung des EDÖB aufzuzeigen, wie der Datenschutz bei der Verwendung von Personenidentifikationsnummern durch Kantone, Gemeinden und Dritte verbessert werden könne. In seiner Stellungnahme vom 20. Dezember 2017 erklärte der Bundesrat, er sei sich der möglichen Risiken im Zusammenhang mit der Verwendung der AHVN13 bewusst, und er werde die Studie Basin und die Anliegen des Beauftragten in seiner Gesetzesvorlage berücksichtigen.

Während der Ämtervorkonsultation zur Gesetzesvorlage konnte der Beauftragte mehrere Änderungsvorschläge erfolgreich einbringen, namentlich die Pflicht für sämtliche zur systematischen Verwendung der AHVN13 berechtigten Stellen, Risikoanalysen vorzunehmen sowie ein Verzeichnis über die Datenbanken zu führen, in denen die AHVN13 registriert ist. Weiter wurde das Erfordernis des Ausbaus der technischen und organisatorischen Massnahmen zur Minimierung der Datenschutzrisiken anerkannt und in die Gesetzesvorlage aufgenommen (s. 27. TB, Kap. 1.7.).

Am 7. November 2018 eröffnete der Bundesrat die Vernehmlassung zur Änderung des Gesetzes über die AHV, welche die systematische Verwendung der AHVN13 vorsieht. Die datenschutzbezogenen Forderungen des EDÖB wurden in der Vorlage berücksichtigt. Eine Behörde kann Sachdaten (Name, Vorname, Geburtsdatum usw.) mit der AHVN13 verbinden und deren Richtigkeit in der UPI-Datenbank (Unique Person Identification), die von der Zentralen Ausgleichsstelle (ZAS) verwaltet wird, überprüfen. Sie hat jedoch weder Zugriff auf die übrigen Register, das heisst auf das zentrale Versichertenregister und auf das Leistungsregister der ZAS, noch auf die Register anderer Behörden, in denen Sachdaten geführt werden. Folglich besteht für die Behörde keine Möglichkeit, Verknüpfungen zwischen verschiedenen Datenbanken herzustellen und – naturgemäss sehr präzise – Persönlichkeitsprofile auf der Grundlage der AHVN13 anzufertigen.

Es ist begrüssenswert, dass sämtliche Einheiten von Bund und Kantonen, aber auch die dezentralisierten Einheiten der Bundesverwaltung sowie die Personen und Organisationen des öffentlichen oder privaten Rechts, die nicht Verwaltungen angehören, welche über solche Datenbanken verfügen, zu periodischen Risikoanalysen verpflichtet sind, die insbesondere dem Risiko einer unerlaubten Zusammenführung von Datenbanken Rechnung tragen. Gestützt auf diese Risikoanalysen sind Massnahmen zur Wahrung der Sicherheit und des Datenschutzes, die der Risikolage angepasst sind und dem Stand der Technik entsprechen, zu treffen und umzusetzen. Die im Gesetzesentwurf aufgeführten Einheiten, welche die AHVN13 systematisch verwenden, sind im Hinblick auf die Risikoanalyse gehalten, Verzeichnisse zu führen, in denen die entsprechenden Datenbanken aufgelistet sind. Zur systematischen Verwendung der AHVN13 ermächtigt das Gesetz nebst den Bundes-, Kantons- und Gemeindeverwaltungen Bildungsinstitutionen, private Versicherungsunternehmen (einschliesslich Anbieter von Zusatzversicherungen) sowie Organisationen und Personen des öffentlichen oder privaten Rechts, die nicht den bereits genannten Verwaltungen angehören und durch Bundesrecht, kantonales Recht oder kommunales Recht oder durch Vertrag mit Verwaltungsaufgaben betraut sind, sofern das anwendbare Recht die systematische Verwendung der AHV-Nummer vorsieht. Indes ist die Nutzung der AHVN zu rein privaten Zwecken ausgeschlossen. Dies gilt auch für den Fall, dass sich die betroffenen Personen mit der systematischen Verwendung ihrer AHVN13 durch Private einverstanden erklären.



Zusätzlich zu den vorgenannten Massnahmen sieht das Gesetz erfreulicherweise auch verbindliche technische und organisatorische Massnahmen zur Vermeidung allfälliger missbräuchlicher Verwendungen der AHV-Nummer vor. Dazu gehört, dass der gesetzlich verankerte Grundsatz des Zugangs zu Datenbanken, welche die AHVN13 enthalten, auf Personen zu beschränken ist, die diese Nummer zur Erfüllung ihrer Aufgaben benötigen. Ferner müssen Übertragungen von Datensätzen, welche die AHVN13 enthalten und über ein öffentliches Netz erfolgen, verschlüsselt werden. Schliesslich werden die zur Verwendung der AHV-Nummer berechtigten Behörden, Organisationen und Personen dazu verpflichtet, Vorkehrungen für den Fall eines unbefugten Zugriffs auf oder einer missbräuchlichen Nutzung von Datenbanken zu treffen und ihre Mitarbeitenden hinsichtlich der gesetzeskonformen Nutzung der AHV-Nummer zu schulen. Verstösse gegen diese Pflichten können strafrechtlich geahndet werden.

Die Vorlage hat im Anschluss an das Vernehmlassungsverfahren keine wesentlichen Änderungen erfahren. Kurz vor der Schlussabstimmung in der Bundesversammlung erweiterte das Parlament im Dezember 2020 die Liste der Einheiten, die zur systematischen Verwendung der AHNV13 berechtigt sind und nahm darin Vollzugsorgane auf, die Kontrollen im Zusammenhang mit allgemeinverbindlichen Gesamtarbeitsverträgen vornehmen.

Im Verlauf des Gesetzgebungsprozesses wurde der Beauftragte von den Parlamentskommissionen vielfach angehört und konnte auf diese Weise bewirken, dass der Datenschutz zu einem Kernthema der gesetzlichen Bestimmungen wurde. Die neuen Normen dürften nicht vor Ende 2021 in Kraft treten.

1.8 Verkehr

Starke Zunahme der Bürgeranfragen zu Drohnen

Im laufenden Berichtsjahr haben die Anfragen von Privatpersonen rund um das Thema Drohnen stark zugenommen. Dies betrifft sowohl Anfragen von Drohnenbesitzern als auch von Personen, welche sich durch Drohnenaufnahmen gestört fühlen.

Drohnen scheinen im Privatbereich immer beliebter zu werden. Zumindest hat der EDÖB im laufenden Berichtsjahr eine starke Zunahme der Anfragen von Privatpersonen zu dieser Thematik verzeichnet. Einerseits handelt es sich bei den Anfragenden um Bürgerinnen und Bürgern, welche mittels einer Drohne Foto- oder Videoaufnahmen vornehmen und die (datenschutz-)rechtlichen Voraussetzungen mit dem Beauftragten sowie anderen Behörden (namentlich dem Bundesamt für Zivilluftfahrt BAZL) abklären möchten. Andererseits melden sich Privatpersonen, welche sich durch Drohnen, die in der Nähe ihres Wohn- und Arbeitsraums herumkreisen und möglicherweise Ton- und Bildaufnahmen vornehmen, gestört fühlen.

Neben einer rechtlichen Beratung wünschen sich die Anfragenden oftmals einen Entscheid des Beauftragten in ihrem Einzelfall. Der EDÖB weist in diesen Fällen darauf hin, dass die allgemeinen Datenschutzgrundsätze einzuhalten sind und private Datenbearbeiter über einen Rechtfertigungsgrund verfügen müssen. Für Bewilligungen oder Verbote weist er auf die dafür zuständigen Behörden, insbesondere das BAZL sowie die kantonalen Zivil- und Strafgerichte.

Weiterführende Informationen zur Videoüberwachung mit Drohnen durch Private finden sich auf unserer Website.

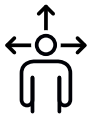
Revision des Personenbeförderungsgesetzes: Diskriminierende Schranken für anonym Reisende im ÖV sind zu verhindern – Art. 19a Bearbeitung von Personendaten zur Personenbeförderung

Der EDÖB hat sich im Rahmen der «Ämterkonsultation zur Botschaft zur Änderung des Personenbeförderungsgesetzes – zeitgemässe Grundlage für den ÖV» geäussert.

Seit der Ämterkonsultation haben mehrere Sitzungen mit Vertretern des Bundesamts für Verkehr und des Bundesamts für Justiz stattgefunden, in denen insbesondere erörtert wurde, inwieweit Transportunternehmen den datenschutzrechtlichen Bestimmungen für Private oder Behörden unterstehen sollen.

Der EDÖB wies insbesondere darauf hin, dass bei einer Unterstellung unter die für private Datenbearbeiter geltenden Bestimmungen neben der Einwilligung alle weiteren Rechtfertigungsgründe wie die gesetzliche Grundlage oder ein überwiegendes Interesse zur Verfügung stehen. Auf Letzteres können sich die Transportunternehmen beispielsweise berufen, wenn sie Daten in unmittelbarem Zusammenhang mit dem Abschluss oder Abwicklung eines Vertrags bearbeiten.

Wenn sich die Datenbearbeitung auf eine Einwilligung stützt, sind die Anforderungen an deren Rechtsgültigkeit zu beachten: Eine Einwilligung muss freiwillig, nach angemessener und transparenter Information erfolgen. Bei besonders schützenswerten Personendaten und Persönlichkeitsprofilen müssen die Einwilligungen



ausdrücklich erfolgen. Ferner darf die Personenbeförderung nicht von der Einwilligung in eine Datenbearbeitung zu anderen Zwecken abhängig gemacht werden. Für Datenbearbeitungen zu weiteren Zwecken müssen separate Einwilligungen der Betroffenen vorliegen.

Auch wo eine implizite Einwilligung genügt, muss vollständig informiert werden, sodass die Kundinnen und Kunden die Persönlichkeitsverletzungen erkennen und eine echte Wahl haben, sich entweder für das datensammelnde Angebot oder für ein alternatives anonymes Angebot zu vergleichbaren Konditionen zu entscheiden. Wählen sie die datensammelnde Lösung, liegt darin eine implizite Einwilligung vor. Der EDÖB hielt weiter fest, dass die anonymen Alternativangebote mit keinen abschreckenden resp. diskriminierenden finanziellen oder administrativen Schranken ver-

bunden sein dürfen. Da es bei einer vollen Überwälzung der Mehrkosten von Alternativangeboten unter Umständen zu einem faktischen Ausschluss von Teilen der Bevölkerung kommen kann, verlangte der EDÖB, die betreffende Bestimmung im Personenbeförderungsgesetz entsprechend zu ergänzen und die Begründung in der Botschaft zu präzisieren.
Betreffend die Vertriebsinfrastruktur, resp. die zentrale Bestellplattform, die zurzeit noch nicht umgesetzt wird, machte der EDÖB auf die bereits heute geltenden allgemeinen Grundsätze sowie die nach dem totalrevidierten DSG neu zu beachtenden Anforderungen aufmerksam, die beim Aufbau der digitalen Plattform zu berücksichtigen sind, wie beispielsweise die datenschutzfreundliche technische Ausgestaltung und Voreinstellung («Privacy by Design» und «Privacy by Default») sowie der Schutz von persistenten Daten.

Der EDÖB wird das Gesetzgebungsverfahren weiter begleiten und darauf hinwirken, dass die datenschutzrechtlichen Anforderungen berücksichtigt werden.

Nutzung von Flugpassagierdaten zur Terrorismusbekämpfung

Das EJPD arbeitet aktuell ein Gesetzgebungsprojekt aus, um die von den Fluggesellschaften erhobenen Flugpassagierdaten für die Terrorismus- und Kriminalitätsbekämpfung in der Schweiz zu verwenden. Der EDÖB hat Einsitz im externen Fachausschuss dieses Projekts.

Der Bundesrat hat sich am 12. Februar 2020 in einem Grundsatzentscheid für die Nutzung von Flugpassagierdaten (Passenger Name Records, kurz PNR) zur Terrorismus- und Kriminalitätsbekämpfung in der Schweiz ausgesprochen. Das EJPD wurde zu diesem Zweck beauftragt, die ersten Schritte zur Einführung eines nationalen PNR-Systems einzuleiten (s. 27. TB, Kap. 1.2, S. 27). Das EJPD ist nun angewiesen, bis Mitte 2021 zusammen mit dem UVEK eine Vernehmlassungsvorlage zu einem Bundesgesetz über die Erhebung und Nutzung von PNR-Daten durch die Schweiz sowie ihre Übermittlung an Staaten auszuarbeiten, deren Datenschutz und Datenbearbeitung dem Standard der 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) entspricht. Weiter soll das EJPD mit dem EDA bis Mitte 2021 ein Mandat für Verhandlungen mit der EU über ein Abkommen zum PNR-Informationsaustausch zwischen den zuständigen Koordinationsstellen (Passenger Information Unit, PIU) in der Schweiz und den EU-Mitgliedstaaten vorbereiten.

Der EDÖB hat Einsitz in den externen Fachausschuss des PNR-Projektes genommen und begleitet dessen datenschutzrechtliche Ausgestaltung. Bei der Einrichtung eines PNR-Systems dürfen die sich daraus ergebenden Beschränkungen der Grundrechte nur soweit erfolgen, wie dies für den verfolgten Zweck nötig ist. Das Gleichgewicht zwischen der Garantie der Grundrechte und den für die Gewährleistung der öffentlichen Sicherheit unerlässlichen Einschränkungen muss gewahrt bleiben. Dazu gehört namentlich, dass die Bereitstellung der Daten nach dem «Push»-System erfolgt, wodurch ein direkter Zugriff auf die Daten durch ausländische Behörden verunmöglicht wird. Der Beauftragte setzt sich darüber hinaus gemäss seiner langjährigen Praxis dafür ein, dass ein Deliktskatalog erstellt wird. Dies entspricht dem Verhältnismässigkeitsprinzip und dient der Transparenz.

Das Privacy Shield garantiert Betroffenen in der Schweiz kein adäquates Schutzniveau bei Datenbekanntgaben in die USA

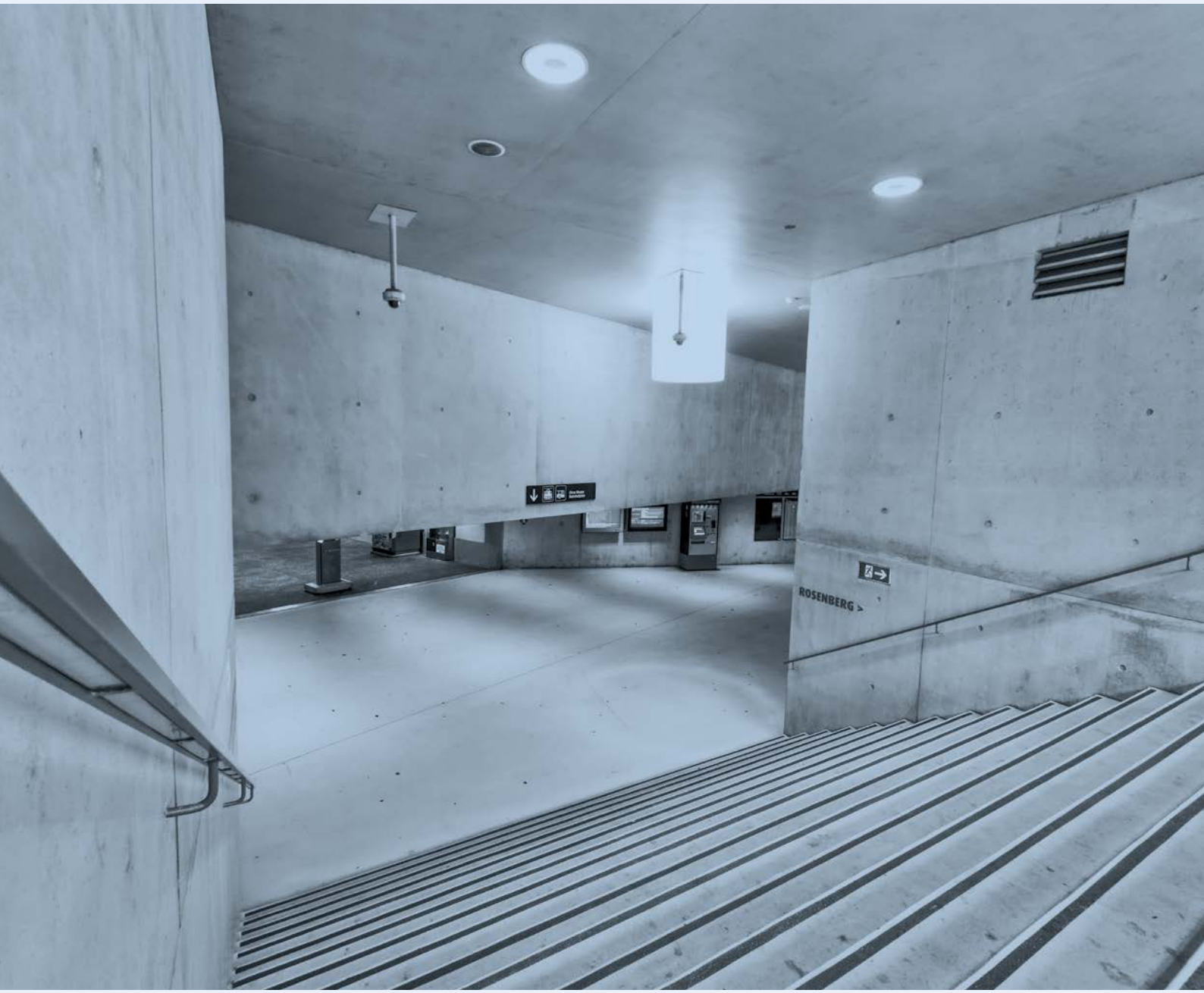
Der EDÖB evaluierte die Datenschutzkonformität des Privacy Shield Regimes vor dem Hintergrund seiner jährlichen Überprüfungen sowie der jüngsten Rechtsprechung des Europäischen Gerichtshofs (EuGH) neu. Er kam zum Schluss, dass das Privacy Shield Regime Betroffenen in der Schweiz kein adäquates Schutzniveau bietet und fordert Schweizer Unternehmen auf, bei der Übermittlung von Daten in die USA auf der Grundlage von vertraglichen Garantien eine Risikobeurteilung im Einzelfall vorzunehmen.

