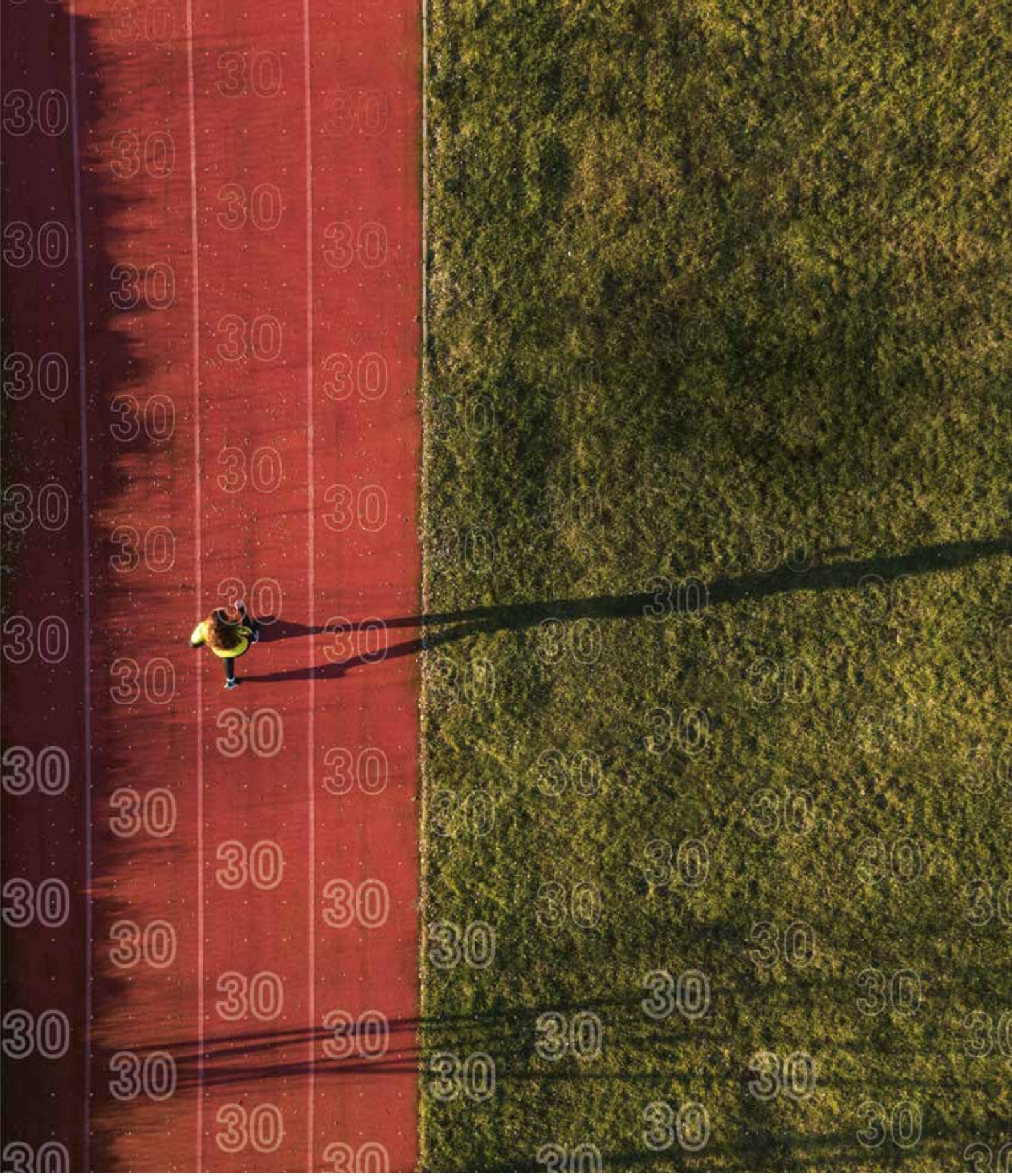


30. Tätigkeitsbericht 2022/23

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Tätigkeitsbericht 2022/2023
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 für den Bereich Datenschutz den Zeitraum zwischen 1. April 2022 und 31. März 2023 ab. Für den Bereich Öffentlichkeitsprinzip entspricht er dem Kalenderjahr 1. Januar bis 31. Dezember 2022.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Vorwort

Am 1. Juli 1993 trat das erste Bundesgesetz über den Datenschutz vom 19. Juni 1992 in Kraft. Bereits in der Gesetzesbotschaft von 23. März 1988 hatte der Bundesrat den gesetzgeberischen Handlungsbedarf mit dem «Einsatz der modernen Informations- und Kommunikationstechnologien in fast allen Lebensbereichen und der enormen Intensivierung der Datenverarbeitung und Verbreitung in Gesellschaft, Wirtschaft und Staat» begründet.

30 Jahre später spielt sich unser Alltag in einer digitalen Realität ab, wie sie damals nicht vorausgesehen werden konnte. Das Smartphone und die permanente Verbindung mit dem Internet, über das die digitale Gesellschaft von heute die Verrichtungen des Alltags vom Banking bis zum Dating «online» abwickelt, hat den Umfang und die Intensität, mit der personenbezogene Informationen bearbeitet werden, um Potenzen erhöht.

Am 1. September 2023 kann das totalrevidierte Bundesgesetz über den Datenschutz vom 25. September 2020 in Kraft treten. Mit diesem Erlass stellt der Gesetzgeber der Wirtschaft, der Bundesverwaltung und der Datenschutzaufsicht des Bundes neue Instrumente zur Verfügung, um den berechtigten Erwartungen der Bevölkerung an einen rechtsstaatlichen und robusten Schutz ihrer Privatsphäre und informationellen Selbstbestimmung in zeitgemässer Weise gerecht zu werden.

Die Arbeiten des EDÖB-Teams zur Vorbereitung des Übergangs zum neuen Recht sind in vollem Gang und verlaufen weiterhin plangemäss (s. Schwerpunkt).

Adrian Lobsiger
Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter

Bern, den 31. März 2023

Aktuelle Herausforderungen 6

Datenschutz

1.1 **Digitalisierung und Grundrechte** 14

- Cloud Strategie Bund: Herausforderndes Cloud-Projekt der Bundeskanzlei
- Nationale Datenbewirtschaftung: Projekt «SpiGes» des BFS
- Zertifizierung: Neue Verordnung über die Datenschutzzertifizierungen
- Wahlen und Abstimmungen: Aktualisierung des bestehenden Leitfadens
- E-ID: Self-Sovereign-Identity-Ansatz
- Onlineportal Post: Zugang nur noch mit SwissID möglich
- Strategie Digitale Schweiz: Projekt digitaler Führerausweis

Schwerpunkt 18

30 Jahre Datenschutz in der Schweiz

1.2 **Justiz, Polizei, Sicherheit** 26

- BAZG: Zollgesetz
- Schutzstatus S: Web-Applikation «RegisterMe»
- Mitto AG: Vorabklärung zu einer möglichen missbräuchlichen Verwendung des «Signalling System»-Zugangs

1.3 **Handel und Wirtschaft** 30

- Datenbekanntgabe an ausländische Steuerbehörden: Bundesgericht entscheidet gegen das Recht auf Information von Drittpersonen in der internationalen Steueramtshilfe
- Tracking-Technologien: Prüfung möglicher Persönlichkeitsverletzung der Schweizer Bevölkerung durch Oracle
- Postfinance: Verzicht auf Kontoöffentlichkeit
- Bonitätsauskünfte: Datenbankeinträge gestützt auf «negative Haushaltstreffer»
- Cyberangriff: Vorabklärung bei Infopro AG und Fiducial Winbiz SA
- Vorabklärung bei einem Voice-Dienst: Sicherheitsschwachstelle wurde rasch behoben
- Dating App: Analyse der Datenbearbeitungen
- Virtuelle Läufe: Verbesserter Datenschutz bei einem Lauf-Anbieter

1.4 **Gesundheit** 37

- Nationales Organspenderegister: Online-Authentifizierung mangelhaft
- Onlineregister: Datenschutzrisiken beim Brustimplantatregister
- Mangelnde Datensicherheit: Sachverhaltsabklärung zur Datenbank privater Covid-19-Testzentren
- Online-Plattform: Projekt Datenrettung «meineimpfungen.ch»
- Elektronisches Patientendossier: Neue Entwicklungen
- Elektronischer Rechnungsversand: Pflicht zur Zustellung einer Kopie der Arztrechnung
- Elektronischer Rechnungsversand: Entwurf betreffend die elektronische Rechnungsübermittlung im Bereich der obligatorischen Krankenpflegeversicherung

1.5 **Arbeit** 47

- Bundespersonal: Aufbewahrung von Personaldossiers beim BFS

1.6 **Verkehr** 48

- SBB: Kundenfrequenzmesssystem an Bahnhöfen

1.7 **International** 50

- Europa: Europarat
- Europa: Europäische Konferenz der Datenschutzbeauftragten in Dubrovnik
- Europa: European Case Handling Workshop
- International: Global Privacy Assembly
- GPA: Arbeitsgruppe Entwicklungshilfe
- AFAPDP: Französischsprachige Vereinigung der Datenschutzbehörden
- Bilateral: Empfang einer tunesischen Delegation
- Internationale Zusammenarbeit: Privacy Symposium in Venedig
- Schengen: Border Travel and Law Enforcement Group
- Schengen: Aufsichtskoordinationsgruppen über die Informationssysteme SIS II, VIS und Eurodac
- Schengen: Schengen Koordinationsgruppe der schweizerischen Datenschutzbehörden
- Schengen: Tätigkeiten betreffend Schengen auf nationaler Ebene

Öffentlichkeitsprinzip

2.1 **Allgemein** ... 62

2.2 **Zugangsgesuche – leichter Rückgang im Jahr 2022** ... 64

2.3 **Schlichtungsverfahren – leichter Rückgang der Schlichtungsanträge** ... 68
- Anteil einvernehmlicher Lösungen
- Dauer der Schlichtungsverfahren
- Anzahl hängiger Fälle

2.4 **Gesetzgebungsverfahren** ... 72
- Cybersicherheit: Änderung des Informationssicherheitsgesetzes (ISG)
- Strombranche: Vorentwurf des Bundesgesetzes über einen Rettungsschirm für die Elektrizitätswirtschaft
- Archivierungsgesetz: Notwendigkeit einer Revision des Bundesgesetzes über die Archivierung
- Finanzen: Inkraftsetzung Geldwäschereigesetz und Geldwäschereiverordnung
- Tabakproduktegesetz: Teilrevision des Bundesgesetzes über Tabakprodukte und elektronische Zigaretten (TabPG)
- Wirtschaft: Neues Bundesgesetz für die Prüfung ausländischer Investitionen

2.5 **Spezialgesetzliche Vorbehalte nach Art. 4 BGÖ** ... 80

Der EDÖB

3.1 **Aufgaben und Ressourcen** ... 85
- Leistungen und Ressourcen im Bereich Datenschutz
- Leistungen und Ressourcen im Bereich Öffentlichkeitsgesetz
- Teilnahme an Kommissionsberatungen und Anhörungen durch parlamentarische Kommissionen

3.2 **Kommunikation** ... 88
- Zahlen
- Themenschwerpunkte
- Datenweitergabe und Datenhandel
- Neue Website

3.3 **Statistiken** ... 90
- Statistiken über die Tätigkeiten des EDÖB vom 1. April 2022 bis 31. März 2023 (Datenschutz)
- Übersicht der Zugangsgesuche vom 1. Januar bis 31. Dezember 2022
- Statistiken über Zugangsgesuche nach Öffentlichkeitsgesetz vom 1. Januar bis 31. Dezember 2022
- Zugangsgesuche 2022 mit Corona-Bezug
- Anzahl Schlichtungsgesuche nach Kategorien der Antragstellenden
- Zugangsgesuche der gesamten Bundesverwaltung vom 1. Januar bis 31. Dezember 2022

3.4 **Organisation EDÖB** ... 100
- Organigramm
- Mitarbeiter und Mitarbeiterinnen des EDÖB

Abkürzungsverzeichnis ... 102

Abbildungsverzeichnis ... 103

Impressum ... 104

Umschlag
- Kennzahlen
- Anliegen des Datenschutzes

Aktuelle Herausforderungen

I Digitalisierung

Digitale Verantwortung

Die digitale Transformation ist eine gesamtgesellschaftliche Erscheinung und geht mit wichtigen Fragestellungen einher, welche die Behörden, Unternehmen sowie Bürgerinnen und Nutzer betreffen. Statt einer blinden Unterwerfung unter die technologische Entwicklung, gilt es über die Analyse von Prozessen für einen verantwortungsvollen Einsatz digitaler Technologie im Dienst der Menschen zu sorgen.

Von zentraler Bedeutung ist in diesem Kontext die digitale Verantwortung – ein breitgefächertes Konzept, in das namentlich finanztechnische, rechtliche, ökologische, gesellschaftliche und ethische Betrachtungen einfliessen. Weil das Entwicklungspotenzial der Digitalisierung auch die Datenbearbeitungsverantwortlichen neuen Risiken aussetzt, gehört aus Sicht des EDÖB die digitale Verantwortung fortan zur guten Führung. Die Einhaltung des Datenschutzgesetzes, die den Schutz von Persönlichkeitsrechten bei der Bearbeitung von Personendaten gewährleistet, ist Teil dieser Verantwortung.

Die Revision des Bundesgesetzes über den Datenschutz (s. Schwerpunkt) verpflichtet die Bearbeitungsverantwortlichen zu einer proaktiven Herangehensweise bei der Umsetzung automatisierter Bearbeitungen und der Digitalisierung. Das neue Gesetz bietet ihnen Instrumente für globale und spezifische Analysen der Bearbeitungen und Techniken sowie zur Herstellung von Transparenz, Vertrauen und Glaubwürdigkeit gegenüber den betroffenen Personen. Auch wenn es bei der Bearbeitung von Personendaten kein Nullrisiko geben muss, können mit diesen Instrumenten Bearbeitungsverantwortliche Restrisiken ermitteln, mindern und eigenverantwortlich eingehen und mit diesem Vorgehen die Privatsphäre und die informationelle Selbstbestimmung aller Betroffenen gewährleisten.

Auch bei der technischen Sicherheit spielt proaktives Denken eine entscheidende Rolle; gilt es doch, Cyberangriffen mit vorausschauenden Massnahmen zu begegnen. Unrühmliche Beispiele wie Meineimpfungen oder Swisstransplant in Kapitel 1.4 zeigen, dass die Regeln und Instrumente des neuen Rechts zur Wahrung der Grundrechte und der digitalen Verantwortung unerlässlich sind.

Aufsichtsrechtliche Beratung und Projektführung mit risikobasiertem Ansatz

Die praktische Bedeutung des Konzepts der digitalen Verantwortung als unternehmerische Selbstverantwortung offenbart sich bei den aufsichtsrechtlichen Beratungsleistungen, die der

«Als Aufsichtsbehörde für Datenschutz erteilt der EDÖB keine Bewilligungen.»

EDÖB gegenüber den Verantwortlichen digitaler Projekte der Wirtschaft erbringt: Privaten ist die Bearbeitung von Personendaten nach der schweizerischen Datenschutzgesetzgebung grundsätzlich erlaubt und bedarf auch keiner behördlichen Bewilligung.

Als Aufsichtsbehörde für Datenschutz erteilt der EDÖB somit keine Bewilligungen. Im Rahmen seiner Beratungen wirkt er darauf hin, dass die Vorgaben der Datenschutzgesetzgebung eingehalten werden, was aber nichts daran ändert, dass die Durchführung der Projekte in der alleinigen Verantwortung der Projekteigner liegt. Gleichzeitig sensibilisiert der EDÖB die Eigner für Aspekte ihrer digitalen Verantwortung, die unter Umständen über die Vorgaben der Datenschutzgesetzgebung hinausgehen können: Zu denken ist etwa an «psychologische Emissionen», die von Sensoren ausgehen können, die Private in Arbeitsbereichen, Läden oder kommerziellen Begegnungszonen einsetzen. Der sog. «Chilling Effekt» kann dazu führen, dass die Menschen ihr Verhalten an die Anwesenheit von Sensoren anpassen und so in ihrer selbstbestimmten Lebensführung eingeschränkt werden. Zum «Chilling Effekt» beitragen kann nebst der Anzahl von Sensoren eine für die Betroffenen schwer überschaubare Vermengung von Zwecken, zu denen die über die Sensoren beschafften Daten weiterverarbeitet werden. Inwieweit sich die Projektverantwortlichen mit Blick auf den «Chilling Effekt» im Rahmen des datenschutzrechtlich Vertretbaren beim Einsatz der Sensorik Zurückhaltung auferlegen sollen, ist primär eine Frage der Unternehmensstrategie resp. der digitalen Selbstverantwortung (s. dazu Kap. 1.6 Verkehr).

Indessen hat der Gesetzgeber des neuen DSG der digitalen Selbstverantwortung auch Grenzen gesetzt, die der Beauftragte durch eine Verstärkung seiner aufsichtsrechtlichen Tätigkeit durchsetzen wird. Wenn sich für die Projektverantwortlichen bei der Planung abzeichnet, dass eine zukünftige Bearbeitung potenziell mit einem hohen Risiko verbunden sein dürfte, verpflichtet sie das neue DSG, rechtzeitig eine sog. Datenschutz-Folgenabschätzung oder DSFA durchzuführen, das sich abzeichnende Risiko näher zu evaluieren und angemessene Schutzmassnahmen zu dessen Senkung vorzusehen. Führt die Evaluation im

«Der ‹Chilling Effekt› kann dazu führen, dass die Menschen in ihrer selbstbestimmten Lebensführung eingeschränkt werden.»

Rahmen der DSFA zur Prognose, dass das potenziell hohe Anfangsrisiko der Bearbeitung nach Durchführung der als angemessen erachteten Schutzmassnahmen hoch bleibt, schliesst das neue DSG zwar immer noch nicht aus, dass die Bearbeitung trotzdem durchgeführt werden darf. Allerdings verlangt das Gesetz bei dieser Risikoeinschätzung, dass die Verantwortlichen vorgängig den EDÖB einschalten und ihm ihre DSFA vorlegen.

Der EDÖB prüft sodann, ob die ihm vorliegende DSFA die ausgewiesenen Risiken verständlich, nachvollziehbar und vollständig ausweist und ob die geplante Bearbeitung unter Berücksichtigung der auszuweisenden Risiken mit den Vorgaben der Datenschutzgesetzgebung als Ganzes vereinbar ist, indem sie sich hinsichtlich des geplanten Umfangs und der Intensität als für die Betroffenen zumutbar und somit insgesamt als vertretbar erweist. Der Beauftragte teilt dem Verantwortlichen innert zwei Monaten allfällige Einwände und Änderungsvorschläge mit. Diese können sich sowohl auf die Ausgestaltung der DSFA als auch die geplante Bearbeitung beziehen. Ersteres kommt in der Praxis vor, wenn der Verantwortliche davor zurückscheut, imminente Risiken angemessen zu bewerten und transparent auszuweisen. Die Stellungnahme des EDÖB mündet nicht in einer Bewilligung eines geplanten Vorhabens.

Weigert sich ein Verantwortlicher, wichtige Einwände und Anregungen des EDÖB zu befolgen, kann Letzter aufsichtsrechtlich tätig werden, eine Untersuchung eröffnen und angeregte Ergänzungen oder Änderungen bis hin zum Verbot der Bearbeitung zu gegebener Zeit formell verfügen. Ein formelles Tätigwerden des EDÖB ist angezeigt, wenn der Verantwortliche den Betroffenen die Inkaufnahme eines Risikos namentlich aufgrund der Eintretenswahrscheinlichkeit und Schwere der Persönlichkeitsverletzungen nicht zumuten darf und sich die geplante Bearbeitung demzufolge datenschutzrechtlich als unzulässig erweist. So etwa, wenn mit der Realisierung einer Bearbeitung mit hohem Restrisiko datenschutzrechtliche Grundsätze nach Art. 6 nDSG wie die Verhältnismässigkeit oder Vorgaben an die technische Sicherheit nach Art. 8 nDSG verletzt würden.

«Der Gesetzgeber des neuen DSG hat der digitalen Selbstverantwortung Grenzen gesetzt, die der Beauftragte durch eine Verstärkung seiner aufsichtsrechtlichen Tätigkeit durchsetzen wird.»

II Wachsende Anzahl spezialgesetzlicher Ausnahmen vom BGÖ und Notrecht

In der Notverordnung vom 16. März 2023 über zusätzliche Liquiditätshilfe-Darlehen und die Gewährung von Ausfallgarantien des Bundes für Liquiditätshilfe-Darlehen der Schweizerischen Nationalbank an systemrelevante Banken hat der Bundesrat u. a. festgehalten, dass der Zugang zu amtlichen Dokumenten nach Öffentlichkeitsgesetz ausgeschlossen ist. Der Ausschluss der vom Öffentlichkeitsgesetz garantierten Zugangsrechte der Bürgerinnen und Bürger über den Weg einer notrechtlichen Verordnung wirft grundsätzliche Rechtsfragen auf.

Nach der von notrechtlichen Entscheiden geprägten Phase der Pandemie und dem Rettungsschirm für die Stromwirtschaft hat der Bundesrat mit der erwähnten Verordnung vom 16. März 2023 innert kurzer Zeit ein weiteres Mal Tätigkeiten, die er seiner Verwaltung mittels Notrechts übertrug, mit dem gleichen Notrecht dem Öffentlichkeitsgesetz entzogen. Beide Fälle können den Einsatz von Steuergeldern in der Grössenordnung von Milliarden von Franken nach sich ziehen.

Das Vorgehen des Bundesrates wirft grundsätzliche Rechtsfragen auf: Aus der Begründung für den Erlass des unmittelbar auf die Bundesverfassung gestützten Notrechts zur Stützung der Elektrizitäts- oder Finanzwirtschaft lässt sich aufgrund der dem EDÖB zurzeit vorliegenden Informationen in keinem dieser Fälle eine Notwendigkeit ableiten, über den Weg des Notrechts auch noch den Anspruch der Bürgerinnen und Bürger aufzuheben, das notrechtliche Wirken der Verwaltung nachvollziehen zu können. Wenn sich keine Notwendigkeit zur notrechtlichen Einschränkung der Bürgerrechte nach dem Öffentlichkeitsgesetz ergibt, stellt sich die Frage, woraus der Bundesrat das Recht ableitet, dieses Bundesgesetz auf dem Verordnungsweg aufzuheben.

Im Falle der Fortgeltung des Öffentlichkeitsgesetzes wäre der Bundesverwaltung in beiden Fällen offen gestanden, den Zugang zu amtlichen Dokumenten nach diesem Gesetz unter Anrufung des Schutzes öffentlicher und privater Interessen einzuschränken oder zumindest so lange aufzuschieben, bis die Bundesversammlung im ordentlichen Gesetzgebungsverfahren über den Ausschluss der Verwaltungstransparenz befinden und – sofern sie einen solchen für nötig erachtet – im formellen Gesetz verankern kann.

Angesichts der beschleunigt anwachsenden Anzahl der spezialgesetzlichen Ausschlüsse des BGÖ hat sich der Beauftragte entschlossen, ab diesem Tätigkeitsbericht eine Tabelle zu publizieren, in der fortan der aktuelle Stand dieser Ausschlüsse ausgewiesen wird (s. Kap. 2.5).

«Der Ausschluss der vom Öffentlichkeitsgesetz garantierten Zugangsrechte der Bürgerinnen und Bürger über den Weg einer notrechtlichen Verordnung wirft grundsätzliche Rechtsfragen auf.»

III Nationale und internationale Kooperation

Ausbau der Zusammenarbeit mit den Kantonen

Die Komplexität der Bearbeitung von Personendaten nimmt mit dem fortschreitenden digitalen Wandel zu, denn sie führt eine Vielzahl von öffentlichen und privaten Akteuren zusammen und bringt eine Zunahme der Bearbeitung von Datenkaskaden durch Dritte mit sich. Die jüngsten Meldungen über Cyberangriffe und Verletzungen der Datensicherheit, beispielsweise der Fall Infopro und Winbiz, verdeutlichen diese Entwicklung (s. Kap. 1.3).

Die Datenschutzbehörden von Bund und Kantonen streben eine Intensivierung der Zusammenarbeit an, um eine wirksame und umfassende Aufsicht zu gewährleisten, namentlich aufgrund der Berührungspunkte zwischen den Datenschutzgesetzen des Bundes und der Kantone. Konkret geht es dabei etwa um Fälle, in denen kantonale oder kommunale Behörden private Auftragsdatenbearbeiter einsetzen; ebenso, wenn private oder öffentliche Stellen sowohl privatrechtlich als auch hoheitlich tätig werden oder kantonale Regelungen vorliegen, nach denen das Bundesgesetz über den Datenschutz anwendbar ist. Auch um die digitale Transformation unter Wahrung der Zuständigkeiten und der Unabhängigkeit aller Beteiligten gemeinsam anzugehen, hat der EDÖB die Intensivierung der Zusammenarbeit mit seinen kantonalen und kommunalen Amtskollegen in den Bereichen Datenschutz und Öffentlichkeitsgesetz in seine Strategie für 2023 aufgenommen.

Im Hinblick auf die eidgenössischen Wahlen 2023 erneuerte der EDÖB zusammen mit der Konferenz der schweizerischen Datenschutzbeauftragten (privatim) den Leitfaden zur digitalen Bearbeitung von Personendaten im Rahmen von Wahlen und Abstimmungen (s. Kap. 1.1).

Ausserdem werden die Datenschutzbehörden an der Cloud-Thematik weiterarbeiten und sich dabei namentlich der Übermittlung von Datenbanken, Applikationen und dem Verschieben von On-Premise-Lösungen in die Cloud widmen. Der EDÖB verfolgt die diesbezüglichen Entwicklungen in der Europäischen Union aufmerksam und pflegt den Austausch mit den massgeblichen Akteuren.

«Die Datenschutzbehörden von Bund, Kantonen und Gemeinden streben eine Intensivierung der Zusammenarbeit an.»

Europarat

Der beratende Ausschuss für das Übereinkommen zum Schutz des Menschen bei der Verarbeitung personenbezogener Daten (Übereinkommen 108) des Europarates steht auch Staaten offen, die nicht Mitglied des Europarates sind. Das ausserordentliche Ausscheiden Russlands aus dem Europarat führte dazu, dass sich der beratende Ausschuss mit der Frage der weiteren Teilnahmebedingungen in solchen Fällen befasste (s. Kap. 1.7). Eine aktive Teilnahme beim Ausschuss ist insbesondere im Hinblick auf das modernisierte Übereinkommen 108 (sogenanntes Übereinkommen 108+) von Bedeutung. Dieses gilt als wichtiges Instrument, das eine «Brücke» zwischen den verschiedenen Regionen der Welt und den verschiedenen nationalen Gesetzgebungen bildet. Der EDÖB bringt sich im Ausschuss weiterhin aktiv ein.

Internationale Kooperation

Die Datenbekanntgabe von Personendaten in ein Land ohne angemessenes Datenschutzniveau wirft in verschiedenen Staaten ähnliche datenschutzrechtliche Fragen auf. Der EDÖB verfolgt diesbezüglich insbesondere die Entwicklung in der EU und in den Mitgliedstaaten der EU resp. des EWR, insbesondere auch in Zusammenhang mit den Gesprächen, welche die EU diesbezüglich mit den USA führt.

Evaluation des Datenschutzniveaus

Die Schweiz wartet immer noch darauf, dass die EU dem Schweizer Datenschutzrecht ein angemessenes Schutzniveau nach der im Jahre 2018 in Kraft getretenen DSGVO zuerkennt. In der Zwischenzeit bleibt der Angemessenheitsbeschluss aus dem Jahre 2000 weiterhin in Kraft. Dieser erfolgte gestützt auf die frühere Datenschutzrichtlinie 95/46/EG, welche durch die DSGVO ersetzt wurde. Es ist damit zu rechnen, dass die EU-Kommission die Angemessenheitsberichte sämtlicher Staaten, welche bereits vor der DSGVO als angemessen galten, (Andorra, Argentinien, Kanada [kommerzielle Organisationen], Färöer-Inseln, Guernsey, Israel, Insel Man, Jersey, Neuseeland, Uruguay) gleichzeitig veröffentlichen wird. Es ist zu hoffen, dass die EU-Kommission ihren neuen Angemessenheitsbeschluss für die Schweiz im Laufe des Jahres 2023 treffen wird.

«Es ist zu hoffen, dass die EU-Kommission ihren neuen Angemessenheitsbeschluss für die Schweiz im Laufe des Jahres 2023 treffen wird.»

Datenschutz

1.1 Digitalisierung und Grundrechte

CLOUD-STRATEGIE DES BUNDES

Herausforderndes Cloud-Projekt der Bundeskanzlei

Im Berichtsjahr befasste sich der EDÖB mit Fragen im Zusammenhang mit der Umsetzung der Cloud-Strategie der Bundesverwaltung. Er nahm an mehreren Ämterkonsultationen teil und beriet die Bundeskanzlei bei ihrem Projekt Cloud Enabling Büroautomation CEBA.

Der Bereich Digitale Transformation und IKT-Lenkung (DTI) der Bundeskanzlei unterbreitete dem EDÖB in einer Ämterkonsultation die Cloud-Prinzipien, die Teil der Cloud-Strategie der Bundesverwaltung sind. Diese sollen den einzelnen Verwaltungseinheiten als Empfehlungen für die Beschaffung von Cloud-Anwendungen dienen.

Der EDÖB forderte u. a., dass die Empfehlungen des DTI als verbindliche Mindestvorgaben gelten sollten, die durch die Departemente erweitert, aber nicht abgeschwächt werden dürften. Weiter stellte der EDÖB fest, dass die Prinzipien stark von der Sichtweise der Informationssicherheit geprägt waren und damit dem Datenschutz nicht in geeigneter Weise Rechnung trugen. So beruhten diese insbesondere auf einer Unterscheidung zwischen besonders schützenswerten und übrigen Personendaten, die nach Auffassung des EDÖB ein beschränkt taugliches Kriterium darstellt, um die Risiken für die Persönlichkeit und Grundrechte der betroffenen Personen zu evaluieren. Dies zumal auch die Kombination von Personendaten, die nicht besonders schützenswert sind, zu hohen Bearbeitungsrisiken führen kann. Hohe Risiken können sich namentlich bei Verwendung neuer Technologien oder aus der Art, dem Umfang, den Umständen und dem Zweck der Bearbeitung ergeben. Indikatoren also, die bei Cloud-Auslagerungen oft vorhanden sind. Der EDÖB hat deshalb darauf hingewirkt, dass die Cloud-Prinzipien eine Datenschutz-Folgenabschätzung vorsehen, wenn Personendaten in der Cloud bearbeitet werden sollen.

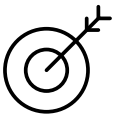
Der Bereich DTI hat den EDÖB in seine Vorarbeiten zur Einführung von Microsoft 365 einbezogen, indem er ihm insbesondere die Entwürfe einer Rechtsgrundlageanalyse und des ISDS-Konzepts unterbreitete. In seinen Stellungnahmen hat der Beauftragte u. a. dargelegt, dass seines Erachtens ungewiss ist, wie lange es technisch durchsetzbar bleibt, ausgewählte Applikationen in eigenen Bundeszentren statt in der vom US-Konzern Microsoft betriebenen Cloud ausführen zu lassen, wie dies das Projekt des DTI heute noch vorsieht. Angesichts dieser Ungewissheit verlangte der Beauftragte, es seien datenschutzrechtlich vorteilhaftere Alternativen zu Microsoft 365 aufzuzeigen. Bezüglich der Rechtsgrundlagenanalyse fordert er, dass eingehender geprüft werde, ob eine genügende Rechtsgrundlage für die Personendatenbearbeitungen in der vom US-Konzern betriebenen Cloud besteht und ob der Grundsatz der Verhältnismässigkeit gewahrt bleibt. Hinsichtlich der Aussonderung von besonders schützenswerten Personendaten durch die Nutzerinnen und Nutzer verbleiben aus Sicht des Beauftragten offene Fragen zu deren Zweckmässigkeit und praktischen Durchführbarkeit. Schliesslich verlangt er vom DTI die Erstellung einer umfassenden Datenschutz-Folgenabschätzung, welche die Risiken der Auslagerung in die Cloud transparent ausweist. Dabei erachtet es der EDÖB als unumgänglich, dass die Problematik von möglichen Zugriffen der US-Sicherheitsbehörden auf Personendaten, welche die Bundesverwaltung in der Cloud von Microsoft bearbeiten lässt, vertieft analysiert wird.

NATIONALE DATENBEWIRTSCHAFTUNG

Projekt «SpiGes» des BFS

Im Berichtsjahr unterbreitete das BFS dem EDÖB einen Bericht zum Stand des Projekts zur Mehrfachnutzung der Daten aus stationären Spitalaufenthalten (SpiGes). Der EDÖB wies auf die datenschutzrechtlichen Risiken dieses Teilprojektes des Programms Nationale Datenbewirtschaftung (NaDB) hin und verlangte die Ausarbeitung von entsprechenden Schutzmassnahmen bei der konkreten Umsetzung.

Das Programm Nationale Datenbewirtschaftung (NaDB) wurde im Oktober 2019 unter der Federführung des BFS gestartet und hat das Ziel, die Mehrfachnutzung von Daten zu ermöglichen und den Austausch von Daten zwischen den Behörden zu erleichtern. Eines der Pilotprojekte im Rahmen des Programms NaDB ist die Mehrfachnutzung der Daten des spitalstationären Gesundheitswesens (Projekt SpiGes). Dabei sollen die Daten aus stationären Spitalaufenthalten unter Nutzung der Interoperabilitäts-Plattform des BFS entsprechend dem Once-only-Prinzip einmalig erhoben und anschliessend sowohl zu administrativen als auch statistischen Zwecken genutzt werden können (s. dazu auch 29. TB, Kap. 1.1).



Ein spezifisches Risiko, welches sich aus der Mehrfachnutzung ergeben kann und worauf der EDÖB explizit hingewiesen hat, ist die Verletzung des Zweckbindungsprinzips. Um dem vorzubeugen, ist eine Datenbearbeitung zu statistischen Zwecken klar von einer Datenbearbeitung zu anderen (bspw. administrativen) Zwecken zu unterscheiden. Auch ist ein besonderes Augenmerk auf Akteure mit Doppelfunktionen (etwa Spitäler und Versicherer, die sowohl Datenlieferanten als auch Datenbezüger sein können) zu richten. Eine klare organisationale und informatische Trennung der bearbeiteten Datenkategorien, gekoppelt mit Zugriffsbeschränkungen auf diese getrennten Datenkategorien, erweisen sich deswegen als unerlässlich.

In diesem Sinne hat der EDÖB das BFS darauf hingewiesen, dass aufgrund des Umfangs des Projekts und des hohen Risikos, welches sich aus der umfangreichen Bearbeitung besonders schützenswerter Personendaten ergibt, Risikoanalysen bezüglich der datenschutzspezifischen Risiken und der zu treffenden Massnahmen, um diesen Risiken zu begegnen, vorgenommen werden müssen, wie dies insbesondere auch das im September 2023 in Kraft tretende neue Datenschutzgesetz vorsieht (Art. 22 nDSG, Datenschutz-Folgenabschätzung).

