



25. Juni 2018

Resümee wichtiger Themen des 25. Tätigkeitsberichts

Datenschutz

Am 15. September 2017 hat der Bundesrat die Botschaft zur **Totalrevision des Bundesgesetzes über den Datenschutz** und die Änderung weiterer Erlasse zum Datenschutz verabschiedet und an das Parlament überwiesen. Das Ziel der Revision besteht darin, den Datenschutz zu stärken, insbesondere indem die Transparenz der Datenbearbeitung erhöht wird und jede Person die sie betreffenden Daten besser kontrollieren kann. Während wir die Grundzüge der Revision befürworteten, haben wir zum Entwurf des Bundesrats Vorbehalte geäussert betreffend der terminologischen und materiellen **Abweichungen von der Datenschutz-Grundverordnung der EU** und vom modernisierten Übereinkommen 108. Sie komplizieren die Rechtslage der Schweizer Unternehmen und Behörden, die der Datenschutz-Grundverordnung direkt unterliegen, und schaffen Rechtsunsicherheit. Wir haben uns im Übrigen vergeblich für eine rasche Verabschiedung des Projekts eingesetzt (Kap. 1.1.1).

Der Bundesrat hat das Eidgenössische Departement des Innern (EDI) mit der Erstellung eines Gesetzesentwurfs beauftragt, um die **Verwendung der AHV-Nummer als Personenidentifikator** auch ausserhalb der Sozialversicherungen durch alle Behörden des Bundes, der Kantone und der Gemeinden zu vereinfachen. Aufgrund eines vom EDÖB mit dem Bundesamt für Justiz (BJ) erteilten Mandats hat ETH-Professor David Basin Ende September 2017 mit Blick auf die Verwendung von Personenidentifikatoren und die geplante Weiterausbreitung der AHVN13 eine Analyse der datenschutzrechtlichen Risiken vorgelegt (Kap. 1.1.2).

Hinsichtlich der eidgenössischen Wahlen 2019 hat der EDÖB datenschutzrechtliche Erläuterungen für den **Einsatz von digitalen Kampagnentools** auf seiner Website publiziert. Diese Tools erlauben es politischen Gruppierungen und Interessenverbänden, persönliche Kontakte digital zu organisieren und gezielt auf Interaktionen auszurichten sowie bestimmte Aktionen in ihre Webseitenumgebung zu integrieren. Wir haben zunächst darauf hingewiesen, dass die betroffenen Personen vor der Registrierung vollständig und verständlich über die Datenbearbeitung informiert werden müssen. Erst wenn die Nutzer auf Basis dieser Informationen ausdrücklich und selbstbestimmt zugestimmt haben, dürfen deren Daten verwendet werden (Kap. 1.1.3).

Die SBB haben uns über mehrere datenschutzrelevante Projekte informiert. Dabei ging es um den Einsatz von **Bodycams** und um die Entwicklung neuer Apps. Die datenschutzrechtliche Analyse dieser Vorhaben erfolgte jeweils vorgängig durch den Datenschutzberater der SBB. Bei der „**SwissPass Mobile**“-App hat der EDÖB darauf hingewiesen, dass alle Personen, die dies wünschen, die Möglichkeit behalten, anonym zu reisen, ohne dafür besondere Tarifzuschläge in Kauf nehmen zu müssen (Kap. 1.2.1).

Swisscom hat den EDÖB Ende Dezember 2017 darüber in Kenntnis gesetzt, dass im vorangehenden Herbst unberechtigte Zugriffe auf die Kontaktdaten von rund 800'000 Kundinnen und Kunden erfolgt



sind. Wir haben das Unternehmen mit Blick auf Minimierung der Risiken und Wahrung der Informationsrechte ihrer Kunden beraten. Nachdem die nötigen Sachverhaltsklärungen und Schutzmassnahmen getroffen und die Kunden über das **Datenleck** informiert wurden, konnte der EDÖB den Fall ohne Einleitung formeller Schritte abschliessen (Kap. 1.3.2).

Mit der Schaffung einer **elektronischen Identität (E-ID)** soll in erster Linie die Rechtssicherheit im digitalen Verkehr gestärkt werden. Wir verfolgten dieses Grossvorhaben einerseits im Rahmen der Vernehmlassung zur gesetzlichen Grundlage. Andererseits begleiten wir zwei private Initiativen (Kap. 1.3.3).

Das Bundesgericht hat die Position des EDÖB bezüglich des **Auskunftsrechts zu den Randdaten des Fernmeldeverkehrs** bestätigt. Die Fernmeldediensteanbieter müssen bei Auskunftsgesuchen alle Angaben, die sich auf die gesuchstellende Person beziehen beziehungsweise ihr zugeordnet werden können herausgeben (Kap. 1.3.4).