Bereits anlässlich der 2018 und 2019 durchgeführten Überprüfungen des Swiss-US Privacy Shield Regimes hielt der EDÖB in seinen Evaluationsberichten fest, dass das Privacy Shield Regime – trotz Verbesserungen seit dessen Inkraftsetzung – den Betroffenen bei Datenzugriffen durch US-Behörden keine genügenden durchsetzbaren Rechtsansprüche bietet (vgl. auch 27. TB, S. 34 und 26. TB, Kap. 1.2). Insbesondere bemängelte er, dass sich die Wirksamkeit des sog. Ombudsperson-Mechanismus, der einen indirekt durchsetzbaren Rechtsbehelf garantieren soll, mangels Transparenz nicht beurteilen lässt. Auch sind die Entscheidkompetenzen der Ombudsperson gegenüber den US-Geheimdiensten sowie ihre tatsächliche Unabhängigkeit unbelegt. Dieser Mangel an Transparenz und das daraus abzuleitende Fehlen von Garantien bei Eingriffen der US-Behörden in die Privatsphäre von Personen in der Schweiz erachtete der EDÖB als problematisch.

Am 16. Juli 2020 erging das Urteil des EuGH in der Rechtssache C311/18 Data Protection Commissioner v. Facebook Ireland Ltd und Maximilian Schrems (sog. Schrems II Urteil), das den Angemessenheitsbeschluss 2016/1250 der EU-Kommission betreffend die unter dem Privacy Shield Regime zertifizierten US-Unternehmen für ungültig erklärte. Zudem stellte der EuGH klar, dass der Einsatz von Standardvertragsklauseln (SCC) für die USA und für andere Drittländer ohne angemessenen Datenschutz einer Einzelfallprüfung ihrer Eignung und gegebenenfalls einer Ergänzung bedürfe. Dieses Urteil ist für die Schweiz nicht verbindlich. Nach DSGVO werden das Datenschutzrecht der EU und die darauf gestützte Rechtsprechung des EuGH jedoch von den Behörden und Gerichten der EU resp. des EWR auch gegenüber Schweizer Unternehmen angewendet, wenn letztere in der Weise Daten bearbeiten, dass sie unter den Anwendungsbereich der DSGVO fallen. Der EDÖB kam nach vertiefter Analyse des EuGH-Urteils und der Schweizer Rechtslage in seiner Stellungnahme vom 8. September 2020 (s. Medienmitteilung) zum Schluss, dass das Privacy Shield Regime trotz der Gewährung von besonderen Schutzrechten auch für Betroffene in der Schweiz für

Datenbekanntgaben von der Schweiz an die USA kein adäquates Schutzniveau gemäss DSG bietet. Aufgrund dieser auf das schweizerische Recht gestützten Einschätzung hat der EDÖB in seiner Staatenliste den Verweis auf einen «angemessenen Datenschutz unter bestimmten Bedingungen» für die USA gestrichen. Diese Liste hat indikativen Charakter. Zurzeit liegt in der Schweiz keine mit dem erwähnten Urteil des EuGH vergleichbare Judikatur vor. Eine abweichende Beurteilung durch die schweizerischen Gerichte bleibt vorbehalten.

Die neben dem Privacy Shield Regime für Datenbekanntgaben in die USA und andere Drittländer ohne Angemessenheitsbeschluss verwendeten vertraglichen Garantien, wie beispielsweise die auch in der Schweiz häufig verwendeten Standardvertragsklauseln (SCC) der EU oder wie sog. «Binding Corporate Rules» vermögen den Zugriff auf Personendaten durch ausländische Behörden nicht zu verhindern, wenn das öffentliche Recht des Importstaates vorgeht und den behördlichen Zugriff auf die transferierten Personendaten ohne hinreichende Transparenz und unabhängigen Rechtsschutz der Betroffenen erlaubt.



In seiner vorerwähnten Stellungnahme vom 8. September 2020 sensibilisierte der EDÖB die Wirtschaftskreise für dieses Problem und zeigte erste beschränkte Lösungsmöglichkeiten wie eigene Verschlüsselung oder vollständige Anonymisierung auf.

Der EDÖB fordert die Unternehmen auf, bei der Übermittlung von Daten in die USA auf der Grundlage von vertraglichen Garantien eine Risikobeurteilung im Einzelfall vorzunehmen. Nur auf der Grundlage einer solchen Risikobeurteilung kann ein Unternehmen beurteilen, ob eine Datenübermittlung in die USA datenschutzkonform ist, und dies gegebenenfalls dem EDÖB auch nachvollziehbar belegen. Die EU erarbeitet zurzeit neue Standardvertragsklauseln. Der EDÖB verfolgt diese Bemühungen und wird sich zu gegebener Zeit dazu äussern.

1.9 International

Einführung

Die internationale Zusammenarbeit wurde im vergangenen Geschäftsjahr von der COVID-19-Krise geprägt. So konnten praktisch keine Konferenzen vor Ort stattfinden. Sie mussten entweder abgesagt oder per Videokonferenz durchgeführt werden, was vor allem zu Beginn mit technischen Herausforderungen verbunden war. An den durchgeführten Videokonferenzen nahmen aufgrund der wegfallenden Reisezeiten und Kosten zum Teil mehr Datenschutzbehörden und Personen pro Behörde als sonst üblich teil. Dagegen konnten die für die Zusammenarbeit wichtigen informellen Gespräche und Kontakte kaum durchgeführt werden. Die Krise machte deutlich, wie wichtig ein Austausch zwischen den Datenschutzbehörden auf internationaler Ebene ist.

Die grenzüberschreitende Übermittlung von Daten nahm – nicht zuletzt auch wegen der Pandemie – weiter zu; sei es durch die direkte Bekanntgabe von Personendaten ins Ausland oder durch die Speicherung von Daten in Clouds und auf Servern im Ausland. Für die betroffenen Personen ist oft kaum abschätzbar, welche Unternehmen und Behörden im Ausland ihre Daten bearbeiten. Umso wichtiger ist es daher, auf eine verbesserte Durchsetzung des Datenschutzes auf internationaler Ebene hinzuwirken, die internationale Zusammenarbeit unter den Datenschutzbehörden zu fördern und auf ein gemeinsames Verständnis und eine einheitliche Auslegung von internationalen Normen und Vorgaben hinzuwirken.

International abgestimmte Vorgaben ermöglichen es, den betroffenen Personen unabhängig ihres Wohnortes die gleichen Rechte zu gewährleisten. Auch müssen sich die Datenschutzbehörden auf internationaler Ebene untereinander beraten, wie sie technisch und bei der praktischen Ausgestaltung ihrer Beratungs- und Aufsichtstätigkeit auf die globalen datenschutzrechtlichen Herausforderungen wie Big Data, das Internet der Dinge und die künstliche Intelligenz reagieren.

Der EDÖB ist auf internationaler Ebene weiterhin präsent und bringt sich in verschiedenen internationalen Gremien aktiv ein. Dazu gehören insbesondere der Europarat, die europäische und die internationale Konferenz der Datenschutzbeauftragten, die französischsprachige Vereinigung der Datenschutzbehörden, die OECD sowie die Zusammenarbeit und Koordination der Datenschutzbehörden der Schengen Mitgliedstaaten und der Austausch mit dem Europäischen Datenschutzausschuss (EDSA).

Europarat

Der Beratende Ausschuss zum Übereinkommen 108 hielt sechs Remotesitzungen zu verschiedenen Themen ab. Er verabschiedete Leitlinien über den Schutz der personenbezogenen Daten von Kindern im Bildungskontext sowie über die Gesichtserkennung. Zudem wählte die Vollversammlung das Büro.

Anstelle der 40. Vollversammlung des Ausschusses, die pandemiebedingt verschoben werden musste, führten das Büro des Beratenden Ausschusses zum Übereinkommen 108 und der Organisationsbereich Datenschutz an den betreffenden Daten öffentliche Remotesitzungen durch. Damit gewährten sie nicht nur den Delegationen, die üblicherweise an den Sitzungen in Strassburg teilnehmen, sondern auch einem breiteren Publikum Einblick in die Tätigkeiten des Ausschusses. Am 1., 2. und 3. Juli fanden sechs erkenntnisreiche Sitzungen zu spezifischen Themen statt:

- Sitzung 1: Wie kann dafür gesorgt werden, dass sich Länder, die sich dem Übereinkommen 108+ verpflichtet haben, an die Bestimmungen des Übereinkommens halten? Weshalb braucht es einen Follow-Up- und Evaluationsmechanismus, und wie ist dieser zu gestalten?
- Sitzung 2: Wie ist mit den neuesten Herausforderungen des Profiling im Zeitalter der künstlichen Intelligenz umzugehen?
- Sitzung 3: Was bedeutet das Recht auf den Schutz personenbezogener Daten im Erziehungs- und Bildungskontext? Was müssen Schulen tun, und was dürfen sie nicht mehr tun?
- Sitzung 4: Werden Projektvorhaben auf dem Gebiet der künstlichen Intelligenz von Beginn weg nach den Grundsätzen des Datenschutzes entwickelt («privacy by design»)?
- Sitzung 5: Die Spiegel unserer Seelen: Lehren aus Cicero ziehen und mit den Risiken der Gesichtserkennung umgehen.
- Sitzung 6: Politische Kampagnen und Wahlkampagnen: Weshalb Datenschutz so wichtig ist.

Der Beratende Ausschuss konnte seine ursprünglich für den 1. bis 3. Juli anberaumte Vollversammlung schliesslich vom 18. bis 20. November 2020 über Videokonferenz abhalten und eine revidierte Fassung der Leitlinien über den Schutz der personenbezogenen Daten von Kindern im Bildungskontext verabschieden. Diese enthalten eine Zusammenstellung der Grundrechte von Kindern im Rahmen von Erziehung und Bildung und sollen Gesetzgeber und politische Entscheidungsträger, aber auch Datenschutzbeauftragte sowie Vertreter der Industrie bei der Achtung dieser Rechte unterstützen. Weiter wählte der Beratende Ausschuss sein Büro und nahm unter anderem eine Vertreterin des EDÖB, Frau Caroline Gloor Scheidegger, Leiterin internationale Angelegenheiten, in diesen Vorstand auf.

Der Ausschuss zum Übereinkommen 108 genehmigte zudem auf dem Schriftweg Leitlinien über die Gesichtserkennung. Diese enthalten Orientierungshilfen für Gesetzgeber und Entscheidungsträger und verweisen namentlich auf das Erfordernis der Einbindung von Aufsichtsbehörden. Sie sollen auch richtungsweisend für Entwickler, Hersteller und Dienstanbieter sein, indem sie unter anderem festhalten, dass die Zuverlässigkeit der verwendeten Tools von der Effizienz des Algorithmus abhängig ist. Die dritte Kategorie von Orientierungshilfen spricht Benutzereinheiten von Gesichtserkennungs-Technologien an und erinnert sie an ihre Verantwortung: Sie sollen Datenschutz-Folgenabschätzungen vornehmen und den Datenschutz von Beginn weg gewährleisten («privacy by design»). Schliesslich erinnern die Leitlinien daran, dass sämtliche einschlägigen Rechte der betroffenen Personen gewahrt bleiben, namentlich das Recht auf Information, das Auskunftsrecht, das Recht auf Information bei automatisierten Einzelfallentscheidungen, das Widerrufsrecht und das Berichtigungsrecht.

Global Privacy Assembly

Die 42. Internationale Konferenz der Datenschutzbeauftragten fand unter ihrer neuen Bezeichnung «Global Privacy Assembly (GPA)» vom 13. bis 15. Oktober statt und wurde erstmals online durchgeführt.

Zu Beginn der 42. geschlossenen Sitzung der Global Privacy Assembly würdigte die Datenschutzbeauftragte des Vereinigten Königreichs Elizabeth Denham die Bemühungen, die von der Internationalen Konferenz der Datenschutzbeauftragten in den zurückliegenden Jahren mit dem Ziel unternommen wurden, die Konferenz zu modernisieren, ihre strategische Orientierung zu definieren sowie ihre Kapazitäten auszubauen, um 2020 die COVID-19-bedingten Herausforderungen meistern zu können.

Die diesjährige Veranstaltung war in drei Online-Sessionen mit jeweils anschliessender Diskussion gegliedert. Über 100 Mitglieder nahmen an diesem wichtigen Jahrestreffen teil.

Am ersten Konferenztag stand die Beurteilung der Fortschritte bei der Umsetzung des strategischen Plans, der an der 41. Internationalen Konferenz im vergangenen Jahr in Tirana verabschiedet wurde, im Vordergrund der Beratungen. Insbesondere ging es hierbei um die Prüfung der wichtigsten Ergebnisse hinsichtlich der drei strategischen Prioritäten, die definiert worden waren: weltweiter Ausbau des Schutzes der Privatsphäre im digitalen Zeitalter, Bedeutung und Einfluss der GPA auf dem internationalen Parkett maximieren sowie Erweiterung ihrer Kapazitäten.

Der zweite Konferenztag war den COVID-19-bedingten Herausforderungen gewidmet. In diesem Zusammenhang wurde der Arbeitsgruppe COVID-19 der GPA Anerkennung für ihren herausragenden Einsatz und Beitrag ausgesprochen. Die Tätigkeiten der Arbeitsgruppe wurden diskutiert, und die spezifischen Ergebnisse ihrer Arbeiten wurden vorgestellt. Dazu gehört das Kompendium der besten Praktiken bei der Bewältigung von COVID-19, das beispielsweise das Thema der Kontaktverfolgung behandelt.

Der dritte Tag begann mit einer Aussprache über die Zukunft der Konferenz. Anschliessend wurden die Ergebnisse der Abstimmung der Mitglieder über die Berichte der Arbeitsgruppen, den Bericht des Exekutivrats für 2020 und den Bericht über die 41. Internationale Konferenz 2019 bekanntgegeben: Sämtliche Berichte wurden angenommen.

Am 15. Oktober 2020 wurden fünf Resolutionen verabschiedet:

- Resolution zur Gesichtserkennungs-Technologie;
- Resolution zur Rolle des Schutzes personenbezogener Daten in der internationalen Entwicklungshilfe, in der internationalen humanitären Hilfe sowie bei der Krisenbewältigung;
- Resolution zur Schärfung des Verantwortungsbewusstseins auf dem Gebiet der Entwicklung und des Einsatzes der künstlichen Intelligenz;
- Resolution zu den datenschutzbezogenen Herausforderungen im Zusammenhang mit der COVID-19-Pandemie;
- Resolution betreffend gemeinsame Erklärungen zu neu auftretenden internationalen Fragen.

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

Die Arbeiten in der Arbeitsgruppe wurden auch in diesem Berichtsjahr fortgesetzt, wobei das Meeting im November 2020 nur virtuell abgehalten werden konnte. Zwei Themenbereiche sind in dieser Hinsicht hervorzuheben: Zum einen die «Datenportabilität», wo das Sekretariat einen Zwischenstand für einen möglichen Bericht präsentierte, und zum anderen der Bericht des Sekretariats über die Umsetzung der «OECD Privacy Guidelines».

Brexit – Angemessenheit des Datenschutzes

Das Vereinigte Königreich bleibt weiterhin auf der Liste der Staaten, deren Gesetzgebung einen angemessenen Datenschutz gemessen am Schweizer Datenschutzgesetz gewährleisten. Umgekehrt anerkennt das Vereinigte Königreich auch die Schweiz als Land mit gleichwertigem Datenschutz an.

Wie bereits im letzten Tätigkeitsbericht ausgeführt (s. 27. TB, Kap. 1.9), trat das Vereinigte Königreich nach einigen Verzögerungen am 1. Februar 2020 aus der EU (Brexit) aus. Es stellte sich damit die gegenseitige Angemessenheitsfrage. Dazu führte der EDÖB zahlreiche Gespräche mit Behörden des Bundes und mit Vertretern des Vereinigten Königreichs. Diese Gespräche wurden während des laufenden Geschäftsjahres regelmässig weitergeführt. Parallel dazu fanden Gespräche mit Vertretern der EU-Kommission statt, weil lange unklar war, ob die EU dem Vereinigten Königreich ab dem Jahr 2021 die Angemessenheit noch gewähren würde. Andererseits anerkannte das Vereinigte Königreich auf gesetzlicher Stufe alle Länder als gleichwertig, welche am 31. Dezember 2020 auch von der EU als gleichwertig anerkannt waren.

Weil der Kommissionsentscheid bezüglich der Schweiz Ende 2020 noch ausstand, bedeutete dies aber auch, dass die Schweiz zu diesem Zeitpunkt von der EU anerkannt blieb – und damit nach dem Recht des Vereinigten Königreichs automatisch anerkannt sein würde und zwar voraussichtlich für die nächsten vier Jahre. Dies bedeutete indes nicht, dass die Schweiz automatisch Gegenrecht gewähren würde. Das Datenschutzrecht im Vereinigten Königreich wurde aber in der Berichtsperiode nicht wesentlich verändert, sodass das Land weiterhin auf der Liste der Staaten verbleibt, deren Gesetzgebung einen angemessenen Datenschutz nach Art. 6. Abs. 1 DSG gewährleisten. Eine Überprüfung bleibt jedoch vorbehalten und hängt davon ab, wie die Datenschutzgesetzgebung im Vereinigten Königreich in Zukunft aussehen wird.