ZERTIFIZIERUNG

Neue Verordnung über die Datenschutzzertifizierungen

Im Berichtsjahr hat der EDÖB das Bundesamt für Justiz bei den Rechtsetzungsarbeiten zur neuen Verordnung über die Datenschutzzertifizierung (VDSZ) beraten.

Für die Anerkennung von Zertifizierungsverfahren und die Einführung eines Datenschutz-Qualitätszeichens hat der Bundesrat die Verordnung über Datenschutzzertifizierungen (VDSZ) vom 31. August 2022 erlassen, die mit dem neuen DSG am 1. September 2023 in Kraft treten soll.

Der EDÖB hat das Bundesamt für Justiz zusammen mit der Schweizerischen Akkreditierungsstelle SAS bei der Erarbeitung der VDSZ in juristischen als auch informationstechnischen Belangen unterstützt. Ausserdem erarbeitet er derzeit spezifische Richtlinien über die Mindestanforderungen an ein Managementsystem sowie Richtlinien über die datenschutzrechtlichen Kriterien, nach welchen die Prüfung von Produkten, Dienstleistungen und Prozessen zu erfolgt hat.

Für Datenbearbeitungen im Rahmen von zertifizierten Systemen, Produkten oder Dienstleistungen entfällt beim Verantwortlichen auch bei hohem Risiko für die Persönlichkeit die Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung. Eine Zertifizierung

bietet Herstellern und Verantwortlichen zudem die Möglichkeit, ihr Einhalten des Datenschutzgesetzes zu dokumentieren. Aus Sicht des EDÖB

kann das Instrument der Datenschutzzertifizierungen den Datenschutz in der Schweiz stärken. Die Zertifizierung fördert insbesondere die Transparenz, indem immer komplexer werdende Datenbearbeitungsvorgänge von einer unabhängigen Stelle analysiert werden.

Die Zertifizierung von Managementsystemen geht über die Möglichkeiten einer europäischen Datenschutzzertifizierung hinaus, die nur Produkte, Dienstleistungen und Prozesse umfasst. Ausländische Datenschutzzertifizierungen, welche die Anforderungen der schweizerischen Gesetzgebung erfüllen, werden nach Rücksprache mit der Schweizerische Akkreditierungsstelle SAS anerkannt. Ebenso anerkennt der EDÖB nach Rücksprache mit der SAS ausländische Zertifizierungsstellen, sofern sie die schweizerischen Anforderungen erfüllen.

WAHLEN UND ABSTIMMUNGEN

Aktualisierung des bestehenden Leitfadens

Der EDÖB hat in Absprache mit der Konferenz der kantonalen Datenschutzbeauftragten (privatim) und der Bundeskanzlei den Leitfaden zu Wahlen und Abstimmungen, insbesondere im Hinblick auf die Eidgenössischen Erneuerungswahlen im Herbst 2023, aktualisiert und im Dezember 2022 auf der Webseite publiziert. Die aktualisierte Version zeigt insbesondere die herausragende Bedeutung auf, die dem datenschutzrechtlichen Grundsatz der Transparenz im Kontext mit Wahlen und Abstimmungen zukommt.

Der Leitfaden wurde erstmals im Berichtsjahr 2018/2019 in Zusammenarbeit mit der Konferenz der kantonalen Datenschutzbeauftragten (privatim), in enger Absprache mit der Bundeskanzlei und einer Arbeitsgruppe verfasst (s. 26. TB, Kap. 1.1) Seither wird der Leitfaden regelmässig aktualisiert (s. 27. TB, Kap. 1.1). In der vorliegenden Berichtsperiode wurde der Leitfaden insbesondere verständlicher strukturiert sowie mit den im Berichtsjahr 2019/2020 erarbeiteten Kontrollfragen betreffend die Einhaltung der datenschutzrechtlichen Grundsätze bei Webseiten erweitert.

ELEKTRONISCHE IDENTITÄT

Self-Sovereign-Identity-Ansatz

Der EDÖB konnte seine Anliegen in der Ämterkonsultation zur Vernehmlassungsvorlage zum neuen E-ID-Gesetz einbringen. Der Gesetzesentwurf wird im Sommer 2023 erwartet.

Mit der Ablehnung des ersten Entwurfs des E-ID-Gesetzes im Jahr 2021 hat die Schweizer Bevölkerung eine neue Lösung einer staatliche anerkannten, elektronischen Identität gefordert (s. 29. TB, Kap. 1.1). Im Berichtsjahr hat das Eidgenössische Justiz- und Polizeidepartement (EJPD) die Vernehmlassungsvorlage zum neuen E-ID-Gesetz (Bundesgesetz über die elektronische Identität und die Vertrauensinfrastruktur) in die Ämterkonsultation gegeben. Der Entwurf basiert auf dem Konzept einer Self-Sovereign-Identity, nach der Nutzerinnen und Nutzer grösstmögliche Kontrolle über ihre Daten haben sollen.

Eine E-ID beim Staat beantragen können alle Inhaberinnen und Inhaber eines von den Schweizer Behörden ausgestellten Ausweises. Der Bund schafft und betreibt hierzu eine staatliche Vertrauensinfrastruktur, die es einerseits ermöglicht, die E-ID auf Echtheit zu verifizieren, und die andererseits durch andere öffentliche und private Akteure verwendet werden kann, um weitere elektronische Beweismittel auszustellen und zu prüfen. Der Gesetzesentwurf regelt entsprechend in einem ersten Teil die staatliche E-ID und in einem zweiten Teil die Vertrauensinfrastruktur und die anderen elektronischen Beweismittel. Er regelt aber nicht die Details des Ausstellungsprozesses einer E-ID.

Der EDÖB nahm zum Vorlageentwurf Stellung und konnte verschiedene seiner Forderungen erfolgreich einbringen. So hat der EDÖB an der Ausarbeitung von Bestimmungen mitgewirkt, welche der Bearbeitung von Metadaten, die bei der Nutzung entstehen, und der Erhebung von Daten über Schnittstellen, die zur Ausstellung der E-ID erforderlich sind, Schranken setzen. Weiter sieht der Entwurf, wie vom EDÖB gefordert, eine Unterstützung der Nutzerinnen und Nutzer bei der Verwendung der neuen E-ID durch kantonale Anlaufstellen vor. Der EDÖB legt zudem Wert darauf, dass in der Botschaft zur Vorlage klargestellt wird, dass die E-ID nicht dazu führen darf, dass sich Bürgerinnen und Bürger im Internet generell ausweisen und identifizieren lassen müssen. Betreffend die Akteure, welche die Vertrauensinfrastruktur verwenden, um weitere elektronische Beweismittel auszustellen, forderte der EDÖB Widerrufspflichten für Ausstellerinnen.

Als problematisch erachtet der EDÖB den weiterhin vorgeschlagenen Ansatz eines offenen Registers mit Gebührenerhebung. Demnach tragen die Ausstellerinnen für eine E-ID ihre Daten selbst in das Register ein, ohne dass ihre Identität vorgängig verifiziert wurde. Der EDÖB wies auf das damit verbundene Risiko hin, dass Ausstellerinnen mit vorgetäuschter Identität die Vertrauensinfrastruktur missbrauchen könnten. Nach Auffassung des EDÖB sollte der Bund Massnahmen treffen, um zu verhindern, dass die von ihm betriebene Infrastruktur missbräuchlich verwendet wird. Deshalb haben wir gefordert, dass diese Risiken in der Botschaft an den Bundesrat offenlegt werden. Wir haben ebenfalls darauf hingewiesen,

dass – wenn keine Prüfung der Identitäten vorgängig erfolgt – ein System zur Bestätigung der im Basisregister eingetragenen Identifikatoren wichtig ist. Denn es bestünde die Möglichkeit, dass die bereits im Basisregister eingetragenen Identifikatoren mit einer in der realen Welt existierenden Organisation, Entität oder Einzelperson verknüpft werden.

Das EJPD kündigte nach der Auswertung der Vernehmlassungen an, den Kreis der E-ID-Berechtigten, den Ausstellungsprozess, Aspekte des Datenschutzes, die Benutzerfreundlichkeit (u. a. Barrierefreiheit) sowie die Supportorganisation in den Kantonen noch vertieft abzuklären. Der EDÖB wird die Entwicklungen im Projekt weiterhin verfolgen und seine datenschutzrechtlichen Anliegen einbringen. Der Gesetzentwurf soll bis im Sommer 2023 dem Bundesrat unterbreitet werden.

ONLINEPORTAL POST

Zugang nur noch mit SwissID möglich

Im Berichtsjahr hat die Post eine Migration des Kundenlogins auf ihrer Webseite vorgenommen, so dass der Zugang zu den Onlinediensten der Post seit Dezember 2022 nur noch mit einer SwissID möglich ist. Der EDÖB wurde vorgängig darüber informiert und wies auf die datenschutzrechtlichen Anforderungen hin.

Als die Post die Nutzerinnen und Nutzer der Onlinedienste aufforderte, eine SwissID zu erstellen, erhielten wir zahlreiche Bürgeranfragen zum Vorgehen der Post.

Aus der Auslagerung des Logins und der entsprechenden Datenbearbeitungen an die private Firma SwissSign darf somit für die Kundinnen und Kunden der Post keine Schlechterstellung hinsichtlich ihrer Privatsphäre und informationellen Selbstbestimmung resultieren.

Der EDÖB teilte der Post deshalb mit, dass die Übertragung der Loginfunktion an SwissSign den Vorgaben der Auftragsbearbeitung unterliegt (Art. 10a DSG). Dementsprechend trägt die Post als Auftraggeberin ihren Kundinnen und Kunden gegenüber weiterhin die Verantwortung für die Datenbearbeitungen, welche SwissSign im Zusammenhang mit dem Login zur Webseite der Post durchführt.

Letztere musste vertraglich garantieren, dass die Firma SwissSign die Datensicherheit gewährleistet und die Daten, die sie von Postkunden erhebt, ausschliesslich zum Zweck des Logins bearbeitet.

Aufgrund der Zusicherung der Post, bei der Migration des Logins die datenschutzrechtlichen Anforderungen zur Auftragsbearbeitung anzuerkennen und einzuhalten, konnte der EDÖB auf aufsichtsrechtliche Schritte verzichten.

STRATEGIE DIGITALE SCHWEIZ

Projekt digitaler Führerausweis

Das Bundesamt für Strassen (ASTRA), die Vereinigung der Strassenverkehrsämter (asa) und das Bundesamt für Justiz (BJ) stellten dem EDÖB das Projekt E-Führerausweis vor. Das Projekt des ASTRA soll Teil der Umsetzung «Strategie Digitale Schweiz» werden.

Das ASTRA plant eine auf das Strassenverkehrsrecht des Bundes gestützte, gestaffelte Einführung eines digitalen Lern-, Führer- und Fahrzeugausweises. Die digitalen Ausweise sollen international anerkannt und durch polizeiliche Kontrollorgane überprüfbar sein. Die Ausstellung dieser Ausweise liegt in der Kompetenz der Kantone, die sich auf die vom ASTRA festgelegten Anforderungen an Form, Inhalt und Gestaltung stützen.

Die Ausweisdaten befinden sich bereits heute im Informationssystem Verkehrszulassung (IVZ), das vom ASTRA in Zusammenarbeit mit den Kantonen geführt wird und auf welches die Kantone im Rahmen ihrer gesetzlichen Aufgaben zugreifen.

Gestützt auf die erhaltenen Informationen erachtet der EDÖB eine datenschutzkonforme Umsetzung des Projekts als möglich.

30 Jahre Datenschutz in der Schweiz

Das DSG von 1992

Am 1. Juli 1993 trat das erste Bundesgesetz über den Datenschutz vom 19. Juni 1992 in Kraft.

Bereits in der Gesetzesbotschaft von 23. März 1988 hatte der Bundesrat den gesetzgeberischen Handlungsbedarf mit dem «Einsatz der modernen Informations- und Kommunikationstechnologien in fast allen Lebensbereichen und der enormen Intensivierung der Datenverarbeitung und Verbreitung in Gesellschaft, Wirtschaft und Staat» begründet. 30 Jahre später spielt sich unser Alltag in einer digitalen Realität ab, wie sie vom Gesetzgeber damals nicht vorausgesehen werden konnte. Nichtsdestotrotz haben sich die vom damaligen Gesetzgeber kodifizierten Grundsätze der Personendatenbearbeitung als beständig erwiesen. Auch das neue Bundesgesetz über den Datenschutz vom 25. September 2020, das am 1. September 2023 in Kraft treten wird, richtet sich an ihnen aus: Transparenz, Verhältnismässigkeit und Zweckbindung bilden auch nach neuem Recht die zentralen Pfeiler der Personendatenbearbeitung.

Obwohl sich unser inzwischen von Internet und Smartphone geprägte Alltag stark gewandelt hat, haben viele Themen im Datenschutzbereich nichts an Aktualität eingebüsst: Bereits im ersten Tätigkeitsbericht beschäftigte uns die polizeiliche Datenbearbeitung im Zusammenhang mit der «Bekämpfung des organisierten Verbrechens» oder der «Grenzüberwachung mittels Videokamera». Und auch die «Telefonüberwachung/Observation zu Zwecken der Strafverfolgung» war schon damals ein Thema. Doch das Telefon, die Kamera, den Fernseher, die Bibliothek und den Computer trug damals noch niemand in der Hosentasche mit sich herum.

Die permanente Verbindung mit dem Internet, über das die digitale Gesellschaft von heute die Verrichtungen des Alltags vom Banking bis zum Dating «online» abwickelt, hat den Umfang und die Intensität, mit der personenbezogene Informationen bearbeitet werden, um Potenzen erhöht. Dennoch ist die Mission der unabhängigen Datenschutzaufsicht des Bundes, die Grundrechte und Persönlichkeit der Menschen über das technologisch Machbare zu setzen, bis heute aktuell geblieben. Eine Herausforderung, die der aktuelle Beauftragte nach dem Vorbild seiner Vorgänger Odilo Guntern und Hanspeter Thür, welche die ersten 23 Jahre der Datenschutzaufsicht des Bundes prägten, annimmt und trotz der Dynamik des technologischen Fortschritts als «mission possible» betrachtet.

Neues oder altes Gesetz – was gilt bei hängigen Verfahren?

Einige Verfahren konnten im Berichtsjahr nicht abgeschlossen werden. Wichtig zu wissen ist hier, dass diese gemäss der Übergangsbestimmung nach Art. 70 nDSG noch nach aktuell geltendem Recht beurteilt werden, auch wenn sie erst nach Inkrafttreten des neuen Datenschutzgesetzes am 1.9.2023 zum Abschluss kommen. Dies gilt insbesondere für die Sachverhaltsabklärung, die der EDÖB im Frühjahr 2021 betreffend die Datenbearbeitungen eines Schweizer Onlineshops eröffnet hat und die Sachverhaltsabklärung betreffend die Datenbearbeitungen der Auktionsplattform Ricardo AG und die TX Group AG, die beide noch hängig sind (s. 29. TB, Kap. 1.3).

Das neue Datenschutzgesetz

Mit dem totalrevidierten Datenschutzgesetz stellt der Gesetzgeber von 2020 den Verantwortlichen und der Datenschutzaufsicht neue Instrumente zur Verfügung, um den berechtigten Erwartungen der Bevölkerung an einen rechtsstaatlichen und robusten Persönlichkeitsschutz gerecht zu werden. Der EDÖB wird seine Aufsichtstätigkeit somit intensivieren.

Rolle des EDÖB

Das neue Datenschutzrecht tritt am 1. September 2023 in Kraft. Neuerungen gibt es nicht nur für Datenbearbeiter und betroffene Personen, sondern auch bezüglich der Aufgaben und Befugnissen des EDÖB, der seine aufsichtsrechtliche Tätigkeit intensivieren und die Anzahl Untersuchungen erhöhen wird.

Institutionelle Neuerung

Die Leiterin, der Leiter des EDÖB, also die oder der Beauftragte, wird in Zukunft vom Parlament gewählt. Bisher erfolgte die Wahl durch den Bundesrat und wurde von der Bundesversammlung lediglich bestätigt. Die neue Regelung verstärkt die Unabhängigkeit des Amtes von der Exekutive und dessen demokratische Legitimation. Er oder sie stellt sein Personal selbst an und verfügt über ein eigenes Budget, dessen Entwurf unverändert an die Bundesversammlung weitergeleitet wird.

Wie bisher bleibt der EDÖB als Behörde administrativ der Bundeskanzlei zugeordnet, zumal die Kommunikation zwischen dem Bundesrat und dem EDÖB über den Bundeskanzler erfolgt. Aufgrund einer Leistungsvereinbarung erbringt die Bundeskanzlei für den EDÖB eine Reihe von Dienstleistungen im Bereich der Personaladministration, Finanzen und Büroautomatisation.

Neu stellt der Bundesrat fest, ob die Gesetzgebung eines Drittstaats einen angemessenen Schutz gewährt und somit Daten ohne weitere Massnahmen von der Schweiz ins Ausland bekanntgegeben werden dürfen. Die Liste wird als Anhang zur Datenschutzverordnung geführt.

Neue Aufgaben für den EDÖB

Können geplante Bearbeitungen von Personendaten ein hohes Risiko für die Persönlichkeit oder die Grundrechte mit sich bringen, muss der private oder behördliche Verantwortliche eine Datenschutz-Folgenabschätzung (DSFA) erstellen. Ergibt sich aus der DSFA, dass mit der Bearbeitung trotz geeigneter Massnahmen weiterhin ein hohes Risiko für die Persönlichkeit oder die Grundrechte der Betroffenen einhergeht, muss sich der Verantwortliche vor deren Durchführung an den EDÖB wenden. Der EDÖB prüft die DSFA und teilt dem Verantwortlichen allfällige Einwände innert zwei Monaten mit. Die Stellungnahme des EDÖB stellt keine «Bewilligung» der geplanten Datenbearbeitung dar. Sie ist nicht anfechtbar, aber gebührenpflichtig.

Mit dem revidierten Gesetz erhält der EDÖB neue Aufgaben. Berufs-, Branchen- und Wirtschaftsverbände können eigene Verhaltenskodizes entwickeln und diese dem EDÖB zur Stellungnahme vorlegen. Diese Stellungnahmen werden vom EDÖB veröffentlicht. Ebenso veröffentlicht er eine Liste der von ihm genehmigten, ausgestellten oder anerkannten Standarddatenschutzklauseln. Für seine Stellungnahme zu einem Verhaltenskodex wie auch für die Genehmigung von Standarddatenschutzklauseln und verbindlichen unternehmensinternen Datenschutzvorschriften kann der EDÖB neu Gebühren verlangen.

«Der EDÖB wird seine Aufsichtstätigkeit intensivieren und die Anzahl der formellen Untersuchungen schrittweise erhöhen.»

Verantwortliche müssen Verletzungen der Datensicherheit, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen führen, dem EDÖB melden. Der EDÖB stellt dazu ein Meldeportal auf seiner Webseite zur Verfügung.

Untersuchungen

Der EDÖB hat als Aufsichtsorgan sicherzustellen, dass Bundesorgane und Privatpersonen die bundesrechtlichen Datenschutzvorschriften, insbesondere das Datenschutzgesetz (DSG), einhalten. Bestehen genügend Anzeichen, dass eine Datenbearbeitung gegen Datenschutzvorschriften verstossen könnte, eröffnet der EDÖB eine Untersuchung; vorbehalten bleibt eine Verletzung der Datenschutzvorschriften von geringfügiger Bedeutung. Im Rahmen der Untersuchung ermittelt der EDÖB, in welcher Art und Weise ein Bundesorgan oder eine private Person resp. ein privates Unternehmen Personendaten bearbeitet, die sich auf eine natürliche Person beziehen. Sodann beurteilt er gestützt auf den festgestellten Sachverhalt, ob ein Verstoss gegen Datenschutzvorschriften des Bundes vorliegt.

Mit dem Inkrafttreten des revidierten Datenschutzgesetzes wird die Schweiz die Konvention 108+ des Europarats ratifizieren. Dabei handelt es sich um ein verbindliches, multilaterales Instrument im Bereich des Datenschutzes, das ursprünglich von 1981 datiert und nun modernisiert und an die Herausforderungen des digitalen Zeitalters angepasst worden ist. Um den Anforderungen der Konvention 108+ zu genügen, hat der Gesetzgeber die Untersuchungsbefugnisse des EDÖB ausgeweitet. Während dieser bei Datenbearbeitungen durch Privatpersonen bisher nur dann eine Sachverhaltsabklärung eröffnen durfte, wenn die Bearbeitungsmethoden geeignet waren, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen (Systemfehler), fällt diese Schwelle unter dem revidierten Recht weg.

Der Beauftragte wird somit ab Inkrafttreten des neuen Rechts die aufsichtsrechtliche Tätigkeit des EDÖB intensivieren und die Anzahl der formellen Untersuchungen schrittweise erhöhen. Die Behörde ist für den Vollzug des neuen Gesetzes mit zusätzlichen Personalressourcen ausgestattet worden und konnte die entsprechenden Rekrutierungen im Frühjahr 2023 erfolgreich abschliessen.

Informelle Vorabklärungen

Hinweise auf mögliche Datenschutzverstösse können sich aus der laufenden Aufsichtstätigkeit ergeben oder dem EDÖB von betroffenen Personen oder Dritten, etwa Medienhäusern oder Konsumentenschutzorganisationen, angezeigt werden. Liegen dem EDÖB erste Hinweise auf einen Verstoss gegen Datenschutzvorschriften vor, prüft er zunächst im Rahmen informeller Abklärungen seine Zuständigkeit, ob genügend Anzeichen für einen Verstoss vorliegen und ob es sich um einen Verstoss von mehr als geringfügiger Bedeutung handelt. Dem EDÖB ist es dabei unbenommen, den Verantwortlichen zunächst formlos um die freiwillige Beantwortung von Fragen zu ersuchen, wenn z. B. seine Zuständigkeit unklar ist oder er es für denkbar hält, dass sich infolge der Kontaktaufnahme mit dem Verantwortlichen eine Untersuchung erübrigen könnte. Letzteres ist namentlich der Fall, wenn der Verantwortliche erste Anzeichen für einen Verstoss umgehend entkräften kann oder er aber innert nützlicher Frist freiwillig Massnahmen trifft, um die Einhaltung der Datenschutzvorschriften zu gewährleisten.

Formelles Untersuchungsverfahren

Nach bisherigem Recht erfolgte die Abklärung des Sachverhalts und der Frage, ob ein Verstoss gegen Datenschutzvorschriften vorliegt, im Rahmen einer Sachverhaltsabklärung, welche der EDÖB gegebenenfalls mit einer rechtlich nicht durchsetzbaren Empfehlung abschloss, eine bestimmte Datenbearbeitung zu ändern oder einzustellen. Nach neuem Recht richtet sich das Untersuchungsverfahren nach dem Verwaltungsverfahrensgesetz des Bundes (VwVG). Stellt der EDÖB im Verfahren einen Verstoss gegen Datenschutzvorschriften fest, hat er die Kompetenz, eine rechtlich durchsetzbare Verfügung im Sinne von Art. 5 VwVG zu erlassen,

welche der Verantwortliche vor Bundesverwaltungsgericht anfechten muss, wenn er sich ihr nicht unterziehen will. Der EDÖB kann verfügen, dass eine Datenbearbeitung angepasst, unterbrochen oder abgebrochen wird oder Personendaten gelöscht werden.

Amtshilfe

Das revidierte Gesetz enthält zwei spezifische Bestimmungen zur Zusammenarbeit des EDÖB mit schweizerischen und ausländischen Behörden. Schweizer Behörden sind dem EDÖB gegenüber zur Amtshilfe verpflichtet, währenddem sich die Verpflichtung des EDÖB zur Leistung von Amtshilfe auf die schweizerischen Datenschutzbehörden, die Strafverfolgungsbehörden im Zusammenhang mit seinen Anzeigen und die für den Vollzug seiner Massnahmen beigezogenen Bundesbehörden und Polizeiorgane beschränkt.

Die Amtshilfe des EDÖB gegenüber ausländischen Behörden erstreckt sich auf Behörden, die für den Datenschutz zuständig sind. Gegenstand des Austauschs sind Informationen und Personendaten, die von der Behörde für die Erfüllung ihrer gesetzlichen Aufgaben erforderlich sind. Dabei müssen eine ganze Reihe von Voraussetzungen erfüllt sein, so zum Beispiel das Gegenrecht der anderen Behörde, die Geheimniswahrung und die Verwendung der Informationen nur für das fragliche Verfahren.

Gebührenregelung

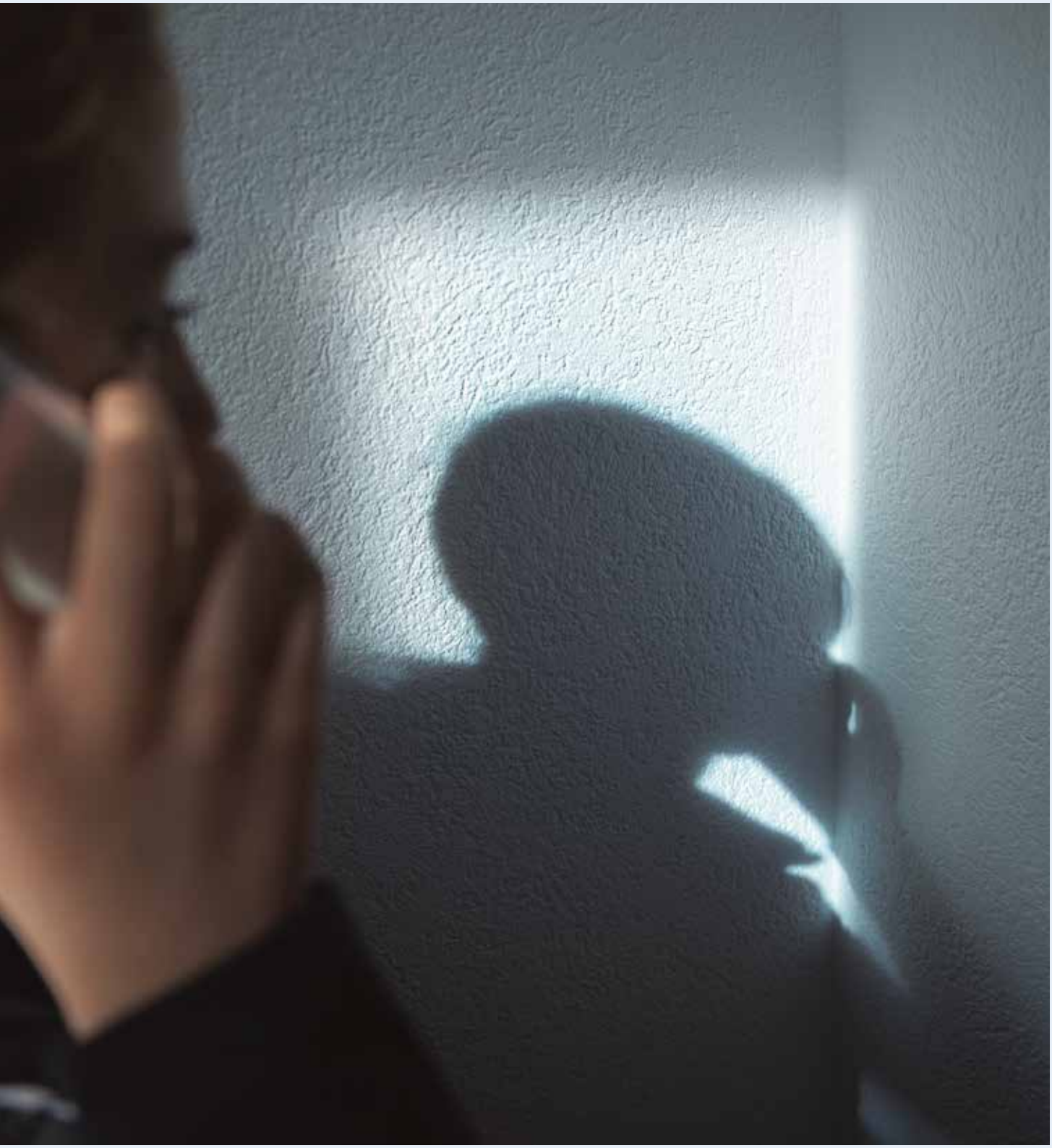
Neu wird der EDÖB von privaten Datenbearbeitern für eine Reihe seiner Aufgabenerfüllungen Gebühren erheben. Neben den oben bereits erwähnten gebührenpflichtigen Tätigkeiten (Stellungnahme zu Verhaltenskodizes und Datenschutz-Folgenabschätzungen, Genehmigung von Standardvertragsklauseln und verbindlichen unternehmensinternen Datenschutzvorschriften) wird der EDÖB auch im Untersuchungsverfahren Gebühren auferlegen. Zudem sind Beratungen von privaten Datenbearbeitern in Zukunft gebührenpflichtig. Gebühren werden nach Zeitaufwand erhoben, und es gilt – je nach Funktion des ausführenden Personals – ein Stundenansatz von 150 bis 250 Franken. Zuschläge sind möglich, wenn eine Dienstleistung aussergewöhnlichen Aufwand verursacht oder besonders schwierig oder dringlich ist. Zudem kann ein Zuschlag erhoben werden, wenn die Dienstleistung zu kommerziellen Zwecken weiterverwendet wird. Der EDÖB kann auf Gebühren verzichten, wenn ein öffentliches Interesse an der Dienstleistung besteht oder sein Aufwand gering war.

Strafrecht

Wie bisher hat der EDÖB – im Unterschied zu den Aufsichtsbehörden in der EU – auch nach neuem Recht keine Sanktionskompetenz. Die nebenstrafrechtlichen Bestimmungen im DSG wurden indessen ausgebaut. Strafbar sind die vorsätzliche Missachtung von Informations-, Auskunfts- und Meldepflichten sowie die vorsätzliche Verletzung von Sorgfaltspflichten. So insbesondere bei der Bekanntgabe von Personendaten ins Ausland, der Auftragsbearbeitung und der Bereitstellung der Datensicherheit. Die Obergrenze der Bussen liegt bei 250 000 Franken, gebüsst wird die verantwortliche natürliche Person. Die Obergrenze für die lediglich subsidiär vorgesehene Büssung juristischer Personen liegt bei 50 000 Franken.

Anlässlich der parlamentarischen Beratungen zum neuen DSG hat der Bundesrat in Aussicht gestellt, die Einführung von verwaltungsstrafrechlichen Sanktionen gegen fehlbare Unternehmen mit Blick auf den Erlass eines neuen Bundesgesetzes zu prüfen.

«Der EDÖB kann neu verfügen, dass eine Datenbearbeitung abgebrochen wird oder Personendaten gelöscht werden.»



DSFA

Beratung des BJ betreffend verwaltungsinterner Richtlinien zur Datenschutz-Folgenabschätzung

Nach dem totalrevidierten Datenschutzgesetz des Bundes (nDSG) müssen die verantwortlichen Stellen der Bundesverwaltung eine sog. Datenschutz-Folgenabschätzung (DSFA) erstellen, wenn sie Datenbearbeitungen mit potenziell hohen Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Bürgerinnen und Bürger planen. Der EDÖB beriet das Bundesamt für Justiz (BJ) betreffend Richtlinien und Hilfsmittel für Bundesorgane.

Bei der Planung von Projekten zur digitalen Transformation der Bundesverwaltung haben die verantwortlichen Stellen die potenziellen Risiken für die Persönlichkeit oder Grundrechte der betroffenen Bürgerinnen und Bürger zu evaluieren. Für Projekte, bei denen die Evaluation der geplanten Bearbeitung von Personendaten auf potenziell hohe Risiken hinweist, müssen die verantwortlichen Bundesorgane eine Datenschutz-Folgenabschätzung erarbeiten, in welcher sie diese Risiken und die Massnahmen zu deren Senkung ausweisen.

Der EDÖB hat das BJ bei der Formulierung von Richtlinien und Hilfsmitteln unterstützt, welche den verantwortlichen Bundesstellen die entsprechenden Arbeiten erleichtern sollen. Er äusserte sich dahingehend, dass sowohl bei der Vorprüfung, ob eine DSFA erstellt werden muss, als auch beim Erstellen der DSFA selbst nicht ausschliesslich auf (softwareunterstützte) Hilfsmittel und abschliessende Checklisten zurückgegriffen werden soll. Vielmehr verlangt die Durchführung einer DSFA eine wertende Evaluation der Gesamtrisiken unter Einbezug aller Umstände des konkreten Einzelfalls. Aufgrund der praktischen Erfahrungen mit Risikobeurteilungen, welche die Bundesverwaltung nach dem geltenden Schengen-Datenschutzgesetz vorgenommen hat, setzte sich der EDÖB zudem dafür ein, dass die verantwortliche Verwaltungsstelle im Falle einer bereits bestehenden Datenbearbeitung deren wesentlichen Unterschiede zur geplanten Bearbeitung gemäss den Richtlinien in der DSFA ausweisen soll. Dieser Vergleich soll sowohl die systemischen (Umfang, Intensität und Dauer der Bearbeitung sowie Kreis der Zugriffsberechtigten) wie auch die sicherheitstechnischen Aspekte der Bearbeitung umfassen.

MELDEPORTALE

Drei neue Onlineportale

Vor dem Inkrafttreten des neuen Datenschutzgesetzes führt der EDÖB neue Meldeportale ein: Das neue Portal für Bundesorgane zur Meldung von Bearbeitungsverzeichnissen ist bereits verfügbar. Es folgen die Portale zur Meldung der Datenschutzberater und –beraterinnen sowie zur Meldung von Verletzungen der Datensicherheit.

Der EDÖB startete 2021 ein Projekt zur Initialisierung von drei Meldeportalen.

Mit der Einführung des neuen Verzeichnisses der Bearbeitungstätigkeiten der Bundesorgane gemäss Art. 12 nDSG (DataReg), das die bestehende Lösung für die Meldung von privaten und behördlichen Datensammlungen (WebDataReg) ablöst, konnten wir im November 2022 die Einführung des ersten Meldeportales bereits realisieren. Das komplett neu entwickelte DataReg dient der Meldung und Veröffentlichungen von Verzeichniseinträgen der Bundesorgane und unterstützt diese bei der Führung ihrer Verzeichnisse. Der Betrieb des bisherigen WebDataReg, wo auch die Meldungen von Datensammlungen privater Unternehmen veröffentlicht werden, wird per 1. September 2023 eingestellt. Letztere sind nach neuem Recht nicht mehr meldepflichtig.

Das Meldeportal der Datenschutzberaterinnen und -berater dient der Übermittlung der Kontaktangaben von ernannten Personen.

Das Meldeportal zur Meldung von Verletzungen der Datensicherheit nach Art. 24 nDSG (DataBreach) stellt den Verantwortlichen einen sicheren digitalen Kanal zur Verfügung, um Verletzungen der Datensicherheit mit einem hohen Risiko für die Betroffenen zu melden. Das Online-Formular unterstützt den Verantwortlichen bei einer strukturierten und vollständigen Erfassung der benötigten Daten und soll eine effiziente Bearbeitung der Meldungen durch den EDÖB sicherstellen sowie statistische Auswertungen vereinfachen.