Im Falle des Entwurfs zu einem Bundesgesetz über polizeiliche Massnahmen zur **Bekämpfung von Terrorismus** hatte der EDÖB deutliche Divergenzen mit Fedpol. Das Polizeirecht des Bundes wird in verschiedenen Gesetzen geregelt, was eine Gesamtsicht der verschiedenen Bearbeitungen von Personendaten erschwert. Dieses Gesetzesprojekt verschärft die Komplexität der Lage. Daher fordern wir die Ausarbeitung eines Gesetzes über die Tätigkeit der Polizeiorgane des Bundes analog zu den bestehenden kantonalen Gesetzen. Es muss klar geregelt werden, in welchem Informationssystem die Daten zu den polizeilichen Massnahmen zur Terrorismusbekämpfung verarbeitet werden sollen (Kap. 1.4.3).

Der EDÖB hat die Datenbearbeitungen beim Staatssekretariat für Migration (SEM) in Zusammenhang mit **Schengenvisa** überprüft sowie eine Kontrolle vor Ort durchgeführt. Im Rahmen der Schengen-Assoziierungsabkommen hat er beim SEM als Endbenutzer des Schengener Informationssystems (SIS) eine Kontrolle der Ausschreibungen zwecks Einreise- oder Aufenthaltsverweigerung durchgeführt (Kap. 1.4.6 und 1.4.7).

Anfang 2018 fand die **dritte Schengen-Evaluation** der Schweiz als assoziiertes Mitglied statt. Sie betrifft sämtliche Bereiche der Schengener Zusammenarbeit: Management der Aussengrenze (Flughäfen), Rückkehr/Rückführung, Schengener Informationssystem SIS II/SIRENE, gemeinsame Visapolitik, polizeiliche Zusammenarbeit und Bearbeitung personenbezogener Daten. Die Arbeiten wurden vom Bundesamt für Justiz (BJ) in Zusammenarbeit mit der Direktion für Europäische Angelegenheiten (DEA) koordiniert. Der EDÖB hat in datenschutzrechtlicher Hinsicht beraten (Kap. 1.4.5).

Weil auch im **Krankenversicherungsbereich zunehmend ein Outsourcing** von Aufgaben an branchenfremde Dienstleister stattfindet, hat der EDÖB einen Fall untersucht, bei dem der Auftragnehmer die Korrespondenz zwischen Versicherten und ihrer Krankenversicherung geöffnet und weiterverarbeitet hat (Kap. 1.6.3). Die Dienstleister Swisscom Health und die Ärztekasse wurden von uns zu mehr Transparenz auf ihren Internetseiten aufgefordert, damit Patientinnen und Patienten besser über das Outsourcing informiert sind (Kap. 1.5.3).

Mehrere Krankenversicherungen bieten **Gesundheitsapps und Bonusprogramme** an. Wir prüften, ob die Versicherten ihre Gesundheitsdaten den Versicherungen freiwillig zur Verfügung stellen und die Vorgaben des Datenschutzes und der Datensicherheit eingehalten werden. Der EDÖB hat gegenüber der Helsana Krankenkasse eine formelle Sachverhaltsabklärung des Bonusprogramms „Helsana+“ durchgeführt. Er hat der Helsana Zusatzversicherungen AG infolge Fehlens der vom DSG verlangten gesetzlichen Grundlage empfohlen, die Bearbeitung von Grundversicherungsdaten zu unterlassen, und in der Folge Klage vor Bundesverwaltungsgericht eingereicht (Kap. 1.6.4).



In Gastronomiebetrieben werden vermehrt **biometrische Zeiterfassungs- und Zutrittssysteme** (z.B. Arbeitszeiterfassung per Fingerabdruck) eingesetzt. Weil diese Daten besonders schützenswert sind, sollte ihr Einsatz sorgfältig und restriktiv erfolgen (Kap. 1.7.4). Navigationsgeräte in Geschäftsfahrzeugen und andere **Geräte mit GPS-Funktion** scheinen immer häufiger zur Überwachung von Mitarbeitenden eingesetzt zu werden. Wir erhielten im Berichtsjahr mehrere Anfragen von Betroffenen. Diese Art der Überwachung ist nur zulässig, wenn sowohl die Rahmenbedingungen des Datenschutzrechts als auch des Arbeitsrechts berücksichtigt werden (Kap. 1.7.3). Arbeitgeber sollten im Sinne der Transparenz den Umgang des Personals mit Informatikmitteln in einem Reglement festlegen und darin aufzeigen, wer welche Rechte und Pflichten hat. Dies verhindert Konflikte während und nach Beendigung des Arbeitsverhältnisses und erleichtert einen **«sauberen Abgang» bei Kündigung der Arbeitsstelle** (Kap. 1.7.2).