Arbeitsgruppe über die Rolle des Schutzes personenbezogener Daten in der internationalen Entwicklungshilfe, in der internationalen humanitären Hilfe sowie bei der Krisenbewältigung

Der EDÖB reichte an der 42. Internationalen Konferenz der Datenschutzbeauftragten (GPA) eine Resolution zur Rolle des Schutzes personenbezogener Daten in der internationalen Entwicklungshilfe, in der internationalen humanitären Hilfe sowie bei der Krisenbewältigung ein. Sie wurde dank der Unterstützung von 15 Datenschutzbehörden einstimmig angenommen.
Mit dieser Resolution soll die Position der GPA-Mitglieder zu mehreren Zielen der politischen Strategie der Konferenz definiert werden. Konkret geht es um die Zielsetzungen betreffend den weltweiten Ausbau des Schutzes der Privatsphäre und die Intensivierung der Beziehungen zu anderen internationalen Gremien und Netzwerken, die sich für Datenschutznormen im Bereich der Privatsphäre einsetzen.

Im Anschluss an die Verabschiedung der Resolution wurde die Einsetzung einer Arbeitsgruppe über die Rolle des Schutzes personenbezogener Daten in der internationalen Entwicklungshilfe, in der internationalen humanitären Hilfe sowie bei der Krisenbewältigung beschlossen. Die Arbeitsgruppe hat sich zwei Schwerpunktziele gesetzt:

- Auf Zusammenarbeitsgesuche massgeblicher Akteure eingehen, um Leitlinien zu entwickeln sowie um beste Praktiken auf dem Gebiet des Schutzes der Privatsphäre auszutauschen. Dabei soll auf die spezifischen Gegebenheiten der internationalen Entwicklungshilfe und der internationalen humanitären Hilfe eingegangen und das Anliegen berücksichtigt werden, ihnen Erleichterungen in ihrem Tätigkeitsbereich zu ermöglichen.
- Entwicklung einer Strategie der Anwaltschaft und der Mobilisierung bei den massgeblichen Akteuren.

Der EDÖB übernahm die Koordinierung der Arbeitsgruppe, an der Datenschutzbehörden aus der ganzen Welt sowie das IKRK und die Internationale Organisation für Migration mitwirken.

Europäische Datenschutz-Grundverordnung

Die neue europäische Datenschutz-Grundverordnung (DSGVO) trat am 25. Mai 2018 in Kraft und gilt unter bestimmten Voraussetzungen auch für Datenverarbeitungen durch Unternehmen aus Drittländern. An einem Treffen in der Schweiz wurden zahlreiche nach wie vor offene Fragen mit den Datenschutzbehörden von Albanien, Jersey und Monaco erörtert.
Die europäische Datenschutz-Grundverordnung (DSGVO) wurde am 27. April 2016 verabschiedet und ist in sämtlichen Mitgliedstaaten der Europäischen Union seit dem 25. Mai 2018 direkt anwendbar. Ihr Geltungsbereich erstreckt sich jedoch weit über das Gebiet der EU hinaus. Wenn nämlich 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 Union niedergelassen ist. Die französischsprachigen europäischen Behörden der Nicht-Mitgliedstaaten der Europäischen Union stehen vor den gleichen Herausforderungen. Nach einer ersten erfolgreichen Gesprächsrunde 2018 in Monaco organisierte der EDÖB im Februar 2020 ein Treffen in Bern, an dem sich die Behörden über das Inkrafttreten der DSGVO und über die diesbezüglichen Erfahrungen aus-

tauschen konnten, um Fragen, die an sie gerichtet wurden, im Hinblick auf eine koordinierte Antwort gemeinsam anzugehen.

Etwas über ein Jahr nach Inkrafttreten der DSGVO veröffentlichte der Europäische Datenschutzausschuss (EDSA), der als unabhängiges europäisches Organ an der einheitlichen Einhaltung der Datenschutzvorschriften in der Europäischen Union mitwirkt, seine Leitlinien zum Anwendungsbereich der DSGVO. Der EDÖB hatte sich zusammen mit der monegassischen Behörde (Commission de contrôle des informations nominatives, CCIN) an der öffentlichen Konsultation beteiligt, die den Leitlinien vorausging. Dies um eine Reihe von Aspekten dieser Thematik zu klären, die für Drittländer, welche in das EU-Gefüge eingebunden sind, eminent wichtig sind. Die neueste Fassung der Leitlinien wurde am Treffen in Bern ebenfalls analysiert und diskutiert, wobei festgestellt werden musste, dass eine Reihe von Fragen nach wie vor unbeantwortet ist.

Aufsichtskoordinationsgruppen über die Informationssysteme SIS II, VIS und Eurodac

Im Berichtsjahr führten die Aufsichtskoordinationsgruppen ihre beiden Sitzungen per Videokonferenz durch. Diskutiert wurde unter anderem, wie der Schwierigkeit, jeweils genügend Expertinnen und Experten aus den Datenschutzbehörden für die Schengen Evaluationen zu finden, begegnet werden kann.

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 17./18 Juni 2020 sowie 25./26. November 2020 per Videokonferenz statt. Vertreten waren der europäische Datenschutzbeauftragte (EDSB) sowie die nationalen Datenschutzbehörden der Mitgliedstaaten.

Die Aufsichtskoordinationsgruppen SIS und VIS beschäftigten sich unter anderem mit der Frage, weshalb es für die von der EU-Kommission durchgeführte Schengen Evaluation in Sachen Datenschutz schwierig ist, genügend Fachpersonen aus den verschiedenen Datenschutzbehörden aufzubieten. Die EU Kommission, die zurzeit das Verfahren der Schengen Evaluationen neu prüft, organisierte im Januar 2021 zu diesem Thema eine Videokonferenz mit den Datenschutzbehörden der Schengen Mitgliedstaaten und dem Europäischen Datenschutzbeauftragten. Es fand ein konstruktiver Austausch über mögliche Ursachen und Verbesserungsmöglichkeiten statt. Auf beiden Seiten wird die Frage der Bildung eines Pools mit Datenschutzexpertinnen und -experten für die Schengen Evaluationen geprüft. Weiter wird die EU Kommission nach Möglichkeit eine Weiterbildung für künftige Fachpersonen für Datenschutz-Evaluationen einführen. Die Aufsichtskoordinationsgruppe VIS hat an ihrer Sitzung vom 18. Juni die Vertreterin des Beauftragten als Vorsitzende der Koordinationsgruppe für weitere zwei Jahre bestätigt.

Öffentlichkeitsprinzip

2.1 Allgemein

Die Corona-Pandemie hat auch die Umsetzung des Öffentlichkeitsprinzips in der Bundesverwaltung geprägt. Der Anspruch der Medien und der Gesellschaft nach spezifischen und transparenten Informationen zu Dokumenten mit Corona-Bezug war hoch. Dementsprechend sahen sich einzelne Behörden nicht nur mit einer grossen Anzahl von Zugangsgesuchen, sondern mit z.T. auch umfangreichen und komplexen Anfragen konfrontiert, die oftmals eine amts- oder gar departementsübergreifende Koordination notwendig machten. Insgesamt zeigte sich, dass die Umsetzung des Öffentlichkeitsprinzips in Pandemiezeiten anspruchsvoll und herausfordernd sein kann. Während sich die unter Zeitdruck handelnde Verwaltung hohen Erwartungen und nachträglicher Kritik der Öffentlichkeit ausgesetzt sieht, verlangen die Gesuchstellenden einen raschen und umfassenden Zugang, um die teilweise auf notrechtlichen Kompetenzen beruhenden Handlungen des Staates zur Pandemiebekämpfung nachvollziehen zu können. Gleichwohl zeigen die Statistiken, dass es den Bundesbehörden – trotz des im Pandemiejahr bisweilen dringlichen Tagesgeschäfts – in der Mehrheit aller Fälle gelang, das Öffentlichkeitsprinzip in der Bundesverwaltung mit Erfolg umzusetzen.

Aus den nachfolgend aufgeführten Zahlen (s. Kap. 2.2) ist weiter zu entnehmen, dass die in den letzten Jahren festgestellten Tendenzen – eine stetige Zunahme der Zugangsgesuche und ein überwiegend konstant hoher Anteil an Fällen, in denen der Zugang vollständig gewährt wird – auch für das Berichtsjahr bestätigt werden.

Das vom Beauftragten im Jahr 2017 eingeführte Primat der mündlichen Schlichtungsverhandlungen hat sich im 2020 erneut bewährt. Dass dies die Zahlen auf den ersten Blick nur bedingt zu bestätigen scheinen, liegt an den durch die Pandemie verursachten Anpassungen des Schlichtungsverfahrens. Als der Bundesrat an seiner Sitzung vom 16. März 2020 angesichts der weiteren Ausbreitung des Corona-Virus die Home-Office-Pflicht eingeführt und Menschenansammlungen von mehr als fünf Personen verboten hatte, sah sich der Beauftragte aus Gründen der öffentlichen Gesundheit sowie zum Schutz der Gesundheit der Beteiligten gezwungen, während der ersten Ausbreitung der Pandemie (zwischen März und Juni 2020) wie dann auch während der zweiten Welle auf die Durchführung von Schlichtungssitzungen zu verzichten.

Aus den genannten Gründen mussten für zahlreiche Fälle schriftliche Schlichtungsverfahren durchgeführt werden. Dieses Vorgehen führte im Berichtsjahr einerseits zu einem geringeren Anteil von einvernehmlichen Lösungen und anderseits zu einer längeren Bearbeitungsdauer der Schlichtungsverfahren und einem damit verbundenen Rückstau bei der Erledigung von Verfahren. Wie nachteilig sich die schriftliche Durchführung der Schlichtungsverfahren auf Bearbeitungsdauer und Verfahrensergebnisse ausgewirkt hat, wird in Kapitel 2.3 präzisiert.

Die Einhaltung der gesetzlichen Frist von 30 Tagen für die Durchführung von Schlichtungsverfahren ist nicht nur in Pandemiezeiten herausfordernd. Die Erfahrung zeigt, dass diese Frist bei komplexen Drei- oder Mehrparteienverfahren betreffend Zugangsgesuche zu Unterlagen mit geschäftsgeheimnisrelevanten Informationen oder mit Bezug zum Persönlichkeitsschutz von Privatpersonen häufig überschritten wird.

Für die Durchführung des Schlichtungsverfahrens müssen die Behörden dem Beauftragten die von den Gesuchstellenden nachgefragten Dokumente zustellen – im Gegenzug unterliegt der Beauftragte dem Amtsgeheimnis im gleichen Ausmass wie die Behörden, in deren Dokumente Einsicht verlangt wird. In der Praxis lassen die Behörden die Unterlagen dem Beauftragten in aller Regel ohne weiteres zukommen. Nicht in jedem Fall gestaltet sich die Zusammenarbeit indes optimal. Dies zeigt exemplarisch ein Fall, indem es um die Mitwirkungspflicht im Schlichtungsverfahren ging. Aufgrund des vom Öffentlichkeitsgesetz eingeführten Prinzips der Öffentlichkeit der Bundesverwaltung obliegt es nicht

mehr in deren freien Ermessen, ob sie Informationen und amtliche Dokumente zugänglich machen will oder nicht. Die Behörden sind im Schlichtungsverfahren zur Mitwirkung verpflichtet und müssen dem Beauftragten alle Dokumente, die Gegenstand eines Gesuches sind, von Gesetzes wegen zustellen. Im angesprochenen Fall weigerte sich die Behörde, dem Beauftragten die streitgegenständlichen Dokumente zuzustellen. Sie argumentierte, diese fielen nicht in den Anwendungsbereich des Öffentlichkeitsgesetzes. Indem die beweisbeschwerte Behörde die Anwendbarkeit des Öffentlichkeitsgesetzes nach eigenem Ermessen abschliessend verneinte, sah sich der Beauftragte ausser Stande, die Dokumentenqualität nach Art. 5 BGÖ zu prüfen und das von der Behörde geltend gemachte Vorliegen von Nichteintretens- und Ausnahmegründen zu beurteilen. Demzufolge sah sich der Beauftragte gezwungen, den vollständigen Zugang zu den verlangten Dokumenten zu empfehlen, weil es der beweispflichtigen Behörde zum eigenen Nachteil gereichen muss, wenn sie nicht bereit ist, die gesetzliche Vermutung des Zugangs zu amtlichen Dokumenten durch deren Offenlegung gegenüber der Schlichtungsbehörde zu widerlegen (s. Empfehlung vom 28. Januar 2021).

Wie schon in den Vorperioden sind Bestrebungen der Verwaltung festzustellen, das Öffentlichkeitsprinzip durch Einführung von Ausnahmen in neuen Gesetzesbestimmungen weiter einzuschränken. Im Berichtsjahr war dies der Fall beim COVID-19-Solidarbürgschaftsgesetz (s. Kap. 2.4).

2.2 Zugangsgesuche – erneute Zunahme im 2020

Gemäss den Zahlen, die von den Bundesbehörden gemeldet wurden, gingen im Berichtsjahr vom 1. Januar bis 31. Dezember 2020 gesamthaft 1193 Zugangsgesuche ein. 2019 waren es noch 916 Gesuche. Dies entspricht einer Steigerung gegenüber dem Vorjahr um 30 Prozent. Eingerechnet sind auch die Zugangsgesuche der Bundesanwaltschaft (13 Gesuche) und der Parlamentsdienste (6).

Einer der Gründe für die Zunahme ist im ausgeprägten Bedürfnis zu finden, das staatliche Handeln zur Bekämpfung der Corona-Pandemie nachvollziehbar zu machen. Gemäss Angaben der Bundesbehörden wiesen 308 von den insgesamt 1193 Zugangsgesuchen (26 Prozent) einen Bezug zur Thematik Corona auf. Die Behörden waren in der Lage, die Zugangsgesuche für «Corona»-Dokumente statistisch zu erfassen. Diese Statistik ist separat aufgeführt (s. Kap. 3.3). Dabei zeigt sich, dass der vollständige Zugang in 121 Fällen (39 Prozent) im Vergleich zur Gesamtstatistik (s. unten) weniger oft gewährt wurde, während bei der vollständigen Zugangsverweigerung (38 resp. zwölf Prozent) nur ein geringfügig höherer Anteil im Verhältnis zur Gesamtstatistik festgestellt werden.

Zu den höheren Zahlen an eingereichten Zugangsgesuchen dürfte auch beigetragen haben, dass die Bevölkerung nicht zuletzt dank Medienberichten über die Jahre hinweg laufend bessere Kenntnisse über das Öffentlichkeitsgesetz erlangt und dessen Möglichkeiten vermehrt aktiv nutzt. Der Beauftragte erwartet, dass diese Tendenz in den kommenden Jahren anhalten wird.

In 610 Fällen (51 Prozent) gewährten die Behörden einen vollständigen Zugang (gegenüber 542 bzw. 59 Prozent im Vorjahr), während bei 293 Gesuchen (25 Prozent) ein teilweiser respektive aufgeschobener Zugang zu den Dokumenten genehmigt wurde. In 108 Fällen (neun Prozent) wurde die Einsichtnahme vollständig verweigert. Nach Angaben der Behörden wurden drei Prozent bzw. 35 Zugangsgesuche zurückgezogen, 80 Gesuche waren Ende 2020 noch hängig, und in 67 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.

Im Vergleich mit den Vorjahren kann insgesamt festgestellt werden, dass sich im Corona-Jahr der Anteil mit vollständiger Zugangsgewährung um acht Prozent vermindert hat, während der Anteil mit teilweiser Zugangsgewährung respektive Zugangsaufschub um sechs Prozent erhöht hat. Eine Erklärung für diese Veränderungen liegt in der Tatsache, dass die Behörden im Zusammenhang mit Zugangsgesuchen zu Corona-Dokumenten – die, wie erwähnt, rund einen Viertel der Gesuche ausmachen – prozentual weniger oft einen vollständigen Zugang gewährten, den Zugang häufiger teilweise verweigert oder aufgeschoben beziehungsweise vollständig verweigert haben.