1.2 Justiz, Polizei, Sicherheit

BAZG

Zollgesetz

Der Entwurf zur Totalrevision des Zollgesetzes liegt den Kommissionen für Wirtschaft und Abgaben des Parlaments zur Prüfung vor. Der Beauftragte wurde von der Nationalratskommission angehört. Er monierte insbesondere den sensiblen Charakter des Vorhabens und den unverhältnismässigen Zugriff des Nachrichtendienstes des Bundes auf das Informationssystem des Bundesamtes für Zoll und Grenzsicherheit (BAZG).

Am 24. August 2022 unterbreitete der Bundesrat dem Parlament den Entwurf zum Bundesgesetz über den allgemeinen Teil der Abgabenerhebung und die Kontrolle des grenzüberschreitenden Waren- und Personenverkehrs durch das Bundesamt für Zoll und Grenzsicherheit (Vollzugsaufgabengesetz des BAZG). Für die Prüfung des Gesetzesentwurfs ist die Kommission für Wirtschaft und Abgaben des Nationalrats zuständig. Der EDÖB wurde am 24. Oktober 2022 von der Kommission angehört.

Die Zusammenführung von zolltechnischen und polizeilichen Aufgaben innerhalb des BAZG stellte bezüglich der datenschutzrechtlichen Aufsicht durch den Bund eine Herausforderung dar, denn die Schaffung des neuen Zollpolizeiamts bringt eine Erhöhung der Anzahl Personen mit sich, die mit der Bearbeitung sowohl von zollrechtlichen als auch von polizeirechtlichen Personendaten beauftragt ist. Durch die Uniformierung und Bewaffnung der Zollverwaltung entstand eine dritte, grosse Sicherheitsbehörde auf Bundesebene, zusätzlich zum Bundesamt für Polizei (fedpol) und zum Nachrichtendienst des Bundes (NDB).

Wie aus unserem 28. Tätigkeitsbericht 2020/21 (Kap. 1.2) hervorgeht, schickte das Eidgenössische Finanzdepartement zunächst eine Vorlage in die Vernehmlassung, die hinsichtlich der aufsichtsrechtlichen Aufgaben des Bundes im Bereich des Datenschutzes nicht akzeptabel war. Die Ausgestaltung der Regeln für die Bearbeitung von Personendaten durch das Zollpolizeiamt war darin ungenügend präzisiert und wurde dem Ermessen der Direktion des BAZG überlassen.

Im Rahmen einer intensiven Begleitung über längere Zeit konnten wir im Einvernehmen mit dem Bundesamt für Justiz das BAZG überzeugen, eine vergleichende Tabelle mit der gegenwärtigen Personendatenbearbeitung durch die EZV und der künftigen Bearbeitung durch das BAZG anzufertigen. Die vergleichende Tabelle floss in die Datenschutz-Folgenabschätzung ein. Davon ausgehend überarbeitete das BAZG das Kapitel über die Datenbearbeitung (s. 29. TB, Kap. 1.2) und brachte entsprechende Präzisierungen an. Dank dieser Verbesserungen konnten die grundsätzlichen Vorbehalte des Beauftragten im Rahmen der dritten Ämterkonsultation schliesslich ausgeräumt werden. Damit konnte die dem Parlament unterbreitete Vorlage als datenschutzrechtlich annehmbar eingestuft werden.

Das BAZG-VG ist jedoch trotz der vorgenommenen Verbesserungen als datenschutzsensibles Vorhaben zu

betrachten. Nach der dritten und letzten Ämterkonsultation blieb die neu vorgesehene Möglichkeit für den NDB, Zugang zum Informationssystem des BAZG zu erhalten, umstritten. Gemäss geltendem Zollgesetz wird dieser Zugang nicht gewährt, da die sporadische Zusammenarbeit zwischen den Zollbehörden und dem NDB von Fall zu Fall und im Rahmen der Amtshilfe erfolgen kann. Mit dem Beharren auf diesen Zugriff wird die Absicht der drei grossen Sicherheitsbehörden des Bundes deutlich, die Bearbeitung von personenbezogenen Daten zu intensivieren, indem sie sich gegenseitigen, grosszügigen Zugriff auf ihre Informationssysteme gewähren. Trotz unserer Einwände beliess der Bundesrat den nach unserer Beurteilung unnötigen und somit unverhältnismässigen Zugang des NDB zum Informationssystem im Gesetz.

SCHUTZSTATUS S

Web-Applikation «RegisterMe»

Das Staatssekretariat für Migration (SEM) hat für Flüchtende eine Web-Applikation zum Einreichen eines Gesuchs um den Schutzstatus S eingerichtet. Der Beauftragte äusserte Sicherheitsbedenken zur Speicherung der Personendaten dieser vulnerablen Gruppe und begrüsst die daraufhin getroffene Massnahme des SEM.

Zehntausende Menschen, die vor dem Krieg in der Ukraine flüchten mussten und in die Schweiz eingereist sind, haben beim Staatssekretariat für Migration (SEM) um vorübergehenden Schutz (Schutzstatus S) ersucht. Für die Terminvereinbarung bei einem Bundesasylzentrum wird die eigens dafür eingerichtete Web-Applikation «RegisterMe» eingesetzt, um die hohe Anzahl an Gesuchen und damit verbundenen Terminen zeitnah bearbeiten zu können.

Der Beauftragte hat bereits wenige Tage nach der Einführung von RegisterMe potenzielle Risiken für die Personendaten Betroffener identifiziert und diese Sicherheitsbedenken dem SEM gegenüber geäussert. Der EDÖB hatte zudem bemerkt, dass die Löschung der Registrierungsdaten dieser vulnerablen Personen in der Web-Applikation nicht vorgesehen war. Deshalb hat er dem SEM geraten ein Löschkonzept zu erstellen und diese Daten nach der Wahrnehmung des Termins umgehend zu löschen. Konkret riet er zur Erstellung und Umsetzung eines Löschkonzeptes.

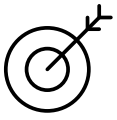
Das SEM hat den Zugriff auf Personendaten mittels Zwei-Faktor-Authentisierung geschützt und die Speicherung der Daten auf einem Rechenzentrum eingerichtet, das für besonders schützenswerte Daten ausgelegt ist. Weiter hat das SEM ein Löschkonzept erstellt und per September 2022 umgesetzt.

MITTO AG

Vorabklärung zu einer möglichen missbräuchlichen Verwendung des «Signalling System»-Zugangs

Im Dezember 2021 wurde der EDÖB durch internationale Medienberichterstattungen auf eine angeblich unrechtmässige Datenbearbeitung durch einen Mitarbeiter der in Zug ansässigen Mitto AG aufmerksam. Seine Vorabklärungen haben ergeben, dass keine Hinweise auf eine Verletzung der Datenschutzbestimmungen vorliegen. Somit schliesst der EDÖB die Vorabklärung in seinem Schlussbericht ohne Erlass von Empfehlungen ab.

Aufgrund von Medienberichten wurde der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte im Dezember 2021 durch eine Publikation des Bureau of Investigative Journalism und Bloomberg News auf eine angeblich unrechtmässige Datenbearbeitung durch einen Mitarbeiter der in Zug domizilierten Mitto AG aufmerksam. In der erwähnten Publikation wurde der Vorwurf erhoben, dass der besagte Mitarbeiter den von den Mobilfunk-Betreibern zum SMS-Versand gewährten Zugang auf ihre Netze zur Gewinnung von Informationen zu anderen



Zwecken missbraucht habe. Gemäss dem Bericht soll er insbesondere den «Signalling System (SS7)»-Zugang genutzt haben, um gegen Entgelt die unerlaubte Überwachung von Personen zu ermöglichen. (s. 29. TB, Kap. 1.3)

Der EDÖB hat daraufhin von der Mitto AG in mehreren Schritten weitgehende Angaben zu den technischen und organisatorischen Schutzmassnahmen in der Firma verlangt. Die Mitto AG hat allen Aufforderungen des EDÖB Folge geleistet und eigene externe Untersuchungen veranlasst, deren Ergebnisse dem EDÖB zur Verfügung gestellt wurden.

So hat die Mitto AG Nachweise zu den organisatorischen Rahmenbedingungen des Systembetriebs erbracht und dargelegt, mit welchen Massnahmen unerlaubte Änderungen an der Software verhindert bzw. aufgedeckt werden können. Die Auswertung von Protokollierungsdaten hat gemäss den Angaben der Mitto AG keine Hinweise ergeben, die eine missbräuchliche Verwendung der Systeme in der vorgeworfenen Weise nahelegen würden.
Nach Angaben der Mitto AG – bestätigt durch die Ausführungen der ebenfalls zur Stellungnahme eingeladenen Mobilfunkanbieter in der Schweiz – sei es den Mitarbeitenden der Mitto AG nicht möglich, ohne eine Veränderung der Systeme bzw. der Software, Zugriff auf Lokalisierungsangaben von SMS-Empfängerinnen und -Empfängern zu erlangen.

Der EDÖB hat im Rahmen seiner ihm zur Verfügung stehenden Mittel die notwendigen und möglichen Prüfungen veranlasst und sieht keine Hinweise, die den Verdacht bestätigen würden, dass es zu einer Verletzung von Datenschutzbestimmungen gekommen ist.

Da es sich bei den Vorwürfen zum Fehlverhalten des Mitarbeiters der Mitto AG um technisch wenig spezifische Anschuldigungen handelte, hat der EDÖB die Vorabklärung in Sachen Mitto AG im Schlussbericht ohne Empfehlungen abgeschlossen.

1.3 Handel und Wirtschaft

DATENBEKANNTGABE AN AUSLÄNDISCHE STEUERBEHÖRDEN

Bundesgericht entscheidet gegen das Recht auf Information von Drittpersonen in der internationalen Steueramtshilfe

Das Bundesverwaltungsgericht hiess im Jahr 2019 eine Beschwerde des EDÖB zum Recht auf Information von Drittpersonen in der internationalen Steueramtshilfe gut. Im anschliessenden Beschwerdeverfahren vor Bundesgericht setzte sich der Beauftragte erneut für dieses Recht von Drittpersonen ein. Im Dezember 2021 hiess das Bundesgericht die Beschwerde der ESTV aufgrund eines zwischenzeitlich erfolgten Praxiswechsels gut und hob das Urteil des Bundesverwaltungsgerichts auf.

In der internationalen Steueramtshilfe knüpft das Recht, über ein laufendes Amtshilfeverfahren informiert zu werden, an die Beschwerdeberechtigung einer Person an (vgl. Art. 14 Steueramtshilfegesetz). 2017 erliess der EDÖB eine 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 Ansicht 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 den Rechtsweg bis vor Bundesverwaltungsgericht beschritt (s. 26. TB, Kap. 1.3). Letzteres 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 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 Verfahrenssistierung hob das Bundesgericht auf, nachdem es am 13. Juli 2020 in einer anderen Angelegenheit 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, nur ausnahmsweise, nämlich aufgrund besonderer Umstände, legitimiert sind, sich 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 Rechtsprechung anerkannte der EDÖB vor Bundesgericht, dass Drittpersonen in der internationalen Steueramtshilfe 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 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 skizzierte vor Bundesgericht sodann erneut, wie sich

eine grundsätzliche Informationsverpflichtung der ESTV umsetzen liesse, ohne dass dieser daraus unverhältnismässiger Aufwand entsteht und die internationale Steueramtshilfe übermässig verzögert wird (s. 28. TB, Kap. 1.3).

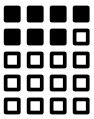
Mit Urteil vom 21. Dezember 2021 (BGE 148 II 349) bestätigte das Bundesgericht die im erwähnten BGE 146 I 172 entwickelte Rechtsprechung, wonach die ESTV vorgängig der Datenübermittlung nur solche Drittpersonen von Amtes wegen informieren muss, deren Beschwerdeberechtigung aufgrund der Akten geradezu offensichtlich ist. Entgegen der Auslegung des EDÖB befand es, dies werde in Art. 14 Abs. 2 des Steueramtshilfegesetzes ausdrücklich so geregelt. Eine generelle vorgängige Informationspflicht gestützt auf Art. 18a Abs. 3 DSG verneinte das Bundesgericht mit Hinweis darauf, dass die Bekanntgabe der Daten von Drittpersonen ausdrücklich im Steueramtshilfegesetz geregelt ist. Es hiess folglich die Beschwerde der ESTV gut und hob das Urteil des Bundesverwaltungsgerichts vom 3. September 2019 auf.

TRACKING-TECHNOLOGIEN

Prüfung möglicher Persönlichkeitsverletzung der Schweizer Bevölkerung durch Oracle

Der EDÖB hat von einer US-amerikanischen Klage vom August 2022 gegen das Unternehmen Oracle America Inc. Kenntnis erlangt. In der erwähnten Klage erheben die Klageparteien schwere Vorwürfe wegen unzulässigem Tracking. Nun wird geprüft, ob die erhobenen Vorwürfe auch Personen in der Schweiz betreffen.

In der US-Klage wird Oracle America Inc. vorgeworfen, mit Tracking-Technologien Daten von 5 Milliarden Internetnutzerinnen und -nutzern gesammelt und in einer Datenbank zusammengetragen zu haben. Die gesammelten Informationen würden durch das US-Unternehmen analysiert und ausgewertet, um eine Datensammlung über alle erfassten Personen zu erstellen. Erfasst würden neben Namen und Adresse jegliches Verhalten im Internet, beispielsweise Kaufverhalten, GPS-Daten oder Informationen über die Gesundheit – dies erfolge sogar geräteübergreifend. Dabei verwende Oracle America Inc. verschiedene Technologien, insbesondere sogenannte «Cookies» oder «Pixel» sowie integrierte Java-Scripts in Webseiten und Apps, um User zu verfolgen. Die US-Klage ist noch hängig; das US-Gericht hat noch nicht über die beschriebenen Vorwürfe entschieden.



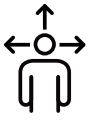
Der EDÖB hat die Vorwürfe in der Klage zur Kenntnis genommen und, analysiert diese und mögliche datenschutzrechtliche Auswirkungen auf Personen in der Schweiz. Er steht mit Oracle Schweiz GmbH in Kontakt. Die technischen Hintergründe erweisen sich als komplex, weshalb bis zum jetzigen Zeitpunkt keine formelle Untersuchung eröffnet wurde.

POSTFINANCE

Verzicht auf Kontoöffentlichkeit

Nachdem der EDÖB von Postfinance verlangt hat, für die Kontoöffentlichkeit eine Opt-out-Möglichkeit einzurichten, soll die automatische Ergänzung von Kontoangaben im E-Banking von Postfinance künftig auf das branchenübliche Mass reduziert werden.

Im vergangenen Berichtsjahr haben wir eine Vorabklärung zur automatischen Ergänzung von Kontoangaben (sog. Kontoöffentlichkeit) im E-Banking von Postfinance durchgeführt. Dies nachdem wir durch Bürgeranfragen darauf aufmerksam gemacht wurden, dass Angaben zu beliebig vielen Inhaberinnen und Inhabern von Postkonti abgegriffen werden konnten, weil das System die auf der Zahlungseingabemaske eingegebene Kontonummer mit Name und Adressdaten ergänzte



(s. 29. TB 2021/2022 Kap. 1.3). Nachdem Postfinance bereits Massnahmen ergriffen hatte, um Massenabfragen über ihr E-Banking-Portal zu verhindern, haben wir verlangt, dass den Kundinnen und Kunden für die Kontoöffentlichkeit ein Opt-out gewährt werden muss und diese dementsprechend der automatischen Ergänzung ihrer Kontoangaben widersprechen können.

Postfinance hat daraufhin die Möglichkeiten zur Implementierung eines solchen Opt-outs geprüft und entschieden, künftig auf die Kontoöffentlichkeit zu verzichten. So sollen gemäss Mitteilung von Postfinance im E-Banking nur noch diejenigen Kontoangaben automatisch ergänzt werden, welche die Nutzerinnen und Nutzer für die Eingabe eines Zahlungsauftrages bereits einmal verwendet haben, was dem branchenüblichen Standard entspreche. Die hierzu notwendigen Anpassungen sollen im Laufe des Jahres 2023 vorgenommen werden. Wir werden die Umsetzung dieser Massnahme prüfen.

BONITÄTSAUSKÜNFTE

Datenbankeinträge gestützt auf «negative Haushaltstreffer»

Der EDÖB hat die Sachverhaltsabklärung bei einem Inkasso- und Bonitätsunternehmen abgeschlossen. Dabei erwies sich das Instrument der sogenannten «negativen Haushaltstreffer» als unzulässig.

Der EDÖB eröffnete im Berichtsjahr 2019/2020 ein Verfahren bei einem grossen Anbieter von Inkasso- und Bonitätsdienstleistungen wegen angeblich zu vielen fehlerhaften Datenbankeinträgen und daraus folgenden Verwechslungen von Personen mit gleichen oder ähnlichen Namen. Als Folge der Verwechslungen seien Zahlungsaufforderungen an falsche Personen versendet oder unzutreffende, negative Bonitätsauskünfte gespeichert und bekannt gemacht worden. Zudem untersuchte der EDÖB, ob Schwierigkeiten bei der Korrektur von fehlerhaften Einträgen bestehen. Im Verlauf des Verfahrens wurde der Untersuchungsgegenstand auf die Zulässigkeit von sogenannten «negativen Haushaltstreffern» erweitert (s. 27. TB, S. 37; 28. TB, S. 34; 29. TB, S. 39)

Wer Personendaten bearbeitet, muss sich über deren Richtigkeit vergewissern (Art. 5 Abs. 1 DSG). Verwechslungen aufgrund von fehlerhaften Datenbankeinträgen führen regelmässig zu Persönlichkeitsverletzungen, die im Einzelfall für die Betroffenen schwerwiegend sein können. Nach eingehender Prüfung gelangte der EDÖB zum Schluss, dass das untersuchte Unternehmen die datenschutzrechtlichen Anforderungen an die Massnahmen zur Gewährleistung der Richtigkeit, Aktualität und Vollständigkeit der Daten erfüllt. Auch bei sorgfältiger Bearbeitung und Ergreifung der nötigen Massnahmen kann es allerdings zu fehlerhaften Datenbankeinträgen kommen. Deshalb ist es wichtig, dass die Datenbearbeitung für die Betroffenen erkennbar erfolgt (Transparenz) und ein wirksamer Berichtigungs- und Löschprozess besteht, um negative Konsequenzen von fehlerhaften Datenbankeinträgen zu vermeiden. Im Rahmen der Untersuchung hat sich gezeigt, dass das untersuchte Unternehmen auch diese Anforderungen erfüllt.

Weiter beurteilte der EDÖB im Rahmen der Sachverhaltsabklärung die Zulässigkeit von Bonitätsauskünften gestützt auf «negative Haushaltstreffer». Dabei werden im Rahmen von Bonitätsauskünften zu einer Person negative Bonitätsinformationen über andere Personen aus dem gleichen Haushalt bekannt gegeben. Diese Datenbekanntgabe – etwa an Onlinehändler – sollte angeblich verhindern, dass Personen mit negativer Bonität einen Kauf auf Rechnung unter dem Namen eines Haushaltsmitglieds mit positiver Bonität tätigen können (sog. Umgehungsgeschäft). Aufgrund dieser Praxis werden die Bonitäten von Haushaltsmitgliedern verknüpft, sodass Personen mit guter Bonität ihrerseits keine Käufe mehr auf Rechnung vornehmen können. Der EDÖB gelangte in seiner Untersuchung zum Schluss, dass diese Bearbeitungsmethode den Transparenz- und den Verhältnismässigkeitsgrundsatz des Datenschutzgesetzes verletzt. Solche Datenbearbeitungen können nicht gerechtfertigt werden. Insbesondere ist das überwiegende Interesse, welches die Prüfung der Kreditwürdigkeit rechtfertigt (Art. 13 Abs. 2 lit. c DSG), nicht einschlägig, weil die schlechte Bonität eines Haushaltsmitglieds für die Bonität der vertragsschliessenden Person nicht ausschlaggebend sein kann. Aus diesen Gründen hat der EDÖB dem Unternehmen im Schlussbericht empfohlen, Bonitätsauskünfte gestützt auf «negative Haushaltstreffer» einzustellen.

Das Unternehmen hat die Empfehlung angenommen.

CYBERANGRIFF

Vorabklärung bei Infopro AG und Fiducial Winbiz SA

Nach Bekanntwerden eines Cyberangriffs gegen einen Schweizer Anbieter von Clouddiensten eröffnete der EDÖB eine Vorabklärung. Er beurteilte die eingeleiteten Massnahmen und erinnerte die betreffenden Akteure an ihre datenschutzrechtlichen Pflichten.

Ende November 2022 erfuhren wir, dass der Hosting-Provider Infopro AG Opfer eines Cyberangriffs wurde. Diese Firma bearbeitete unter anderem Personendaten im Auftrag der Firma Fiducial Winbiz SA, die eine cloudgestützte Verwaltungs- und Buchhaltungssoftware anbietet, welche in der Westschweiz stark verbreitet ist. Aufgrund der Cyberattacke und der damit verbundenen Massnahmen verloren Geschäftskunden vorübergehend den Zugriff auf die Cloud-Applikation und auf die in der Cloud gespeicherten Personendaten.

Beim EDÖB gingen zahlreiche Anfragen von Geschäftskunden der Infopro AG zu dieser Cyberattacke ein. Der Beauftragte beriet sie und machte sie auf ihre datenschutzrechtlichen Informations- und Schadenminderungspflichten aufmerksam. Die betreffenden Unternehmen bemühten sich, diesen Verpflichtungen innert kurzer Frist nachzukommen.

Der EDÖB nahm mit Infopro und Winbiz Kontakt auf, um den Sachverhalt raschestmöglich abzuklären und insbesondere die Aussagen zu überprüfen, wonach Kunden von Winbiz

aufgrund einer Sicherheitslücke in der Software auf Daten anderer Kunden

Zugriff erhielten. Der EDÖB stellte Winbiz einen Fragenkatalog zu und bat insbesondere um eine Stellungnahme zur angezeigten Verletzung der Zugriffsbeschränkungen. Ein weiterer Fragenkatalog ging an Infopro. Parallel dazu fand ein Austausch mit den kantonalen Datenschutzbehörden (privatim) und dem Nationalen Zentrum für Cybersicherheit (NCSC) statt, das zusammen mit den zuständigen Strafverfolgungsbehörden tätig wird.

Ausgehend von den gelieferten Antworten konnte der EDÖB feststellen, dass die beiden Firmen die nötigen Vorkehrungen zur Wiedererlangung der Kontrolle über die Personendaten getroffen und die betroffenen Kunden informiert hatten. Da die vermeintliche Sicherheitslücke nicht bestätigt wurde, gelangte der EDÖB zum Schluss, dass vorerst kein weiterer Handlungsbedarf besteht. Er forderte jedoch Infopro und Winbiz auf, ihm jegliche besonderen Vorfälle zu melden.

VORABKLÄRUNG BEI EINEM VOICE-DIENST

Sicherheitsschwachstelle wurde rasch behoben

Aufgrund der Meldung einer Sicherheitsschwachstelle führte der EDÖB eine Vorabklärung bei einem Anbieter von Voice-Dienstleistungen durch. Da der Anbieter umgehend die notwendigen Massnahmen getroffen hatte, konnte der EDÖB von einem formellen Verfahren absehen.

Im Berichtsjahr wurde der EDÖB durch eine Bürgeranfrage und einen Journalisten darauf aufmerksam gemacht, dass über die Webseite eines Voice-Dienstleisters ungeschützt Personendaten abrufbar seien. Eine Grosszahl aufgenommener Telefongespräche könnten ohne Passwortschutz abgerufen werden, und die Daten seien teilweise mit weiteren Daten versehen, sodass eine Zuordnung zu einer bestimmten Person ohne weiteres möglich sei.

Aus diesem Anlass eröffnete der EDÖB gegenüber dem betreffenden Voice-Dienstleister eine informelle Vorabklärung. Der Dienstleister zeigte auf, dass er die Schwachstelle umgehend behoben, den Sicherheitsvorfall untersucht und weitere notwendige Massnahmen getroffen hatte. Der EDÖB konnte sich auf wenige Verbesserungsvorschläge beschränken, die der Dienstleister umsetzte. Unter diesen Umständen sah der EDÖB keinen Grund, eine formelle Sachverhaltsabklärung zu eröffnen, und schloss die Vorabklärung dementsprechend ab.

DATING-APPS

Analyse der Datenbearbeitungen

Im Berichtsjahr stellte der EDÖB einer in der Schweiz ansässigen, aber international tätigen Anbieterin einer Dating-App seinen Schlussbericht zu und machte Empfehlungen, welche angenommen wurden.

Im Frühjahr 2021 eröffnete der EDÖB eine Sachverhaltsabklärung betreffend die Datenbearbeitungen einer Dating-App. Sein Ziel war insbesondere zu klären, ob der Umgang mit Löschbegehren und die Weitergabe von Personendaten an Dritte datenschutzkonform ist, sowie die Einhaltung der Anforderungen an die Transparenz und an die Datensicherheit zu überprüfen (s. 28. und 29. TB, jeweils Kap. 1.1).

Der EDÖB kam bei seiner Untersuchung unter anderem zum Schluss, dass die eingegangenen Löschbegehren zwar innert kurzer Frist bearbeitet wurden, das Löschkonzept jedoch unzureichend war. Darüber hinaus waren die Informationen über die Löschmöglichkeiten, die den Nutzerinnen und Nutzern zur Verfügung gestellt wurden, unzureichend und missverständlich. Es bestanden auch Mängel in den Informationen über die Datenbearbeitungen, die im Rahmen der Nutzung

der Anwendung durchgeführt werden. Dies namentlich betreffend die Frage, welche Daten zu welchen Zwecken bearbeitet werden. Der EDÖB sprach mehrere Empfehlungen aus, um die Mängel zu beheben und die Einhaltung der Bearbeitungsgrundsätze der Transparenz, der Verhältnismässigkeit, von Treu und Glauben und der Rechtmässigkeit zu gewährleisten.

Die Anbieterin verlässt sich auf Applikationen Dritter, um verschiede Funktionen der App auszuführen, anstatt diese selbst zu entwickeln. Dabei überträgt die Anbieterin die Bearbeitung von Personendaten an die Dienstleister. Nach unserer Beurteilung traf die Anbieterin als Verantwortliche jedoch nicht die erforderlichen Massnahmen, inkl. Abklärungen und Vereinbarungen, um sicherzustellen, dass diese Dienstleister lediglich die Daten im Auftrag und im Einklang mit dem Datenschutzrecht bearbeiten. Die Anbieterin führte ausserdem lediglich interne Sicherheitstests durch, was angesichts der Sensibilität der bearbeitenden Daten den Anforderungen an die Datensicherheit nicht genügt. Der EDÖB gab vor diesem Hintergrund Empfehlungen ab, mit dem Zweck, die Datensicherheit zu verstärken und die Rechtmässigkeit des Outsourcings zu gewährleisten.

Die Anbieterin hat alle unsere Empfehlungen angenommen. Sobald alle Empfehlungen umgesetzt werden, wird der EDÖB sein Verfahren abschliessen können.

VIRTUELLE LÄUFE

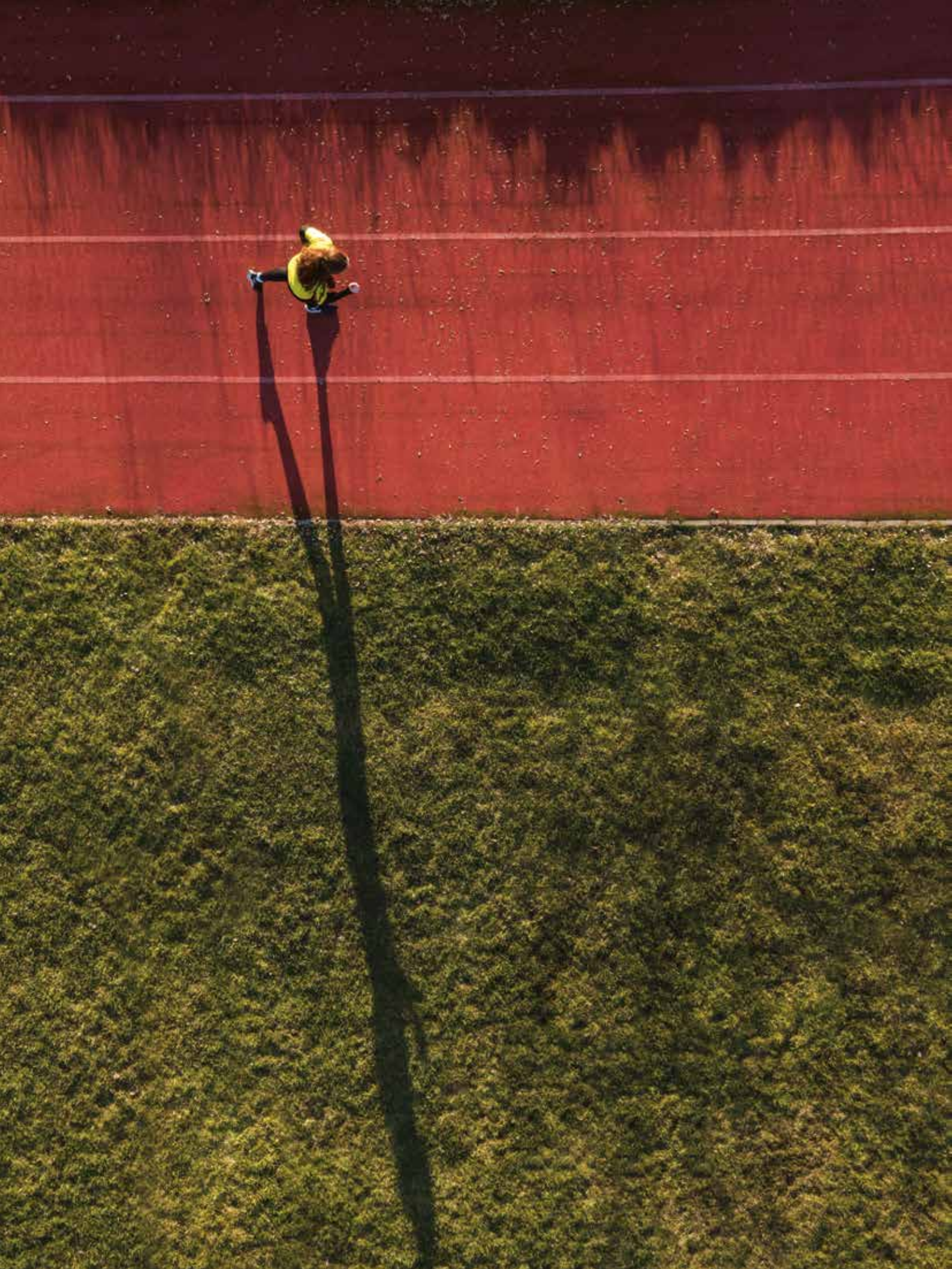
Verbesserter Datenschutz bei einem Lauf-Anbieter

Dem EDÖB wurden datenschutzrechtliche Problemfelder bei einem Anbieter von Lauf-Veranstaltungen gemeldet. Gestützt auf die Meldung wurden erste Untersuchungshandlungen vorgenommen und der Anbieter kontaktiert. Dieser ergriff umgehend Massnahmen zur Erhöhung des Datenschutzes, sodass der EDÖB auf die Eröffnung einer formellen Untersuchung verzichten konnte.

Ein Anbieter bietet Läuferinnen und Läufern die Möglichkeit, über eine App «virtuelle Läufe» zu bestreiten und sich untereinander zu messen. Die Läufe können zeitversetzt (d. h. innerhalb eines individuell wählbaren Zeitfensters) je nach Angebot an einem fix vorbestimmten oder auch selbst bestimmbaren Ort durchgeführt werden. Die Ergebnisse werden anschliessend in einer Rangliste zusammengetragen. Bedenklich war, dass mittels des Web-Entwicklungstools die Daten der Ranglisten von zahlreichen Personen mit ein paar Klicks zusammengetragen werden konnten und dies für die Betroffenen nicht transparent war.

Gestützt auf den Austausch mit dem EDÖB hat der Anbieter seine Datenschutzerklärung präzisiert und in den Registrierungsprozess integriert. Zudem hat er den Parameter «Wohnort» von der Rangliste entfernt, was Rückschlüsse auf konkrete Personen erschwert. Weiter haben wir festgestellt, dass die Nutzerinnen und Nutzer bei der Anmeldung für einen virtuellen Lauf ein Pseudonym wählen können, zahlreiche Personen jedoch bewusst ihren richtigen Vor- und Nachnamen angeben. Auch haben die Nutzerinnen und Nutzer die Möglichkeit, ihre Ranglisteneinträge selbst zu löschen.

Durch den informellen Austausch des EDÖB mit dem Lauf-Anbieter konnte das datenschutzrechtliche Niveau somit umgehend verbessert werden, sodass der EDÖB auf die Eröffnung einer formellen Untersuchung verzichten konnte.



1.4 Gesundheit

NATIONALES ORGANSPENDEREGISTER NOSR

Online-Authentifizierung mangelhaft

Das Verfahren zum Nationalen Organspenderegister wurde abgeschlossen und der Schlussbericht auf der Website des EDÖB veröffentlicht. Dieser Fall unterstreicht die Bedeutung von zuverlässigen Online-Authentifizierungsprozessen. Entsprechende einfach handhabbare Lösungen sind verfügbar.

2022 führte der EDÖB eine Sachverhaltsabklärung zum Nationalen Organspenderegister (NOSR) durch. In diesem von der Stiftung Swisstransplant betriebenen Register konnten Personen ihren Willen bezüglich der Entnahme von Organen im Falle ihres Todes auf einer Online-Plattform deklarieren. Die Angaben im Register betreffen die Intimsphäre und gelten somit als sensible Daten im Sinne von Art. 3 lit. c Ziff. 2 DSG. Das Verfahren war infolge

von Medienberichten eröffnet worden, die Schwachstellen bei der Registrierung publik machten: es war möglich, eine andere Person in das Register einzutragen, ohne dass diese darüber informiert wurde. Der Registrierungsprozess wurde unverzüglich ausgesetzt. Das Verfahren verlief in mehreren Etappen:

- In einem ersten Bericht unterbreitete der EDÖB der Stiftung Mitte Juni mehrere Empfehlungen im Hinblick auf die Verbesserung der Prozesse zur Authentifizierung der Nutzer bei der Ersteintragung, beim Einloggen und bei späteren Änderungen.
- Swisstransplant nahm im Sommer 2022 zu diesem Bericht Stellung und teilte insbesondere ihren Verzicht auf die Wiederaufnahme des aktiven Betriebs mit: Das Register sollte lediglich zur Einsichtnahme bestehen bleiben, ohne Neuregistrierungen oder Änderungen bestehender Profile zu ermöglichen; Löschungen sollten noch möglich sein. Mit diesem Entscheid wurde ein Teil der Empfehlungen des EDÖB gegenstandslos, namentlich jene zur Verbesserung der Online-Authentifizierungsprozesse. Zwei Empfehlungen zum Restrisiko beim Löschprozess blieben indes bestehen.
- Mitte Oktober legte der EDÖB seinen Schlussbericht vor. Kurz darauf kündigte Swisstransplant an, den Betrieb des Registers definitiv einzustellen. Die Schliessung erfolgte im Dezember 2022. Sämtliche Daten wurden gelöscht.

In der Volksabstimmung vom 15. Mai 2022 haben sich die Schweizer Stimmberechtigten für die Widerspruchsregelung und die Schaffung eines neuen, vom Bund beaufsichtigten Organspenderegisters entschieden. Es wird ähnlich wie das von Swisstransplant betriebene Register aufgebaut sein und soll 2025 eingeführt werden.

Online-Authentifizierungstools

Der Fall des Registers von Swisstransplant ist ein Anschauungsbeispiel für heikle Punkte, die beim Aufbau eines Online-Registers beachtet werden müssen. Das Tool ist praktisch, da es Online-Abfragen und die Profilverwaltung durch die Nutzer selbst erlaubt. Der Registrierungsprozess und die Profilverwaltung sind einfach gestaltet und für ein breites Publikum ansprechend. Eine zu starke Vereinfachung kann allerdings zu mangelnder Sicherheit führen und böswilligen Personen ein missbräuchliches Verhalten erleichtern (Identitätsdiebstahl, Hacking, Anfeindungen usw.). Dem Betreiber muss bewusst sein, dass er die Verantwortung für die Richtigkeit und Sicherheit der registrierten Daten trägt, insbesondere wenn das Register anderen Akteuren – im Falle der Organspende etwa Angehörige und Ärzte – als Entscheidungsgrundlage dienen soll.

Zuverlässige und benutzerfreundliche Online-Authentifizierungstools sind heute durchaus verfügbar und namentlich im Bankwesen verbreitet. Auch im Bereich der elektronischen Identität sind bereits verschiedene Lösungen im Einsatz. Wer ein Register mit Online-Authentifizierung aufbauen will, muss sich bereits im Vorfeld um sichere Lösungen bemühen. Die Digitalisierung eröffnet neue Möglichkeiten im Bereich der Gesundheit, bringt jedoch auch neue Risiken mit sich. Es ist im Interesse der massgeblichen Akteure, das Vertrauen der Nutzerinnen und Nutzer durch zuverlässige und ausgereifte digitale Instrumente zu bewahren.

ONLINEREGISTER

Datenschutzrisiken beim Brustimplantatregister

Das Verfahren zur Sachverhaltsabklärung betreffend das Brustimplantatregister (Mammaregister) wurde abgeschlossen. Anhand dieses Falls wird deutlich, dass die Onlineschaltung medizinischer Daten per se ein erhöhtes Risiko mit sich bringt und die Frage nach sich zieht, ob es notwendig ist, dieses Risiko einzugehen. Gegebenenfalls sind Vorkehrungen zu treffen, um die Datensicherheit zu gewährleisten.

Der EDÖB eröffnete 2022 ein Verfahren zur Sachverhaltsabklärung betreffend das von Swiss Plastic Surgery betriebene Brustimplantatregister (s. 29. TB, Kap. 1.4). Dessen Zweck ist die Erfassung sämtlicher Eingriffe der plastischen Chirurgie im Zusammenhang mit Brustimplantaten sowie allfälliger Schwierigkeiten, die bei diesen Operationen auftreten. Dabei werden mehrere Ziele verfolgt: Einerseits soll die Information über Vorfälle zur Verbesserung der Dienstleistungsqualität beitragen. Das Register dient ausserdem der Rückverfolgung der chirurgischen Eingriffe und erleichtert Rückrufaktionen, falls in einer Serie schadhafte Implantate entdeckt werden. Andererseits werden die erfassten Daten auch für die Führung von Branchenstatistiken verwendet.

Die Eröffnung der Untersuchung erfolgte, nachdem beim EDÖB ein Hinweis auf einen IT-Designfehler im Register eingegangen war. Wegen dieses Fehlers konnten sich beliebige Personen in wenigen Schritten Zugang zu Dossiers von Patientinnen verschaffen. Nebst Angaben zur Person (Name, Vorname, Geburtsdatum usw.) waren auch detaillierte medizinische Daten zur Operation einsehbar. Der Bericht des EDÖB ist in Arbeit und wird dieses Jahr abgeschlossen. Das Register wurde einstweilen vom Netz genommen.

Risikopotenzial und Notwendigkeit

Der Fall unterstreicht einen weiteren heiklen Aspekt im Zusammenhang mit medizinischen Onlineregistern. Sie enthalten Daten zur Gesundheit, welche naturgemäss besonders schützenswert sind. Dabei handelt es sich oftmals um Informationen, welche die Intimsphäre betreffen. Die Möglichkeit des Onlinezugriffs bedeutet für die Daten der Patientinnen und Patienten zwangsläufig ein erhöhtes Risiko und kann zudem das Vertrauensverhältnis zwischen Arzt und Patientin belasten. Die Daten werden regelmässig direkt durch die Ärzteschaft weitergegeben. Aufgrund des Arztgeheimnisses braucht es für diese Datenübermittlung a priori die vorgängige Einwilligung der Patientin oder des Patienten. Auch stellt sich immer die Frage, ob der

Zweck des Registers das einzugehende Risiko rechtfertigt und welche Daten zur Erfüllung des Zwecks unbedingt erforderlich sind (dies im Sinne des Verhältnismässigkeitsprinzips nach Art. 4 Abs. 2 DSG). Die Registerbetreiber müssen geeignete Massnahmen treffen und ausreichend Mittel zur Verfügung stellen, um bestehende Risiken abzuwenden.

MANGELNDE DATENSICHERHEIT

Sachverhaltsabklärung zur Datenbank privater Covid-19-Testzentren

Der EDÖB führte eine Sachverhaltsabklärung zu einer unzureichend gesicherten Datenbank privater Covid-19-Testzentren durch. Im Schlussbericht hielt er fest, dass die Daten aufgrund einer bekannten Schwachstelle beträchtlichen Sicherheitsrisiken ausgesetzt waren. Da die Verantwortlichen nach Bekanntwerden des Mangels jedoch angemessene Sofortmassnahmen eingeleitet hatten, konnte das Risiko für die Betroffenen minimiert und das Verfahren ohne Empfehlungen des EDÖB abgeschlossen werden.

Im November 2022 meldete eine Privatperson dem EDÖB und dem NCSC einen Datensicherheitsmangel bei einer Datenbank, auf der die Resultate aus Covid-19-Testzentren mit mehreren Standorten in der Schweiz gespeichert waren. Aufgrund einer Schwachstelle des Webservers für den Zugriff auf die Datenbank hatte sich die Privatperson über die in einer frei zugänglichen Konfigurationsdatei einsehbaren Informationen Zugang zur Datenbank verschafft und eine Kopie der Datenbank heruntergeladen. Die Verantwortlichen nahmen die Datenbank noch am Tag der Meldung vom Server und verschoben sie auf einen verschlüsselten physischen Datenträger.

Im Rahmen der Sachverhaltsabklärung, die der EDÖB im Nachgang an die erhaltene Meldung und darauf gestützte erste Abklärungen eröffnete, stellte er verschiedene Mängel in Bezug auf die Datensicherheit fest. Die durch eine Systemwartung verursachte freie Zugänglichkeit der Konfigurationsdatei stellte eine kritische Schwachstelle dar, da darin die Zugangsdaten enthalten waren, wodurch ein Zugriff auf die Datenbank durch unbefugte Personen möglich war. Darüber hinaus erwies sich die gewählte Authentifizierungsmethode mittels Benutzername und Passwort (welche beide in der exponierten Datei enthalten waren) in der vorliegenden Konstellation als unzulänglich; es hätte zur Gewährleistung der Datensicherheit beispielsweise eine Zwei-Faktoren-Authentifizierung eingerichtet werden müssen.

Aufgrund des Auslandbezugs des Systems tauschte sich der EDÖB mit den Datenschutzbehörden Österreichs und des Fürstentums Liechtenstein amtshilfeweise aus.

Gestützt auf die Zugriffslogs, konnte der für die Testzentren Verantwortliche bestätigen, dass kein weiterer unbefugter Zugriff auf die Daten stattgefunden hatte. Durch die ergriffenen Sofortmassnahmen bestand zudem kein Risiko für die betroffenen Personen mehr. Aufgrund dieser spezifischen Konstellation und angesichts der Tatsache, dass der Betrieb der Covid-Testzentren schon einige Zeit vor Bekanntwerden der Schwachstelle eingestellt worden war, schloss der EDÖB das Verfahren ohne Erlass einer Empfehlung ab.

Immer mehr Fälle mit ethischen Hackern

Neben der steigenden Zahl von journalistischen Recherchen zu Datenschutz- und Datensicherheitslücken sieht sich der EDÖB zunehmend auch mit Meldungen von ethischen Hackern (gemeinhin als «White Hat Hacker» bezeichnet) und IT-Aktivisten konfrontiert. White Hat Hacker sind in ihrer idealtypischen Definition gut gesinnt und melden dem EDÖB einen Fall, damit dieser beim Betreiber vorstellig wird und gegebenenfalls eine Untersuchung einleitet. Sie handeln regelmässig ausserhalb eines offiziellen Rahmens und ohne die Zustimmung der Systembetreiber und bearbeiten dabei oft personenbezogene Daten (z. B. Kundendaten, die im System gespeichert sind, Daten von Angestellten usw.).

Neben den Meldungen an den EDÖB informieren die Hacker manchmal auch direkt die Öffentlichkeit oder die Medien über ihre Entdeckungen – wie etwa im Fall der Covid-Testcenter. Je nachdem, welche Informationen übermittelt werden, ist diese Art der breiten Kommunikation heikel, da sie zusätzliche Risiken für die Personen mit sich bringen kann, deren Daten betroffen sind.

ONLINE-PLATTFORM

Projekt Datenrettung «meineimpfungen.ch»

Ende 2021 wurde über die ehemalige Betreiberin der Plattform meineimpfungen.ch der Konkurs eröffnet. Im Mai 2022 erhielt der EDÖB Kenntnis von einer geplanten Veräusserung der Impfdaten durch das zuständige Konkursamt an ein privates Unternehmen, was ihn zum Erlass einer Löschungsempfehlung bewog. Daraufhin forderten Behörden und Private eine Rettung der Daten. Gestützt auf eine vom EDÖB verlangte öffentlich-rechtliche Vereinbarung übernahm im Juni 2022 der Kanton Aargau die Daten, um im Rahmen eines noch laufenden Vorprojekts zu prüfen, ob eine datenschutzkonforme Rückgabe der Daten an die Betroffenen möglich ist.

Im Jahr 2021 wurden bei der Plattform meineimpfungen.ch gravierende Mängel festgestellt und vergebliche Versuche unternommen, den betroffenen Personen unter Einhaltung des Datenschutzrechts Zugriff auf ihre Daten zu ermöglichen. Ende 2021 wurde über die Betreiberin der Plattform der Konkurs eröffnet (s. 29. TB, Kap. 1.4). Im Mai 2022 erhielt der EDÖB Kenntnis davon, dass die fraglichen Impfdaten im Rahmen der konkursamtlichen Verwertung im Freihandverfahren an ein privates Unternehmen veräussert werden sollten. Daraufhin intervenierte der EDÖB in Absprache mit dem Datenschutzbeauftragten des Kantons Bern, indem er dem für die Konkursmasse handelnden Konkursamt am 20. Mai 2022 mittels formeller Empfehlung die Veräusserung untersagte und die Löschung sämtlicher Impfdaten der Plattform verlangte. Das Konkursamt nahm die Empfehlung an.

Aufgrund der Empfehlung des EDÖB sprachen sich mehrere Behörden, worunter auch das Bundesamt für Gesundheit (BAG), und Private öffentlich dafür aus, dass die Daten gerettet und den Betroffenen zurückgegeben werden sollten. Angesichts des dabei geltend gemachten öffentlichen Interesses an einer Datenrettung erklärte sich der Beauftragte im Juni 2022 in einem Schreiben an die Direktorin des BAG bereit, auf seine Löschungsanordnung zurückzukommen. Dies unter der Bedingung, dass die Daten gestützt auf eine öffentlich-rechtliche Vereinbarung und zum dort ausdrücklich festzuhaltenden Zweck der Wahrung der Datenschutzrechte der betroffenen Personen an eine Gesundheitsbehörde des Bundes oder der Kantone übertragen würden.

Am 16. Juni 2022 schloss die Konkursmasse, handelnd durch das Konkursamt Bern-Mittelland, mit Unterstützung des BAG eine solche Vereinbarung mit dem Kanton Aargau ab, worauf der EDÖB seine Empfehlung vom 20. Mai 2022 widerrufen konnte. Die Daten wurden sodann vereinbarungsgemäss dem Kanton Aargau und der im Auftrag des Kantons handelnden Stammgemeinschaft eHealth Aargau übertragen, damit im Rahmen eines Vorprojekts geprüft werden konnte, ob eine datenschutzkonforme Rückübertragung der Daten an die Betroffenen – unter Berücksichtigung der Integrität der Daten und der technischen und wirtschaftlichen Machbarkeit – realisiert werden kann. Auch sollte eine, von einer ausdrücklichen Zustimmung im Einzelfall abhängig zu machende Überführung in ein elektronisches Patientendossier geprüft werden. Würde die Klärung im Rahmen des Vorprojektes negativ ausfallen, sehen die zwischen dem Kanton Aargau, der Stammgemeinschaft und dem BAG ausgetauschten Erklärungen die Beendigung des Projekts und die Löschung der Daten vor.

Zur Zeit der Drucklegung war das Ergebnis des Vorprojekts des Kantons Aargau, das der Aufsicht der Datenschutzbeauftragten des Kantons Aargau untersteht, noch offen.

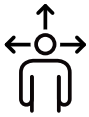
ELEKTRONISCHES PATIENTENDOSSIER

Neue Entwicklungen

Im Berichtsjahr unterbreitete das Eidgenössische Departement des Innern (EDI) dem Bundesrat eine Vernehmlassungsvorlage für die Sicherstellung der Übergangsfinanzierung des elektronischen Patientendossiers (EPD). Mit dem Ziel, die Einführung und Verbreitung des EPD erfolgreich voranzutreiben, soll im Sommer 2023 zudem eine umfassende Revision des Bundesgesetzes über das elektronische Patientendossier (EPDG) in die Vernehmlassung geschickt werden.

An seiner Sitzung vom 27. April 2022 beschloss der Bundesrat, das EPDG mit verschiedenen Massnahmen weiterzuentwickeln und beauftragte das EDI, ausgehend von einer Reihe von Eckwerten eine Vernehmlassungsvorlage auszuarbeiten. Die umfassende Revision des EPDG dürfte im Sommer 2023 in die Vernehmlassung geschickt werden (ein Inkrafttreten ist frühestens für 2027 vorgesehen). Nach dem Willen des Bundesrats soll das EPD künftig als Instrument der obligatorischen Krankenversicherung gelten, wodurch dem Bund eine weitreichende Regelungskompetenz zukommt. Die Versicherer sollen jedoch keinen Zugriff auf das EPD erhalten.

Die Aufgaben und Kompetenzen und damit auch die Sicherstellung der Finanzierung des EPD durch Bund und Kantone werden klar geregelt. Wegen der Freiwilligkeit für Patientinnen und Patienten, sich am EPD zu beteiligen, sollen zwei Varianten vernehmlasst werden: die Beibehaltung



der Freiwilligkeit und die Einführung eines Opt-out-Modells, wobei letzteres vom Bundesrat bevorzugt wird. Alle ambulant tätigen Gesundheitsfachpersonen sollen zur Führung eines EPD verpflichtet werden. Für neu zugelassene Ärztinnen und Ärzte gilt diese Pflicht bereits seit dem 1. Januar 2022. Forschende sollen Zugriff auf Daten des EPD haben, sofern die Patientinnen und Patienten ihre Einwilligung dazu geben. Eine zentrale Speicherung soll die Bearbeitung der dynamischen Daten erleichtern. Die Nutzung der technischen Infrastruktur des EPD soll für Zusatzdienste ermöglicht werden, beispielsweise für die Überweisung von Patientinnen und Patienten an andere Gesundheitsfachpersonen. Für den Zugang zum EPD soll die Nutzung einer E-ID geklärt werden.

Um die Finanzierung des EPD bis zur Revision des EPDG sicherzustellen, beauftragte der Bundesrat das EDI, bis zum Frühjahr 2023 einen Gesetzesentwurf über die Übergangsfinanzierung des EPD in die Vernehmlassung zu geben. Danach wird die Vorlage an das Parlament überwiesen und möglichst rasch in Kraft gesetzt. Das Bundesamt für Gesundheit (BAG) hat mit den Arbeiten zu diesen beiden Revisionen begonnen.

Im Rahmen der Jahresrevision des Ausführungsrechts zum EPDG prüfen das BAG und eHealth Schweiz weitere Weiterentwicklungs- und Aktualisierungsbedürfnisse, die im Frühjahr 2023 vorliegen dürften. Die Revisionsvorhaben sollen die Verbreitung und den Nutzen des EPD namentlich durch die Einführung eines elektronischen Impfausweises sowie eines elektronischen Medikationsplans fördern. Weitere Massnahmen zur Erhöhung der Attraktivität des EPD werden evaluiert.

Der EDÖB pflegt regelmässigen Austausch mit dem BAG und nimmt zu dessen Vorhaben Stellung. Er hat wiederholt daran erinnert, dass er nicht gegen eine beschleunigte Einführung des EPD im Interesse der Patientinnen und Patienten ist, solange dies nicht zu einer Schwächung des Datenschutzes führt. Er wird die Entwicklung des EPD weiterhin aufmerksam mitverfolgen und sich für die Gewährleistung des Datenschutzes einsetzen, insbesondere wenn die Persönlichkeitsrechte der betroffenen Personen durch die angestrebten Massnahmen tangiert würden sowie für den Fall einer Aufhebung des freiwilligen Charakters des EPD für die Patientinnen und Patienten.

ELEKTRONISCHER RECHNUNGSVERSAND

Pflicht zur Zustellung einer Kopie der Arztrechnung

Die Pflicht der Leistungserbringer zur Zustellung einer Rechnungskopie an die Versicherten verunsichert diese. Insbesondere der elektronische Versand wirft zahlreiche Fragen in Bezug auf Datenschutz und Datensicherheit auf.

Seit dem 1. Januar 2022 sind sämtliche Leistungserbringer nach Art. 35 Abs. 2 des Bundesgesetzes über die Krankenversicherung KVG (Ärzte, Apotheker, Chiropraktoren, Spitäler, Laboratorien usw.) gesetzlich verpflichtet, den Versicherten in jedem Fall und unaufgefordert eine Rechnungskopie zuzustellen. Die Übermittlung der Kopie kann mit ausdrücklicher Genehmigung der versicherten Person auch elektronisch erfolgen. Die Zustellungspflicht ist Teil eines Pakets von Massnahmen zur Kostendämpfung im Gesundheitswesen, das anlässlich der Anpassung von Art. 42 Abs. 3 KVG angenommen wurde. Die Versicherten können auf diese Weise ihre Rechnungen überprüfen und allfällige Fehler dem Versicherer melden. Die Zustellungspflicht ist an sich nicht neu. Sie bestand bereits im System des Tiers payant, war jedoch nur auf Verordnungsstufe geregelt.

Der EDÖB ist in dieser Frage beim Bundesamt für Gesundheit (BAG), das für den Vollzug der Massnahme zuständig ist, tätig geworden und hat verlangt, dass die Leistungserbringer gründlich über ihre Datenschutzpflichten informiert werden, insbesondere was den elektronischen Versand von Rechnungskopien anbelangt. Da Gesundheitsdaten gemäss Bundesgesetz über den Datenschutz (DSG) zu den besonders schützenswerten Daten zählen, müssen bei ihrer Bearbeitung besondere Vorkehrungen getroffen werden. Leistungserbringer, die ihre Rechnungskopien elektronisch zustellen möchten,

haben für eine sichere Übermittlung zu sorgen, indem sie angemessene technische und organisatorische Massnahmen im Sinne von Art. 7 DSG und von Art. 8 ff. der Verordnung zum Bundesgesetz über den Datenschutz (VDSG) treffen und beispielsweise Verschlüsselungs- und Multi-Faktor-Authentifizierungsverfahren verwenden. (Weitere Ausführungen zum Erfordernis angemessener Sicherheitsmassnahmen befinden sich im Beitrag über das Vorhaben, inskünftig sämtliche Abrechnungen im Rahmen der obligatorischen Krankenversicherung elektronisch zu übermitteln; s. nachfolgenden Text).

Verstösse der Leistungserbringer gegen die Pflicht, geeignete Datenschutzmassnahmen vorzusehen, können ernste zivil- und strafrechtliche Folgen nach sich ziehen: Geschädigte können im Falle einer Persönlichkeitsverletzung als Einzelperson zivilrechtlich vorgehen oder Schadenersatz- und Genugtuungsforderungen stellen, wenn sich Unbefugte Zugriff auf nicht verschlüsselte Mails verschaffen konnten und Gesundheitsdaten dadurch an Dritte gelangt sind. Bei einer Verletzung des Arztgeheimnisses ist ausserdem eine Strafverfolgung denkbar, etwa wenn medizinische Angaben an unbefugte Empfänger übermittelt wurden.

Leistungserbringer, die sich für die elektronische Übermittlung der Rechnungskopie entscheiden, müssen die versicherte Person vorgängig über die Risiken informieren, die dieser Form der Zustellung innewohnen. Sie müssen sich zudem vergewissern, dass die versicherte Person der Zustellung auf elektronischem Weg ausdrücklich und freiwillig zugestimmt hat. Erklärt sich die versicherte Person mit der elektronischen Übermittlung der Rechnungskopie nicht einverstanden, sind die Leistungserbringer gehalten, diese Willensäusserung zu respektieren und die Rechnungskopie auf Papier ohne zusätzliche Kosten auf dem herkömmlichen Postweg zuzustellen. Das Gesetz sieht ferner auch die Möglichkeit vor, dass Versicherer und Leistungserbringer vereinbaren, die Rechnungskopie durch den Versicherer zustellen zu lassen.

ELEKTRONISCHER RECHNUNGSVERSAND

Entwurf betreffend die elektronische Rechnungsübermittlung im Bereich der obligatorischen Krankenpflegeversicherung

Mit den vom Bundesrat beschlossenen Massnahmen zur Dämpfung der Gesundheitskosten ist vorgesehen, dass sämtliche Leistungserbringer im stationären und im ambulanten Bereich verpflichtet werden, ihre Rechnungen in elektronischer Form zu übermitteln. Der EDÖB verlangte im Rahmen der Vernehmlassung eine Präzisierung der Anforderungen im Bereich Datenschutz und Datensicherheit.

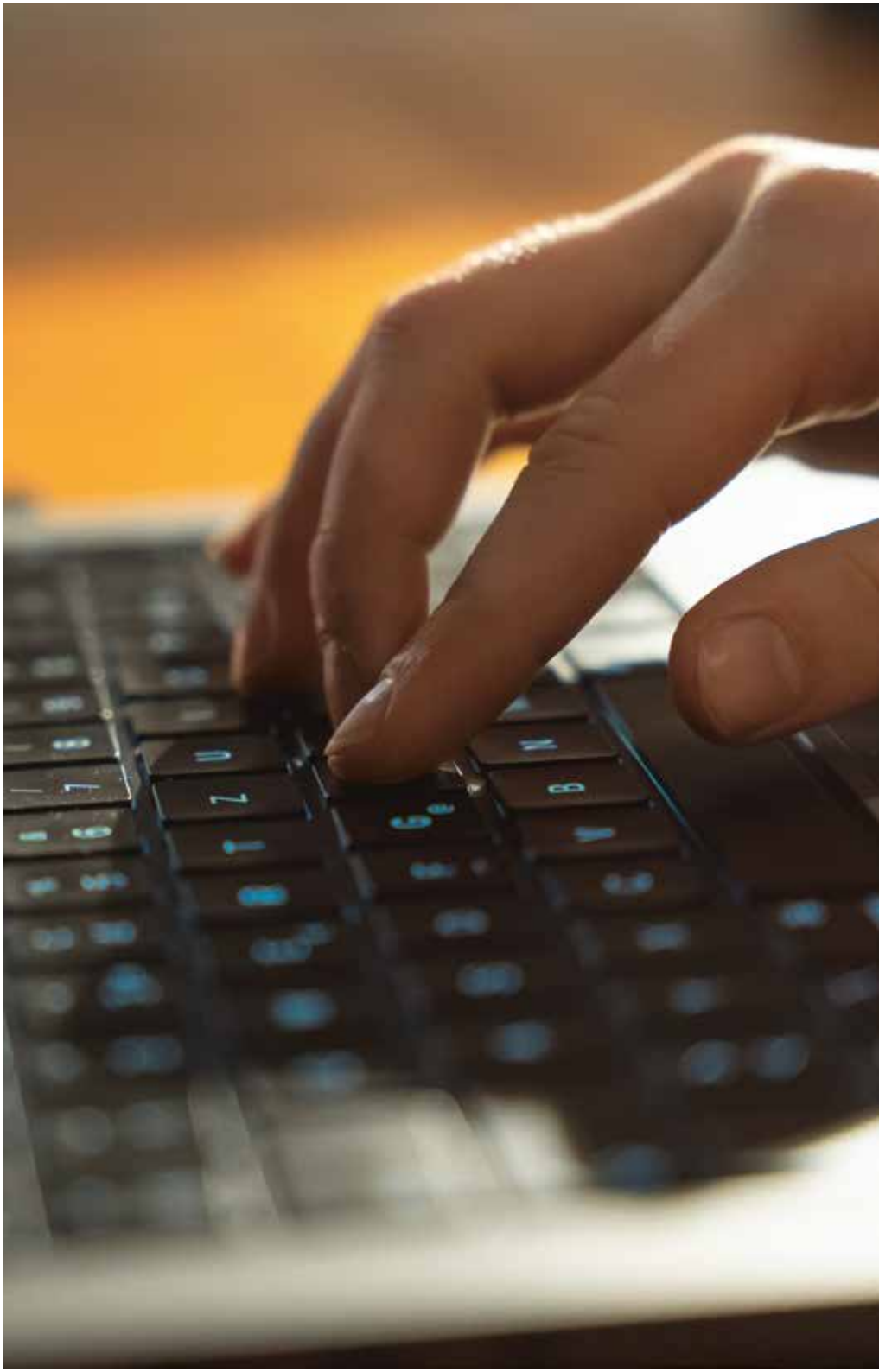
Am 7. September 2022 verabschiedete der Bundesrat die Botschaft zur Änderung des Bundesgesetzes über die Krankenversicherung (KVG) bezüglich des zweiten Massnahmenpakets zur Kostendämpfung im Gesundheitswesen. Darin ist eine Änderung von Art. 42 Abs. 3ter KVG vorgesehen, wonach sämtliche Leistungserbringer im stationären und im ambulanten Bereich verpflichtet werden, ihre Rechnungen künftig in elektronischer Form zu übermitteln, unabhängig davon, ob der Krankenversicherer (Tiers payant) oder die versicherte Person (Tiers garant) die Vergütung der Leistung schuldet. Im System des Tiers payant wird die Rechnung der versicherten Person elektronisch oder auf Wunsch kostenlos in Papierform zur Kontrolle und Bezahlung übermittelt. Anschliessend leitet die versicherte Person die Rechnung elektronisch an den Krankenversicherer weiter oder gibt sie in einem dafür vorgesehenen Onlineportal des Versicherers ein. Papierrechnungen werden von der versicherten Person dem Versicherer weitergeleitet. Danach verlangt letzterer die Rechnung vom Leistungserbringer elektronisch. Das genaue Verfahren wird auf Verordnungsstufe geregelt.

Die Ausgestaltung der elektronischen Rechnungsübermittlung wird an die Tarifpartner übertragen. Die Leistungserbringer und die Versicherer oder deren Verbände sind gehalten, sich auf einen gesamtschweizerisch einheitlichen Standard zu einigen und eine diesbezügliche Vereinbarung abzuschliessen. Die Vorlage sieht vor, dass die Rechnungsstellung über ein standardisiertes Formular mittels einer Plattform stattfindet, wobei die Datensicherheit zu gewährleisten ist. Wenn sich die Parteien innerhalb der vorgesehenen zweijährigen Übergangsfrist nicht auf ein einheitliches System einigen können, sorgt der Bundesrat für die Festlegung des Standards.

Im Rahmen der Ämterkonsultation zum Botschaftsentwurf verlangte der EDÖB eine genauere Umschreibung der erforderlichen technischen und organisatorischen Massnahmen. Ausserdem wies er darauf hin, dass mit dem Inkrafttreten des neuen Art. 42 Abs. 3 KVG im Januar 2022 bezüglich der elektronischen Übermittlung von Rechnungskopien an die Versicherten deutlich wurde, welche Gefahren bestehen, wenn elektronische Rechnungen an die Stelle von Papierrechnungen treten, sowie dass die Leistungserbringer angemessene technische und organisatorische Massnahmen treffen und insbesondere Verschlüsselungs- und Multi-Faktor-Authentifizierungsverfahren einsetzen müssen. (Weitere Ausführungen zum Erfordernis angemessener Sicherheitsmassnahmen befinden sich im Beitrag über die geltende Pflicht zur Übermittlung einer Rechnungskopie an Patientinnen und Patienten (s. vorangehenden Text).

Der Botschaftsentwurf wurde aufgrund der Vorschläge des Datenschutzbeauftragten überarbeitet. Im Kapitel über den Datenschutz wurde ein Verweis auf die Bestimmungen des DSG und speziell auf die Verpflichtung aufgenommen, angemessene technische und organisatorische

Massnahmen zum Schutz gegen jegliche Bearbeitung durch Unbefugte zu treffen. Zudem wurde daran erinnert, dass die Rechnungen besonders schützenswerte Daten nach DSG enthalten, da die Leistungserbringer darauf alle administrativen und medizinischen Angaben machen müssen, die für die Überprüfung der Berechnung der Vergütung notwendig sind, insbesondere Angaben zu den einzelnen erbrachten Leistungen und zu den Diagnosen. In der Botschaft wird festgehalten, dass zur Bearbeitung dieser besonders schützenswerten Daten besondere Massnahmen vorzusehen sind (verschlüsselte Übermittlung, Multi-Faktor-Authentifizierungsverfahren), die von den Tarifpartnern im Rahmen der Erarbeitung eines gesamtschweizerisch einheitlichen Standards zu berücksichtigen sind, der die Datensicherheit garantiert. Schliesslich wurde die Botschaft mit dem Verweis auf weitere Pflichten ergänzt, die die Tarifpartner bei der Erarbeitung eines einheitlichen Standards hinsichtlich der Revision des DSG erfüllen müssen, namentlich dass bei einem solchen Vorhaben eine Datenschutz-Folgenabschätzung gemäss Artikel 22 des neuen Gesetzes zu erstellen ist.



1.5 Arbeit

BUNDESPERSONAL

Aufbewahrung von Personaldossiers beim BFS

Der EDÖB eröffnete beim Bundesamt für Statistik (BFS) eine Sachverhaltsabklärung betreffend Aufbewahrung physischer Personaldossiers des Bundespersonals über die gesetzliche Frist von zehn Jahren hinaus aufbewahrt wurden. Nachdem er feststellen konnte, dass einschlägige Korrekturmassnahmen umgesetzt wurden, schloss er die Abklärung ohne Empfehlung ab.

In seinem letzten Tätigkeitsbericht 2021/22 informierte der EDÖB über Abklärungen, die er beim Bundesamt für Statistik (BFS) betreffend die Handhabung von physischen Personaldossiers von ehemaligen Mitarbeitenden vornahm (s. 29. TB, Kap. 1.5). Der EDÖB war darauf aufmerksam gemacht worden, dass das BFS zahlreiche Personaldossiers über die gesetzlich erlaubte Frist von zehn Jahren hinaus aufbewahrte. Das BFS erkannte den Handlungsbedarf und legte auf Verlangen des EDÖB einen Umsetzungs- und Zeitplan zur Wiederherstellung des rechtmässigen Zustands vor. Der Abschluss der notwendigen Arbeiten war für Ende Sommer 2022 vorgesehen. Weil diese Arbeiten zu diesem Zeitpunkt jedoch noch nicht durchgeführt worden waren und eine Verzögerung im Zeitplan entstand, sah sich der EDÖB zur Einleitung eines formellen Aufsichtsverfahrens nach Art. 27 DSG gezwungen. Damit sollte sichergestellt werden, dass das BFS die Massnahmen zur Wiederherstellung des rechtmässigen Zustands zeitnah ergreift und den EDÖB über die getroffenen Massnahmen informiert.

Das BFS teilte dem EDÖB im November 2022 mit, dass der Auftrag zur Wiederherstellung des rechtmässigen Zustands erfüllt werden konnte: Die Personaldossiers von ehemaligen Mitarbeitenden wurden an das Bundesarchiv geliefert, das den Erhalt bestätigte. Nicht archivwürdige Dossiers wurden vernichtet (darunter auch jenes der Person, die uns den Fall gemeldet hatte) und das Löschprotokoll dem Bundesarchiv übermittelt. Letzteres hat das Vorgehen für Personaldossiers von 2012 bis 2017 (E-Personaldossiers ab 2018) bereits geklärt und das künftige Vorgehen festgelegt.

Der EDÖB erhielt die Bestätigung, dass archivwürdige Papierdossiers dem Bundesarchiv übergeben bzw. nicht archivwürdige Dossiers vernichtet wurden. Er konnte feststellen, dass beim BFS nunmehr keine Personaldossiers

länger als gesetzlich erlaubt aufbewahrt werden und klare Anweisungen für die gesetzeskonforme Archivierung und Vernichtung künftiger Dossiers bestehen, deren Archivierungsfrist derzeit unter zehn Jahren liegt.

Da das BFS Massnahmen zur Wiederherstellung des rechtmässigen Zustands gemäss Bundespersonal- und Datenschutzrecht umgesetzt hat, konnte der EDÖB sein Verfahren im März 2023 ohne Erlass von Empfehlungen abschliessen.

1.6 Verkehr

SBB

Kundenfrequenzmesssystem an Bahnhöfen

Die SBB haben den EDÖB im Oktober 2022 über ein Projekt zur Kundenfrequenzmessung an Bahnhöfen informiert. Da das Projekt mit hohen potenziellen Risiken für die betroffenen Passantinnen und Passanten behaftet ist, wird die SBB vor der Umsetzung eine Datenschutz-Folgenabschätzung (DSFA) durchführen und diese dem EDÖB zur Stellungnahme vorlegen.

Die Medien berichteten im Februar über ein Projekt der SBB betreffend Erhebung von Daten in Bahnhöfen, mit denen Personenflüsse optimiert werden sollen. Der Text der entsprechenden Ausschreibungsunterlagen waren zu Beginn teilweise missverständlich formuliert, so dass den SBB vorgeworfen wurde, ihre Kundinnen und Kunden mit Gesichtserkennungstechnologie überwachen zu wollen. Dies wurde von den SBB dementiert. Sie haben öffentlich versichert, dass das Kundenfrequenz-Messsystem mit anonymisierten Daten arbeite, die zu keinem Zeitpunkt personenbezogen ausgewertet würden.