Departemente und Bundesämter

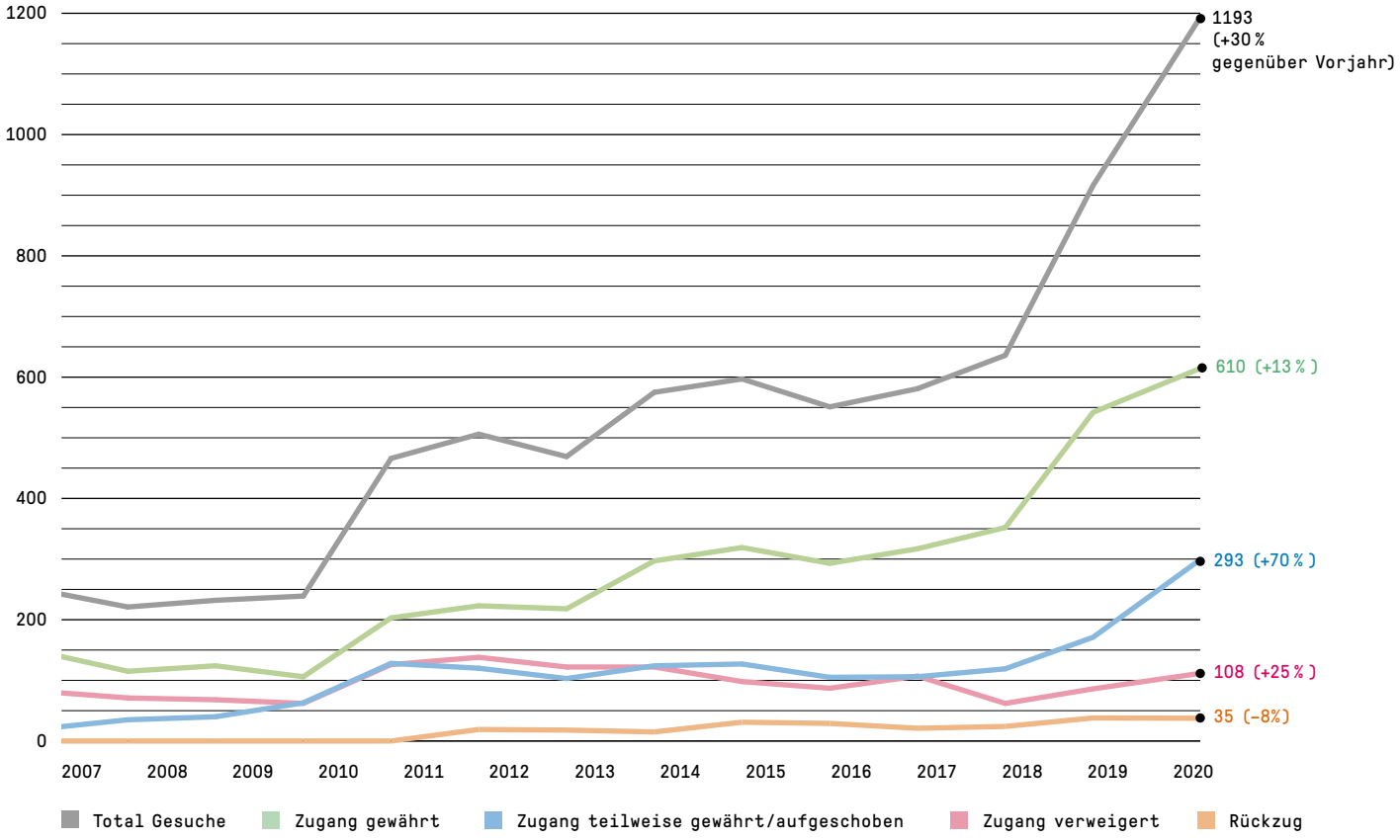
Einzelne Verwaltungseinheiten standen 2020 aufgrund der Corona-Pandemie besonders im Fokus der Medien und der Gesellschaft. Aufgabenbedingt sahen sich insbesondere das BAG, das VBS oder das EFD mit einer grossen Anzahl von Zugangsgesuchen konfrontiert. Gemäss diesen Behörden handelte es sich dabei teilweise um sehr umfangreiche und komplexe Gesuche. In einer Vielzahl von Fällen war eine aufwändige verwaltungsinterne Koordination zwischen Ämtern oder Departementen notwendig, etwa bei Dokumenten betreffend die Beschaffung von medizinischen Gütern. Für diese Behörden war der Bearbeitungsaufwand im Vergleich zu früheren Jahren aus nachvollziehbaren Gründen höher.

Auf Stufe Amt zeigen die gemeldeten Zahlen, dass das BAG mit 181 Fällen 2020 am meisten eingegangene Zugangsgesuche meldete, wovon alleine 134 Corona-relevante Dokumente betrafen (s. Kap. 3.3). Danach folgen das BASPO mit 150, Swissmedic mit 42 sowie das BAFU mit 38 Gesuchen. Bei den Departementen liegen das EDI (312) und das VBS (251) an der Spitze. 13 Behörden meldeten hingegen, dass im Berichtsjahr bei ihnen kein Zugangsgesuch eingegangen sei. Beim Beauftragten selbst gingen zehn Zugangsgesuche ein, wobei er den Zugang in acht Fällen vollständig gewährte. In einem Fall war kein entsprechendes Dokument vorhanden und in einem Fall war das Gesuch Ende 2020 noch hängig.

Der 2020 für den Zugang zu amtlichen Dokumenten erhobene Gebührenbetrag beläuft sich auf insgesamt CHF 15189 und liegt damit unter der Vorjahressumme (CHF 18185). Nur bei zwei Zugangsgesuchen zu «Corona»-Dokumenten wurde insgesamt eine Gebühr von CHF 450 verlangt.

Während das EJPD und die Bundeskanzlei überhaupt keine Gebühren erhoben, verrechneten die übrigen sechs Departemente den Gesuchstellenden einen Teil ihres Zeitaufwands (EDI: CHF 4643; WBF: CHF 3786; UVEK: CHF 3310; EFD: CHF 1900; EDA: CHF 900; VBS: CHF 650). Dazu sei vermerkt, dass lediglich bei 25 der 1193 eingereichten Zugangsgesuche eine Gebühr erhoben wurde. Gegenüber dem Vorjahr, in dem in 31 Fällen eine Gebühr verlangt wurde, stellt dies – sowohl in Bezug auf die Anzahl Fälle, in welchen eine Gebühr erhoben wurde, wie auch bezüglich des Gesamtbetrages der Gebühren – einen Rückgang dar. Dies ist insofern bemerkenswert, als die Anzahl der Zugangsgesuche (erneut) merklich zugenom-

Grafik 1: Beurteilung Zugangsgesuche – Entwicklung seit 2006



men hat. Wie bereits in den Vorjahren stellt die Erhebung von Gebühren weiterhin eine Ausnahme dar: In beinahe 98 Prozent der Zugangsgesuche besteht Gebührenfreiheit. Die gelebte Verwaltungspraxis untermauert den von der Staatspolitischen Kommission des Nationalrats vorgeschlagenen Grundsatz der Gebührenfreiheit beim Zugang zu amtlichen Dokumenten (s. Kap. 2.4, Stellungnahme des EDÖB).

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. 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 5010 Stunden im Vergleich zu 2019 (4375 Stunden) zugenommen.

Die Zunahme der Anzahl der Zugangsgesuche (30 Prozent) hat sich folglich nicht im gleichen Ausmass auf die Erhöhung des Zeitaufwands (15 Prozent) ausgewirkt. Ebenfalls zugenommen hat der gemeldete Zeitaufwand für die Vorbereitung von Schlichtungsverfahren: 569 Stunden (gegenüber 473 Stunden für 2019).

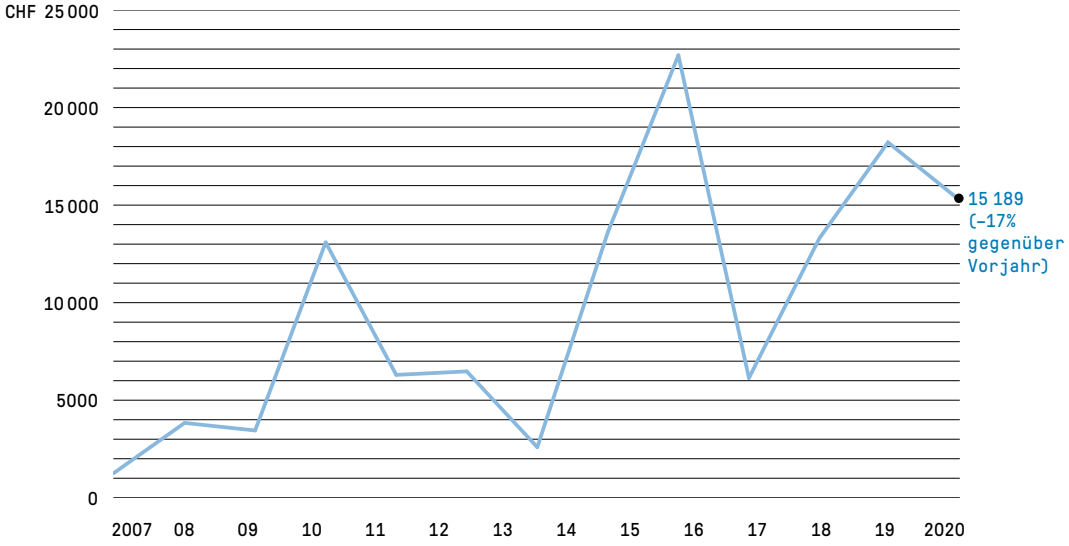
Parlamentsdienste

Die Parlamentsdienste meldeten den Eingang von sechs Zugangsgesuchen. Abgesehen von dem einen Fall, in welchem kein amtliches Dokument vorhanden war, wurden die restlichen fünf Zugangsgesuche vollumfänglich abgelehnt.

Bundesanwaltschaft

Die Bundesanwaltschaft meldete für 2020 den Eingang von 13 Gesuchen. In sechs Fällen wurde dem Zugangsgesuch vollständig entsprochen, in einem Fall wurde der Zugang vollumfänglich verweigert. Für die übrigen Gesuche gilt, dass in zwei Fällen keine amtlichen Dokumente vorhanden waren und vier Fälle am Ende des Berichtsjahres noch hängig sind.

Grafik 2: Erhobene Gebühren seit Inkrafttreten des BGÖ



2.3 Schlichtungsverfahren – weniger Schlichtungsanträge

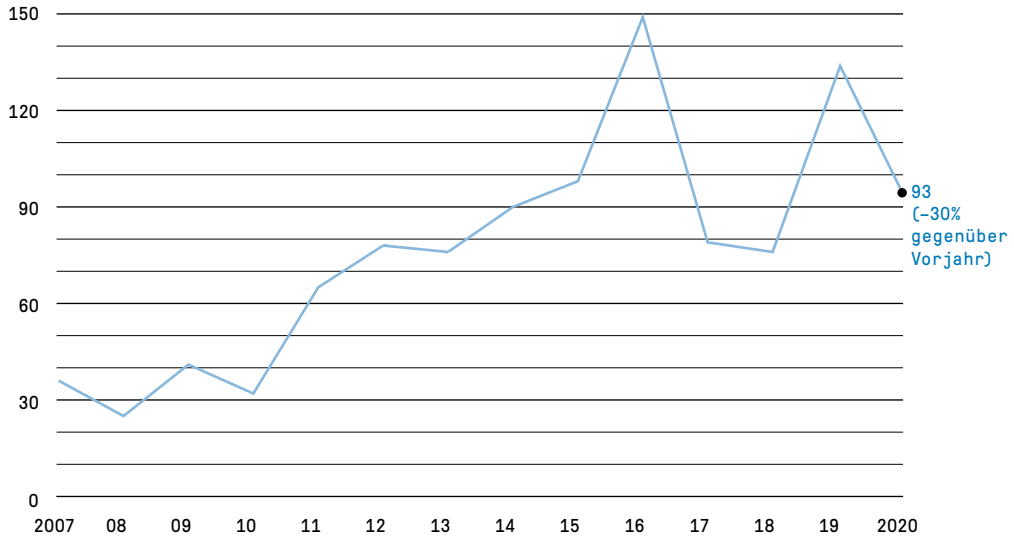
Im Jahr 2020 wurden beim Beauftragten 93 Schlichtungsanträge eingereicht. Verglichen mit den 2019 eingegangenen 133 Anträgen (wovon 28 Schlichtungsverfahren den gleichen Sachverhalt betrafen) entspricht dies einem Rückgang von 30 Prozent. Die meisten Schlichtungsanträge wurden von Privatpersonen (42) und Medienschaffenden (31) eingereicht. Diese Zahlen lassen folgende Feststellungen zu: In den 401 Fällen, in denen die Bundesverwaltung den Zugang vollständig oder teilweise verweigerte, kam es 93-mal bzw. in 23 Prozent der Fälle, in denen das Gesuch abschlägig beschieden wurde, zur Einreichung eines Schlichtungsantrags beim Beauftragten. Davon betrafen 24 Schlichtungsanträge (26 Prozent) amtliche Dokumente mit einem Bezug zu Corona.

119 Schlichtungsanträge wurden 2020 abgearbeitet, von denen 79 im Berichtsjahr und 40 im Jahr davor eingegangen waren. In 40 Fällen konnten sich die Beteiligten auf eine Konsenslösung einigen. Ausserdem erliess der Beauftragte 27 Empfehlungen, durch die 55 Fälle erledigt werden konnten, in denen eine einvernehmliche Lösung zwischen den Parteien nicht ersichtlich war.

Zu den abgeschlossenen Fällen zu zählen sind auch elf Anträge, die nicht fristgerecht eingereicht wurden, zwölf Fälle, in denen die Voraussetzungen für die Anwendung des Öffentlichkeitsgesetzes nicht gegeben waren, sowie ein Schlichtungsantrag, der zurückgezogen wurde.

Per Ende Jahr war in acht Schlichtungsverfahren im Einvernehmen der Beteiligten eine Sistierung erfolgt.

Grafik 3: Schlichtungsanträge seit Inkrafttreten des BGÖ



Anteil einvernehmlicher Lösungen

Zu den vielen Vorteilen der einvernehmlichen Lösungen gehört, dass sie eine Beschleunigung des Zugangsverfahrens ermöglichen und die Basis für eine allfällige zukünftige Zusammenarbeit zwischen den an der Schlichtungssitzung Beteiligten schaffen.

Wie wirksam sich die 2017 eingeführten Massnahmen und die Durchführung von Schlichtungssitzungen erwiesen haben, lässt sich vor allem am Anteil der einvernehmlichen Lösungen im Verhältnis zu den Empfehlungen ablesen. Im Berichtsjahr konnten 40 einvernehmliche Lösungen erzielt werden, und der Beauftragte gab 27 Empfehlungen zur Lösung von 55 Fällen ab. Im Verhältnis zu den Empfehlungen machen die einvernehmlichen Lösungen somit nur einen Anteil von 34 Prozent aus, der verglichen mit den Vorjahren deutlich tiefer ausfällt (s. Tabelle 1).

Wie in Kapitel 2.1 bereits erwähnt, hat die Corona-Pandemie dazu geführt, dass im Zeitraum zwischen März und Juni 2020 und damit in 13 Fällen auf die Durchführung von Schlichtungssitzungen verzichtet werden musste. Eine einvernehmliche Lösung kann in aller Regel nur erreicht werden, wenn eine Schlichtungsverhandlung durchgeführt wird. So konnte im Berichtsjahr in den 40 Schlichtungsverhandlungen, die durchgeführt werden konnten, in 24 Fällen (60 Prozent) eine Einigung erzielt werden, was den Werten der Vorjahre entspricht.

Die im Vergleich zu den Vorjahren scheinbar zahlreichen Schlichtungsverfahren, in denen der Beauftragte eine Empfehlung abgab, ist hauptsächlich auf eine statistische Auffälligkeit zurückzuführen: In zwei Zugangsgesuchen hat eine ungewöhnliche grosse Anzahl an Drittbetroffenen einen Schlichtungsantrag eingereicht (in einem Fall zehn und im anderen Fall 18 Drittbetroffene). Aus diesen 28 Schlichtungsanträgen resultiert mehr als die Hälfte aller Fälle, die mit einer Empfehlung abgeschlossen wurden.

Im Ergebnis stellt der Beauftragte fest, dass sich mündliche Schlichtungsverhandlungen unverändert bewähren, um zu raschen und einvernehmlichen Lösungen zu gelangen. In einigen Fällen wurde von den Beteiligten angesichts der Corona-Massnahmen eine Sistierung des Verfahrens bis zu dem Zeitpunkt beantragt, in welchem mündliche Verhandlungen wieder möglich sein werden.

Der EDÖB publiziert sämtliche Empfehlungen auf seiner Website.

Tabelle 1: Einvernehmliche Lösungen

2020	**34 %**
2019	61 %
2018	55 %

Dauer der Schlichtungsverfahren

Die Tabelle 2 ist in vier von der Verfahrensdauer abhängige Spalten aufgeteilt. Zu beachten ist, dass der Zeitraum, während dem ein Schlichtungsverfahren auf Antrag resp. mit Einverständnis der Beteiligten sistiert ist, nicht zur Behandlungsdauer gezählt wird. Eine Sistierung erfolgt insbesondere dann, wenn eine Behörde nach der Schlichtungssitzung ihre Position überprüfen möchte oder wenn sie betroffene Dritte anhören muss. Wird die Schlichtungssitzung auf Antrag einer beteiligten Partei verschoben (bspw. aufgrund von Ferienabwesenheit, Krankheit etc.), wird die Zeitspanne zwischen dem ursprünglich vorgesehenen Termin und dem neu angesetzten Termin bzw. die daraus resultierende Verfahrensverlängerung ebenfalls nicht zur Bearbeitungsdauer hinzugerechnet.

Aus der Tabelle 2 wird ersichtlich, dass 43 Prozent der im 2020 abgeschlossenen Schlichtungsverfahren innerhalb der ordentlichen Frist von 30 Tagen abgearbeitet wurden. In 30 Prozent der Fälle dauerte das Schlichtungsverfahren zwischen 31 und 99 Tagen und in 27 Prozent gar länger als 100 Tage.

Häufige Gründe für eine Fristüberschreitung sind Abwesenheiten von betroffenen Personen oder Behörden (Ferien, Krankheit, Reisen), eine grosse Zahl der am Verfahren beteiligten Drittpersonen oder die juristische Komplexität der Fragestellung, wobei im Berichtsjahr Corona-bedingte Verhinderungen von Parteien sowie eigenen Personals dazukamen. Solche Gründe treffen auch auf jene 32 Fälle zu, deren Bearbeitung mehr als 100 Tage in Anspruch nahm, wobei davon in einem Fall zehn und in einem zweiten Fall 18 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 erschwert. Weil die Bearbeitung in derartigen Fällen oftmals besonders aufwändig ist, steht es dem Beauftragten gemäss Artikel 12a der Verordnung über das

Tabelle 2: Bearbeitungsdauer Schlichtungsverfahren

Bearbeitungsdauer in Tagen	Zeitraum 2014–August 2016*	Pilotphase 2017	Zeitraum 2018	Zeitraum 2019	Zeitraum 2020
innert 30 Tagen	11 %	59 %	50 %	57 %	43 %
zwischen 31 und 99 Tagen	45 %	37 %	50 %	38 %	30 %
mehr als 100 Tage	44 %	4 %	0 %	5 %	27 %

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

Öffentlichkeitsprinzip der Verwaltung (VBGÖ; SR 152.31) frei, die ordentliche Frist angemessen zu verlängern. Im Berichtsjahr wurde den von der Corona-Pandemie stark betroffenen Behörden verschiedentlich Fristverlängerungen im Schlichtungsverfahren gewährt.