Der Datenschutzverantwortliche der SBB hatte den EDÖB bereits im Oktober 2022 über das Projekt informiert. Obwohl das neue Kundenfrequenz-Messsystem lediglich der Optimierung der Personenflüsse in den Bahnhöfen dienen soll und keine Personen identifiziert werden sollen, die Daten also nicht personenbezogen verwendet werden sollen, ist das Projekt mit einem potenziell hohen (Re-) Identifikations-Risiko behaftet. Daher sicherten die SBB dem EDÖB zu, dass sie vor der Umsetzung des Projekts eine DSFA durchführen und diese dem EDÖB vorlegen werden.

Die SBB gehen davon aus, dass das Projekt datenschutzkonform umsetzbar ist. Dem EDÖB lagen zum Ende des Berichtzeitraums keine Informationen vor, welche dies ausschliessen würden. Der EDÖB wird zum Projekt nach Erhalt der DSFA Stellung nehmen.

1.7 International

Im vergangenen Geschäftsjahr konnten nach Beruhigung der pandemiebedingten Situation verschiedene internationale Konferenzen wieder vor Ort durchgeführt werden. So nutzte auch der EDÖB die Gelegenheit, an verschiedenen internationalen Anlässen physisch teilzunehmen. Dies insbesondere an den Sitzungen des Europarates, der Europäischen Konferenz der Datenschutzbeauftragten und der französischsprachigen Vereinigung der Datenschutzbehörden.

Die internationale Tragweite des Datenschutzes zeigte sich auch im vergangenen Geschäftsjahr. Bei der grenzüberschreitenden Übermittlung von Personendaten stellen sich für international tätige Unternehmen hinsichtlich der Speicherung von Daten in Clouds und auf Servern im Ausland heikle Rechtsfragen, zu denen in der Schweiz noch keine Rechtsprechung besteht (s. Kap. 1.1). Mit besonderem Interesse verfolgt der EDÖB vor diesem Hintergrund die gegenwärtigen Bestrebungen der EU, einen neuen Angemessenheitsbeschluss bezüglich den USA zu erlassen.

EUROPA

Europarat

Nach dem Ausscheiden Russlands aus dem Europarat musste der Beratende Ausschuss über die Teilnahmebedingungen Russlands entscheiden. Die Behandlung dieses Geschäfts führte dazu, dass die Plenarsitzung vom Juni auf den November verschoben wurde. Weiter verabschiedete der Beratende Ausschuss Richtlinien zur digitalen Identität. Sodann wählte er die Vertreterin der Schweiz zu seiner ersten Vize-Präsidentin.

Die Sitzungen des Beratenden Ausschusses zum Übereinkommen 108 und seines Büros konnten wieder vor Ort durchgeführt werden. Beim Übereinkommen 108 handelt es sich um ein sogenanntes offenes Übereinkommen, welches auch Vertragsparteien, die nicht Mitgliedstaat des Europarats sind, offensteht. Nach dem aussergewöhnlichen Ausscheiden Russlands aus dem Europarat stellte sich daher bei allen offenen Übereinkommen die Frage der Bedingungen der weiteren Teilnahme dieses Staates. Angesichts der Notwendigkeit, die Vorgaben des Ministerkomitees abzuwarten und sich mit anderen betroffenen Ausschüssen abzusprechen, wurde das Plenum vom Juni auf den November verschoben. Dadurch konnte im Jahr 2022 nur eine statt wie üblich zwei Plenarsitzungen durchgeführt werden, was zu Verzögerungen in der Behandlung von verschiedenen Geschäften führte.

An der Plenarversammlung vom November hat der Ausschuss als erstes die Frage der Teilnahmebedingungen Russlands im Ausschuss besprochen. Die rechtliche Ausgangslage war, dass ein Mitgliedstaat nach einem ausserordentlichen Ausscheiden aus dem Europarat zwar weiterhin Vertragspartei des Übereinkommens 108 bleibt, dessen Teilnahme aber gestützt auf die Verfahrensregeln eingeschränkt oder suspendiert werden kann. Vor diesem Hintergrund hat der Ausschuss die Verfahrensordnung angepasst und die Teilnahme Russlands auf die allgemeinen Diskussionen über die Auslegung des Übereinkommens 108 beschränkt. Zudem hat er festgelegt, dass Russland weder den Ausschuss präsidieren noch Mitglied seines Büros sein dürfe.

Weiter besprach der Ausschuss Entwürfe betreffend den zwischenstaatlichen Datenaustausch zum Zweck der Bekämpfung der Geldwäscherei und Terrorismusfinanzierung sowie zu steuerlichen Zwecken und Standardvertragsklauseln für die

grenzüberschreitende Übermittlung von personenbezogenen Daten. Bezüglich Standartvertragsklauseln fungiert die Vertreterin des EDÖB als Berichterstatterin.

Der Ausschuss hat sodann eine Arbeitsgruppe beauftragt, eine Auslegungshilfe betreffend die Ausnahmen und Beschränkungen des Anwendungsbereichs des modernisierten Übereinkommens 108 (sogenanntes Übereinkommen 108+) vorzubereiten.

An der Plenarversammlung verabschiedete der Ausschuss Richtlinien über die digitale nationale Identität. Diese publizierten Richtlinien umschreiben, wie die Datenschutzgrundsätze des Übereinkommens 108+ in diesem Zusammenhang zu verstehen sind, und enthalten mehrere Empfehlungen für die folgenden Akteure: Organe mit rechtssetzenden Funktionen, Verantwortliche für die Datenbearbeitung, Gerätehersteller und Dienstleistungsanbieter sowie Datenschutzbehörden.

Schliesslich fanden an der Plenarversammlung die Erneuerungswahlen des Büros des Beratenden Ausschusses statt. Dabei wurde die Vertreterin des EDÖB, welche bis anhin Mitglied des Büros war, zur ersten Vize-Präsidentin gewählt. Präsidentin des Ausschusses ist neu die deutsche Vertreterin, zweite Vize-Präsidentin wie bis anhin die senegalesische Vertreterin.

EUROPA

Europäische Konferenz der Datenschutzbeauftragten in Dubrovnik

An der Europäischen Konferenz der Datenschutzbeauftragen wurden die neusten Entwicklungen bei der grenzüberschreitenden Datenbekanntgabe sowie die Zusammenarbeit der Datenschutzbehörden in diesem Bereich diskutiert. Mit einer Resolution soll die Ratifizierung des Übereinkommens 108+ beschleunigt werden.

Nach einem pandemiebedingten Unterbruch von zwei Jahren fand vom 19. bis 20. Mai 2022 die 30. Europäische Konferenz der Datenschutzbeauftragten auf Einladung der kroatischen Datenschutzbehörde in Dubrovnik statt. Dort wurden die letzten Entwicklungen und offene Punkte bezüglich der grenzüberschreitenden Datenbekanntgabe diskutiert. Auch wurde anhand praktischer Beispiele die Zusammenarbeit zwischen den Datenschutzbehörden erörtert und Fragen der Sensibilisierung für die Anliegen des Datenschutzes besprochen.

Die Konferenz rief dazu auf, die Ratifizierung des «Übereinkommens 108+», der modernisierten Fassung des Übereinkommens 108, als einziges internationales, rechtlich bindendes Instrument auf dem Gebiet des Datenschutzes, voranzutreiben. In einer Resolution werden die Regierungen der Mitgliedstaaten des Europarates, die Regierungen von Drittländern, die dem Europarat angehören, die Europäische Union und internationale Organisationen aufgefordert, den Prozess der Unterzeichnung und Ratifizierung dieses Übereinkommens zu beschleunigen. Eine zweite Resolution soll sicherstellen, dass die Konferenz weiterhin zu allen vorrangigen Themen der europäischen Datenschutzbehörden durchgeführt werden kann. Der EDÖB beteiligte sich in einer Arbeitsgruppe, die sich auf die Zukunft dieser Konferenz konzentriert und die vorgenannte Resolution vorschlug.

EUROPA

European Case Handling Workshop

Der Schwerpunkt des diesjährigen Workshops lag beim Umgang der Datenschutzbehörden mit den eingehenden Beschwerden, die seit dem Inkrafttreten der DSGVO stark zugenommen haben.

Die georgische Datenschutzbehörde (PDPS) organisierte als Gastgeberin vom 17.–19. November 2022 in Tiflis den «European Case Handling Workshop», eine Arbeitsgruppe zur Bearbeitung von Datenschutzfällen.

Es nahmen über 50 Mitarbeitende aus 26 EU- und Nicht EU-Datenschutzbehörden, wie dem EDÖB, teil. Vertreten waren auch der Europäische Datenschutzbeauftragte und der Beauftragte des Internationalen Komitees vom Roten Kreuz.

Der EDÖB wird Gastgeber des nächsten Workshops sein, der im November 2023 in Bern stattfindet.

INTERNATIONAL

Global Privacy Assembly

Die 44. Tagung der Global Privacy Assembly (GPA) fand vom 25. bis 28. Oktober 2022 statt. Die Teilnehmenden verabschiedeten zwei Resolutionen zur Stärkung der Cybersicherheit sowie zur Erarbeitung von Grundsätzen zur Regulierung der Gesichtserkennung.

Die Teilnahme des EDÖB an der 44. Global Privacy Assembly (GPA) erfolgte virtuell. Thema dieser Jahrestagung war «A Matter of Balance: Privacy in the Era of Rapid Technological Advancements» (etwa: Schutz der Privatsphäre in einer Zeit des raschen technologischen Fortschritts – eine Frage des Ausgleichs). Die Konferenz hat die Wichtigkeit des Gleichgewichts zwischen der Privatsphäre und den Technologien, die auf der Bearbeitung von personenbezogenen Daten beruhen, verdeutlicht.

Die öffentliche Sitzung war hauptsächlich dem Austausch über Privatsphäre und Menschenrechte gewidmet. In verschiedenen Panels wurden die Überwachung im Bereich Handel und Gewerbe, Datenschutz-Herausforderungen bei humanitären Krisen sowie Datenschutz und Wettbewerb diskutiert. Weitere Panels waren aktuellen Themen wie der künstlichen Intelligenz, dem Schutz der Privatsphäre von Kindern und dem grenzüberschreitenden Datentransfer gewidmet.

An der geschlossenen Sitzung vereinbarten die Teilnehmenden, unter denen sich der EDÖB befand, sich für den Ausbau der internationalen Zusammenarbeit auf dem Gebiet der Cybersicherheit einzusetzen und Grundsätze für die Regulierung der Gesichtserkennung zu erarbeiten.

Parallel dazu leitete der EDÖB die Arbeiten über die Rolle des Schutzes personenbezogener Daten in der internationalen Entwicklungshilfe, in der internationalen humanitären Hilfe sowie bei der Krisenbewältigung. Schliesslich verabschiedete die GPA zwei Resolutionen:

- Die Resolution zur Cybersicherheit mit dem Ziel, die Regulierung in diesem Bereich zu verbessern und das Bewusstsein für die durch Cybervorfälle verursachten Schäden zu schärfen. Die Möglichkeiten der

internationalen Zusammenarbeit, sowie der Wissens- und Informationsaustauschs zwischen GPA-Mitgliedern, sollen geprüft werden, einschliesslich technisches Fachwissen und Best Practices, damit einschlägige Untersuchungen und Regulierungsbestrebungen vereinfacht werden können. Eine Arbeitsgruppe erhielt den Auftrag, bis zum Herbst 2023 eine erste Auslegeordnung für die Arbeit an dieser Thematik vorzulegen.

- In der Resolution zur Gesichtserkennung wurden sechs Grundsätze und die Erwartungen an jene Einrichtungen definiert, die diese Technologie anwenden möchten.

Der EDÖB beteiligte sich aktiv an diesen Arbeiten und gehört zu den Mitverfassern der beiden Resolutionen. Paul Vane, Beauftragter für Datenschutz und Informationsfreiheit aus Jersey, wurde seinerseits in den Exekutivrat der GPA gewählt.

GPA

Arbeitsgruppe Entwicklungshilfe

Der Schutz personenbezogener Daten spielt im Rahmen der humanitären Hilfe eine zentrale Rolle. Die AG Entwicklungshilfe der GPA ist dieser spezifischen Thematik gewidmet. Sie hat verschiedene Vorhaben zur Stärkung des Schutzes der Privatsphäre in Notsituationen umgesetzt.

Die Grundsätze rechtsstaatlichen Handelns werden im Zusammenhang mit bewaffneten Konflikten, Naturkatastrophen oder anderen humanitären Krisen nicht immer vollumfänglich eingehalten. Die Arbeitsgruppe zur Rolle des Datenschutzes in der internationalen Entwicklungshilfe, in der humanitären Hilfe sowie bei der Krisenbewältigung (AG Entwicklungshilfe), die vor zwei Jahren eingerichtet wurde, hat deshalb ihre Tätigkeit ausgebaut.

Im Berichtsjahr konzentrierte sich die Arbeitsgruppe auf die Überarbeitung ihres Arbeitsplans 2021–2022 in Übereinstimmung mit den strategischen Prioritäten der GPA und dabei insbesondere auf den weltweiten Ausbau des Schutzes der Privatsphäre. Sie versandte zu diesem Zweck einen Fragebogen, aktualisierte die Kartierung der massgeblichen Akteure und baute die Beziehungen zu anderen internationalen Gremien und Netzwerken aus, die sich für Fortschritte beim Datenschutz und beim Schutz der Privatsphäre einsetzen.

Im Sinne der Ziele der Resolution setzten sich die Mitglieder der AG Entwicklungshilfe folgende grundlegende Ziele:

- auf die Bedürfnisse massgeblicher Akteure nach Zusammenarbeit eingehen, um Leitlinien zu entwickeln sowie beste Praktiken auszutauschen. Dabei sollen die spezifischen Gegebenheiten der internationalen Entwicklungshilfe und humanitären Hilfe berücksichtigt und die jeweiligen Tätigkeiten unterstützt werden.
- Entwicklung einer Strategie der Anwaltschaft und der Mobilisierung bei den massgeblichen Akteuren.

Um diese zwei Ziele zu erreichen, unternahm die AG Entwicklungshilfe hauptsächlich Folgendes:

- Schaffung eines ständigen Austauschs mit den massgeblichen Akteuren, sowohl auf bilateraler als auf multilateraler Ebene, um der Stimme der GPA maximales Gehör zu verleihen, indem die Beziehungen zu den Akteuren der internationalen Entwicklungshilfe verstärkt werden

- zusammen mit den übrigen relevanten Arbeitsgruppen der GPA Unterlagen und Tools für eine bessere Einbindung des Datenschutzes in den verschiedenen Tätigkeitsbereichen erarbeiten
- die Integration in die internationale Datenschutzgemeinschaft jener Empfängerländer vorantreiben, die über kein entsprechendes Regelwerk verfügen.

Die AG Entwicklungshilfe wurde 2020 anlässlich der 42. Global Privacy Assembly auf der Grundlage einer vom EDÖB eingereichten Resolution zur Rolle des Datenschutzes in der internationalen Entwicklungshilfe, in der internationalen humanitären Hilfe sowie bei der Krisenbewältigung ins Leben gerufen. Die Arbeitsgruppe zählt heute über 20 Mitglieder und steht seit ihrer Schaffung unter der Leitung des EDÖB.

AFAPDP

Französischsprachige Vereinigung der Datenschutzbehörden

Die Mitglieder der französischsprachigen Vereinigung der Datenschutzbehörden (AFAPDP), darunter der EDÖB, trafen sich am 3. und 4. Oktober 2022 in Tunis. Am französischsprachigen Treffen über den Schutz personenbezogener Daten nahmen Behörden aus 23 Ländern teil, die durch eine gemeinsame Sprache, eine gemeinsame juristische Tradition und gemeinsame Werte verbunden sind. Im Mittelpunkt der diesjährigen Arbeiten unter der Moderation des EDÖB standen das Konzept der Identität in all ihren Formen – hoheitlich oder digital – sowie Fragen betreffend der Zusammenarbeit und der Rolle des Datenschutzes im Bereich der internationalen Hilfe. In ihrer Rolle als Generalsekretärin der AFAPDP rief Marie-Laure Denis, Präsidentin der französischen Datenschutzbehörde CNIL, die unabhängigen Datenschutzbehörden auf, ihre Kräfte bei der Umsetzung der Strategie der digitalen Frankophonie 2022–2026 zu bündeln, um sich insbesondere auf dem Gebiet der Entwicklung des Datenschutzes und der Regulierung der Datenwirtschaft Gehör zu verschaffen.

Parallel zur Veranstaltung hielt die AFAPDP ihre Jahresversammlung ab und verabschiedete die Erklärung von Tunis über den Schutz personenbezogener Daten. Die Erklärung bekräftigt die Bedeutung des Datenschutzes, der zu den Grundvoraussetzungen für die Ausübung der übrigen Persönlichkeits- und Freiheitsrechte zählt. Er stellt in diesem Sinne ein Grundrecht unserer demokratischen Gesellschaften dar. Schliesslich wählten die Mitglieder das Büro, dem auch der EDÖB angehört.

BILATERAL

Empfang einer tunesischen Delegation

Im Rahmen des Programms TRUST (Transition redevable pour la société tunisienne) möchte die Schweiz ihre Erfahrung einbringen, um die öffentlichen Dienste Tunesiens durch mehr Rechenschaftspflicht zu stärken und letztlich das Vertrauen der Bürger in diese Stellen zu fördern.

Im Rahmen dieses Programms empfing Adrian Lobsiger, Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter, am 11. Mai 2022 seine tunesischen Amtskollegen Chawki Gaddès, Präsident der nationalen Behörde für den Schutz personenbezogener Daten (INPDP), und Adnène El Assoued, Präsident der nationalen Behörde für den Zugang zu Informationen (INAI), in Bern.

Im Mittelpunkt der Gespräche standen die verschiedenen Rechtsrahmen und die Herausforderungen hinsichtlich der fortschreitenden Digitalisierung in der Gesellschaft. Das Treffen bestätigte den hohen Stellenwert, den die internationale Zusammenarbeit für den EDÖB einnimmt. Der Anlass bot namentlich Gelegenheit, an den universellen Charakter des Datenschutzes zu erinnern und zu betonen, wie wichtig dieses Grundrecht in einer demokratischen Gesellschaft ist, und dass es die Voraussetzung für die Ausübung weiterer Grundrechte darstellt.

INTERNATIONALE ZUSAMMENARBEIT

Privacy Symposium in Venedig

Vom 5. bis 7. April 2022 trafen sich über 170 Teilnehmende, darunter der EDÖB, in Venedig zum ersten internationalen «Privacy Symposium». Ziel des Anlasses war die Förderung des internationalen Dialogs, der Zusammenarbeit sowie des Wissensaustauschs über Regularien, Compliance und neue Technologien.

Vom Schutz von Gesundheitsdaten über die künstliche Intelligenz bis hin zur Quanteninformatik und weiteren Themen, welche für die Gegenwart und Zukunft der Privatsphäre relevant sind: Das Symposium konnte klar aufzeigen, wie wichtig es ist, dass Rechtsexperten sowie Vertreter der Praxis und der Forschung zusammenkommen und ihre Kräfte bündeln, um den Datenschutz jenseits von Landes- und technologischen Grenzen zu stärken.

Eine Vertreterin des EDÖB konnte das neue Bundesgesetz über den Datenschutz vorstellen und über die neuesten Entwicklungen im Bereich der Zertifizierung in der Schweiz sowie über die Rolle des Datenschutzes in der humanitären Hilfe referieren.

SCHENGEN

Borders, Travel and Law Enforcement Group

Die Borders, Travel and Law Enforcement Gruppe des Europäischen Datenschutzausschusses behandelte in Anwesenheit des EDÖB Themen zum Schengen-Besitzstand wie die Gesichtserkennung bei der Strafverfolgung und das 2022 ergangene «Passenger Name Record»-Urteil des Europäischen Gerichtshofes.

Der EDÖB nahm an den Sitzungen der Borders, Travel and Law Enforcement (BTLE) Gruppe, einer Experten-Untergruppe des Europäischen Datenschutzausschusses (EDSA) zur Behandlung der Schengen relevanten Themen, teil.

Die Gruppe hat einen Praxis-Leitfaden für Strafverfolgungsbehörden bei der Anwendung von Gesichtserkennungstechnologie behandelt, den sie im Mai 2022 verabschiedet hat (Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement).

Weiter hat die Gruppe das am 21. Juni 2022 ergangene Urteil des Europäischen Gerichtshofes (EuGH) betreffend die Umsetzung der sog. PNR-Richtlinie («Passenger Name Record) besprochen. Die Richtlinie regelt die Verwendung von Fluggastdatensätzen (PNR-Daten) zu Zwecken der Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung

von terroristischen Straftaten und schwerer Kriminalität. Der EuGH führte aus, dass die Staaten bei der Umsetzung der PNR-Richtlinie die Eingriffe unbedingt auf das erforderliche Mass zu beschränken haben. So seien die in der PNR-Richtlinie genannten Zwecke abschliessend geregelt. Die Anwendung des PNR-Systems sei nur auf terroristische Straftaten und schwere Kriminalität gerichtet, das heisst, dass gewöhnliche Kriminalität ausgeschlossen sei. Es dürfe keine unterschiedslose Anwendung der allgemeinen Speicherfrist von fünf Jahren auf alle personenbezogenen Daten von Fluggästen erfolgen.

Aufgrund der Vorarbeiten von BTLE hat der EDSA die Stellungnahme 5/2022 zu den Auswirkungen des EuGH-Urteils C-817/19 betreffend die Umsetzung der Richtlinie (EU) 2016/681 über die Verwendung von Fluggastdatensätzen in den Mitgliedstaaten vom 13. Dezember 2022 erlassen. Auch wenn die Schweiz nicht an Urteile des EuGH gebunden ist, dürfte dieses im aktuellen Gesetzgebungsprozess zu einem neuen Flugpassagierdatengesetz (FPG) Beachtung finden.

SCHENGEN

Aufsichtskoordinationsgruppen über die Informationssysteme SIS II, VIS und Eurodac

Thema der SIS-Aufsichtskoordinationsgruppe waren insbesondere der neue Evaluierungs- und Überwachungsmechanismus sowie der neue Rechtsrahmen betreffend das SIS.

Die Koordinierungsgruppen SIS II, VIS und Eurodac sind vom EU-Recht eingerichtete Gremien, die den Schutz personenbezogener Daten in den entsprechenden Informationssystemen überwachen. Sie bestehen aus Vertretern der nationalen Datenschutzbehörden und dem Europäischen Datenschutzbeauftragten.

Mit dem neuen Evaluierungs- und Überwachungsmechanismus sollen die Schengen-Mitgliedstaaten, darunter auch die Schweiz, nicht mehr alle fünf, sondern alle sieben Jahre evaluiert werden. Gleichzeitig wird ein Expertenpool geschaffen. Für die Schengen-Evaluierungen in Sachen Datenschutz hat der EDÖB einen Experten gemeldet, der inzwischen für eine Evaluierung nominiert worden ist.

Der neue SIS-Rechtsrahmen sieht weiterhin vor, dass der Europäische Datenschutzbeauftragte und die nationalen Aufsichtsbehörden – darunter auch der EDÖB – mindestens zweimal jährlich im Rahmen des Europäischen Datenschutzausschusses (EDSA) zusammenkommen. Im Weiteren wurde der zweijährliche Tätigkeitsbericht der SIS II SCG verabschiedet.

Wie in anderen Bereichen der Schengen-Evaluierung seit Jahren üblich, soll nun auch im Bereich Datenschutz den künftigen Expertinnen und Experten ermöglicht werden, eine Ausbildung zu durchlaufen. Weiter soll künftig darauf verzichtet werden, dass für die Aufnahme in den Expertenpool eine Personensicherheitsprüfung (PSP), sog. Security Clearance, vorzuweisen ist.

SCHENGEN

Schengen Koordinationsgruppe der schweizerischen Datenschutzbehörden

Im Rahmen der vom EDÖB präsidierten Schengen Koordinationsgruppe haben sich die Datenschutzbehörden von Bund und Kantonen sowie des Fürstentums Liechtenstein ausgetauscht.

Der EDÖB informierte über die Arbeitsergebnisse der europäischen Aufsichtskoordinationsgruppen über die Informationssysteme SIS II und VIS vom 1./2. Juni und 22./23. November 2022 in Brüssel, während die kantonalen Datenschutzbehörden über Erfahrungen aus den von ihnen durchgeführten Kontrollen berichteten.

Eine Unterarbeitsgruppe aus Vertretern des EDÖB und der Kantone Basel-Land und Zürich passte den Leitfaden zur Kontrolle der Nutzung des Schengener Informationssystems in Bezug auf die veränderte europäische Rechtslage an. Der Leitfaden dient primär den kantonalen Aufsichtsbehörden als Orientierungshilfe bei der Durchführung von Kontrollen. Ferner haben die Vertreterinnen und Vertreter von ihren Erfahrungen und Feststellungen aus den behördlichen Kontrollen, insbesondere von Log-Files, berichtet. Die Erfahrungen sollen künftig strukturiert gesammelt werden.

SCHENGEN

Tätigkeiten betreffend Schengen auf nationaler Ebene

EU verschiebt die Evaluierung der Schweiz um zwei Jahre auf 2025.

Die von der EU auf Anfang 2023 vorgesehene Schengen-Evaluierung der Schweiz wurde um zwei Jahre verschoben. Hintergrund für diesen Entscheid ist der Erlass der europäischen Verordnung (EU) 2022/922 über die Einführung und Anwendung eines Evaluierungs- und Überwachungsmechanismus für die Überprüfung der Anwendung des Schengen-Besitzstands, die im EU-Raum bereits ab Februar 2023 anwendbar ist. Als Weiterentwicklung des Schengen- Besitzstands ist diese Verordnung in der Schweiz erst in einem späteren Zeitpunkt anwendbar, weil sie zunächst durch die Bundesversammlung genehmigt und danach in nationales Recht umgesetzt werden muss. Diese spätere Anwendbarkeit führte auch dazu, dass die EU-Kommission die Schweiz im Jahr 2025 und nicht wie ursprünglich geplant im Jahr 2023 evaluieren will.

Ferner hat die EU-Kommission die Schengen-Staaten aufgefordert, im Bereich Datenschutz Expertinnen und Experten für die Evaluierung anderer Staaten zu ernennen. Dafür haben das Bundesamt für Justiz und das EDA am 12. Mai 2022 ein Expertentreffen Schengen-Evaluierung (SCHEVAL) organisiert. Expertinnen und Experten aus den verschiedenen Fachgebieten wie Polizeikooperation, SIS/SIRENE und Datenschutz haben Interessierte und künftige Expertinnen und Experten über die Zusammenarbeit mit der europäischen Kommission, den Ablauf einer Evaluierung und Angebote von Trainings informiert sowie praktische Ratschläge erteilt.

Der EDÖB hat zudem im Berichtsjahr bei fedpol als zentrale Zugangsstelle des C-VIS betreffend die Abfrage von VIS-Daten zum Zwecke der Verhütung, Aufdeckung oder Ermittlung terroristischer und sonstiger schwerwiegender Straftaten eine Kontrolle eröffnet. Zunächst hat er einen Fragebogen versandt und sich bei einem Besuch vor Ort Restfragen beantworten lassen. Nach Erstellung des Sachverhalts wird der EDÖB die rechtliche Analyse durchführen.

Öffentlichkeitsprinzip

2.1 Allgemein

Das Öffentlichkeitsgesetz soll die Transparenz über den Auftrag, die Organisation und die Tätigkeit der Verwaltung fördern, indem es der Öffentlichkeit den Zugang zu amtlichen Dokumenten gewährleistet (vgl. Art. 1 BGÖ). Das Öffentlichkeitsprinzip soll das Vertrauen in Staat und Behörden fördern, das Verwaltungshandeln nachvollziehbar machen und dadurch die Akzeptanz staatlichen Handelns erhöhen.

Das Berichtsjahr 2022 war im ersten Semester noch geprägt von den Folgen der abklingenden Pandemie. Die von der Bundesverwaltung gelieferten Zahlen zu den 2022 eingegangenen Gesuchen um Zugang zu amtlichen Dokumenten lassen erkennen, dass das Bedürfnis von Medien und Gesellschaft nach spezifischer, transparenter Information weiterhin gross ist. Auch wenn im Berichtsjahr leicht weniger Zugangsgesuche bei den Bundesbehörden eingereicht worden sind als im Vorjahr, ist deren Anzahl nach wie vor auf einem hohen Niveau.

Die Bearbeitung der Zugangsgesuche generierte in vielen Fällen einen grossen Ressourcenaufwand, nicht zuletzt, weil die Gesuche oftmals umfangreich waren oder eine amts- oder departementsübergreifende Koordination notwendig war. Aus den nachfolgenden Zahlen (s. Kap. 2.2) ist zu entnehmen, dass die in den letzten Jahren festgestellte Tendenz eines konstant hohen Anteils an Fällen, in welchen der Zugang vollständig gewährt wird, auch für das Berichtsjahr bestätigt werden kann.

Sind Gesuchstellende oder von der Zugangsgewährung betroffene Dritte mit der von der Behörde beabsichtigten Zugangsgewährung nicht einverstanden, bietet das Öffentlichkeitsgesetz diesen die Möglichkeit, beim Beauftragten einen Antrag auf Schlichtung einzureichen. Der Beauftragte verzeichnete im Berichtsjahr 129 eingegangene Schlichtungsanträge, was im Vergleich zum Vorjahr einen Rückgang von 13 Prozent bedeutet. Ziel des Schlichtungsverfahrens ist die rasche Einigung zwischen den Beteiligten. Die zu diesem Zweck mit dem Pilotversuch im Jahr 2017 eingeführten Massnahmen und insbesondere das Primat der mündlichen Schlichtungsverhandlungen haben sich auch im 2022 bewährt. Die Auswertung der im Berichtsjahr erledigten Schlichtungsanträge ergibt, dass in jenen Fällen, in welchen eine Schlichtungssitzung durchgeführt werden konnte, in 75 Prozent eine einvernehmliche Lösung resultierte.

Im Januar 2022 sah sich der Beauftragte angesichts der epidemiologischen Lage und der in der in diesem Zeitraum noch geltenden Homeoffice-Pflicht veranlasst, auf die Durchführung von Schlichtungssitzungen zu verzichten, da diese u. a. aus Gründen des Informationsschutzes nicht per Videokonferenz durchgeführt werden können. In den elf Schlichtungsverfahren, in welchen pandemiebedingt auf eine Schlichtungssitzung verzichtet werden musste, konnte im schriftlichen Verfahren in keinem der Fälle eine Einigung erzielt werden.

Wegen dem pandemiebedingt geringeren Anteil an einvernehmlichen Lösungen und höheren Anteil an schriftlich durchgeführten Verfahren kam es auch zu einer längeren Bearbeitungsdauer der Schlichtungsverfahren und einem damit verbundenen

Rückstau bei der Erledigung der Verfahren. Damit unterstreichen die ausgewerteten Zahlen, dass die Durchführung von Schlichtungssitzungen vor Ort mit Anwesenheit der Beteiligten für die Erreichung des Ziels der raschen Verfahrenserledigung unverzichtbar ist.

Die Pandemie, die ungebrochen hohe Zahl an Schlichtungsanträgen und die zunehmende Komplexität der Rechtsfragen führten dazu, dass der Beauftragte bei einem ansteigenden Anteil der Verfahren die gesetzliche Erledigungsfrist von 30 Tagen überschreitet. Der Beauftragte geht davon aus, dass es u. a. dank den vom Parlament zusätzlich gesprochenen Ressourcen gelingen wird, die Bearbeitungsfristen wieder zu senken (s. Kap. 2.3).

Auch in diesem Berichtsjahr mussten Bestrebungen festgestellt werden, zusätzliche Teilbereiche der Verwaltungstätigkeit oder bestimmte Kategorien von Dokumenten vom Öffentlichkeitsgesetz auszunehmen (z. B. Rettungsschirm Strombranche, s. Kap. 2.4). Solche Ausnahmen vom Geltungsbereich des Öffentlichkeitsgesetzes führen zu einer Schwächung des Öffentlichkeitsprinzips und der damit bezweckten Verwaltungstransparenz. Neu publiziert der Beauftragte im Tätigkeitsbericht eine aktuelle Übersicht über die spezialgesetzlichen Vorbehalte gemäss Art. 4 BGÖ (s. Kap. 2.5).

Der Beauftragte stellt fest, dass der mit dem Öffentlichkeitsgesetz erfolgte Paradigmenwechsel vom Gros der Verwaltung vollzogen ist und auch aktiv umgesetzt wird. In der Tat haben die dem Öffentlichkeitsgesetz unterstellten Bundesbehörden keinen direkten Einfluss auf die Zahl, den Umfang und den Erledigungsaufwand der Zugangsgesuche. Für das Berichtsjahr lässt sich eine Tendenz zu vermehrten Gesuchen um Zugang zu Verschriftungen der elektronischen Kommunikation feststellen.

Im Einflussbereich der Verwaltung und ihrer Öffentlichkeitsberatenden liegt hingegen die konsequente Anwendung der Bestimmungen des Öffentlichkeitsgesetzes und der einschlägigen Rechtsprechung. In der Praxis des Beauftragten zeigt sich, dass Teile der Bundesverwaltung die vom Öffentlichkeitsgesetz zur Verfügung gestellten Möglichkeiten zur Wahrung ihrer Geheimhaltungsinteressen ungenügend nutzen und es u. a. unterlassen, Zugangsbeschränkungen mit der von der Rechtsprechung verlangten Begründungsdichte geltend zu machen. Der Beauftragte verweist in diesem Zusammenhang auf seine schriftliche Empfehlungspraxis, die auf seiner Webseite integral publiziert ist (www.derbeauftragte.ch) und aufzeigt, dass es im Berichtsjahr vereinzelt zu Fällen gekommen ist, in denen die Verwaltung die Anwendung des Öffentlichkeitsgesetzes verweigerte. So u. a. indem sie dem Beauftragten die vom Gesetz zwingend und ausnahmslos vorgeschriebene Einsicht in Dokumente versagte, welche Gegenstand eines eingereichten Schlichtungsgesuches waren, was zur Folge hatte, dass er seine Schlichtungstätigkeit nicht wahrnehmen konnte.

2.2 Zugangsgesuche – leichter Rückgang im Jahr 2022

Gemäss den Zahlen, die von den Bundesbehörden gemeldet wurden, gingen im Berichtsjahr 1153 Zugangsgesuche ein (2021 waren es 1385 Gesuche); dies entspricht einem Rückgang von 15 Prozent gegenüber 2021. Hinzu kommen 27 im Jahr 2022 bearbeitete Zugangsgesuche, welche in Vorjahren eingereicht worden sind. Dabei gewährten die Behörden insgesamt in 624 Fällen (53 Prozent) einen vollständigen Zugang (gegenüber 694 bzw. 50 Prozent im Jahr 2021), währenddem bei 236 Gesuchen (20 Prozent) ein teilweiser respektive aufgeschobener Zugang zu den Dokumenten gewährt wurde (Vorjahr: 324 Gesuche resp. 23 Prozent). In 99 Fällen (acht Prozent) wurde die Einsichtnahme vollständig verweigert (gegenüber 126 bzw. neun Prozent im Jahr 2021). Nach Angaben der Behörden wurden 53 Zugangsgesuche zurückgezogen (fünf Prozent gegenüber 48 bzw. drei Prozent im Jahr 2021), 69 Gesuche waren Ende 2022 noch hängig, und in 99 Fällen war kein amtliches Dokument vorhanden.