Die Vorgabe der gesetzlichen Frist von 30 Tagen für die Durchführung von Schlichtungsverfahren kann in der Regel eingehalten 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 der Beauftragte seine schriftliche Empfehlung den Beteiligten nicht in jedem Fall innert 30 Tagen nach Eingang des Antrags zustellen.

Aus dem pandemiebedingt angestiegenen Anteil an schriftlichen Schlichtungsverfahren und schriftlichen Empfehlungen resultierte für den Beauftragten ein deutlich erhöhter Arbeitsaufwand. Letzterer führte zu einem Anstieg der Bearbeitungsdauer der Verfahren und entsprechenden Bearbeitungsrückständen. Angesichts des neuerlichen Lockdowns zu Beginn des Jahres 2021 muss der Beauftragte damit rechnen, dass die Rückstände noch zunehmen werden.

Desweiteren haben auch in diesem Berichtsjahr angehörte Drittbetroffene bereits im Stadium des Zugangs- und Schlichtungsverfahrens Rechtsvertretungen beigezogen, was einer einfachen, pragmatischen und raschen Lösungsfindung in der Regel wenig förderlich ist.

Anzahl hängiger Fälle

Die unten aufgeführten Angaben geben Auskunft über die Anzahl der Fälle, die am Ende der jeweiligen Berichtsjahre hängig waren. Anfang Januar 2021 waren 17 Schlichtungsverfahren hängig, wovon acht sistiert sind (drei aus dem Jahr 2019, fünf aus dem Jahr 2020). Sieben Fälle konnten bis zum Redaktionsschluss des vorliegenden Berichts abgeschlossen werden.

Tabelle 3: Hängige Schlichtungsverfahren

Ende 2020	**17 (davon 9 bis zum Redaktionsschluss erledigt und 8 sistiert)**
Ende 2019	43 (davon 40 bis zum Redaktionsschluss erledigt und 3 sistiert)
Ende 2018	15 (davon 13 im Februar 2019 erledigt und 2 sistiert)

2.4 Gesetzgebungsverfahren

CORONA

Gesetzgebungsverfahren für die Überführung der COVID-19-Solidarbürgschaftsverordnung ins COVID-19-Solidarbürgschaftsgesetz

Nach dem COVID-19-Solidarbürgschaftsgesetz müssen im Rahmen des Bürgschaftsprogrammes des Bundes Identität und Bankverbindungen von Unternehmen und Personen sowie die gesprochenen und verweigerten Kreditbeträge geheim gehalten werden. Der Beauftragte hatte sich im Gesetzgebungsverfahren erfolglos gegen diese Einschränkung des Öffentlichkeitsprinzips ausgesprochen.

Mit der Einführung einer befristeten Notverordnung hat der Bundesrat am 25. März 2020 einen raschen Zugang zu Überbrückungsfinanzierungen für zahlreiche Unternehmen ermöglicht, um ihnen die notwendige Liquidität zur Krisenbewältigung infolge der Pandemie sicherzustellen. Die Inhalte dieser Notverordnung wurden in ein dringliches und befristetes Bundesgesetz überführt, welches vom Parlament im Dezember 2020 verabschiedet wurde.

Nach Art. 12 Abs. 2 des COVID-19-Solidarbürgschaftsgesetzes (COVID-19-SBüG) dürfen Personendaten und Informationen zu einzelnen kreditsuchenden und -nehmenden Unternehmen und Personen nicht bekannt gegeben werden, soweit diese deren Identität und Bankverbindungen sowie die zugesprochenen und verweigerten Kreditbeträge zum Inhalt haben. Gemäss der Botschaft zum COVID-19-SBüG handelt es sich dabei um eine Spezialbestimmung i.S.v. Art. 4 BGÖ, was zur Folge hat, dass diese Informationen vom Geltungsbereich des Öffentlichkeitsgesetzes ausgenommen sind und damit auf Zugangsgesuch hin nicht zugänglich sind.

Der Beauftragte hatte sich sowohl in der Vernehmlassung zum COVID-19-SBüG wie auch in der daran anschliessenden Ämterkonsultation betr. die Botschaft und den Gesetzesentwurf gegen die Einführung dieser Spezialbestimmung ausgesprochen. Er hat dabei auch auf die mit dem Öffentlichkeitsgesetz verfolgten Ziele, wie den Nachvollzug des Verwaltungshandeln oder die Verhinderung von Misswirtschaft und Korruption, hingewiesen. Angesichts des Einsatzes von 40 Milliarden Franken an Steuergeldern war die voraussetzungslose Geheimhaltung der in Frage stehenden Informationen nach seinem Dafürhalten nicht angezeigt. Sofern es bei den zugesprochenen Krediten zu Verlusten kommt, müssen diese mit Steuergeldern gedeckt werden. Angesichts der nachträglichen Beanstandungen des Verwaltungshandelns im Zusammenhang mit den Bürgschaftsvergaben in der Hochseeschifffahrt zeigt sich der Beauftragte erstaunt, dass das Parlament die vom Bundesrat vorgeschlagene Geheimhaltung im am 19. Dezember 2020 verabschiedeten Gesetz verankert hat.

Der Beauftragte hatte im Vernehmlassungsverfahren vergeblich aufgezeigt, dass die berechtigten privaten Interessen auch bei Anwendbarkeit des Öffentlichkeitsgesetzes geschützt bleiben. So gewährleistet es explizit den Schutz von Geschäftsgeheimnissen (Art. 7 Abs. 1 Bst. g BGÖ) und der Privatsphäre sowie der Personaldaten von natürlichen und juristischen Personen (Art. 7 Abs. 2 BGÖ, Art. 9 Abs. 2 BGÖ sowie Art 19 DSG). Auch hat der Beauftragte dargelegt, dass das Bankgeheimnis, dem Öffentlichkeitsgesetz gemäss Lehre und Rechtsprechung vorgeht. Ebenso erfolglos hat der Beauftragte in seiner Stellungnahme auf das Bundesgesetz über Finanzhilfen und Abgeltungen (Subventionsgesetz) und das Bundesgesetz über die Finanzhilfen an Bürgschaftsorganisationen für KMU hingewiesen. Obwohl beide Gesetze offensichtliche Gemeinsamkeiten zum vorliegenden Erlass aufweisen, sehen sie keine Spezialbestimmungen im Sinne von Art. 4 BGÖ vor.

Ämterkonsultation Entwurf der Stellungnahme des Bundesrates zum Bericht vom 15. Oktober 2020 der Staatspolitischen Kommission des Nationalrates zur parlamentarischen Initiative 16.432 Graf-Litscher. Gebührenregelung. Öffentlichkeitsprinzip in der Bundesverwaltung

Die Staatspolitische Kommission des Nationalrats hat eine Vorlage ausgearbeitet, nach welcher der Zugang zu amtlichen Dokumenten grundsätzlich kostenlos sein soll und nur in Ausnahmefällen eine Gebühr verlangt werden darf. Der Bundesrat möchte den Maximalbetrag der Gebühr selber in der Verordnung festlegen können. Demgegenüber spricht sich der Beauftragte für die Verankerung des Maximalbetrages direkt im Öffentlichkeitsgesetz aus.

Mit der parlamentarische Initiative 16.432 «Gebührenregelung. Öffentlichkeitsprinzip in der Bundesverwaltung» sollen die rechtlichen Grundlagen im Öffentlichkeitsgesetz so angepasst werden, dass der Zugang zu amtlichen Dokumenten in der Regel gebührenfrei sein soll.

In der Folge verabschiedete die für das Geschäft zuständige Staatspolitische Kommission des Nationalrats (SPK-N) einen Vorentwurf zur Änderung des Öffentlichkeitsgesetzes, den sie nach der Vernehmlassung zuhanden des Nationalrates überarbeitete. Demnach soll neu im Öffentlichkeitsgesetz der Grundsatz der Kostenlosigkeit beim Zugang zu amtlichen Dokumenten verankert werden. Nur noch ausnahmsweise soll eine Gebühr verlangt werden können, nämlich «wenn ein Zugangsgesuch eine besonders aufwendige Beurteilung durch die Behörde erfordert». Dabei soll gemäss der Kommissionsmehrheit eine Maximalgebühr von 2000 Franken im Öffentlichkeitsgesetz festgelegt werden, während der Bundesrat die Einzelheiten und den Gebührentarif nach Aufwand festlegen soll. Eine Minderheit der Kommission will auch die Festlegung der Maximalgebühr dem Bundesrat überlassen.

Der Beauftragte unterstützte den Vorschlag der Kommissionsmehrheit, die Maximalgebühr direkt im Öffentlichkeitsgesetz festzulegen, weil damit auf Stufe des Gesetzes sichergestellt wird, dass die ausnahmsweise Gebührenerhebung nicht ein Ausmass annehmen wird, das einer Behinderung des Zugangs zu amtlichen Dokumenten gleichkommt. Nachdem sich der Bundesrat gegen die gesetzliche Festlegung des Höchstbetrages ausgesprochen hat, liegt es nun am Nationalrat, über diese Frage zu befinden.

Revision des Bundesgesetzes über die Förderung der Forschung und der Innovation (FIFG). Ämterkonsultationen im Rahmen der Vorbereitungsarbeiten für die Botschaft des Bundesrates

In der Vernehmlassung zur Revision des FIFG wurde der Wunsch geäussert, die Bekanntgaberegelung der Namen der Referentinnen und Referenten sowie der wissenschaftlichen Gutachter und Gutachterinnen im Beschwerdeverfahren zu verschärfen. Der Beauftragte hat sich jedoch dagegen ausgesprochen.

Bei Beschwerden wegen nicht zugesprochenen Forschungsbeiträgen sieht Art. 13 Abs. 4 FIFG vor, dass die beschwerdeführende Person die Namen der Referentinnen und Referenten sowie der wissenschaftlichen Gutachter und Gutachterinnen auf Anfrage erhalten kann, wenn diese ihre Zustimmung gegeben haben. Das Bundesverwaltungsgericht hat in seinem Urteil A-6160/2018 vom 4. November 2019 im Rahmen einer Beschwerde nach dem Öffentlichkeitsgesetz Art. 13 Abs. 4 FIFG so ausgelegt, dass besagte Namen weiteren unbeteiligten Personen dann bekannt gegeben werden können, wenn die betroffenen Referenten und Gutachtenden ausdrücklich ihre Zustimmung gegeben haben. Gemäss Bundesverwaltungsgericht handelt es sich dabei zwar um eine Spezialbestimmung im Sinne von Art. 4 BGÖ, was zur Folge hat, dass das Öffentlichkeitsgesetz nicht zur Anwendung gelangt. Laut dem Gericht stellt Art. 13 Abs. 4 FIFG jedoch keine generelle Geheimhaltungspflicht dar.

Im Rahmen der Vernehmlassung zur Revision des FIFG beantragte der Schweizerische Nationalfonds SNF die Bekanntgaberegelung so einzugrenzen, dass ausschliesslich die beschwerdeführenden Personen die Bekanntgabe der in Frage stehenden Namen verlangen können. In der Folge hat sich der Beauftragte gegenüber dem in der Sache federführende Staatssekretariat für Bildung, Forschung und Innovation SBFI erfolgreich gegen die Aufnahme dieses Anliegen in die Vorlage eingesetzt.

In der Botschaft des Bundesrates vom 17. Februar 2021 wurde auf die beantragte Einschränkung der Bekanntgaberegelung verzichtet.

Teilrevision des KVG betreffend Massnahmen zur Kostendämpfung (zweites Paket)

Das Bundesamt für Gesundheit BAG erarbeitet eine Teilrevision des KVG betreffend Massnahmen zur Kostendämpfung. Diese Vorlage sieht unter anderem vor, sämtliche Unterlagen im Zusammenhang mit Preismodellen bei Arzneimitteln in der Krankenversicherung vom Öffentlichkeitsprinzip auszuschliessen. Der Beauftragte wehrt sich gegen dieses Vorhaben.

Im 27. Tätigkeitsbericht 2019/2020 berichtete der Beauftragte über eine zu eröffnende Vernehmlassung für eine Teilrevision des Krankenversicherungsgesetzes, welche im vorliegenden Berichtsjahr durchgeführt wurde. Der Beauftragte hatte sich gegen das Vorhaben des BAG ausgesprochen, das Einsichtsrecht der Öffentlichkeit in die Unterlagen über die Festsetzung von Medikamentenpreisen aufzuheben. Die effektiven Preise der Medikamente, welche von der obligatorischen Krankenpflegeversicherung übernommen werden, und die Unterlagen, welche zur Preisfestsetzung dienen, sollen nach Auffassung des Beauftragten weiter öffentlich zugänglich bleiben. Andernfalls würde eine undurchsichtige Praxis bezüglich der Aufnahme- und Überprüfungskriterien in die Spezialitätenliste und des Rückvergütungsmechanismus entstehen. Sowohl für die Bevölkerung wie für die konkurrierenden Unternehmen soll weiterhin möglich sein, die Genehmigungspraxis des BAG umfassend nachvollziehen und kontrollieren zu können. Das Ergebnis der Vernehmlassung ist zum Zeitpunkt des Redaktionsschlusses noch nicht bekannt.

Im Berichtsjahr führte der Beauftragte ein Schlichtungsverfahren zu Dokumenten des BAG über die Festsetzung von Medikamentenpreisen in der obligatorischen Krankenversicherung durch. Konkret wurde um Zugang zu Informationen betreffend Arzneimittel mit Preismodellen ersucht. Da zwischen dem BAG und der Antragstellerin im Schlichtungsverfahren keine Einigung zustande kam, musste der Beauftragte eine schriftliche Empfehlung erlassen. Das BAG begründete seine Weigerung gegen die Herausgabe der verlangten Dokumente hauptsächlich mit dem Argument, dass die Versorgungssicherheit mit innovativen und hochpreisigen Arzneimitteln ohne Geheimhaltung nicht weiter gewährleistet werden könne. Der Beauftragte hielt in der Empfehlung u.a. fest, dass seiner Ansicht nach das geltende Öffentlichkeitsgesetz keinen Raum lasse, die vom Bundesrat angestrebte Gesetzesänderung vorwegzunehmen. Da das BAG somit keine Ausnahmegründe nach dem geltenden Öffentlichkeitsgesetz nachzuweisen vermochte und damit die gesetzliche Vermutung des Zugangs zu den verlangten Informationen nicht widerlegen konnte, empfahl der Beauftragte den vollständigen Zugang.

Neues Bundesgesetz über den Allgemeinen Teil der Abgabenerhebung und die Kontrolle des grenzüberschreitenden Waren- und Personenverkehrs durch das Bundesamt für Zoll und Grenzsicherheit (BAZG-Vollzugsaufgabengesetz)

Die Eidgenössische Zollverwaltung (EZV) hat im letzten Quartal des Jahres 2020 eine Vernehmlassung für die Einführung eines neuen BAZG-Vollzugabgabengesetzes durchgeführt. In dieser Vorlage sind keine Einschränkungen des Öffentlichkeitsprinzips mehr enthalten.

Im 27. Tätigkeitsbericht 2019/2020 hat der Beauftragte über die Ämterkonsultation zur Eröffnung der Vernehmlassung für ein neues Bundesgesetz über Zoll und Grenzsicherheit berichtet. Der Gesetzesentwurf wurde nach der Ämterkonsultation überarbeitet und trägt neu die Bezeichnung «Bundesgesetz über den Allgemeinen Teil der Abgabenerhebung und die Kontrolle des grenzüberschreitenden Waren- und Personenverkehrs durch das Bundesamt für Zoll und Grenzsicherheit» (BAZG-Vollzugsaufgabengesetz). Die EZV hat den Bedenken des Beauftragten Rechnung getragen und die ursprünglich vorgesehenen Einschränkungen zum Öffentlichkeitsprinzip gestrichen. Die Vernehmlassung wurde erst im aktuellen Berichtsjahr durchgeführt.

Der EDÖB

3.1 Aufgaben und Ressourcen

CORONA

Pandemie

Die krisenbedingt kurzfristig realisierten Datenbearbeitungsprojekte zur Bekämpfung der aktuellen Pandemie und die gesteigerte Nachfrage nach öffentlichen Dokumenten forderten dem gesamten Personal ausserordentliche Leistungen ab.

Als administrativ der Bundeskanzlei zugehörendem Bundesbetrieb hat der EDÖB sämtliche Vorgaben des Bundesrates zum Schutze der Mitarbeitenden vor der Seuche umgesetzt. Das Personal des EDÖB erbrachte demzufolge in der Berichtsperiode einen Grossteil seiner Arbeitsleistung in digitaler Heimarbeit. Persönliche Begegnungen waren nur während weniger Wochen möglich, was insbesondere die Einführung und Betreuung von neuen Mitarbeitenden erschwerte.

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. Nachdem der Bundesrat dieses Gesetz am per 1. März 2019 in Kraft setzte, hat er dem EDÖB für die Umsetzung der neuen Aufgaben und Befugnisse drei zusätzliche Stellen zugesprochen, sodass sich der Stellenetat seit 2020 auf 27 Vollzeitstellen beläuft. Im Frühjahr 2021 hat der EDÖB dem Bundesrat mit Blick auf die für 2022 vorgesehene Inkraftsetzung des revidierten DSG die Schaffung der verbleibenden sechs Vollzeitstellen beantragt.

Aufgrund von Pensionierungen und anderen Abgängen hat sich die Altersstruktur der Behörde in den letzten Jahren verjüngt, was den Personalkredit entlastet.

Tabelle 4: Für DSG-Belange einsetzbare Stellen

2005	22
2010	23
2018	24
2019	24
2020	27
2021	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 1.4.2020 bis 31.3.2021 wurden die beim EDÖB für den Datenschutz einsetzbaren Personalressourcen wie folgt auf diese Gruppen aufgeteilt:

Tabelle 5: Leistungen Datenschutz

Beratung Private	24,8 %	
Beratung Bund	20,1 %	
Zusammenarbeit mit Kantonen	1,8 %	
Zusammenarbeit mit ausl. Behörden	11,1 %	
Total Beratung		**57,8 %**
Aufsicht	15,0 %	
Zertifizierung	0,1 %	
Register Datensammlung	0,4 %	
Total Aufsicht		**15,0 %**
Information	17,0 %	
Ausbildung/Referate	2,4 %	
Total Information		**19,4 %**
Gesetzgebung	7,3 %	
Total Gesetzgebung		**7,3 %**
Total Datenschutz		**100,0 %**

Beratung

Wie im Eingangskapitel «Aktuelle Herausforderungen» dargelegt, sieht sich der EDÖB im Leistungsbereich der Beratung, aufgrund der Notwendigkeit digitale Grossprojekte zu begleiten, mit einer konstant hohen Nachfrage konfrontiert. Die für die Beratung aufgewendeten personellen Mittel erhöhten sich um rund sieben auf 57,8 Prozent. Gemäss dem Kontrollplan des EDÖB für das Jahr 2021 ist die beratende Begleitung von fünfzehn grossen Projekten im Gang. Sechs dieser Projekte stehen im Zusammenhang mit der vom Bundesrat angeordneten digitalen Transformation der Bundesverwaltung, welche den von Politik und Medien gerade auch im Zusammenhang mit der Pandemiebekämpfung angemahnten Digitalisierungsrückstand aufzuholen sucht.

Da die Mittel des EDÖB mit Blick auf die rechtlichen und technologischen Risiken der dynamisch fortschreitenden Digitalisierung nach wie vor knapp bemessen sind, konnte er die gestiegene Nachfrage nach beratender Projektbegleitung auch in der laufenden Berichtsperiode nicht in der gewünschten Tiefe und Zeit erfüllen. Die drei Teams des Direktionsbereichs Datenschutz haben monatlich rund sechzig Anfragen und Anzeigen von Bürgerinnen und Bürgern mit einem Standardschreiben beantwortet, das diese 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 das neue DSG auch für den EDÖB eine ausweitende Pflicht vorsieht, Einzelanliegen der Schweizer Bevölkerung materiell zu behandeln.

Da sich Big Data und «künstliche Intelligenz» in allen 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.

Tabelle 6: Beratungen in umfangreicheren Projekten für 2021

Grundrechte	5
Finanzen	1
Gesundheit und Arbeit	3
Telekom	1
Handel und Wirtschaft	2
Bundesarchiv	1
Migration	1
Zoll	1
Total	**15**

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 den letzten Berichtsperioden konnte zumindest verhindert werden, dass der Anteil unter 15 Prozent sinkt. Gemäss Kontrollplan für das Jahr 2021 werden mit diesen Mitteln dreizehn umfassendere Kontrollen bestritten. Im Vergleich zum Bearbeitungsvolumen durch die Bundesorgane und zur Anzahl von rund 12000 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 formeller Sachverhaltsabklärungen gegenüber Medien und Konsumentenschutzorganisationen zu vermitteln. Mit Blick auf das bevorstehende Inkrafttreten des neuen DSG hat sich der Erwartungsdruck der Öffentlichkeit verstärkt. Vor diesem Hintergrund bleibt zu hoffen, dass der Bundesrat dem EDÖB die sechs beantragten Stellen zusprechen wird.

Gesetzgebung

Die mit der digitalen Transformation der Bundesämter einhergehenden Anpassungen der Personendatenbearbeitungen sind nur auf der Basis gesetzlicher Grundlagen zulässig. Diese zieht eine Vielzahl von neuen und revidierten Bearbeitungsvorschriften im Bundesrecht nach sich, zu denen der EDÖB in diversen Konsultationsverfahren Stellung bezieht. Trotz des diesbezüglichen Aufwands und trotz der aufwändigen Revision des DSG und der dazu gehörenden Verordnung ist es uns in den letzten Berichtsperioden gelungen, die Aufsichtstätigkeit auf tiefem Niveau zu stabilisieren, u.a. indem ausführliche Stellungnahmen auf Schlüsselprojekte beschränken.

Totalrevision des DSG

Mit der bevorstehenden Inkraftsetzung des neuen DSG und der Vollzugsverordnung sind für den EDÖB mit Blick auf neue Aufgaben und Kompetenzen sowie die rechtzeitige Information von Bevölkerung und Wirtschaft aufwändige Vorbereitungsarbeiten verbunden. Die mit Inkraftsetzung des DSG erfolgte Freigabe von drei Stellen durch den Bundesrat hat dazu beigetragen, dass diese Arbeiten voranschreiten.

Teilnahme an Kommissionsberatungen und Anhörungen durch parlamentarische Kommissionen

In der Berichtsperiode hat uns die SPK-N im April 2020 zweimal zum Thema Coronavirus im Zusammenhang mit einer Applikation der Swisscom zur Visualisierung von Menschenansammlungen eingeladen. Daneben hat uns diese Kommission Anfang Mai zur Einführung der Corona Warn App angehört. Etwa zu der gleichen Zeit konsultierte uns die SPK-S sowohl zur Revision des DSG (Differenzenbereinigung) als auch zur Teilrevision des AHV-Gesetzes im Zusammenhang mit der Verwendung der AHV Nummer. Ende Mai hat die SPK-S den EDÖB zweimal zur dringlichen Änderung des Epidemiengesetzes angehört. Bevor uns die gleiche Kommission im Juli 2020 zur Differenzbereinigung der Revision des DSG einlud, hat sie uns im Vorfeld zu dieser Revision sowie zur Revision des AHV-Gesetzes beigezogen. Im Juli dieser Geschäftsperiode wurden wir von den Subkommissionen EJPD/BK der GPK eingeladen, um unseren jährlichen Tätigkeitsbericht zu präsentieren.

Weitere Anhörungen im Berichtsjahr betrafen das elektronische Patientendossier durch die GPK-N und die Befragung der SPK-S zur Jugendsession über den Datenschutz im Gesundheitswesen.

Schliesslich haben uns die SPK beider Räte zu fünf Sitzungen und die SGK beider Räte zu zwei Sitzungen beigezogen, bei denen es um die Erleichterungen für geimpfte Personen und weitere COVID-19 Themen ging, beigezogen.

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:

Leistungen und Ressourcen im Bereich Öffentlichkeitsgesetz

Der Direktionsbereich Öffentlichkeitsprinzip, in dem im Berichtsjahr 4,4 Stellen eingesetzt wurden, 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 hat sich seither bewährt, indem der Anteil der einvernehmlich abgeschlossenen Schlichtungen über die Jahre konstant hoch war und die Überschreitung der gesetzlichen Fristen in der Regel auf prozessual und inhaltlich komplexe Fälle beschränkt werden konnte.

Infolge der Pandemie und der vom Bundesrat ergriffenen Massnahmen zum Schutz der öffentlichen Gesundheit konnten sowohl im Berichtsjahr wie auch im laufenden Jahr über mehrere Monate hinweg keine Schlichtungsverhandlungen vor Ort durchgeführt werden. Der Beauftragte musste für diese Zeitspannen wieder zum schriftlichen Verfahren zurückkehren. Dies wirkte sich unmittelbar nachteilig auf die Bearbeitungsdauer der einzelnen Verfahren aus und führte zusammen mit der unvermindert grossen Anzahl von (komplexen und umfangreichen) Schlichtungsanträgen zu einem Rückstau. Darüber hinaus hat sich im Berichtsjahr einmal mehr gezeigt, dass zahlreiche Schlichtungsanträge innerhalb eines kurzen Zeitraums und personelle Vakanzen rasch Arbeitsrückstände verursachen, welche dazu beitragen, die Einhaltung der gesetzlichen Fristen zusätzlich zu erschweren (s. Kap. 2.2).

Es zeichnet sich ab, dass die Entwicklung bei der Zunahme von Schlichtungsanträgen auch für das Jahr 2021 anhält, und dass der Rückstau die fristgemässe Bearbeitung neuer Fälle mit den vorhandenen Ressourcen zunehmend erschweren 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.


OPEN
RIDE

3.2 Kommunikation

Die Pandemie dominierte die Kommunikationsarbeit

Der Beginn des Berichtsjahres fiel praktisch mit dem Ausbruch der Corona-Pandemie in der Schweiz zusammen. Das Thema sollte schliesslich die gesamte Periode prägen – und tut es auch darüber hinaus. Die Kommunikation des Beauftragten war darauf ausgerichtet, relevante Datenschutzrisiken zu benennen und öffentlich zu machen. Trotz der prinzipiellen Unabhängigkeit des Beauftragten war in vielen Fällen eine behördliche Absprache nötig und sinnvoll – im Dienste einer kohärenten Information der Bevölkerung während der Krise. Dieser Anspruch an die Kommunikation bezog sich fallweise ebenso auf den Austausch mit den kantonalen Datenschutzbeauftragten.

Im Übrigen führte auch ungeachtet der Pandemie-Themen die beschleunigte Digitalisierung und Globalisierung der Gesellschaft zu anhaltend omnipräsenten Datenschutzfragen. Die Kommunikation des EDÖB blieb entsprechend in vielerlei Hinsicht gefordert, Medienschaffende und die breite Öffentlichkeit wirksam über die drängenden Themen zum Schutz der Privatsphäre und des Öffentlichkeitsprinzips in der Verwaltung zu sensibilisieren.

Im Fokus stand schliesslich die parlamentarische Debatte um das neue Datenschutzgesetz, die der Beauftragte kontinuierlich begleitete und im September 2020 mit der Verabschiedung durch die beiden Kammern ihr Ende fand. Nachdem gegen das totalrevidierte DSG kein Referendum ergriffen wurde, haben wir einen Kurzkommentar zu den neuen Bestimmungen auf unserer Website publiziert (s. Schwerpunkt 1). Wenn das Gesetz in Kraft tritt, wird der EDÖB über neue Aufgaben und gestärkte Aufsichtsbefugnisse verfügen, was zu einem weiter ansteigenden Kommunikationsbedarf bzw. einer höheren Präsenz in der Öffentlichkeit führen dürfte. Mit Blick auf die Inkraftsetzung des neuen Gesetzes und der dazugehörigen Verordnung werden zurzeit die bestehenden Merkblätter, Erläuterungen und Leitfäden überarbeitet.

Herausforderungen und Bedingungen der Kommunikation

Der Fachbereich Kommunikation konnte in der zweiten Jahreshälfte 2020 seinen ursprünglichen Stellenetat wiederherstellen und verfügt somit über 2,4 Vollzeitstellen, die sich drei Personen teilen. Mit der Besetzung der Stellen konnte auch die Mehrsprachigkeit der Schweiz wieder besser abgebildet werden. Aufgrund der beschränkten Ressourcen fokussiert der Beauftragte die Öffentlichkeitsarbeit auf drei zentrale Kommunikationskanäle: den (vorliegenden) Tätigkeitsbericht, die Website und die direkte Beziehung zu Medienschaffenden. Twitter wird eingeschränkt genutzt und auf andere social media Plattformen wird nicht zuletzt aus Datenschutzgründen verzichtet.

Im Berichtsjahr haben wir den Tätigkeitsbericht neu ausgeschrieben. Mit dem Zuschlag konnten die redaktionellen und konzeptionellen Rahmenbedingungen im bestehenden Kostenrahmen verbessert werden.

Anhaltend hohes Medieninteresse

Das grosse mediale Interesse spiegelte sich im Berichtsjahr in vielen Stellungnahmen des Beauftragten bzw. der Kommunikation zu aktuellen Anfragen wie auch in den zahlreichen Artikeln und Beiträgen, die allgemein zum Datenschutz und dem Öffentlichkeitsprinzip in der Verwaltung analog und digital erschienen sind. Allein in unserer Medienbeobachtung, die sich auf die Schweizer Medien und eine Auswahl von internationalen Key-Printprodukten stützt, registrierten wir gegen 4000 Beiträge. Das sind rund doppelt soviel wie in der Vorjahresperiode – eine Steigerung, die sich nicht durch die erfolgte Anpassung des Suchprofils begründen lässt, sondern auf die deutlich gesteigerte Relevanz hinweist. Mehr als die Hälfte der Beiträge beziehen sich auf die Corona-Pandemie.

Parallel dazu sehen wir im social web (den sozialen Medien und den Online-Plattformen; s. Kennzahlen Umschlag hinten) eine starke Aktivität. In Bezug auf den EDÖB wurden 7320 Nennungen gezählt, wovon in 1152 Erwähnungen der Beauftragte oder ein Sprecher oder eine Sprecherin direkt zitiert wurde. Über die Hälfte dieser Nennungen erfolgte auf Kanälen im Ausland. Ein zentraler Indikator im social web sind die «Engagements», also die Anzahl der Aktivitäten wie Likes, Weiterleitung oder Kommentierung pro Beitrag. Mit 3,36 Engagements liegt dieser Wert sehr hoch und weist auf eine erhöhte, aktive Vernetzung in den Communities hin.

Insgesamt haben wir rund 600 Medienanfragen bearbeitet – ca. ein Drittel mehr als im Jahr zuvor. Die

überwiegende Zahl der Kontakte erfolgte durch die im Medienzentrum des Bundeshauses akkreditierten Journalistinnen und Journalisten.

Bürger und Bürgerinnen und 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 4200 Anfragen.

Wiederum nahm der Beauftragte bei gegen vierzig Veranstaltungen teil. Unter den Veranstaltern befanden sich Verbände und Vereine, Bildungsinstitutionen, Behörden oder Unternehmen sowie Organisationen im Umfeld der Digitalisierung.

CORONA

Informationen zu Corona

Der Beauftragte und seine Fachpersonen haben neben der umfangreichen Beratungstätigkeit in der Pandemie auch mehrfach die Haltung betreffend Datenschutzkonformität zentraler Herausforderungen öffentlich gemacht. Namentlich zu folgenden Themen:

- Auswertung von Mobilitätsverhalten auf dem Gebiet der Schweiz: Zugang des BAG zu visualisierten Daten der Swisscom
- Proximity Tracing App: Datenschutzkonformität der SwissCovid App
- Massnahmen für eine sichere Nutzung von Audio- und Videokonferenzlösungen
- Corona-Schutzkonzepte durch private Betreiber: Freiwilligkeit der Weitergabe von Personendaten
- Gästelisten und Kontaktdaten: Betreiber müssen bei der Erfassung der Kontaktdaten Datenschutz sicherstellen, Einsatz von Apps freiwillig
- Verfahren gegen Impfplattform bzw. Stiftung meineimpfungen

Im Rahmen des Internationalen Datenschutztages am 28. Januar 2021 erinnerte der EDÖB gemeinsam mit Privatim, der Konferenz der schweizerischen Datenschutzbeauftragten, an den nötigen Schutz der Privatsphäre in der Pandemie. Vor den Medien bekräftigten die Datenschutzbehörden das Recht auf das private und selbstbestimmte Leben, das nicht über die Phase der aktuellen Pandemie hinaus eingeschränkt werden dürfe. Es muss für die Bevölkerung auch künftig möglich sein, bezüglich digitaler Technologien ein echtes Wahlrecht auszuüben und auf anonyme Alternativen auszuweichen.

Stellungnahmen, Empfehlungen und Publikationen

Im Berichtsjahr veröffentlichte der Beauftragte diverse Stellungnahmen und Statements zu aktuellen Projekten und Ereignissen – neben Corona (s. Box) unter anderem zu folgenden Themen:

- Beratung und Bestimmungen des totalrevidierten Datenschutzgesetzes
- Ungenügende Regelung der Datenbearbeitung im neuem Zollpolizeigesetz
- CH- und EU-US Privacy Shield, namentlich zum Urteil des Europäischen Gerichtshofes EuGH betreffend der europäischen Standardvertragsklauseln
- Datenbearbeitung betreffend Diem (vormals Libra)
- KVG-Revision: EDÖB für Transparenz bei Preismodellen

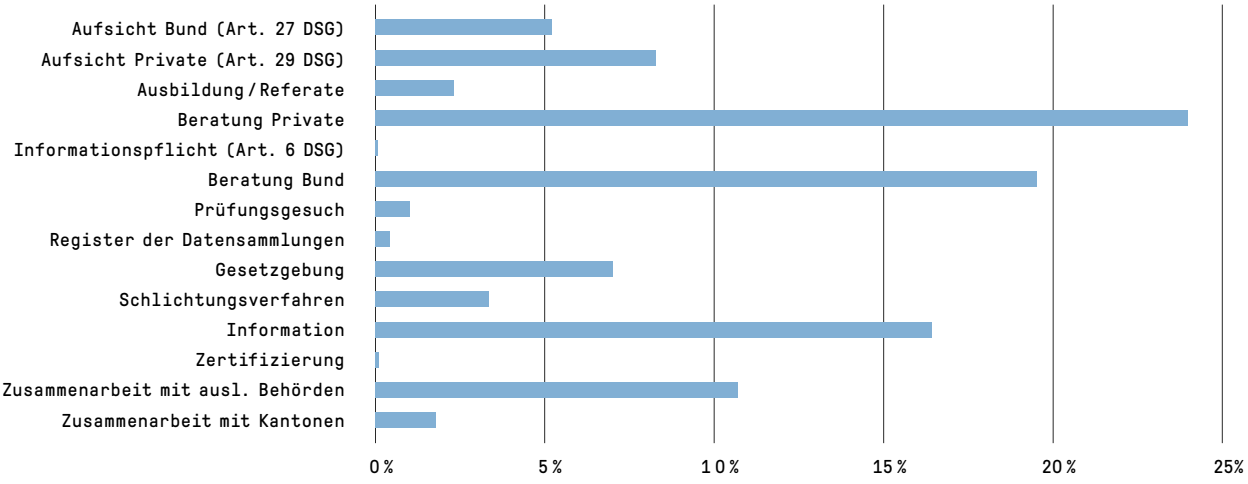
Auf der Website des EDÖB publizierten wir zudem 26 Empfehlungen betreffend das Öffentlichkeitsprinzip.