Es ist davon auszugehen, dass auch in den kommenden Jahren mit einer ähnlich hohen Anzahl Gesuchen wie in den letzten Jahren zu rechnen ist, wenngleich sich das während der Coronapandemie besonders ausgeprägte Informations- und Transparenzbedürfnis im Berichtsjahr abgeflacht hat. Die Behörden konnten die Zugangsgesuche für «Corona-Dokumente» statistisch erfassen und dem Beauftragten zusammen mit den jährlich zu meldenden Angaben übermitteln (s. gelb markierte Statistik Zugangsgesuche zu Corona-Dokumenten). Gemäss Angaben der Bundesbehörden wiesen 93 von den insgesamt 1180 bearbeiteten Zugangsgesuchen (acht Prozent) einen Bezug zu Corona auf, was im Vergleich zum Vorjahr (24 Prozent) einen erheblichen Rückgang darstellt. Dabei zeigt sich, dass der vollständige Zugang in 29 Fällen (31 Prozent) und damit im Vergleich zur Gesamtstatistik weniger oft gewährt wurde. Während die Behörden in 35 Fällen (38 Prozent) und damit in Bezug auf Corona-Dokumente öfter den Zugang teilweise gewährt oder aufgeschoben haben, kann hinsichtlich der vier Fälle der vollständigen Zugangsverweigerung (vier Prozent) ein um die Hälfte tieferer Anteil im Verhältnis zur Gesamtstatistik festgestellt werden. Sieben Zugangsgesuche wurden zurückgezogen, acht Gesuche waren Ende 2022 noch hängig und in zehn Fällen war kein amtliches Dokument vorhanden. Es ist damit zu rechnen, dass die gesellschaftliche Aufarbeitung der behördlichen Massnahmen zur Bekämpfung der Pandemie andauern und auch noch im Jahre 2023 Zugangsgesuche und Schlichtungsanträge mit Bezügen zur Pandemie eingehen dürften.

Zusammenfassend stellt der Beauftragte fest, dass seit 2015 in mindestens 50 Prozent der Fälle ein vollständiger Zugang zu den Dokumenten gewährt wird und sich die vollständigen Zugangsverweigerungen im Laufe der Jahre auf knapp zehn Prozent einpendelten.

Departemente und Bundesämter

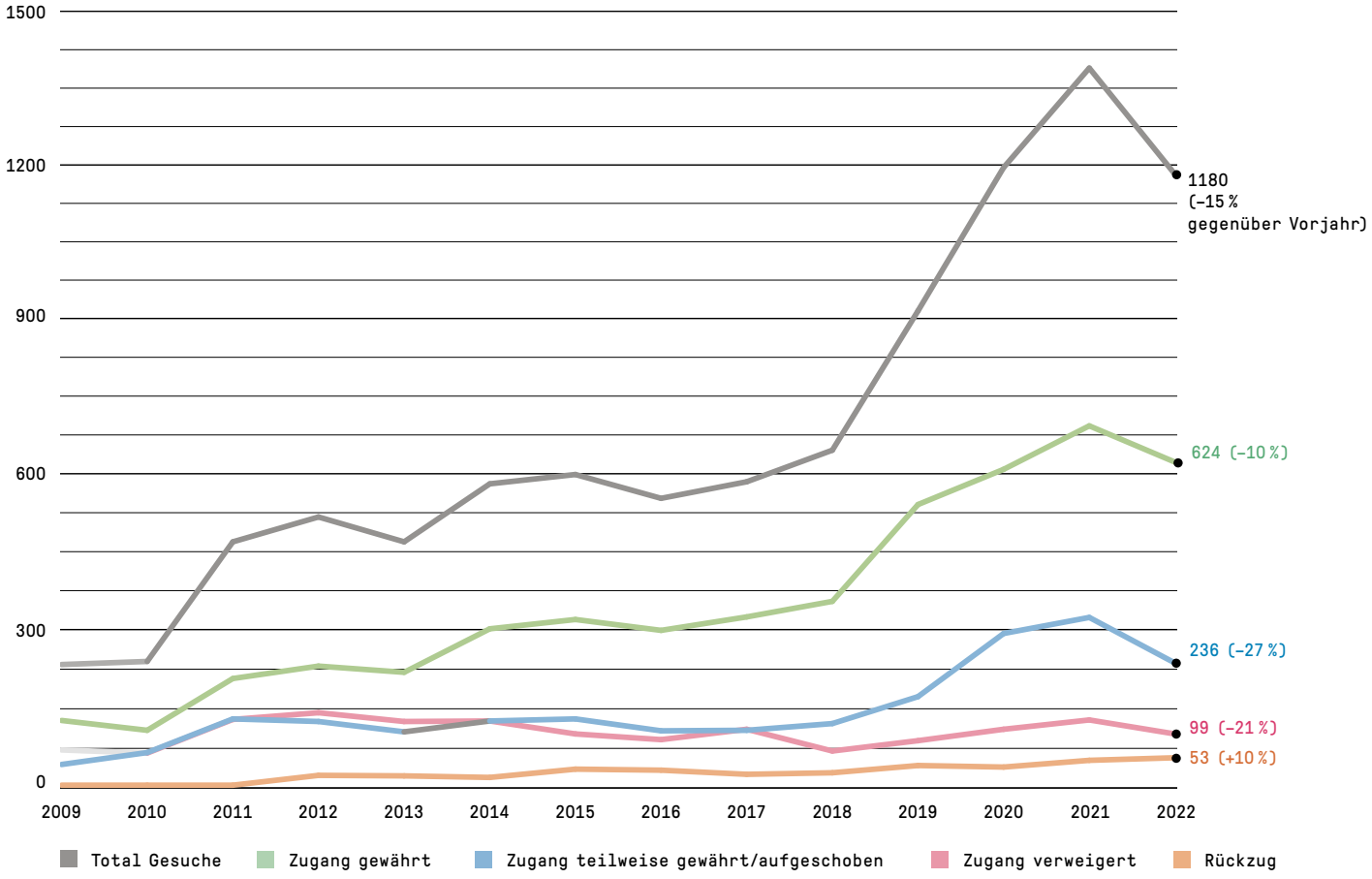
Einzelne Verwaltungseinheiten standen im Jahr 2022 besonders im Fokus der Medien und der Gesellschaft. Aufgabenbedingt sahen sich insbesondere – wie aufgrund der Coronapandemie bereits in den Vorjahren – das EDI (198) und auch das VBS (294) und das EDA (164) mit einer grossen Anzahl von eingegangenen Zugangsgesuchen konfrontiert. Im Fall des EDI richteten sich departementsübergreifend 38 Prozent der Gesuche auf den Zugang zu amtlichen Dokumenten mit Corona-Bezug (Vorjahr 63 Prozent). Gemäss den Behörden handelte es sich dabei teilweise um sehr umfangreiche und komplexe

Gesuche. In einer Vielzahl von Fällen war auch eine verwaltungsinterne Koordination zwischen Ämtern oder Departementen notwendig.

Auf Stufe Amt zeigen die gemeldeten Zahlen, dass das BASPO mit 220 Fällen im Jahr 2022 am meisten eingegangene Zugangsgesuche meldete. Das BAG meldete für das Berichtsjahr 91 eingegangene Gesuche, wovon 57 Zugangsgesuche Dokumente mit einem Bezug zu Corona-Aspekten betrafen. Danach folgen das BAFU mit 61, Swissmedic und das SECO mit je 37 Gesuchen. 17 Behörden meldeten, dass im Berichtsjahr bei ihnen kein Zugangsgesuch eingegangen ist. Beim Beauftragten selbst sind 15 Zugangsgesuche eingegangen, wobei er den Zugang in neun Fällen vollständig gewähren konnte. In zwei Fällen hat er den Zugang vollständig verweigert. Ein Gesuch wurde zurückgezogen und drei Zugangsgesuche waren Ende 2022 noch hängig.

Der 2022 für den Zugang zu amtlichen Dokumenten erhobene Gebührenbetrag beläuft sich auf insgesamt CHF 24 582.05 und liegt 65 Prozent über der Vorjahressumme (CHF 14 924.90). Während das EDA, das EFD, das VBS, die Parlamentsdienste, die Bundesanwaltschaft und die Bundeskanzlei überhaupt keine Gebühren erhoben, verrechneten die übrigen vier Departemente den Gesuchstellenden einen Teil ihres Zeitaufwands (EDI: CHF 19 646.50; WBF: CHF 4 185.55; UVEK: CHF 500.00; EJPD: CHF 250.00). Dazu sei vermerkt, dass lediglich bei 29 der 1180 bearbeiteten Zugangsgesuchen eine Gebühr erhoben wurde.

Grafik 1: Beurteilung Zugangsgesuche – Entwicklung seit 2009



Wie in den Vorjahren stellt die Erhebung von Gebühren eine Ausnahme dar: Knapp 98 Prozent der Zugangsgesuche im Berichtsjahr waren gebührenfrei.

Die auch im Berichtsjahr gelebte Verwaltungspraxis, wonach amtliche Dokumente grundsätzlich kostenlos eingesehen werden können, wird im Öffentlichkeitsgesetz neu verankert werden: Am 30. September 2022 hat das Parlament den Grundsatz der Kostenlosigkeit des Zugangs zu amtlichen Dokumenten beschlossen. Ausnahmsweise können auch nach dem vom Bundesrat noch zu bestimmenden Inkrafttreten der Gesetzesänderung Gebühren erhoben werden, wenn ein Zugangsgesuch eine besonders aufwändige Bearbeitung durch die Behörde erfordert. Entsprechend wird im Rahmen der Überarbeitung der Öffentlichkeitsverordnung die Anzahl Arbeitsstunden vorzugeben sein, ab welcher für die Bearbeitung eines Gesuchs eine Gebühr erhoben werden kann.

Was den Zeitaufwand für die Bearbeitung von Zugangsgesuchen anbelangt, weist der Beauftragte 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 dem Beauftragten auf freiwilliger Basis übermittelten Angaben widerspiegeln die tatsächlich geleisteten Arbeitsstunden daher nur bedingt. Gemäss diesen Angaben hat der Zeitaufwand für das

Berichtsjahr mit 5404 Stunden im Vergleich zum Vorjahr (5562 Stunden) leicht abgenommen.

Dass die von den Behörden gemeldeten Aufwände nur bedingt dem tatsächlichen Zeitaufwand entspricht, lässt sich exemplarisch an den Angaben des BAG erkennen, das in besonderem Mass von Zugangsgesuchen im Zusammenhang mit der Pandemie betroffen war. Zusätzlich zu den von den zuständigen Facheinheiten des BAG punktuell angegebenen Aufwandzeiten von 443 Stunden und der juristischen Unterstützung durch seine Öffentlichkeitsberaterin im Umfang von 40 Stellenprozenten, meldete das BAG für die Bearbeitung der Zugangsgesuche im Zusammenhang mit Covid-19 (einschliesslich Schlichtungs- und Beschwerdeverfahren) einen weiterhin hohen Aufwand, welcher mindestens 3.5 Vollzeitstellen (Full Time Equivalent) betragen haben soll.

Eine Zunahme ist auch beim gemeldeten Zeitaufwand für die Vorbereitung von Schlichtungsverfahren auszumachen: 1006 Stunden gegenüber 865 Stunden im Vorjahr (vgl. dazu im Jahr 2020: 569 Stunden; 2019: 473 Stunden; 2018: 672 Stunden und 2017: 914 Stunden).

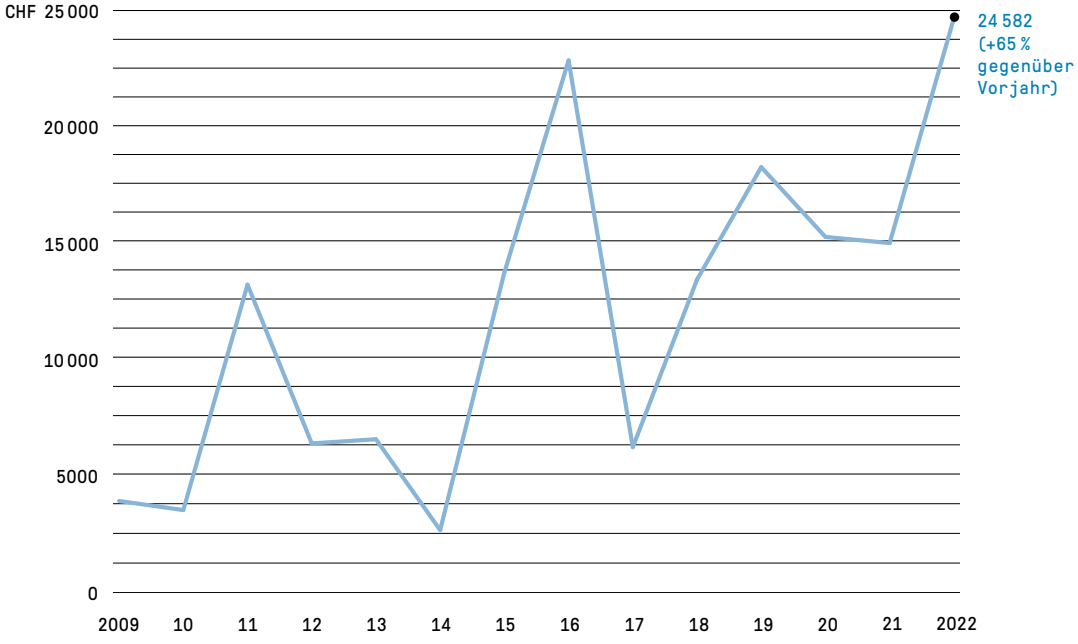
Parlamentsdienste

Gemäss Angabe der Parlamentsdienste ist bei ihnen im Berichtsjahr kein Zugangsgesuch eingegangen.

Bundesanwaltschaft

Die Bundesanwaltschaft meldete für 2022 den Eingang von sechs Gesuchen. In fünf Fällen wurde der Zugang vollumfänglich gewährt und in einem Fall vollständig verweigert.

Grafik 2: Erhobene Gebühren seit Inkrafttreten des BGÖ



2.3 Schlichtungsverfahren – leichter Rückgang der Schlichtungsanträge

Im Jahr 2022 wurden beim Beauftragten 129 Schlichtungsanträge eingereicht. Verglichen mit den 2021 eingegangenen 149 Anträgen entspricht dies einem Rückgang um 13 Prozent. Die meisten Schlichtungsanträge wurden von Medienschaffenden (47) und Privatpersonen (37) eingereicht. In den 434 Fällen, in denen die Bundesverwaltung den Zugang vollständig oder teilweise verweigerte, beziehungsweise aufschob oder vorbrachte, dass keine amtlichen Dokumente vorhanden sind, kam es 129 Mal bzw. in 30 Prozent der Fälle zur Einreichung eines Schlichtungsantrags. Davon betrafen 13 Anträge (neun Prozent) amtliche Dokumente mit einem Bezug zu Corona.

2022 konnten 115 Schlichtungsanträge erledigt werden. Davon waren 93 im Berichtsjahr und 22 im Vorjahr eingegangen. In 50 Fällen konnten sich die Beteiligten auf eine Konsenslösung einigen. Ausserdem erliess der Beauftragte 31 Empfehlungen, durch welche 48 Fälle erledigt werden konnten, in denen eine einvernehmliche Lösung zwischen den Parteien nicht ersichtlich war.

Zu den abgeschlossenen Fällen zu zählen sind auch 13 Anträge, die nicht fristgerecht eingereicht wurden, drei Fälle, in denen die Voraussetzungen für die Anwendung des Öffentlichkeitsgesetzes nicht gegeben waren, sowie ein Schlichtungsantrag, der zurückgezogen wurde.

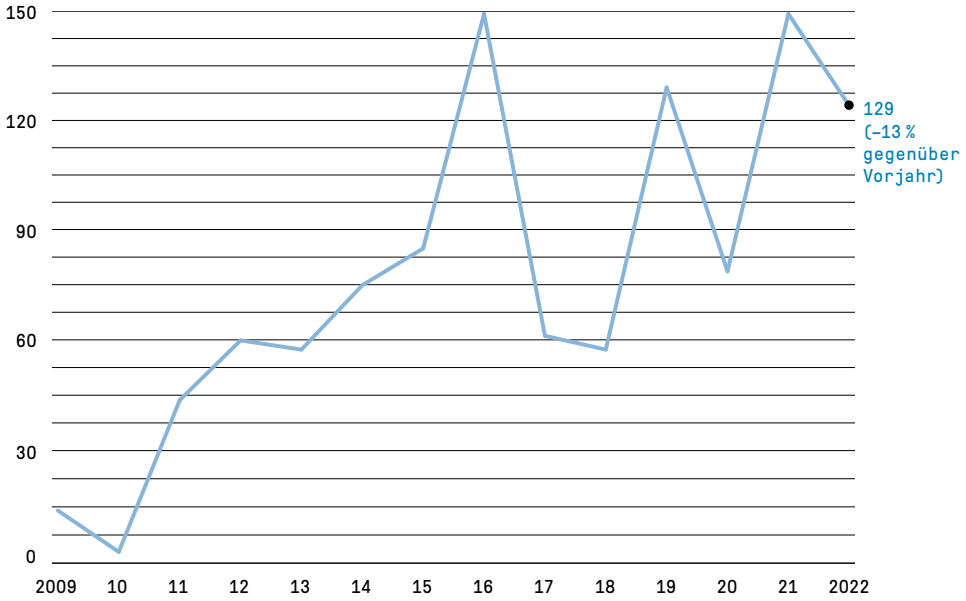
Per Ende Jahr war in 13 Schlichtungsverfahren im Einvernehmen mit den Beteiligten resp. auf Wunsch der Antragstellenden hin eine Sistierung erfolgt.

Anteil einvernehmlicher Lösungen

Zu den vielen Vorteilen der einvernehmlichen Lösungen gehört u. a. auch, dass sie eine Klärung der Sachlage und eine Beschleunigung des Zugangsverfahrens ermöglichen und zudem die allfällige zukünftige Zusammenarbeit zwischen den an der Schlichtungssitzung Beteiligten erleichtern.

Wie wirksam sich die 2017 eingeführten Massnahmen und die Durchführung von mündlichen Schlichtungssitzungen erwiesen haben, lässt sich am Anteil der einvernehmlichen Lösungen im Verhältnis zu den Empfehlungen ablesen. Im Berichtsjahr konnten 50 einvernehmliche Lösungen erzielt werden, und der Beauftragte gab 31 schriftliche Empfehlungen zur Lösung von 48 Fällen ab. Die einvernehmlichen Lösungen machen somit

Grafik 3: Schlichtungsanträge seit Inkrafttreten des BGÖ



einen Anteil von 51 Prozent aus. Hierzu bedarf es allerdings einiger Erläuterungen: Eine einvernehmliche Lösung kann in aller Regel nur dann erreicht werden, wenn eine Schlichtungsverhandlung durchgeführt werden kann. So konnte im Berichtsjahr in den 43 durchgeführten Schlichtungsverhandlungen in 32 Fällen (75 Prozent) eine Einigung erzielt werden. Wie in Kapitel 2.1 bereits erwähnt, haben die zur Eindämmung des Coronavirus in Kraft gesetzten Massnahmen dazu geführt, dass im Zeitraum zwischen 20. Dezember 2021[1] und 3. Februar 2022[2] und damit in 11 Fällen auf die Durchführung von Schlichtungssitzungen mit physischer Anwesenheit der Beteiligten verzichtet werden musste. In keinem der in diesem Zeitraum schriftlich durchgeführten Verfahren konnte eine Einigung erzielt werden, was sich in der Statistik entsprechend negativ auswirkt.

Im Ergebnis führt das Ausgeführte zur Feststellung, dass mündliche Schlichtungsverhandlungen zur Erreichung der gesetzgeberischen Ziele unverzichtbar und für alle Verfahrensbeteiligten vorteilhaft sind. Der Beauftragte wird diese Vorgehensweise gegenüber den schriftlichen Verfahren weiterhin bevorzugen und fördern.

Tabelle 1: Einvernehmliche Lösungen

2022 (Corona-Einfluss)	**51 %**
2021 (Corona-Einfluss)	44 %
2020 (Corona-Einfluss)	34 %
2019	61 %
2018	55 %

Dauer der Schlichtungsverfahren

Nachstehende Tabelle ist in drei von der Verfahrensdauer abhängige Spalten aufgeteilt. Präzisierend ist festzuhalten, 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 die Verwaltung 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 oder Krankheit), wird die Zeitspanne zwischen dem ursprünglich vorgesehenen Termin und dem neu angesetzten Termin bzw. die daraus resultierende Verfahrensverlängerung ebenfalls nicht zur Bearbeitungsdauer gezählt.

[1] Art. 20 der Covid-19-Verordnung besondere Lage; BRB vom 17.12.2022.

[2] Art. 25 Abs. 5 der Covid-19-Verordnung besondere Lage; BRB vom 2.2.2022; Massnahmen und Verordnungen (admin.ch).

Aus der Tabelle wird ersichtlich, dass – teilweise noch pandemiebedingt – nur 25 Prozent der im Jahr 2022 abgeschlossenen Schlichtungsverfahren innerhalb der ordentlichen Frist von 30 Tagen abgearbeitet wurden. In 42 Prozent der Fälle dauerte das Schlichtungsverfahren zwischen 31 und 99 Tagen und in 33 Prozent gar länger als 100 Tage.

Hierzu ist anzumerken, dass von den 29 innerhalb der Frist von 30 Tagen abgearbeiteten Schlichtungsanträgen das Schlichtungsverfahren nur in 17 Fällen (59 Prozent) durch eine Einigung oder Empfehlung erledigt wurde und dementsprechend eine materielle Auseinandersetzung mit dem Schlichtungsgegenstand stattgefunden hat. In den anderen 12 Fällen (41 Prozent) resultierte keine materielle Beurteilung in der Sache; es handelte sich dabei insbesondere um Fälle, welche offensichtlich nicht in den Geltungsbereich des Öffentlichkeitsgesetzes fielen oder in welchen die formellen Voraussetzungen für die Eröffnung eines Schlichtungsverfahrens nicht gegeben waren.

Wie vorne dargelegt, führte die Pandemie auch im Berichtsjahr zu einer verlängerten Verfahrensdauer und damit zu einem weiteren Anwachsen der Bearbeitungsrückstände. Hinzu kommt, dass die Anzahl der eingehenden Schlichtungsanträge Schwankungen ausgesetzt ist. Während beispielswiese im März (21) und im August (27) sehr viele Anträge beim Beauftragten eingegangen sind, gingen im Juni nur drei und im November gar keine Anträge ein.

Die Vorgabe der gesetzlichen Frist von 30 Tagen für die Durchführung von Schlichtungsverfahren konnte in den Vorjahren regelmässig eingehalten werden, wenn die Schlichtungssitzungen erfolgreich mit einer Einigung abgeschlossen werden konnten. Für das Berichtsjahr gilt dies nicht mehr: im Falle der Erledigung des Verfahrens durch eine Einigung konnte die 30-tägige Frist nur noch in 28 Prozent der Fälle eingehalten werden (gegenüber 60 Prozent im Vorjahr). Hatte der Beauftragte mangels einvernehmlicher Lösung eine Empfehlung auszusprechen, konnte er den Beteiligten die schriftliche Empfehlung sogar nur in drei Fällen (sechs Prozent) innert 30 Tagen nach Eingang des Antrags und damit innert gesetzlicher Frist zustellen.

Häufige Gründe für eine Fristüberschreitung waren ausserdem ausserordentlich umfangreiche Zugangsbegehren, eine grosse Zahl der am Verfahren beteiligten Drittpersonen oder die juristische, technische oder politische Komplexität der Fragestellungen. Diese Gründe treffen auch auf jene 38 Fälle zu, deren Bearbeitung mehr als 100 Tage in Anspruch nahm. Auch wurde die Einhaltung der Fristen aufgrund der Fülle an Dokumenten oder der Vielzahl betroffener Personen zusätzlich erschwert. Weil die Bearbeitung in solchen Fällen besonders aufwändig ist, steht es dem Beauftragten gemäss Artikel 12a der Verordnung über das Öffentlichkeitsprinzip der Verwaltung (VBGÖ; SR 152.31) frei, die ordentliche Frist angemessen zu verlängern.

Der Gesetzgeber hat das Schlichtungsverfahren als ein informelles und unpräjudizielles Verfahren zur gütlichen Streitbeilegung ausgestaltet. Die Erfahrung zeigt, dass der Beizug von Rechtsvertretungen durch Gesuchstellende oder angehörte Drittbetroffene bereits im Stadium des Zugangs- und Schlichtungsverfahrens einer einfachen, pragmatischen und raschen Lösungsfindung wenig förderlich ist.

Tabelle 2: Bearbeitungsdauer Schlichtungsverfahren

Bearbeitungsdauer in Tagen	Zeitraum 2014 – August 2016*	Pilotphase 2017	Zeitraum 2018	Zeitraum 2019	Zeitraum 2020	Zeitraum 2021	Zeitraum 2022
innert 30 Tagen	11 %	59 %	50 %	57 %	43 %	42 %	25 %
zwischen 31 und 99 Tagen	45 %	37 %	50 %	38 %	30 %	51 %	42 %
mehr als 100 Tage	44 %	4 %	0 %	5 %	27 %	7 %	33 %

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

Anzahl hängiger Fälle

Die unten aufgeführten Angaben geben Auskunft über die Anzahl der Fälle, die am Ende der jeweiligen Berichtsjahre hängig waren. Anfang Januar 2023 waren 41 Schlichtungsverfahren hängig, wovon 13 sistiert sind (je eines aus den Jahren 2019 und 2020, drei aus dem Jahr 2021 und acht aus dem Berichtsjahr). 16 Fälle konnten bis zum Redaktionsschluss dieses Berichts abgeschlossen werden.

Tabelle 3: Hängige Schlichtungsverfahren

Ende 2022	**41 (davon 16 bis zum Redaktionsschluss erledigt und 13 sistiert)**
Ende 2021	27 (davon 14 bis zum Redaktionsschluss erledigt und 8 sistiert)
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

CYBERSICHERHEIT

Änderung des Informationssicherheitsgesetzes (ISG)

Das vom EFD eröffnete Vernehmlassungsverfahren betrifft den Gesetzesentwurf zur Änderung des Informationssicherheitsgesetzes im Hinblick auf die Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen. Diese Änderung sieht Einschränkungen des Öffentlichkeitsprinzips vor.

Vor dem Hintergrund der sich häufenden Cybervorfälle bei Privatpersonen, in Unternehmen und auch bei Behörden beauftragte der Bundesrat das EFD mit der Erarbeitung von Rechtsgrundlagen für die Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen. Dank dieser Meldepflicht soll sich das Nationale Zentrum für Cybersicherheit (NCSC) einen besseren Überblick über Cyberattacken in der Schweiz verschaffen und somit die betroffenen Opfer bei der Bewältigung von Cyberangriffen unterstützen sowie andere Betreiber kritischer Infrastrukturen warnen können. Das ISG soll nicht nur die Meldepflicht für Cyberangriffe definieren, sondern auch die Aufgaben des NCSC regeln und dessen Funktion als zentrale Meldestelle etablieren.[1]

Der vom EFD erarbeitete Entwurf wurde den mitinteressierten Kreisen zur Vernehmlassung vorgelegt. Eine Minderheit der Angehörten (laut Angaben des EFD 6 von 102) verlangte, dass Meldungen an das NCSC vom Öffentlichkeitsgesetz ausgenommen werden sollen. Diesem Anliegen wurde stattgegeben: Im ISG wurde mit Art. 4 Abs. 1 bis eine Spezialbestimmung nach Art. 4 BGÖ eingeführt, wonach Informationen Dritter, von denen das NCSC durch die Entgegennahme und Analyse von Meldungen Kenntnis erhält, nicht nach dem Öffentlichkeitsgesetz zugänglich gemacht werden dürfen.

Der EDÖB kann zwar nachvollziehen, dass die Meldungen und ihre Bearbeitung für die Sicherheit der Schweiz eine grosse Bedeutung haben, doch er hält die Einführung dieser neuen Spezialbestimmung für unverhältnismässig und lehnte sie deshalb ab. Sie stellt eine Beeinträchtigung des Öffentlichkeitsprinzips dar, weil sie Bürgerinnen und Bürger am Zugang zu Informationen hindert, die in unmittelbarem Zusammenhang mit der Durchführung einer Kernaufgabe des NCSC stehen, und ihnen damit die vom Gesetzgeber gewollte Kontrolle in einem Bereich entzieht, der für die Öffentlichkeit von wesentlicher Bedeutung ist. Aus Sicht des EDÖB enthält das Öffentlichkeitsgesetz bereits eine Reihe von Ausnahmen (z. B. Art. 7 Abs. 1 lit. c BGÖ zum Schutz der inneren oder äusseren Sicherheit der Schweiz, Art. 7 Abs. 1 lit. g BGÖ zum Schutz von Geschäftsgeheimnissen oder auch Art. 7.2 BGÖ zum Schutz der Privatsphäre), die den Schutz diverser Interessen ausreichend gewährleisten. Sodann sieht der EDÖB keinen Grund, weshalb der Vollzug des Öffentlichkeitsgesetzes das NCSC in seiner Aufgabe als zentrale Meldestelle behindern könnte. Er beantragte deshalb den Rückzug der Spezialbestimmung.

[1] Abgeschlossene Vernehmlassungen – 2022 (admin.ch)

Das EFD kam der Forderung des EDÖB nur teilweise nach, indem es den Geltungsbereich der Ausnahme reduzierte. Art. 4 Abs. 1bis lautet nunmehr wie folgt: «Informationen Dritter, von denen das Nationale Zentrum für Cybersicherheit (NCSC) durch die Entgegennahme und Analyse von Meldungen gemäss dem 5. Kapitel Kenntnis erhält, dürfen nicht nach dem BGÖ zugänglich gemacht werden. Nicht als Dritte gelten Behörden, Organisationen und Personen nach Art. 2 Abs. 1 BGÖ». Diese Präzisierung hält der EDÖB zwar für begrüssenswert, doch die Divergenz wurde aus den bereits angeführten Gründen aufrechterhalten und befindet sich sowohl in der Botschaft als auch in der Vorlage an den Bundesrat.

STROMBRANCHE

Vorentwurf des Bundesgesetzes über einen Rettungsschirm für die Elektrizitätswirtschaft

Die von den systemkritischen Unternehmen der Elektrizitätswirtschaft im Zusammenhang mit der Bereitstellung der Finanzhilfen zur Verfügung gestellten Informationen sind vom Zugangsrecht nach dem Öffentlichkeitsgesetz ausgeschlossen. Der Beauftragte hatte sich im Gesetzgebungsverfahren erfolglos gegen diese Einschränkung des Öffentlichkeitsprinzips ausgesprochen.

Der sogenannte Rettungsschirm für die Strombranche ist im Bundesgesetz über subsidiäre Finanzhilfen zur Rettung systemkritischer Unternehmen der Elektrizitätswirtschaft (FiREG) verankert und soll dazu beitragen, die Stromversorgung in der Schweiz zu gewährleisten, indem es insbesondere Finanzhilfen für systemkritische Unternehmen der Elektrizitätswirtschaft regelt. Nach dessen Art. 20 Abs. 4 ist der Zugang nach dem Öffentlichkeitsgesetz zu den von den systemkritischen Unternehmen zur Verfügung gestellten Informationen und Daten ausgeschlossen. In der Botschaft wird dazu ausdrücklich festgehalten, dass es sich bei der erwähnten Bestimmung um eine Spezialbestimmung im Sinne von Art. 4 Bst. a BGÖ handelt.

Nach Art. 4 BGÖ sind Bestimmungen anderer Bundesgesetze vorbehalten, die bestimmte Informationen als geheim bezeichnen (Bst. a) oder vom Öffentlichkeitsgesetz abweichende Voraussetzungen für den Zugang zu bestimmten Informationen vorsehen (Bst. b), was zur Folge hat, dass die Bestimmungen des Öffentlichkeitsgesetzes für den Zugang zu diesen Informationen nicht anwendbar sind. Jede Einführung solcher Vorbehalte führt zu einer Schwächung des Öffentlichkeitsprinzips und der damit bezweckten Verwaltungstransparenz.

Da die Verwaltung den Beauftragten in der Ämterkonsultation nicht begrüsste, hat er sich erst im Rahmen des Mitberichtsverfahrens und der Vernehmlassung gegen die Einführung dieser Spezialbestimmung ausgesprochen und dabei auf die mit dem Öffentlichkeitsgesetz verfolgten Ziele des Nachvollzugs des Verwaltungshandeln und der Verhinderung von Misswirtschaft im Zusammenhang mit der Gewährung staatlicher Kredite und Subventionen zum Nachteil der steuerzahlenden Allgemeinheit hingewiesen.

Das UVEK begründet die Einschränkung des Öffentlichkeitsprinzips damit, dass die zur Verfügung gestellten Informationen und Daten sensibler Natur seien und regelmässig Geschäfts- oder Fabrikationsgeheimnisse im Sinne des Öffentlichkeitsgesetzes enthalten dürften. Der Beauftragte hat 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 Personendaten von natürlichen und juristischen Personen (Art. 7 Abs. 2 BGÖ, Art. 9 Abs. 2 BGÖ sowie Art. 19 DSG). Der Beauftragte gab schliesslich zu bedenken, dass das Öffentlichkeitsgesetz in seiner Substanz ausgehöhlt wird, wenn der Bevölkerung der Zugang zu Dokumenten ausgerechnet beim sensiblen Vollzug von Finanzhilfen verwehrt wird, wie es bereits im Falle des Covid-19-Solidarbürgschaftsgesetzes geschah (s. 28. TB, Kap. 2.4).

Anfang September 2022 hat der Bundesrat entschieden, gestützt auf eine Notverordnung den Rettungsschirm zu aktivieren und der Axpo einen Kreditrahmen im Umfang von 4 Milliarden Franken zur Verfügung zu stellen. Entsprechend dem Gesetzesentwurf des FiREG schloss die Notverordnung den Zugang nach dem Öffentlichkeitsgesetz zu den von den systemkritischen Unternehmen zur Verfügung gestellten Informationen und Daten aus. Das Parlament hat Ende September 2022 das FiREG, inklusive der Ausnahme des Öffentlichkeitsgesetzes, verabschiedet.

ARCHIVIERUNGSGESETZ

Notwendigkeit einer Revision des Bundesgesetzes über die Archivierung

Die Koordination von Archivierungsgesetz und Öffentlichkeitsgesetz und damit verbunden die Frage, welches Recht bei Einsicht in archivierte Dokumente nach dem Öffentlichkeitsgesetz während der Schutzfrist anzuwenden ist, soll durch eine Anpassung der Archivierungsverordnung geklärt werden. Nach Ansicht des Beauftragten lassen sich diese Aspekte durch eine Teilrevision der Archivierungsverordnung nicht rechtsverbindlich klären.