Die Publikation des im Art. 30 DSG vorgeschriebenen 27. Tätigkeitsberichts 2019/2020 erfolgte am 30. Juni 2020. Dieser wurde erneut in vier Sprachen zur Verfügung gestellt – und zwar sowohl als gedruckte Version wie auch als auf der Website verlinktes E-Paper.

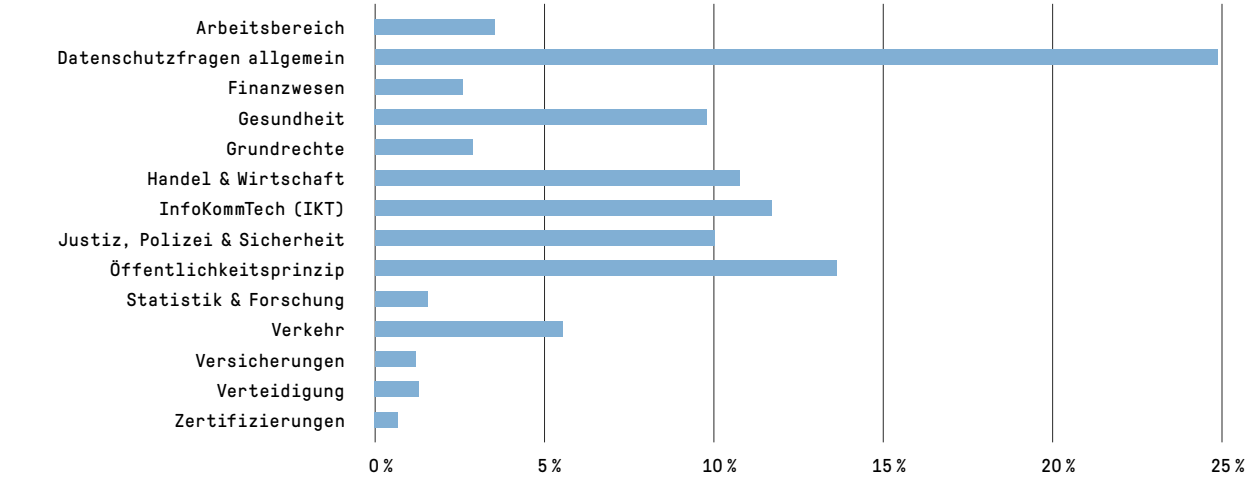
3.3 Statistiken

Statistiken über die Tätigkeiten des EDÖB vom 1. April 2020 bis 31. März 2021 (Datenschutz)

Aufwand nach Aufgabengebiet

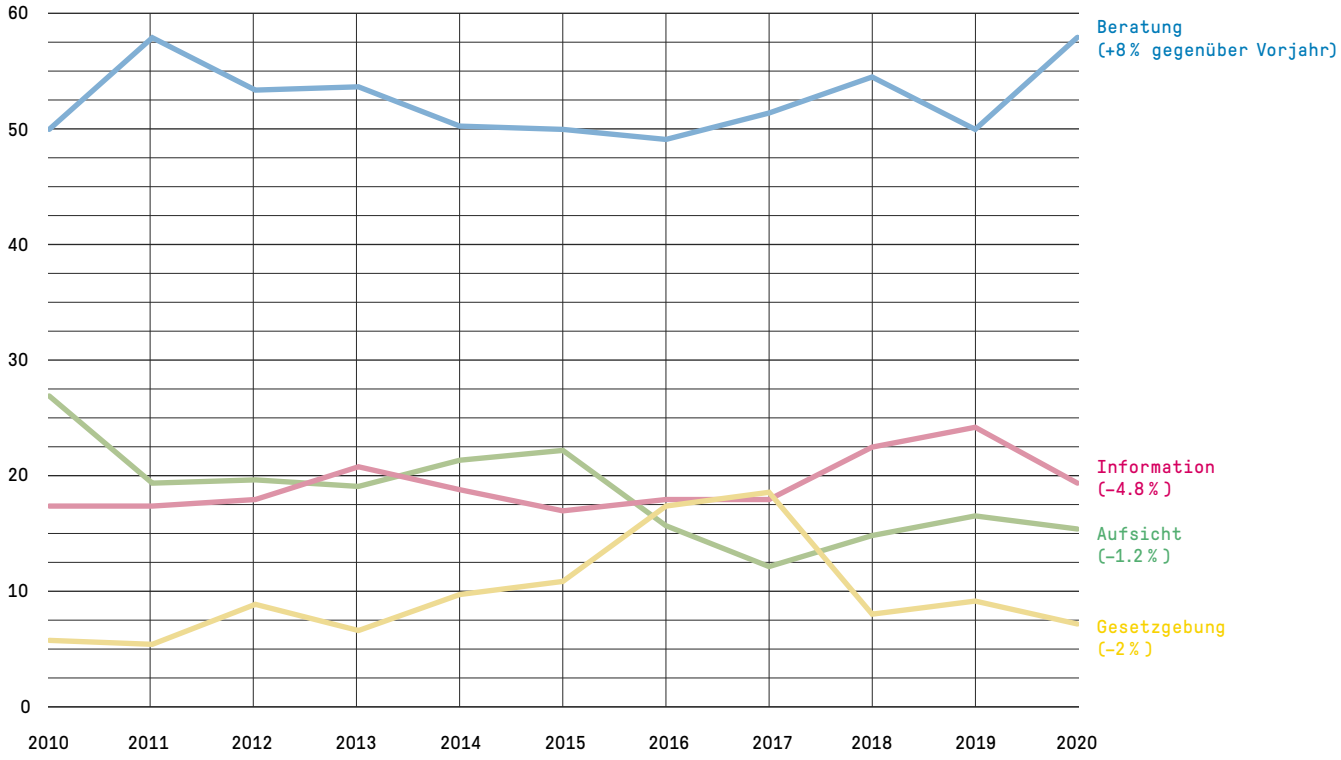


Aufwand nach Sachgebiet



Mehrjahresvergleich Aufwand

(Angaben in Prozent)



Übersicht der Zugangsgesuche vom 1. Januar bis 31. Dezember 2020

Departement	Anzahl Gesuche		Zugang vollständig gewährt		Zugang vollständig verweigert		Zugang teilweise gewährt/aufgeschoben		Zugangsgesuch zurückgezogen		Zugangsgesuch hängig		kein amtliches Dokument vorhanden	
BK	31		20		5		4		0		2		0	
EDA	174		88		14		47		11		4		10	
EDI	312		114		26		100		8		41		23	
EJPD	77		45		11		9		2		3		7	
VBS	251		184		10		37		5		10		5	
EFD	109		51		13		28		3		6		8	
WBF	115		49		15		36		3		7		5	
UVEK	105		53		8		32		3		3		6	
BA	13		6		1		0		0		4		2	
PD	6		0		5		0		0		0		1	
Total 2020 (%)	1193	(100)	610	(51)	108	(9)	293	(24)	35	(3)	80	(7)	67	(6)
Total 2019 (%)	916	(100)	542	(62)	86	(11)	171	(21)	38	(6)	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)	–	

Statistiken über eingereichte Zugangsgesuche nach Öffentlichkeitsgesetz vom 1. Januar bis 31. Dezember 2020

	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	**21**	12	5	3	0	1	0
	EDÖB	**10**	8		1		1	
	Total	**31**	**20**	**5**	**4**	**0**	**2**	**0**
Eidg. Departement für Auswärtige Angelegenheiten EDA	EDA	**174**	88	14	47	11	4	10
	Total	**174**	**88**	**14**	**47**	**11**	**4**	**10**
Eidg. Departement des Inneren EDI	GS EDI	**20**	12	0	5	0	3	0
	EBG	**4**	3	0	0	1	0	0
	BAK	**3**	1	0	2	0	0	0
	BAR	**3**	1	0	2	0	0	0
	METEO CH	**1**	1	0	0	0	0	0
	NB	**0**	0	0	0	0	0	0
	BAG	**181**	51	22	69	3	26	10
	BFS	**7**	4	1	0	0	0	2
	BSV	**19**	15	0	4	0	0	0
	BLV	**25**	8	3	9	4	0	1
	SNM	**0**	0	0	0	0	0	0
	swissmedic	**42**	15	0	9	0	10	8
	Suva	**7**	3	0	0	0	2	2
	Total	**312**	**114**	**26**	**100**	**8**	**41**	**23**
Eidg. Justiz- und Polizeidepartement EJPD	GS EJPD	**5**	4	0	0	0	0	1
	BJ	**29**	18	7	2	0	0	2
	fedpol	**13**	6	2	2	1	0	2
	METAS	**2**	2	0	0	0	0	0
	SEM	**19**	10	1	5	0	3	0
	Dienst ÜPF	**1**	0	1	0	0	0	0
	SIR	**5**	3	0	0	0	0	2
	IGE	**2**	2	0	0	0	0	0
	ESBK	**0**	0	0	0	0	0	0
	ESchK	**0**	0	0	0	0	0	0
	RAB	**1**	0	0	0	1	0	0
	ISC-EJPD	**0**	0	0	0	0	0	0
	NKVF	**0**	0	0	0	0	0	0
	Total	**77**	**45**	**11**	**9**	**2**	**3**	**7**

	Betroffener Fachbereich	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt/aufgeschoben	Zugangsgesuch zurückgezogen	Zugangsgesuch hängig	Kein amtliches Dokument vorhanden
Eidg. Departement für Verteidigung, Bevölkerungsschutz und Sport VBS	GS VBS	**20**	7	0	10	1	0	2
	Verteidig./ Armee	**34**	13	0	9	2	9	1
	NDB	**18**	3	8	3	2	0	2
	armasuisse	**12**	9	0	2	0	1	0
	BASPO	**150**	147	2	1	0	0	0
	BABS	**17**	5	0	12	0	0	0
	swisstopo	**0**	0	0	0	0	0	0
	OA	**0**	0	0	0	0	0	0
	Total	**251**	**184**	**10**	**37**	**5**	**10**	**5**
Eidg. Finanz-departement EFD	GS EFD	**22**	11	1	9	0	1	0
	ISB	**1**	0	0	1	0	0	0
	EFV	**10**	1	1	7	1	0	0
	EPA	**1**	1	0	0	0	0	0
	ESTV	**10**	7	0	3	0	0	0
	EZV	**37**	15	7	5	1	3	6
	BBL	**3**	1	1	1	0	0	0
	BIT	**4**	2	0	0	1	0	1
	EFK	**8**	3	3	1	0	0	1
	SIF	**3**	0	0	1	0	2	0
	PUBLICA	**0**	0	0	0	0	0	0
	ZAS	**10**	10	0	0	0	0	0
	Total	**109**	**51**	**13**	**28**	**3**	**6**	**8**
Eidg. Departement für Wirtschaft, Bildung und Forschung WBF	GS WBF	**9**	6	1	0	1	0	1
	SECO	**35**	16	10	7	1	0	1
	SBFI	**4**	3	0	0	0	0	1
	BLW	**14**	3	0	7	0	3	1
	BWL	**7**	3	0	3	0	0	1
	BWO	**3**	0	0	3	0	0	0
	PUE	**2**	1	0	1	0	0	0
	WEKO	**18**	11	1	3	1	2	0
	ZIVI	**0**	0	0	0	0	0	0
	BFK	**2**	2	0	0	0	0	0
	SNF	**2**	1	0	0	0	1	0
	EHB	**1**	0	0	0	0	1	0
	ETH	**16**	3	3	10	0	0	0
	InnoSuisse	**2**	0	0	2	0	0	0
	Total	**115**	**49**	**15**	**36**	**3**	**7**	**5**

	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 UVEK	**9**	8	0	1	0	0	0
	BAV	**14**	9	0	3	2	0	0
	BAZL	**9**	3	0	2	0	1	3
	BFE	**4**	3	0	0	0	0	1
	ASTRA	**9**	7	0	2	0	0	0
	BAKOM	**14**	2	2	10	0	0	0
	BAFU	**38**	17	5	13	1	0	2
	ARE	**0**	0	0	0	0	0	0
	ComCom	**0**	0	0	0	0	0	0
	ENSI	**7**	3	1	1	0	2	0
	PostCom	**1**	1	0	0	0	0	0
	UBI	**0**	0	0	0	0	0	0
	Total	**105**	**53**	**8**	**32**	**3**	**3**	**6**
Bundesanwaltschaft BA	BA	**13**	6	1	0	0	4	2
	Total	**13**	**6**	**1**	**0**	**0**	**4**	**2**
Parlamentsdienste PD	PD	**6**	0	5	0	0	0	1
	Total	**6**	**0**	**5**	**0**	**0**	**0**	**1**
	Gesamttotal	**1193**	**610**	**108**	**293**	**35**	**80**	**67**

Zugangsgesuche 2020 mit Corona-Bezug

	Betroffener Fachbereich	Gesuche im Zusammenhang mit COVID-19	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt/aufgeschoben	Zugangsgesuch zurückgezogen	Zugangsgesuch hängig	kein amtliches Dokument vorhanden
Bundeskanzlei BK	BK	**6** (100%)	3 (50%)	3 (50%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	EDÖB	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	Total	**6** (100%)	**3** (50%)	**3** (50%)	**0** (0%)	**0** (0%)	**0** (0%)	**0** (0%)
Eidg. Departement für Auswärtige Angelegenheiten EDA	EDA	**13** (100%)	12 (92%)	1 (8%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	Total	**13** (100%)	**12** (92%)	**1** (8%)	**0** (0%)	**0** (0%)	**0** (0%)	**0** (0%)
Eidg. Departement des Inneren EDI	GS EDI	**17** (10%)	11 (6%)	0 (0%)	3 (2%)	0 (0%)	3 (2%)	0 (0%)
	EBG	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	BAK	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	BAR	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	METEO CH	**1** (1%)	1 (1%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	NB	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	BAG	**134** (77%)	44 (25%)	16 (9%)	53 (31%)	1 (1%)	11 (6%)	9 (5%)
	BFS	**1** (1%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	1 (1%)
	BSV	**1** (1%)	1 (1%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	BLV	**4** (2%)	3 (2%)	1 (1%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	SNM	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	swissmedic	**16** (9%)	4 (2%)	0 (0%)	0 (0%)	0 (0%)	9 (5%)	3 (2%)
	SUVA	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	Total	**174** (100%)	**64** (37%)	**17** (10%)	**56** (32%)	**1** (1%)	**23** (13%)	**13** (7%)
Eidg. Finanzdepartement EFD	GS EFD	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	ISB	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	EFV	**9** (36%)	1 (4%)	1 (4%)	6 (24%)	1 (4%)	0 (0%)	0 (0%)
	EPA	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	ESTV	**2** (8%)	2 (8%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	EZV	**11** (44%)	1 (4%)	5 (20%)	3 (12%)	0 (0%)	0 (0%)	2 (8%)
	BBL	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	BIT	**3** (12%)	2 (8%)	0 (0%)	0 (0%)	1 (4%)	0 (0%)	0 (0%)
	EFK	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	SIF	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	PUBLICA	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	ZAS	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	Total	**25** (100%)	**6** (11%)	**6** (11%)	**9** (16%)	**2** (4%)	**0** (0%)	**2** (4%)

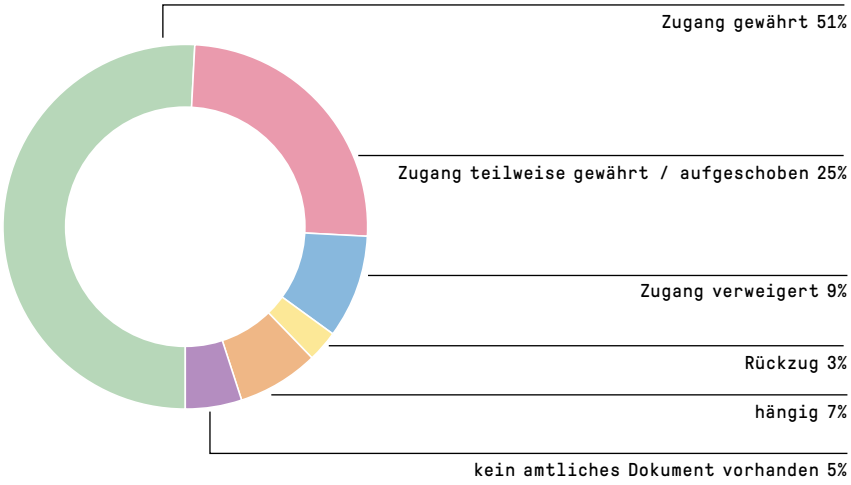
	Betroffener Fachbereich	Gesuche im Zusammenhang mit COVID-19	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt/aufgeschoben	Zugangsgesuch zurückgezogen	Zugangsgesuch hängig	kein amtliches Dokument vorhanden
Eidg. Justiz- und Polizeidepartement EJPD	GS EJPD	**1** (14%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	1 (14%)
	BJ	**6** (86%)	5 (71%)	1 (14%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	fedpol	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	METAS	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	SEM	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	Dienst ÜPF	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	SIR	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	IGE	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	ESBK	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	ESchK	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	RAB	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	ISC-EJPD	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	NKVF	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	Total	**7** (100%)	**5** (71%)	**1** (14%)	**0** (0%)	**0** (0%)	**0** (0%)	**1** (14%)
Eidg. Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK	GS UVEK	**1** (25%)	1 (25%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	BAV	**2** (50%)	1 (25%)	0 (0%)	0 (0%)	1 (25%)	0 (0%)	0 (0%)
	BAZL	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	BFE	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	ASTRA	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	BAKOM	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	BAFU	**1** (25%)	1 (25%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	ARE	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	ComCom	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	ENSI	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	PostCom	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	UBI	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	Total	**4** (100%)	**3** (75%)	**0** (0%)	**0** (0%)	**1** (25%)	**0** (0%)	**0** (0%)
Eidg. Departement für Verteidigung, Bevölkerungsschutz und Sport VBS	GS VBS	**8** (16%)	1 (2%)	0 (0%)	5 (10%)	0 (0%)	0 (0%)	2 (4%)
	Verteidig./ Armee	**23** (46%)	10 (20%)	0 (0%)	3 (6%)	1 (2%)	8 (16%)	1 (2%)
	NDB	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	armasuisse	**1** (2%)	1 (2%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	BASPO	**3** (6%)	3 (6%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	BABS	**15** (30%)	3 (6%)	0 (0%)	12 (24%)	0 (0%)	0 (0%)	0 (0%)
	swisstopo	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	OA	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	Total	**50** (100%)	**18** (36%)	**0** (0%)	**20** (40%)	**1** (2%)	**8** (16%)	**3** (6%)