Das Archivierungsgesetz (BGA) und das Öffentlichkeitsgesetz regeln zwei verschiedene Verfahren für den Zugang zu amtlicher Information, welche in wesentlichen Aspekten unterschiedlich ausgestaltet sind. Das auf den 1. Oktober 1999 in Kraft getretene Archivierungsgesetz kennt weitreichende Schutzfristen, welche nicht zuletzt Ausdruck des damals in der Bundesverwaltung geltenden Geheimhaltungsprinzips sind. Nur wenige Jahre später hat sich der Gesetzgeber mit dem Paradigmenwechsel hin zum Öffentlichkeitsprinzip (passive Information, d. h. Zugang auf Gesuch hin) befasst, ohne sich ausdrücklich zum Umgang mit amtlichen Dokumenten nach dem Öffentlichkeitsgesetz nach dem Zeitpunkt ihrer Archivierung zu äussern, weswegen sowohl für die materielle wie auch für die formelle Koordination von Archivierungsgesetz und Öffentlichkeitsgesetz keine verbindlichen Vorgaben existieren. Daraus resultiert für die Beurteilung der Frage, ob und in welchem Umfang bei der Einsicht in archivierte amtliche Dokumente nach dem Öffentlichkeitsgesetz während der Schutzfrist das Öffentlichkeitsgesetz und/oder das Archivierungsgesetz anzuwenden ist, eine erhebliche Rechtsunsicherheit, welche die rechtsanwendenden Behörden und Private gleichermassen betrifft.

Eine im Auftrag des Bundesarchivs durchgeführte Evaluation identifiziert im entsprechenden Schlussbericht

Handlungsbedarf in neun Stossrichtungen und sieht entsprechende Empfehlungen vor. Im Zusammenhang mit der Koordination von Archivierungsgesetz und Öffentlichkeitsgesetz wird unter anderem die Empfehlung abgegeben, dass der Gesetzgeber explizit festlegt, welches Recht bei Einsicht in archivierte amtliche Dokumente nach dem Öffentlichkeitsgesetz während der Schutzfrist anzuwenden ist.

Nach Einschätzung des Bundesarchivs kann die Umsetzung der Empfehlungen aus dem Bericht zur Evaluation des BGA – und damit auch die Koordination von Archivierungsgesetz und Öffentlichkeitsgesetz – jedoch durch entsprechende Handhabung in der Archivierungspraxis sowie einer Anpassung der Archivierungsverordnung durch den Bundesrat erfolgen. Das Bundesarchiv erachtet daher eine Revision des Archivierungsgesetzes durch den Gesetzgeber als nicht nötig. Nach Ansicht des Beauftragten liegt die zentrale Problematik in der fehlenden gesetzlichen Koordination von Archivierungsgesetz und Öffentlichkeitsgesetz bzw. der entsprechenden Verfahren für den Zugang zu amtlicher Information, welche teilweise bedeutende Unterschiede aufweisen. Die Anzahl archivierter Dossiers mit amtlichen Dokumenten nach dem Öffentlichkeitsgesetz wird zukünftig ansteigen, wodurch auch von einem markanten Anstieg zu beurteilender Gesuche auszugehen ist. Ohne Klärung der sich stellenden Koordinationsfragen auf der Stufe des formellen Gesetzes drohen sich die rechtsanwendenden Behörden und somit auch der Beauftragte durch die (Nicht-)Anwendung des Archivierungsgesetzes oder Öffentlichkeitsgesetz im Einzelfall dem Vorwurf auszusetzen, den im Archivierungsgesetz (mit weitreichenden Schutzfristen) resp. im Öffentlichkeitsgesetz (Verwaltungsöffentlichkeit) zum Ausdruck gebrachten gesetzgeberischen Willen zu übersteuern. Im Ergebnis hat der Beauftragte im Rahmen der Ämterkonsultation zum Aussprachepapier betreffend die Notwendigkeit einer Revision des Archivierungsgesetzes seine Ansicht geäussert, dass der Koordination von Archivierungsgesetz und Öffentlichkeitsgesetz aufgrund der damit zusammenhängenden weitreichenden Konsequenzen eine erhebliche Bedeutung zukommt und einer Legitimation durch den Gesetzgeber bedarf. Folglich erachtet er die vorgesehene Normstufe der Bundesratsverordnung für die Regelung der Koordination als ungenügend.

FINANZEN

Inkraftsetzung Geldwäschereigesetz und Geldwäschereiverordnung

Das Zentralamt für Edelmetallkontrolle ZEMK wird im Bereich der von der FINMA übertragenen Aufsichtstätigkeit vom persönlichen Geltungsbereich des Öffentlichkeitsgesetzes ausgenommen. Der Beauftragte wehrte sich erfolglos gegen diese weitere Zurückdrängung des Öffentlichkeitsprinzips.

Das Eidgenössische Zentralamt für Edelmetallkontrolle ZEMK ist dem Bundesamt für Zoll und Grenzsicherheit angegliedert und besorgt alle Geschäfte, welche die Überwachung des Verkehrs mit Edelmetallen und Edelmetallwaren mit sich bringt. In diesem Bereich übernimmt das ZEMK gemäss der 2021 verabschiedeten Revision des Geldwäschereigesetzes die Aufgabe einer Geldwäschereiaufsichtsbehörde von der Eidgenössischen Finanzmarktaufsicht FINMA bzw. von den Selbstregulierungsorganisationen SRO.

Im Rahmen der Revision der Geldwäschereiverordnung wird die Aufsichtstätigkeit des ZEMK im Bereich der mit Bankedelmetallen handelnden Handelsprüfer gestützt auf die Bestimmung von Art. 2 Abs. 2 BGÖ resp. den darauf gestützten Artikel 1a der Öffentlichkeitsverordnung vom persönlichen Geltungsbereich des Öffentlichkeitsgesetzes ausgenommen. Das für die Änderung der Geldwäschereiverordnung zuständige Staatssekretariat für internationale Finanzfragen SIF begründete dies damit, dass für die bis anhin von der FINMA/den SRO resp. neu vom ZEMK Beaufsichtigten weitgehend die gleichen Regeln wie bisher gelten sollen.

In Art. 2 Abs. 2 BGÖ hat der Gesetzgeber die Schweizerische Nationalbank SNB und die FINMA vom persönlichen Geltungsbereich des Öffentlichkeitsgesetzes ausgenommen. Hingegen hat er im Rahmen der Revision der Geldwäschereigesetzgebung und in Kenntnis des Öffentlichkeitsprinzips darauf verzichtet, das ZEMK resp. dessen neu von der FINMA übernommenen Aufsichtsaufgaben vom persönlichen Geltungsbereich des Öffentlichkeitsgesetzes auszunehmen. Der Gesetzgeber hat damit die Aufsichtstätigkeit des ZEMK dem grundsätzlich für die Bundesverwaltung geltenden Transparenzprinzip unterstellt. Folglich besteht nach Ansicht des Beauftragten gerade kein gesetzgeberischer Wille, den persönlichen Geltungsbereich des Öffentlichkeitsgesetzes entsprechend einzuschränken.

Der Beauftragte hat das SIF zudem darauf hingewiesen, dass der Wortlaut von Art. 2 Abs. 2 BGÖ klar ist und unmissverständlich (nur) die FINMA und die SNB vom persönlichen Geltungsbereich des Öffentlichkeitsgesetzes ausnimmt und auch die entsprechenden Materialien keine Hinweise enthalten, wonach diese Bestimmung in der Öffentlichkeitsverordnung ergänzt werden kann. Für die Ausnahme der Aufsichtstätigkeit des ZEMK vom persönlichen Geltungsbereich des Öffentlichkeitsgesetzes durch Schaffung einer entsprechenden Verordnungsbestimmung stellt Art. 2 Abs. 2 BGÖ nach Ansicht des Beauftragten keine genügende resp. geeignete Rechtsgrundlage dar.

TABAKPRODUKTEGESETZ

Teilrevision des Bundesgesetzes über Tabakprodukte und elektronische Zigaretten (TabPG)

Im dritten Quartal 2022 schickte der Bundesrat eine Vorlage zur Teilrevision des Tabakproduktegesetzes (TabPG) in die Vernehmlassung. Der Entwurf sieht unter anderem vor, dass die von der Tabakbranche an das BAG gemeldeten Werbeausgaben nicht dem Öffentlichkeitsprinzip unterliegen sollen. Der EDÖB sprach sich erfolglos dagegen aus.

Am 1. Oktober 2021 verabschiedete das Parlament das neue Gesetz über Tabakprodukte und elektronische Zigaretten (TabPG). Nachdem die Volksinitiative «Ja zum Schutz der Kinder und Jugendlichen vor Tabakwerbung (Kinder und Jugendliche ohne Tabakwerbung)» am 13. Februar 2022 angenommen wurde, erarbeitete das BAG Bestimmungen zur Einführung zusätzlicher Einschränkungen betreffend Werbung, Verkaufsförderung und Sponsoring für Tabakprodukte und elektronische Zigaretten. Gemäss Vorlage sollen entsprechende Ausgaben, die dem BAG von den Tabakfirmen individuell gemeldet werden, vom Öffentlichkeitsprinzip ausgenommen werden. Dies mit der Begründung, es gehe hierbei um den Schutz privatrechtlicher Interessen der betreffenden Firmen und insbesondere um den Schutz des Geschäftsgeheimnisses.

Während der Ämterkonsultation sprach sich der EDÖB gegen die Einführung dieser Ausnahme aus und bezeichnete sie als überflüssig, weil das BGÖ bereits eine Ausnahmebestimmung zum Schutz von «Berufs-, Geschäfts- oder Fabrikationsgeheimnissen» enthält (Art. 7 Abs. 1 lit. g). Seiner Auffassung nach werden die Einzelinteressen der betreffenden Firmen durch das BGÖ bereits ausreichend wahrgenommen und geschützt, zumal das Hauptziel des TabPG in der Bekämpfung des Tabakmissbrauchs besteht und das öffentliche Interesse an der Transparenz in diesem Zusammenhang einen hohen Stellenwert besitzt.

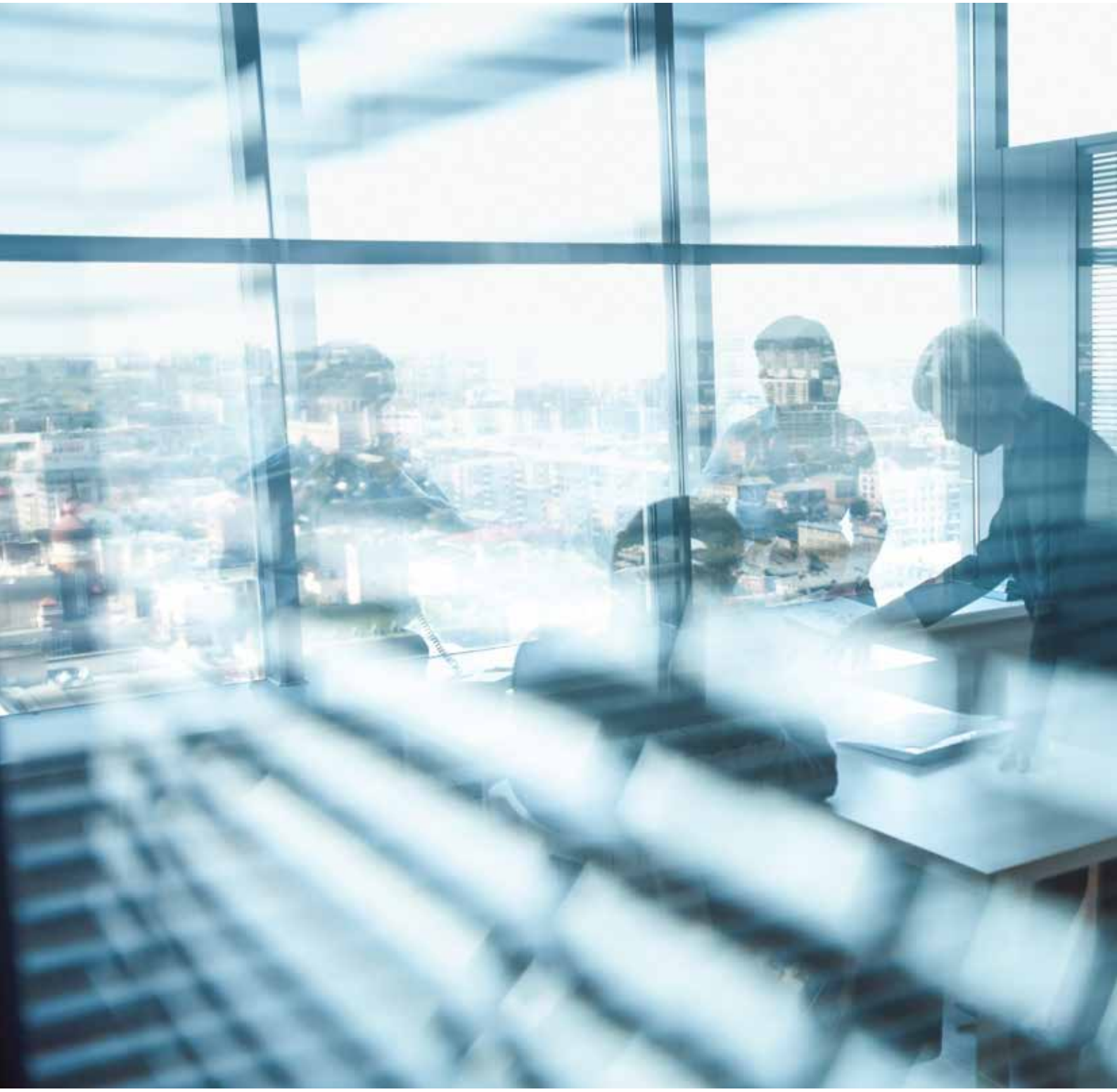
In der Vernehmlassungsvorlage des Bundesrates blieb die betreffende Differenz bestehen. Die Botschaft dürfte dem Parlament im ersten Halbjahr 2023 vorgelegt werden.

WIRTSCHAFT

Neues Bundesgesetz für die Prüfung ausländischer Investitionen

Das Staatssekretariat für Wirtschaft (SECO) hat im zweiten Quartal des Jahres 2022 eine Vernehmlassung für die Einführung des Investitionsprüfungsgesetzes (IPG) durchgeführt. Die zunächst vorgesehene Einschränkung des Öffentlichkeitsprinzips wurde in der Vernehmlassungsvorlage gestrichen.

In Umsetzung der Motion 18.3021 Rieder eröffnete der Bundesrat am 18. Mai 2022 die Vernehmlassung für das neue IPG. Das Ziel der Investitionsprüfung soll die Verhinderung einer Gefährdung oder Bedrohung der öffentlichen Ordnung oder Sicherheit durch Übernahmen von inländischen Unternehmen durch ausländische Investoren sein. Verantwortlich für die Durchführung der Investitionsprüfung sowie



die Koordination mit den mitinteressierten Verwaltungseinheiten, soll das SECO sein. Der ursprüngliche Vorentwurf des SECO sah vor, dass die ihm im Rahmen seiner Investitionsprüftätigkeit mitgeteilten Informationen und eingereichten Unterlagen nicht öffentlich zugänglich sind. Beabsichtigt war ein umfassender Vorbehalt der Anwendbarkeit des Öffentlichkeitsgesetzes, welcher mit der Bearbeitung heikler Daten, wie etwa Geschäftsgeheimnissen oder vom Nachrichtendienst des Bundes (NDB) zur Verfügung gestellten Informationen, begründet wurde.

In einer Vorkonsultation hat sich der Beauftragte gegen die Einführung dieses Vorbehaltes ausgesprochen und auf das bedeutende öffentliche Interesse an der Umsetzung der Investitionsprüfung durch das SECO hingewiesen. Für den Schutz möglicher Geschäftsgeheimnisse der Investoren und von Informationen, welche vom NDB zu Verfügung gestellt werden, sind im Öffentlichkeitsgesetz bereits explizite Zugangsausnahmen vorgesehen (Art. 7 Abs. 1 Bst. g BGÖ und Art. 4 BGÖ i. V. m. Art. 67 NDG). Zudem sind im Einzelfall tangierte öffentliche Interessen bereits geschützt, insbesondere die zielkonforme Durchführung konkreter behördlicher Massnahmen (Art. 7 Abs. 1 Bst. b BGÖ), die wirtschafts-, geld- und währungspolitischen Interessen der Schweiz (Art. 7 Abs. 1 Bst. f BGÖ) sowie die behördliche Meinungsbildung bei anstehenden Entscheiden (Art. 8 Abs. 2 BGÖ). In der Vernehmlassungsvorlage wurde die beabsichtigte Einschränkung gestrichen.

2.5 Spezialgesetzliche Vorbehalte nach Art. 4 BGÖ

Das Öffentlichkeitsgesetz bedarf der Koordination mit Bestimmungen in Spezialgesetzen des Bundes, welche eine Sonderregelung für den Zugang zu amtlichen Dokumenten vorsehen. Nach Art. 4 BGÖ sind Bestimmungen anderer Bundesgesetze vorbehalten, die bestimmte Informationen als geheim bezeichnen (Bst. a) oder vom Öffentlichkeitsgesetz abweichende Voraussetzungen für den Zugang zu bestimmten Informationen vorsehen (Bst. b), was zur Folge hat, dass die Bestimmungen des Öffentlichkeitsgesetzes für den Zugang zu diesen Informationen nicht anwendbar sind.

Tabelle 4: Spezialbestimmungen nach Art. 4 BGÖ

Erlass (Kurzform) und Abkürzung	SR-Nr.	Art./Abs.	Inkraftsetzung am:
Botschaft zur Änderung des Bundesgesetzes über die Krankenversicherung (Massnahmen zur Kostendämpfung – Paket 2)	832.10	E-Art. 52e VE-KVG	Botschaft vom 7. September 2022 Stand: Im Parlament noch nicht behandelt
Informationssicherheitsgesetz (ISG)	128	Art. 4 Abs. 1 bis	(geplant per) 1. Januar 2024
Verordnung über zusätzliche Liquiditätshilfe-Darlehen und die Gewährung von Ausfallgarantien des Bundes für Liquiditätshilfe-Darlehen der Schweizerischen Nationalbank an systemrelevante Banken	952.3	Art. 6 Abs. 3	16. März 2023
Bundesgesetz über Subsidiäre Finanzhilfen zur Rettung systemkritischer Unternehmen der Elektrizitätswirtschaft (FiREG)	734.91	Art. 20 Abs. 4	1. Oktober 2022
Bundesgesetz über das öffentliche Beschaffungswesen (BöB)	172.056.1	Art. 48 Abs. 1 (expliziter Zugang vorgeschrieben); Art. 11 Bst. e (gilt nur während Vergabeverfahren als Spezialbestimmung)	1. Januar 2021
Covid-19-Solidarbürgschaftsgesetz (Covid-19-SBüG)	951.26	Art. 12 Abs. 2	19. Dezember 2020
Bundesgesetz über die Organisation der Bahninfrastruktur (OBI) (Mantelerlass)			
Eisenbahngesetz (EBG)	742.101	Art. 14 Abs. 2	1. Juli 2020
Seilbahngesetz (SebG)	743.01	Art. 24e	1. Juli 2020
Personenbeförderungsgesetz (PBG)	745.1	Art. 52a	1. Juli 2020
Bundesgesetz über die Binnenschifffahrt (BSG)	747.201	Art. 15b	1. Juli 2020
Nachrichtendienstgesetz (NDG)	121	Art. 67	1. September 2017
Lebensmittelgesetz (LMG)	817.0	Art. 24 Spezialbestimmung gemäss Botschaft zum Bundesgesetz über Lebensmittel und Gebrauchsgegenstände vom 25. Mai 2011	1. Mai 2017
Bundesgesetz über die Förderung der Forschung und der Innovation (FIFG)	420.1	Art. 13 Abs. 4 (s. Urteil des BVGer A-6160/2018 vom 4. November 2019 E. 4)	1. Januar 2014

Erlass (Kurzform) und Abkürzung	SR-Nr.	Art./Abs.	Inkraftsetzung am:
Bankengesetz (BankG)	952.0	Art. 47 Abs. 1	1. Januar 2009 (Bst. a und b) bzw. 1. Juli 2015 (Bst. c)
Patentgesetz (PatG) Patentverordnung (PatV)	232.14 232.141	Art. 90 PatV, der sich auf Art. 65 Abs. 2 PatG stützt (s. Urteil des BGer 4A_249/2021 vom 10. Juni 2021)	1. Juli 2008
Inkrafttreten des Öffentlichkeitsgesetzes			1. Juli 2006
Parlamentsgesetz (ParlG)	171.10	Art. 47 Abs. 1 (s. Urteil des BVGer A-6108/2016 vom 28. März 2018 E. 3.1)	1. Dezember 2003
Güterkontrollgesetz (GKG)	946.202	Art. 4 und 5 (s. Urteil des BVGer A-5133/2019 vom 24. November 2021 E. 5.3.2.4)	1. Oktober 1997
Bundesgesetz über die direkte Bundessteuer (DBG)	642.11	Art. 110 Abs. 1	1. Januar 1995
Verrechnungssteuergesetz (VStG)	642.21	Art. 37 Abs. 1	1. Januar 1967
Bundesgesetz über die Stempelabgaben (StG)	641.10	Art. 33 Abs. 1	1. Juli 1974
Mehrwertsteuergesetz (MWSTG)	641.20	Art. 74 Abs. 1	1. Januar 2010
Steuerharmonisierungsgesetz (STHG)	642.14	Art. 39 Abs. 1 Vgl. JAAC 2016.1 (p. 1 – 14), édition du 26 janvier 2016: Secret fiscal et accès à des documents officiels	1. Januar 1993
Bundesstatistikgesetz (BstatG)	431.01	Art. 14 (s. Urteil des BGer 1C_50/2015 vom 2. Dezember 2015 E. 4.2 ff.)	1. August 1993

(Liste nicht abschliessend)

Tabelle 5: Keine Spezialbestimmungen nach Art. 4 BGÖ

Erlass (Kurzform) und Abkürzung	SR-Nr.	Art./Abs.	Inkraftsetzung am:
Revisionsaufsichtsgesetz (RAG)	221.302	Art. 19 Abs. 2 (siehe Urteil des BGer 1C_93/2021 vom 6. Mai 2022 E. 3.6)	1. September 2007
Heilmittelgesetz (HMG)	812.21	Art. 61 und 62 (s. Urteil des BGer 1C_562/2017 vom 2. Juli 2018 E. 3.2; Urteil des BVGer A-3621/2014 vom 2. September 2015 E. 4.4.2.3 ff.)	1. Januar 2002
Bundesgesetz über den Allgemeinen Teil des Sozialversicherungsrechts (ATSG)	830.1	Art. 33 (Im vorliegenden Fall keine Spezialbestimmung nach Art. 4 BGÖ: s. Urteil des BVGer A-5111/2013 vom 6. August 2014 E. 4.1 ff.; A-4962/2012 vom 22. April 2013 E. 6.1.3)	1. Januar 2003
Bundesgesetz über die berufliche Alters-, Hinterlassenen- und Invalidenvorsorge (BVG)	831.40	Art. 86 (s. Urteil des BGer 1C_336/2021 vom 3. März 2022 E. 3.4.3)	1. Januar 2001
Bundesgesetz über die Produktesicherheit (PrSG)	930.11	Art. 10 Abs. 4 i.V.m. Art. 12 (siehe Urteil des BGer 1C_299/2019 vom 7. April 2020 E. 5.5)	1. Juli 2010

(Liste nicht abschliessend)

Der EDÖB

3.1 Aufgaben und Ressourcen

Leistungen und Ressourcen im Bereich Datenschutz

Personalbestände

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). Zunächst 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 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 im Jahr 2020 von 24 auf 27 Vollzeitstellen erhöht hat. Im Frühjahr 2021 hat der EDÖB dem Bundesrat mit Blick auf die damals für 2022 vorgesehene Inkraftsetzung des revidierten DSG die Schaffung der verbleibenden sechs Vollzeitstellen beantragt, welche der Bundesrat am 28. April 2021 bewilligt hat. Damit hat sich der Etat des für den Datenschutz eingesetzten Personals um weitere fünf Stellen erhöht (eine Stelle wurde für die Erbringung administrativer Leistungen an die Bundeskanzlei abgegeben).

2006 ist das Öffentlichkeitsgesetz (BGÖ) in Kraft getreten. Da die drei dafür in der Gesetzesbotschaft vorgesehenen Stellen vom Bundesrat nie bewilligt wurden, musste unsere Behörde zur Erfüllung ihrer Aufgaben nach BGÖ seither auf das bereits bestehende Datenschutz-Personal des EDÖB und teilweise auf Mittel der Bundeskanzlei zurückgreifen. Nachdem das für die Bewilligung des Budgets des EDÖB neu zuständige Bundesparlament am 8. Dezember 2022 dem EDÖB die in der Gesetzesbotschaft vorgesehenen Stellen zugesprochen hatte, konnte der EDÖB eine dieser drei Stellen dem Direktionsbereich Datenschutz zurückgeben, womit dessen Stellenetat um eine weitere Stelle, insgesamt also auf 33 Stellen angewachsen ist. Die beiden übrigen Stellen hat der Beauftragte aufgrund des angewachsenen Arbeitsaufwandes für Schlichtungen dem Direktionsbereich Öffentlichkeitsgesetz zugeordnet (s. nachfolgenden Beitrag zu Leistungen und Ressourcen im Bereich Öffentlichkeitsgesetz).

Angesichts des Umstandes, dass in der Berichtsperiode umfangreiche Vorbereitungsarbeiten zur Inkraftsetzung des neuen DSG geleistet werden mussten (neue Wegleitungen und Texte für Webseite etc.), hat sich der Einsatz des neu rekrutierten Personals wie nachfolgend ersichtlich ist, statistisch schwergewichtig in der Leistungsgruppe Information niedergeschlagen.

Tabelle 6: Für DSG-Belange einsetzbare Stellen

2005	22
2010	23
2018	24
2019	24
2020	27
2021	27
2022	27
2023	**33**

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 1.4.2022 bis 31.3.2023 wurden die beim EDÖB für den Datenschutz einsetzbaren Personalressourcen wie folgt auf diese Gruppen aufgeteilt:

Tabelle 7: Leistungen Datenschutz

Beratung Bund	18,7 %	
Beratung Private	21,1 %	
Zusammenarbeit mit ausl. Behörden	11,4 %	
Zusammenarbeit mit Kantonen	1,3 %	
Total Beratung		**52,5 %**
Aufsicht	14,7 %	
Zertifizierung	0,0 %	
Register Datensammlung	0,4 %	
Total Aufsicht		**15,1 %**
Information	20,2 %	
Ausbildung/Referate	2,0 %	
Total Information		**22,2 %**
Gesetzgebung	10,2 %	
Total Gesetzgebung		**10,2 %**
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 bezifferten sich im Berichtsjahr auf rund 52,5 Prozent. Gemäss dem Kontrollplan des EDÖB für das Jahr 2022 ist die beratende Begleitung von acht grossen Projekten im Gang. Vier dieser Projekte stehen im Zusammenhang mit der vom Bundesrat angeordneten digitalen Transformation der Bundesverwaltung.

Die drei Teams des Direktionsbereichs Datenschutz haben monatlich im Durchschnitt dreiunddreissig Anfragen und Anzeigen von Bürgerinnen und Bürgern mit einem Standardschreiben beantwortet, das diese auf den zivilprozessualen Weg verweist. Ab Einführung des neuen DSG wird ein Teil dieser Anfragen materiell zu behandeln sein.

Da sich Big Data und künstliche Intelligenz als Geschäftsmodelle beschleunigt durchsetzen und die technologischen Datenschutzrisiken den Aufsichtsbereich des EDÖB weiter ausdehnen, ist weiterhin von einer steigenden Anzahl von umfangreichen Datenbearbeitungsprojekten bei Staat und Wirtschaft auszugehen.

Tabelle 8: Beratungen in umfangreicheren Projekten für 2022

Grundrechte	1
Gesetzgebung neues DSG	2
Handel und Wirtschaft	1
Digitale Transformation	4
Total	8

Aufsicht

Aufgrund der Dynamik von Cloud gestützten Applikationen müssen Kontrollen heute rasch durchgeführt werden. Diese Beschleunigung sowie die immer wichtiger werdende Kombination von juristischem und technischem Fachwissen schliessen längere Unterbrüche bei den Sachverhaltsabklärungen aus, sodass umfassendere Kontrollen von mehreren Mitarbeitenden betreut werden müssen. In der aktuellen Berichtsperiode lag der Anteil der für Kontrollen und Aufsichtsverfahren einsetzbaren Ressourcen bei 15,1 Prozent, was dem tiefen Mittelwert der Berichtsjahre ab 2015 entspricht. Gemäss Kontrollplan für das Jahr 2023 werden mit diesen Mitteln zwölf umfassendere Kontrollen bestritten. Nachdem das für den Datenschutz einsetzbare Personal in den beiden letzten Berichtsperioden mit Blick auf das neue DSG aufgestockt werden konnte, wird der Beauftragte darauf hinwirken, dass die Kontrolldichte über die Bundesorgane und die rund 12 000 grossen und mittleren kaufmännischen Unternehmen sowie die rund 10 000 Stiftungen und Vereine der Schweiz sukzessive erhöht wird.

Gesetzgebung

Die mit der digitalen Transformation der Bundesämter einhergehenden Anpassungen der Personendatenbearbeitungen muss im Rahmen gesetzlicher Grundlagen erfolgen. Diese Anpassungen ziehen deshalb eine Vielzahl von neuen und revidierten Bearbeitungsvorschriften im Bundesrecht nach sich, zu denen der EDÖB in diversen Konsultationsverfahren Stellung bezieht. Im Berichtsjahr sind 383 Ämterkonsultationen bei uns eingegangen.

Totalrevision des Datenschutzgesetzes

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. Gerade auch dank dem zusätzlich rekrutierten Personal, können diese Arbeiten plangemäss ab Frühsommer 2023 sukzessive abgeschlossen werden.

Leistungen und Ressourcen im Bereich Öffentlichkeitsgesetz

Das Berichtsjahr war durch die ausklingende Pandemie und die anhaltend hohe Anzahl an Schlichtungsanträgen geprägt (s. Kap. 2.3). Nachdem das Parlament dem EDÖB die drei in der Botschaft zum Öffentlichkeitsgesetz vorgesehenen, aber vom Bundesrat nie zugesprochenen Stellen am 8. Dezember 2022 bewilligt hat, kann der Etat im Direktionsbereich Öffentlichkeitsprinzip von 4,4 auf 6 Vollzeitstellen erhöht werden. Der Beauftragte wird darauf hinwirken, dass die aufgrund der Pandemie und personellen Unterbesetzung entstandenen Bearbeitungsrückstände in den nächsten Berichtsperioden sukzessive abgebaut werden. Ob und wie schnell dies gelingen kann, wird auch von der zukünftigen Entwicklung der Schlichtungsanträge abhängen.

Teilnahme an Kommissionsberatungen und Anhörungen durch parlamentarische Kommissionen

In der Berichtsperiode hat der Beauftragte an folgenden Anhörungen und Kommissionsberatungen teilgenommen:

- Februar 2022: SGK-S zur Thematik Swisstransplant;
- Februar 2022: SPK-N zu den Digitalplattformen;
- April 2022: SPK-N zur Revision der Verordnung zum neuen DSG;
- Juni 2022: Subkommission EJPD/BK der GPK-N zum Tätigkeitsbericht;
- Oktober 2022: SGK-N und SPK-N zur Revision des KVG und den Massnahmen zur Kostendämpfung;
- Oktober 2022: WAK-N zur Totalrevision des Zollgesetzes;
- Oktober 2022: Subkommissionen FK-S und FK-N zum Budget 2023;
- November 2022: SIK-N zur Totalrevision des Zollgesetzes;
- Januar 2023: RK-N zur Totalrevision des Zollgesetzes;
- Februar 2023: Subkommission EJPD/BK der GPK-S zur Umsetzung des BGÖ;
- März 2023: RK-N zum Bundesgesetz über die Plattformen für die elektronische Kommunikation in der Justiz;

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

Tabelle 9: 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. Er verfügt über eine zeitgemässe, benutzerfreundliche Website. Mit der Inkraftsetzung des revidierten Datenschutzgesetzes werden neue Meldepflichten eingeführt und bestehende angepasst. Die Meldungen sollen über Meldeportale sicher, einfach und jederzeit dem EDÖB zugestellt werden können. Damit können auch Medienbrüche reduziert und die Bearbeitung effizienter umgesetzt werden.
Gesetzgebung	Der EDÖB nimmt rechtzeitig und aktiv Einfluss auf alle datenschutzrelevanten Spezialnormen und Regelwerke, die auf nationaler und internationaler Ebene geschaffen werden. Er unterstützt die interessierten Kreise bei der Formulierung von Regeln der guten Praxis.

3.2 Kommunikation

Zahlen

Der EDÖB hat im Berichtsjahr sechs Medienmitteilungen, die auf dem Medienportal des Bundes zu finden sind, sowie zwölf Kurzmitteilung publiziert. Die Medienbeobachtung, die sich auf eine Auswahl der wichtigsten Schweizer Print- und Onlinemedien sowie ein ausgewählte internationale Key-Printprodukte stützt, registrierte letztes Jahr knapp 6000 Beiträge, was den letztjährigen Trend bestätigt, als wir eine starke Zunahme gegenüber dem Vorjahr feststellen konnten (s. 29. TB, Kap. 3.2). Das Kommunikationsteam des EDÖB hat rund 300 Medienanfragen beantwortet. Im Fokus der Medienschaffenden waren dabei die Themen Datenweitergabe (ca. 100 Anfragen), Cybersicherheit (45) und Überwachung (30), wobei teilweise auch Regulierungsvorhaben (15) wie die Chatkontrolle oder das neue Bundesgesetz über Zoll und Grenzsicherheit zu diesen Themen gezählt werden können. Zum Öffentlichkeitsgesetz haben wir 12 Medienanfragen beantwortet.

Die Zahl der Anfragen und Hinweise aus der Bevölkerung beläuft sich in diesem Berichtsjahr auf 6200, was fast der Zahl vom Vorjahr entspricht (6600), als wir einen starken Anstieg von über 50 Prozent feststellen konnten.

Themenschwerpunkte

Ein Überblick über die im Berichtszeitraum eingegangenen Medienanfragen und die von uns initiierten Kommunikationsmassnahmen lässt folgende Rückschlüsse zu: nach der Coronapandemie, die vor allem beim Contact Tracing und der Ausstellung des Covid-Zertifikats viele Fragen punkto Datenschutz aufgeworfen hat, bleibt der Gesundheitssektor im Fokus des allgemeinen Interessens. Investigationsjournalisten haben Schwachstellen bei der Datensicherheit bei Medizinalregistern aufgedeckt, und Cyberkriminelle verschafften sich unerlaubt Zugriff zu Daten von Patientinnen und Patienten, die auf Servern von Arztpraxen und Spitälern unzureichend gesichert waren.

Zur Kompromittierung besonders schützenswerter Daten zur Gesundheit der Betroffenen kam es, wie bereits im Vorjahr beim elektronischen Impfregister der Stiftung meineimpfungen.ch (s. 29. TB, Kap. 1.4), beim nationalen Organspenderegister sowie beim Brustimplantateregister. In beiden Fällen eröffnete der EDÖB eine formelle Sachverhaltsabklärung (s. Kap. 1.4). Die Stiftung Swisstransplant hat die im Untersuchungsbericht des EDÖB festgehaltenen Empfehlungen mehrheitlich angenommen und den Onlinebetrieb des nationalen Organspenderegisters eingestellt. Der Bericht zum Mammoregister ist noch in Arbeit; das Register wurde einstweilen vom Netz genommen.