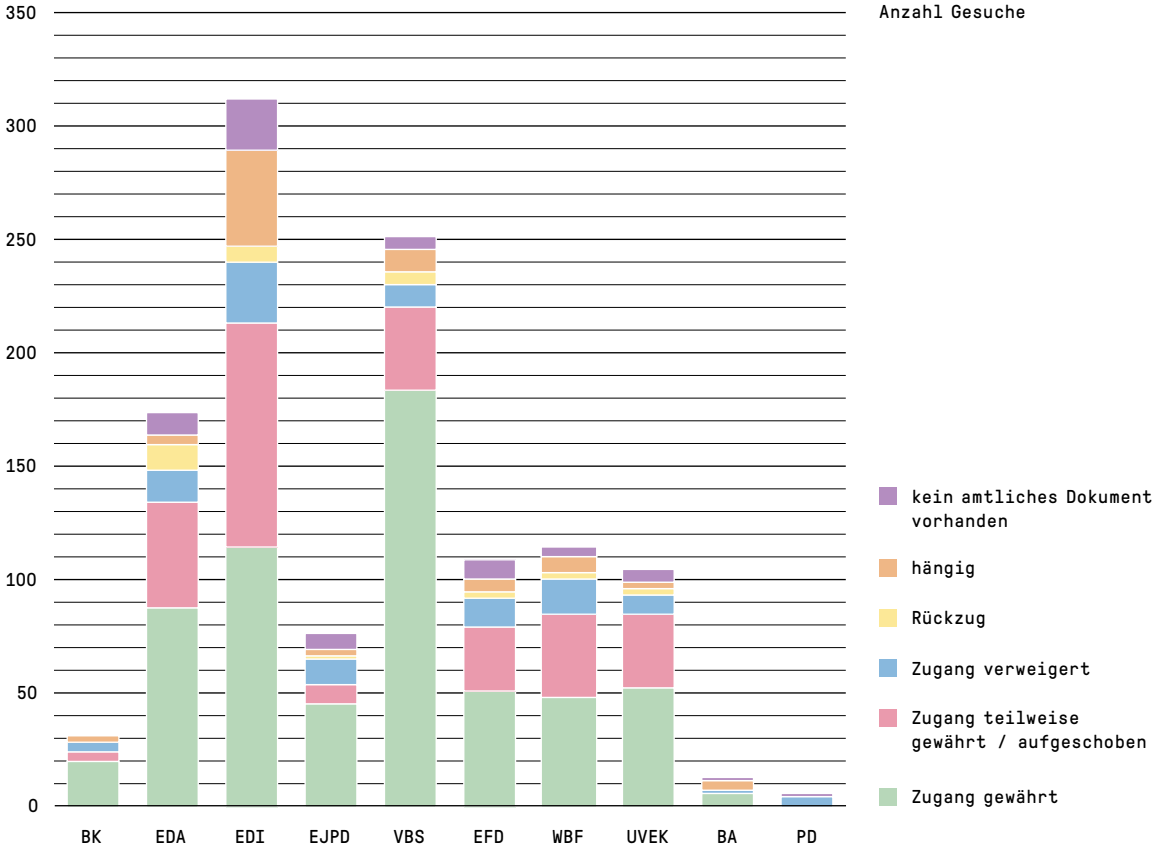
	Betroffener Fachbereich	Gesuche im Zusammenhang mit COVID-19	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt/aufgeschoben	Zugangsgesuch zurückgezogen	Zugangsgesuch hängig	kein amtliches Dokument vorhanden
Eidg. Departement für Wirtschaft, Bildung und Forschung WBF	GS WBF	**2** (8%)	2 (8%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	SECO	**14** (56%)	5 (20%)	7 (28%)	2 (8%)	0 (0%)	0 (0%)	0 (0%)
	SBFI	**1** (4%)	1 (4%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	BLW	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	BWL	**5** (20%)	2 (8%)	0 (0%)	2 (8%)	0 (0%)	0 (0%)	1 (4%)
	BWO	**3** (12%)	0 (0%)	0 (0%)	3 (12%)	0 (0%)	0 (0%)	0 (0%)
	PUE	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	WEKO	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	ZIVI	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	BFK	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	SNF	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	EHB	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	ETH	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	InnoSuisse	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	Total	**25** (100%)	**10** (40%)	**7** (28%)	**7** (28%)	**0** (0%)	**0** (0%)	**1** (4%)
Bundesanwaltschaft BA	BA	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	Total	**0** (0%)	**0** (0%)	**0** (0%)	**0** (0%)	**0** (0%)	**0** (0%)	**0** (0%)
Parlamentsdienste PD	PD	**4** (100%)	0 (0%)	3 (75%)	0 (0%)	0 (0%)	0 (0%)	1 (25%)
	Total	**4** (100%)	**0** (0%)	**3** (75%)	**0** (0%)	**0** (0%)	**0** (0%)	**1** (25%)

Anzahl Schlichtungsgesuche nach Kategorien der Antragssteller

Kategorie Antragsteller	2020
Medien	**31**
Privatpersonen (bzw. keine genaue Zuordnung möglich)	**42**
Interessenvertreter (Verbände, Organisationen, Vereine usw.)	**5**
Rechtsanwälte	**7**
Unternehmen	**7**
Universitäten	**1**
Total	**93**

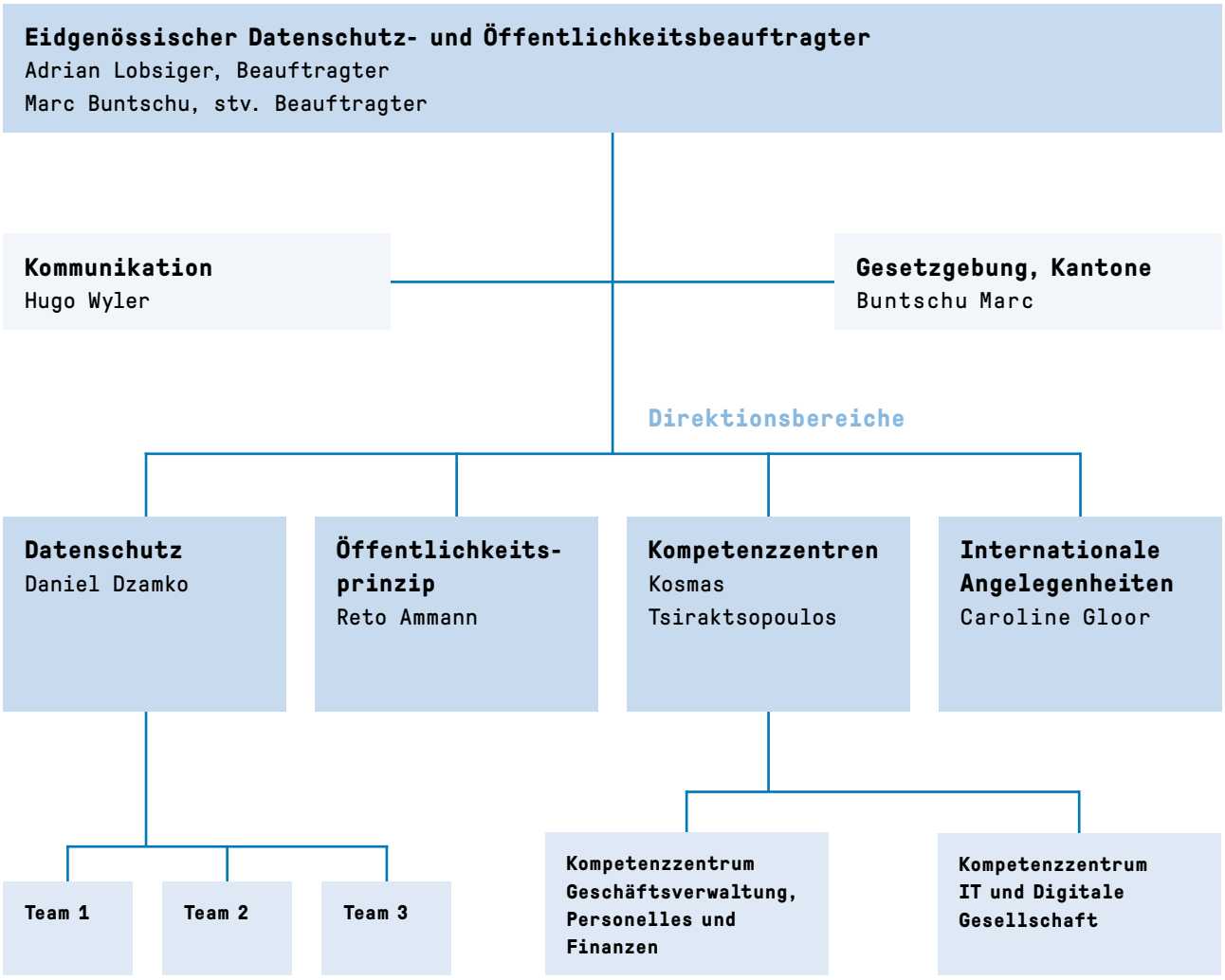
Zugangsgesuche der gesamten Bundesverwaltung vom 1. Januar bis 31. Dezember 2020





3.4 Organisation EDÖB (Stand 31. März 2021)

Organigramm



Mitarbeiter und Mitarbeiterinnen des EDÖB

Anzahl Mitarbeitende	38		
FTE	31.8		
nach Geschlecht	Frauen	20	53 %
	Männer	18	47 %
nach Beschäftigungsgrad	1–89 %	25	63 %
	90–100 %	13	37 %
nach Sprache	Deutsch	30	79 %
	Französisch	7	18 %
	Italienisch	1	3 %
nach Alter	20–49 Jahre	24	63 %
	50–65 Jahre	14	37 %
Kaderpositionen	Frauen	3	33 %
	Männer	6	67 %

Abkürzungsverzeichnis

AHVN13 13-stellige AHV-Nummer

BCR verbindliche Unternehmensregeln

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

BGÖ Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsgesetz BGÖ)

Konvention 108+ Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Datareg Register der Datensammlungen

DSG Datenschutzgesetz

DSGVO EU-Datenschutzgrundverordnung

EDSA Europäischer Datenschutzausschuss

EDSB Europäischer Datenschutzbeauftragter

EpG Bundesgesetz über die Bekämpfung übertragbarer Krankheiten des Menschen (Epidemiengesetz)

EPD Elektronisches Patientendossier

EPDG Bundesgesetz über das elektronische Patientendossier

EuGH Europäischen Gerichtshofs

GPA Internationale Konferenz der Datenschutzbeauftragten

IKT Informations- und Kommunikationstechnologien

KI Künstliche Intelligenz

NaDB Programm Nationale Datenbewirtschaftung

NCSC Nationales Zentrum für Cybersicherheit

NDB Nachrichtendienst des Bundes

PBG Personenbeförderungsgesetz

PNR Flugpassagierdaten

Privatim Konferenz der Schweizer Datenschutz-Beauftragten (kantonale Datenschutzbehörden)

SCC Standardvertragsklauseln

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

Abbildungsverzeichnis

Grafiken

Tabellen

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. 410.028.D

Layout: Ast & Fischer AG, Wabern
Fotografie: Nicolas Stadler
Schriften: Pressura, Documenta
Druck: Ast & Fischer AG, Wabern
Papier: PlanoArt®, holzfrei hochweiss

MIX
Papier aus verantwortungsvollen Quellen
FSC® C004050

Kennzahlen

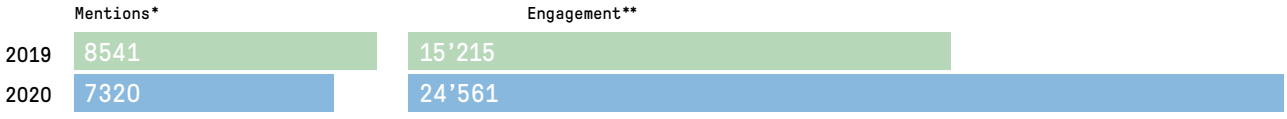
Leistungen Datenschutz

57,8 %	15,0 %	19,4 %	7,3 %
Beratung	Aufsicht	Information	Gesetzgebung

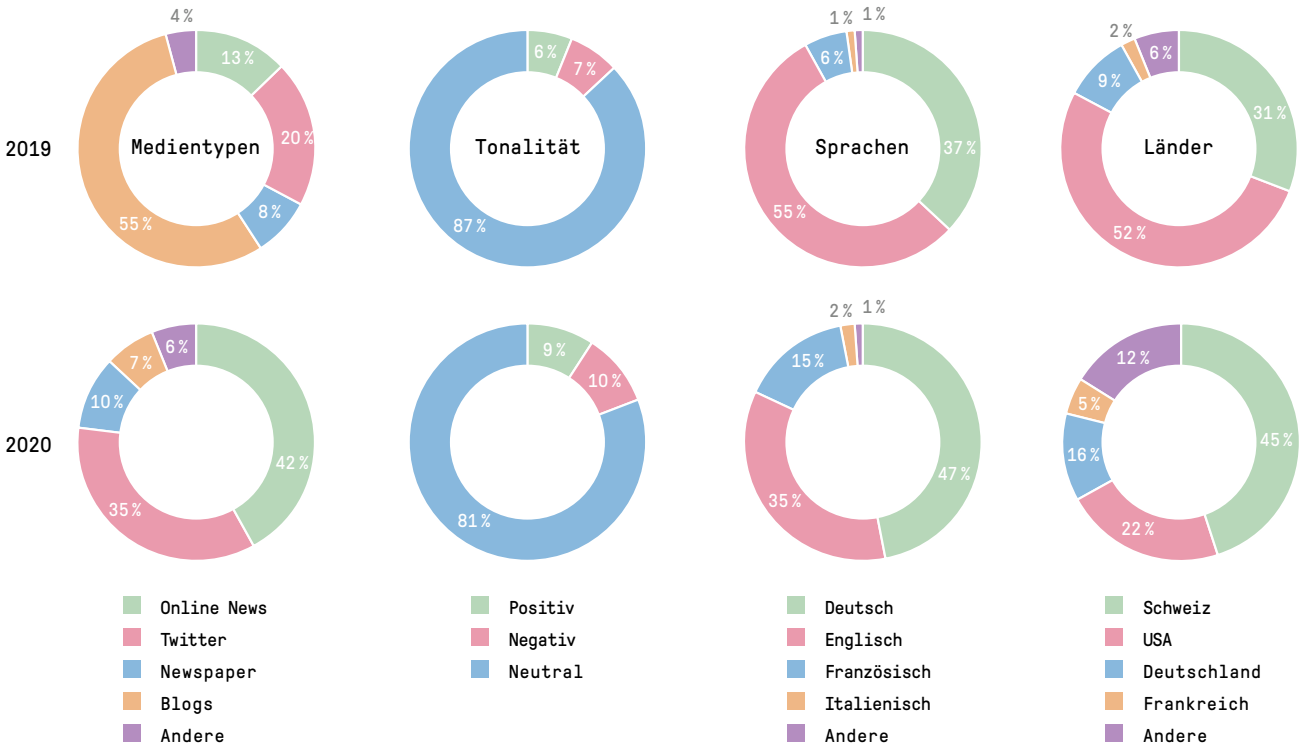
Zugangsgesuche Öffentlichkeitsprinzip (BGÖ)

51 %	25 %	9 %	3 %	7 %	5 %
gewährt	teilweise gewährt/ aufgeschoben	verweigert	Rückzug	hängig	kein amtliches Dokument vorhanden

Mediale Resonanz des Beauftragten im Social Web



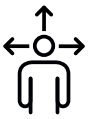
* Anzahl aller Erwähnungen des EDÖB (sog. Mentions auf Blogs, Twitter, Onlinenews, etc.)
** Anzahl aller Interaktionen (Likes, Retweets, etc.)



Anliegen des Datenschutzes

Faire Information

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



Wahlmöglichkeit

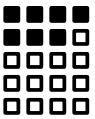
Betroffene geben ihre Einwilligung informiert und erhalten eine echte Wahlfreiheit.

Risikoanalyse

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

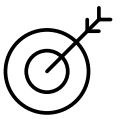
Datenrichtigkeit

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, 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.

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