Im Fall Swisstransplant haben wir sowohl bei Eröffnung des Verfahrens im Januar als auch bei der Publikation des Schlussberichts im Oktober Medienmitteilungen verfasst. Unmittelbar nach Bekanntwerden der Hackerangriffe auf Arztpraxen in der Romandie ist der EDÖB mit diesen in Kontakt getreten, um darauf hinzuwirken, dass die betroffenen Patientinnen und Patienten unverzüglich und umfassend informiert wurden. Wir haben dazu am 31.3.2022 eine Kurzmitteilung auf unserer Website publiziert. Der Beauftragte hat sich mehrmals in den Medien zur Problematik der mangelnden Sicherheit bei der Aufbewahrung von Gesundheitsdaten geäussert.

Nachdem Ende 2021 der Konkurs über die Stiftung meineimpfungen.ch eröffnet worden war und im Mai 2022 eine geplante Veräusserung der Impfdaten durch das zuständige Konkursamt

bekannt wurde, hat der EDÖB zunächst die Löschung der Daten verlangt und dann später einen Versuch der Gesundheitsdirektion des Kantons Aargau zur Rettung der Daten ermöglicht. In einer Medienmitteilung haben wir dazu Stellung genommen (s. Kap. 1.4).

Dass Medizinaldaten auch beim Öffentlichkeitsprinzip Gegenstand des allgemeinen Interesses sind, zeigte sich im Berichtsjahr insbesondere bei den Impfstoffverträgen. Der EDÖB hat dem BAG in seiner Empfehlung vom 29. Juli 2022 empfohlen, diese offenzulegen. Das BAG hat bei der Herausgabe der Dokumente jedoch weite Teile geschwärzt, was öffentliche Kritik zur Folge hatte.

Datenweitergabe und Datenhandel

Neben den Medizinalregistern beschäftigten uns dieses Jahr insbesondere auch die Cloud-Thematik und die Weitergabe von Personendaten an Dritte im kommerziellen Bereich. Wir haben uns in einer ausführlichen Stellungnahme zur Auslagerung von Personendaten durch die Suva in eine Microsoft Cloud geäussert und dazu am 13.06.2022 eine Kurzmitteilung publiziert. Auch gegenüber der Cloud-Strategie des Bundes haben wir uns medial geäussert (s. 29. TB, SP II).

Der EDÖB analysiert zurzeit eine US-amerikanische Klage gegen das Unternehmen «Oracle America Inc.» wegen unzulässigem Tracking von Internetnutzern und hat dazu am 27.09.2022 eine Kurzmitteilung verfasst (s. Kap. 1.3). Dass Datenweitergabe und Personentracking nebst kommerziellen Interessen auch staatliche Überwachungsvorhaben bedienen, zeigte sich anlässlich der Fussball WM 2022 bei der staatlich geforderten Katar-App, die den EDÖB zu einer Kurzmeldung bewog, in welcher er Reisenden zur WM nach Katar das Mitführen eines Zweit-Smartphones empfahl. Das EU-Vorhaben zur Chat-Kontrolle wird vom EDÖB kritisch betrachtet und war im Berichtszeitraum ebenfalls Thema der Medienberichterstattung.

Zum Datenschutztag vom 2023 haben wir auf den neu überarbeiteten Leitfaden zur Datenbearbeitung im Zusammenhang mit Wahlen und Abstimmungen aufmerksam machten, der sowohl für eidgenössische wie kantonale Vorhaben relevant ist.

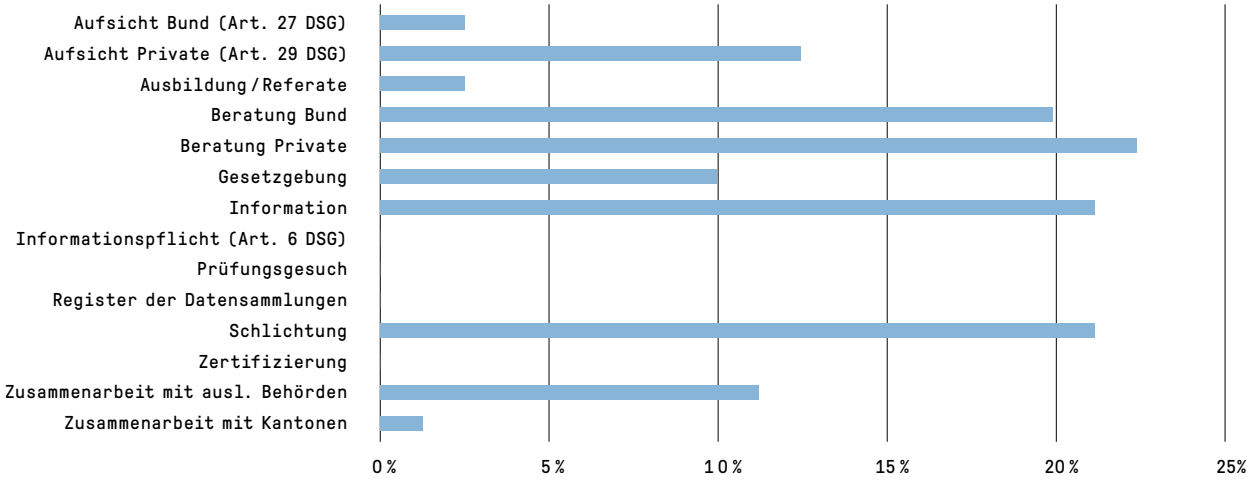
Neue Website

Die Neugestaltung der Website und gleichzeitige Erstellung des vorliegenden Tätigkeitsberichts war eine besondere Herausforderung für das Team des Mediendienstes. Ziel der neuen Website war nicht nur, alle Inhalte hinsichtlich des am 1.9.2023 in Kraft tretenden neuen Datenschutzgesetzes zu aktualisieren, sondern auch die Seite zu verschlanken und neu zu strukturieren, damit die Userinnen und User unserer Website rasch zu den für sie relevanten Informationen finden. Die neue Seite bietet zudem raschen Zugang zu den drei neuen Meldeportalen: dem DataReg zur Meldung von Bearbeitungsverzeichnissen durch Bundesorgane, zum Portal für die Meldung von Verletzungen der Datensicherheit (sog. DataBreach) und zum Portal für die Meldung der Datenschutzberater und -beraterinnen.

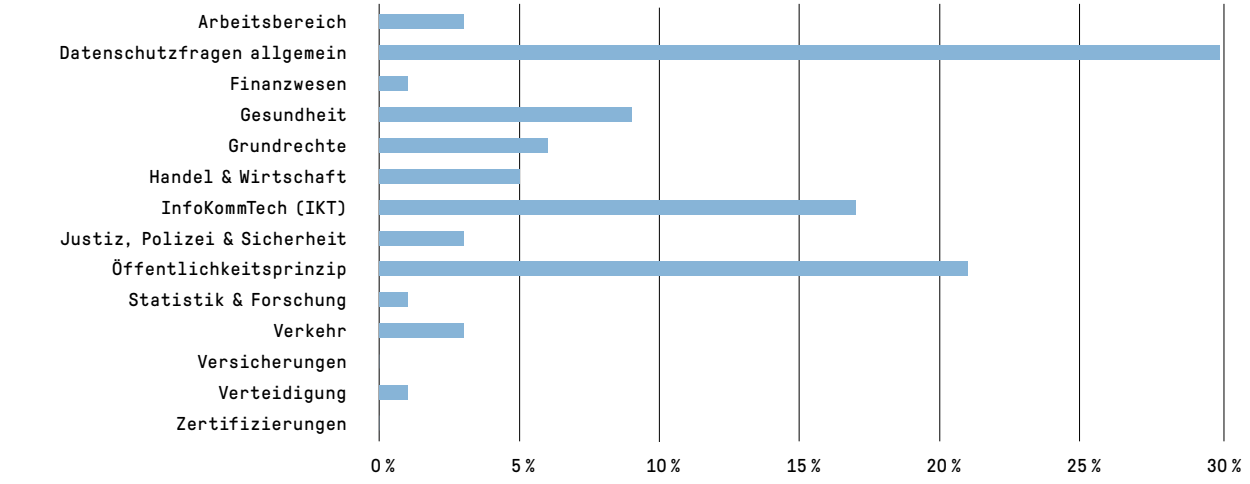
3.3 Statistiken

Statistiken über die Tätigkeiten des EDÖB vom 1. April 2022 bis 31. März 2023 (Datenschutz)

Aufwand nach Aufgabengebiet

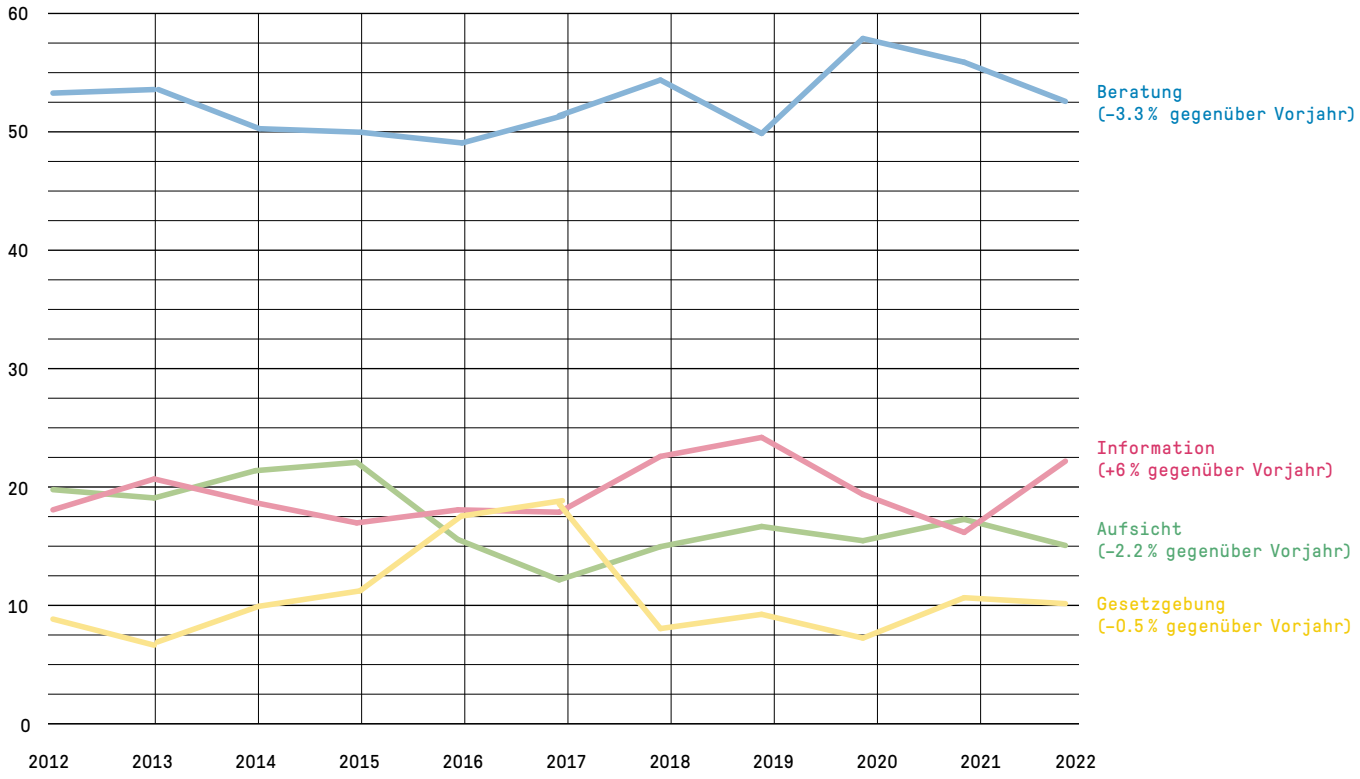


Aufwand nach Sachgebiet



Mehrjahresvergleich Aufwand

(Angaben in Prozent)



Übersicht der Zugangsgesuche vom 1. Januar bis 31. Dezember 2022

Departement	Anzahl Gesuche		Zugang vollständig gewährt		Zugang vollständig verweigert		Zugang teilweise gewährt/aufgeschoben		Zugangsgesuch zurückgezogen		Zugangsgesuch hängig		kein amtliches Dokument vorhanden	
BK	37		23		5		3		1		5		0	
EDA	164		83		18		29		8		10		16	
EDI	207		73		15		73		14		14		18	
EJPD	80		42		9		9		4		1		15	
VBS	295		237		17		18		3		5		15	
EFD	110		37		15		23		10		15		10	
WBF	119		56		11		26		7		8		11	
UVEK	162		68		8		55		6		11		14	
BA	6		5		1		0		0		0		0	
PD	0		0		0		0		0		0		0	
Total 2022 (%)	1180	(100)	624	(53)	99	(8)	236	(20)	53	(5)	69	(6)	99	(8)
Total 2021 (%)	1385	(100)	694	(50)	126	(9)	324	(24)	48	(3)	78	(7)	115	(8)
Total 2020 (%)	1193	(100)	610	(51)	108	(9)	293	(24)	35	(3)	80	(7)	67	(6)
Total 2019 (%)	916	(100)	542	(59)	86	(9)	171	(19)	38	(4)	43	(5)	36	(4)
Total 2018 (%)	647	(100)	355	(55)	66	(10)	119	(18)	24	(4)	50	(8)	33	(5)
Total 2017 (%)	586	(100)	325	(56)	108	(18)	106	(18)	21	(4)	26	(4)	–	
Total 2016 (%)	554	(100)	299	(54)	88	(16)	105	(19)	29	(5)	33	(6)	–	
Total 2015 (%)	600	(100)	320	(53)	99	(17)	128	(21)	31	(5)	22	(4)	–	
Total 2014 (%)	582	(100)	302	(52)	124	(21)	124	(21)	15	(3)	17	(3)	–	
Total 2013 (%)	470	(100)	218	(46)	123	(26)	103	(22)	18	(4)	8	(2)	–	
Total 2012 (%)	518	(100)	230	(44)	140	(27)	123	(24)	19	(4)	6	(1)	–	

Statistiken über Zugangsgesuche nach Öffentlichkeitsgesetz vom 1. Januar bis 31. Dezember 2022

		Anzahl Gesuche	davon eingereicht in Vorjahren	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt/aufgeschoben	Zugangsgesuch zurückgezogen	Zugangsgesuch hängig	kein amtliches Dokument vorhanden
Bundeskanzlei BK	BK	**22**	0	14	3	3	0	2	0
	EDÖB	**15**	0	9	2	0	1	3	0
	Total	**37**	**0**	**23**	**5**	**3**	**1**	**5**	**0**
Eidg. Departement für Auswärtige Angelegenheiten EDA	EDA	**164**	0	83	18	29	8	10	16
	Total	**164**	**0**	**83**	**18**	**29**	**8**	**10**	**16**
Eidg. Departement des Inneren EDI	GS EDI	**10**	0	2	2	1	0	2	3
	EBG	**4**	0	3	0	0	0	1	0
	BAK	**8**	0	5	1	1	1	0	0
	BAR	**2**	0	1	0	0	1	0	0
	METEO CH	**1**	0	1	0	0	0	0	0
	NB	**0**	0	0	0	0	0	0	0
	BAG	**91**	0	22	3	44	8	8	6
	BFS	**4**	0	1	2	1	0	0	0
	BSV	**11**	0	11	0	0	0	0	0
	BLV	**27**	0	14	3	8	0	0	2
	SNM	**0**	0	0	0	0	0	0	0
	swissmedic	**45**	8	10	3	18	4	3	7
	Suva	**4**	1	3	1	0	0	0	0
	compenswiss	**0**	0	0	0	0	0	0	0
	Total	**207**	**9**	**73**	**15**	**73**	**14**	**14**	**18**
Eidg. Justiz- und Polizeidepartement EJPD	GS EJPD	**6**	0	4	0	0	0	0	2
	BJ	**22**	0	9	2	1	0	0	10
	fedpol	**12**	0	5	4	3	0	0	0
	METAS	**3**	0	3	0	0	0	0	0
	SEM	**24**	0	13	2	3	2	1	3
	Dienst ÜPF	**0**	0	0	0	0	0	0	0
	SIR	**3**	0	3	0	0	0	0	0
	IGE	**4**	0	2	0	2	0	0	0
	ESBK	**3**	0	1	0	0	2	0	0
	ESchK	**0**	0	0	0	0	0	0	0
	RAB	**1**	0	1	0	0	0	0	0
	ISC-EJPD	**1**	0	1	0	0	0	0	0
	NKVF	**1**	1	0	1	0	0	0	0
	Total	**80**	**1**	**42**	**9**	**9**	**4**	**1**	**15**

		Anzahl Gesuche	davon eingereicht in Vorjahren	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	**33**	1	6	7	11	1	1	7
	Verteidigung	**3**	0	2	0	0	0	0	1
	NDB	**21**	0	5	7	5	0	0	4
	AB-ND	**0**	0	0	0	0	0	0	0
	armasuisse	**10**	0	3	1	0	0	4	2
	BASPO	**220**	0	218	2	0	0	0	0
	BABS	**4**	0	1	0	2	0	0	1
	swisstopo	**4**	0	2	0	0	2	0	0
	OA	**0**	0	0	0	0	0	0	0
	Total	**295**	**1**	**237**	**17**	**18**	**3**	**5**	**15**
Eidg. Finanzdepartement EFD	GS EFD	**36**	2	8	3	17	2	0	6
	EFV	**1**	0	0	0	0	0	0	1
	EPA	**4**	0	4	0	0	0	0	0
	ESTV	**11**	0	5	3	2	0	0	1
	BAZG	**30**	6	8	6	2	3	11	0
	BBL	**7**	0	4	0	0	0	3	0
	BIT	**4**	0	2	1	1	0	0	0
	EFK	**11**	1	2	2	0	5	0	2
	SIF	**3**	0	1	0	1	0	1	0
	PUBLICA	**1**	0	1	0	0	0	0	0
	ZAS	**2**	0	2	0	0	0	0	0
	Total	**110**	**9**	**37**	**15**	**23**	**10**	**15**	**10**

		Anzahl Gesuche	davon eingereicht in Vorjahren	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	**10**	0	3	4	1	0	0	2
	SECO	**37**	0	11	4	9	3	4	6
	SBFI	**4**	0	2	0	0	0	0	2
	BLW	**15**	1	9	0	5	1	0	0
	Agroscope	**0**	0	0	0	0	0	0	0
	BWL	**9**	0	3	0	4	0	2	0
	BWO	**1**	0	0	0	1	0	0	0
	PUE	**1**	0	1	0	0	0	0	0
	WEKO	**22**	0	15	1	4	1	1	0
	ZIVI	**2**	0	2	0	0	0	0	0
	BFK	**7**	0	7	0	0	0	0	0
	SNF	**0**	0	0	0	0	0	0	0
	EHB	**0**	0	0	0	0	0	0	0
	ETH Bereich	**9**	0	3	1	2	2	1	0
	InnoSuisse	**2**	0	0	1	0	0	0	1
	Total	**119**	**1**	**56**	**11**	**26**	**7**	**8**	**11**
Eidg. Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK	GS UVEK	**9**	1	3	1	2	0	0	3
	BAV	**6**	0	1	2	2	0	0	1
	BAZL	**19**	0	11	2	3	0	3	0
	BFE	**25**	0	5	1	18	0	0	1
	ASTRA	**11**	0	4	0	1	1	2	3
	BAKOM	**19**	1	8	0	6	0	1	4
	BAFU	**62**	1	34	2	18	5	1	2
	ARE	**0**	0	0	0	0	0	0	0
	ComCom	**0**	0	0	0	0	0	0	0
	ENSI	**8**	3	2	0	4	0	2	0
	PostCom	**0**	0	0	0	0	0	0	0
	UBI	**2**	0	0	0	0	0	2	0
	ERI	**0**	0	0	0	0	0	0	0
	SUST	**0**	0	0	0	0	0	0	0
	Total	**1**	0	0	0	1	0	0	0
	Total	**162**	**6**	**68**	**8**	**55**	**6**	**11**	**14**

		Anzahl Gesuche	davon eingereicht in Vorjahren	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt/aufgeschoben	Zugangsgesuch zurückgezogen	Zugangsgesuch hängig	kein amtliches Dokument vorhanden
Bundesanwaltschaft BA	BA	**6**	0	5	1	0	0	0	0
	Total	**6**	**0**	**5**	**1**	**0**	**0**	**0**	**0**
Parlamentsdienste PD	PD	**0**	0	0	0	0	0	0	0
	Total	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
	Gesamttotal	**1180**	**27**	**624**	**99**	**236**	**53**	**69**	**99**

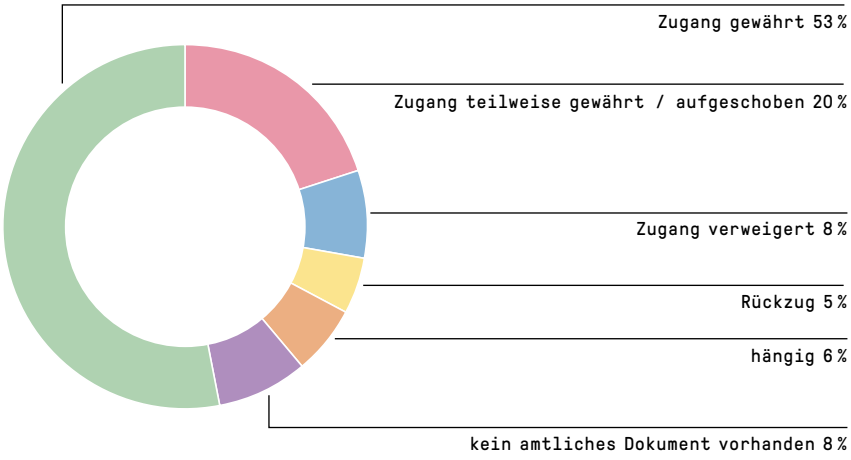
Zugangsgesuche 2022 mit Corona-Bezug

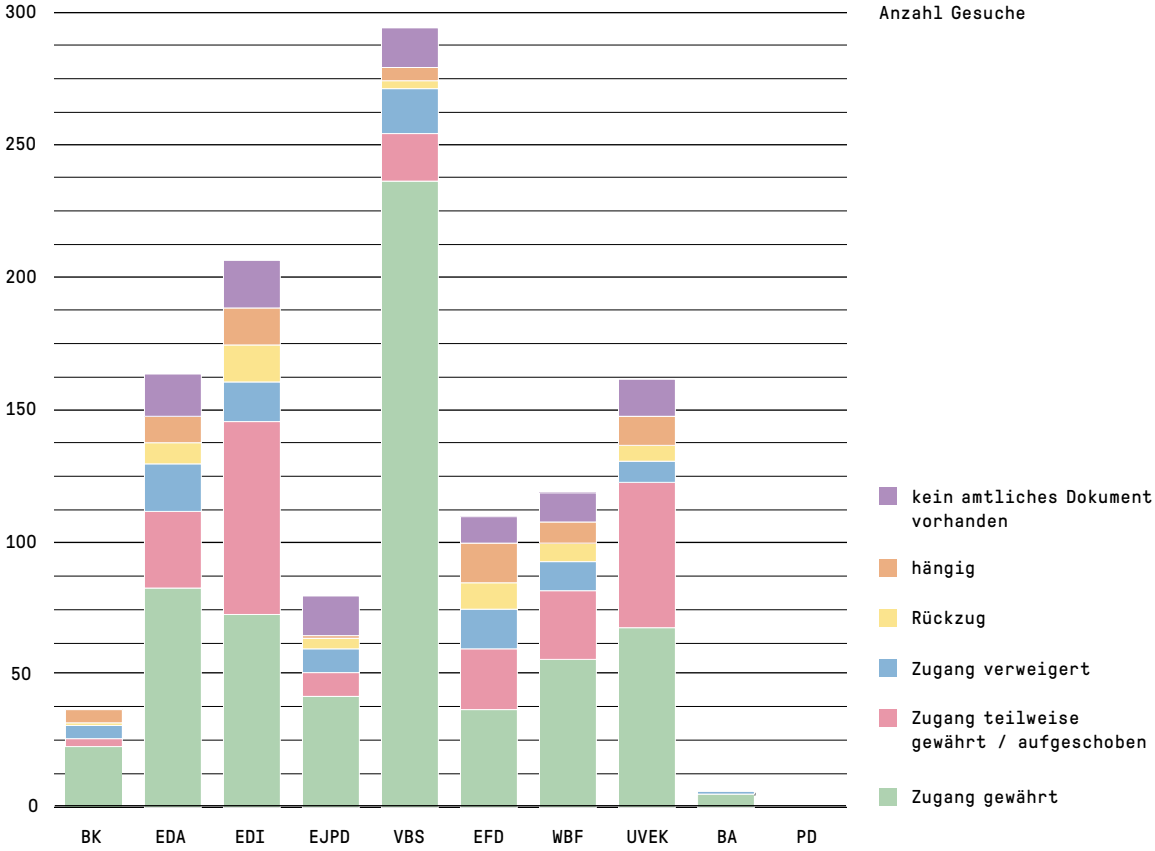
		Gesuche im Zusammenhang mit COVID-19	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt/ aufgeschoben	Zugangsgesuch zurückgezogen	Zugangsgesuch hängig	kein amtliches Dokument vorhanden
Bundeskanzlei BK	**Total**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
Eidg. Departement für Auswärtige Angelegenheiten EDA	**Total**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
Eidg. Departement des Inneren EDI	BAK	**1**	1	0	0	0	0	0
	BAG	**57**	18	2	22	3	6	6
	swissmedic	**18**	4	0	6	4	2	2
	Total	**76**	**23**	**2**	**28**	**7**	**8**	**8**
Eidg. Finanzdepartement EFD	GS EFD	**6**	0	0	5	0	0	1
	ESTV	**1**	0	0	1	0	0	0
	BIT	**2**	1	0	1	0	0	0
	EFK	**1**	0	1	0	0	0	0
	Total	**10**	**1**	**1**	**7**	**0**	**0**	**1**
Eidg. Justiz- und Polizeidepartement EJPD	**Total**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
Eidg. Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK	BAKOM	**1**	1	0	0	0	0	0
	Total	**1**	**1**	**0**	**0**	**0**	**0**	**0**
Eidg. Departement für Verteidigung, Bevölkerungsschutz und Sport VBS	BABS	**1**	0	0	0	0	0	1
	Total	**1**	**0**	**0**	**0**	**0**	**0**	**1**
Eidg. Departement für Wirtschaft, Bildung und Forschung WBF	SECO	**5**	4	1	0	0	0	0
	Total	**5**	**4**	**1**	**0**	**0**	**0**	**0**
Bundesanwaltschaft BA	**Total**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
Parlamentsdienste PD	**Total**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
	Gesamttotal	**93**	**29**	**4**	**35**	**7**	**8**	**10**

Anzahl Schlichtungsgesuche nach Kategorien der Antragstellenden

Kategorie Antragsteller	2022	2021	2020	2019	2018	2017
Medien	47	53	31	34	24	21
Privatpersonen (bzw. keine genaue Zuordnung möglich)	37	49	42	40	26	35
Interessenvertreter (Verbände, Organisationen, Vereine usw.)	9	16	5	7	9	14
Rechtsanwälte	27	12	7	5	4	2
Unternehmen	9	19	7	47	13	7
Universitäten	0	0	1	0	0	0
Total	**129**	**149**	**93**	**133**	**76**	**79**

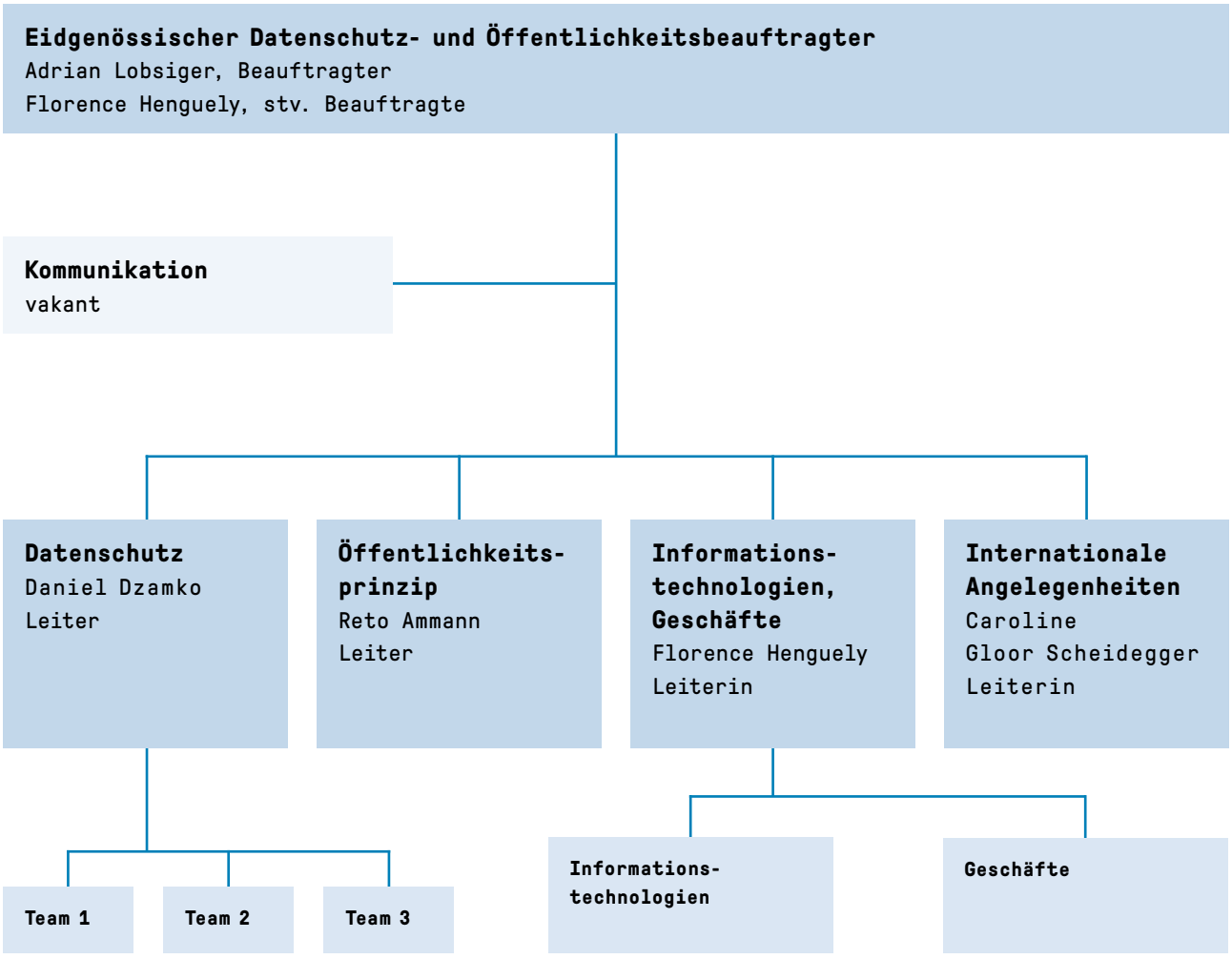
Zugangsgesuche der gesamten Bundesverwaltung vom 1. Januar bis 31. Dezember 2022





3.4 Organisation EDÖB (Stand 31. März 2023)

Organigramm



Mitarbeiter und Mitarbeiterinnen des EDÖB

Anzahl Mitarbeitende	41		
FTE	34.1		
nach Geschlecht	Frauen	20	49 %
	Männer	21	51 %
nach Beschäftigungsgrad	1–89 %	31	76 %
	90–100 %	10	24 %
nach Sprache	Deutsch	32	78 %
	Französisch	8	20 %
	Italienisch	1	2 %
nach Alter	20–49 Jahre	24	59 %
	50–65 Jahre	17	41 %
Kaderpositionen	Frauen	4	40 %
	Männer	6	60 %

Abkürzungsverzeichnis

BAZG Bundesamt für Zoll und Grenzsicherheit (ehem. EZV)

BGA Bundesgesetz über die Archivierung

BGÖ Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsgesetz

DataReg Register der Datensammlungen

DSFA Datenschutz-Folgenabschätzung

DSG Datenschutzgesetz

DSV Verordnung über den Datenschutz

DSGVO EU-Datenschutzgrundverordnung

DTI Bereich Digitale Transformation und IKT-Lenkung der Bundeskanzlei

EDSA Europäischer Datenschutzausschuss

EDSB Europäischer Datenschutzbeauftragter

E-ID elektronische Identität

EPD Elektronisches Patientendossier

EPDG Bundesgesetz über das elektronische Patientendossier

Fedpol Bundesamt für Polizei

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

nDSG neues revidiertes Datenschutzgesetz

NOSR Nationales Organspenderegister

PNR Flugpassagierdaten

Privatim Konferenz der Schweizer Datenschutz-Beauftragten (kantonale Datenschutzbehörden)

SAS Schweizerische Akkreditierungsstelle

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

SIS II Schengener Informationssystem der zweiten Generation

VDSZ Verordnung über die Datenschutzzertifizierungen

VIS Visa-Informationssystem

VwVG Verwaltungsverfahrensgesetz des Bundes

Abbildungsverzeichnis

Grafiken

Grafik 1: Beurteilung Zugangsgesuche – Entwicklung seit 2009 ..... S. 65

Grafik 2: Erhobene Gebühren seit Inkrafttreten des BGÖ ..... S. 67

Grafik 3: Schlichtungsanträge seit Inkrafttreten des BGÖ ..... S. 68

Tabellen

Tabelle 1: Einvernehmliche Lösungen ..... S. 69

Tabelle 2: Bearbeitungsdauer Schlichtungsverfahren ..... S. 70

Tabelle 3: Hängige Schlichtungsverfahren ..... S. 71

Tabelle 4: Spezialbestimmungen nach Art. 4 BGÖ ..... S. 80

Tabelle 5: Keine Spezialbestimmungen nach Art. 4 BGÖ ..... S. 81

Tabelle 6: Für DSG-Belange einsetzbare Stellen ..... S. 85

Tabelle 7: Leistungen Datenschutz ..... S. 86

Tabelle 8: Beratungen in umfangreicheren Projekten für 2022 ..... S. 86

Tabelle 9: Wirkungsziele EDÖB ..... S. 87

Impressum

Dieser Bericht ist in vier Sprachen vorhanden und über das Internet (www.derbeauftragte.ch) aufrufbar.
Vertrieb: BBL, Verkauf Bundespublikationen, CH-3003 Bern
www.bundespublikationen.admin.ch
Art.-Nr. 410.030.D

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

Kennzahlen

Leistungen Datenschutz

53 %	15 %	22 %	10 %
Beratung	Aufsicht	Information	Gesetzgebung

Zugangsgesuche Öffentlichkeitsprinzip (BGÖ)

53 %	20 %	8 %	5 %	6 %	8 %
gewährt	teilweise gewährt/ aufgeschoben	verweigert	Rückzug	hängig	kein amtliches Dokument vorhanden

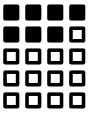
Anliegen des Datenschutzes

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

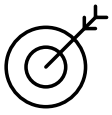
Wahlmöglichkeit
Betroffene geben ihre Einwilligung informiert und erhalten eine echte Wahlfreiheit.

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