Seit April 2017 können sich amerikanische Unternehmen für das **Swiss-US Privacy Shield** zertifizieren lassen und damit ein angemessenes Datenschutzniveau garantieren. Im Berichtsjahr hat der EDÖB die Umsetzung des Swiss-US Privacy Shield begleitet und einen **Ratgeber** für Bürgerinnen und Bürger veröffentlicht. Die Broschüre informiert über die Pflichten der zertifizierten Unternehmen und die Rechte betroffener Personen und wie diese im Beschwerdefall vorgehen können. Im Herbst 2018 erfolgt die erste Evaluation zeitgleich mit der zweiten EU-US Privacy Shield Evaluation (Kap. 1.8.1 und Kap. 3.2).

Zum **Datenleck bei der Inkassofirma EOS Schweiz AG** hat der EDÖB eine Sachverhaltsabklärung eröffnet. Zu den Betroffenen sollen insbesondere Patienten von Schweizer Ärzten und Zahnärzten zählen. In den öffentlichen Stellungnahmen haben wir daran erinnert, dass Medizinalpersonen nur diejenigen Daten von Patienten an Dritte weitergeben dürfen, die für die Rechnungsstellung bzw. das Inkasso tatsächlich erforderlich sind. Geben sie deren Gesundheitsdaten ungerechtfertigt an Dritte weiter, machen sie sich strafbar (Kap. 1.8.2).

Das Werbeunternehmen APG/SGA hat uns um eine datenschutzrechtliche Einschätzung zu einer Plattform für **personalisierte Werbung in Apps aufgrund von Standortdaten** gebeten. Weil dabei umfangreiche Bewegungsprofile und Ortungsdaten grundsätzlich unbefristet bearbeitet werden sollen und eine Identifizierung der betroffenen Personen in vielen Fällen relativ leicht möglich erscheint, hat der EDÖB gezielte Massnahmen vorgeschlagen. Ausserdem müssen die Nutzer bei der Installation der Applikationen der Drittanbieter umfassend und transparent über die Datenbearbeitung informiert werden und ihre ausdrückliche Zustimmung erteilen. Sie müssen auch jederzeit die Möglichkeit haben, ihre einmal erteilte Einwilligung zu widerrufen (Kap. 1.8.4).

Der EDÖB steht im Austausch mit der **Werbevermarkterin Admeira**, welches in Besitz von Ringier, SRG und Swisscom ist. Die betroffenen Personen sollen der Weitergabe ihrer persönlichen Daten zu Werbezwecken widersprechen können. Der EDÖB hat die Swisscom hinsichtlich ihrer Informationspflichten gegenüber der Kundschaft in Zusammenhang mit ihren neuen Datenschutzbestimmungen beraten. Es gilt sicherzustellen, dass die Datenflüsse und Auswertungen für die betroffenen Personen durchgehend erkennbar sind (Kap. 1.8.5).

Die Umsetzung der neuen Standards zur weltweiten Verhinderung von Steuerbetrug und Steuerhinterziehung schreitet weiter fort. Im Rahmen des neu eingeführten **automatischen Informationsaustauschs über Finanzkonten (AIA)** hat die Schweiz ab 2017 Daten gesammelt, welche 2018 erstmals ausgetauscht werden sollen. Die Bundesversammlung hatte 2016 der Einführung des AIA mit einer ersten Serie Länder zugestimmt, darunter mit den EU-Staaten. Im Juni 2017 verabschiedete der Bundesrat die Botschaft über die Einführung des AIA mit weiteren 41 Partnerstaaten. Der EDÖB wies darauf



hin, dass mehr als 30 dieser Staaten über kein angemessenes Datenschutzniveau verfügen, weshalb zusätzliche Datenschutzgarantien nötig seien (Kap. 1.9.1).

In **Anmeldeformularen für Mietwohnungen** müssen Interessentinnen und Interessenten Mieterinnen oft viel Persönliches preisgeben. Welche Auskünfte in einem solchen Formular zulässig sind und aus welchen datenschutzrechtlichen Überlegungen auf gewisse Fragen verzichtet werden sollte, wird in unseren Erläuterungen ausführlich dargelegt (Kap. 3.2).

Die Bestimmungen der **EU-Datenschutzgrundverordnung (DSGVO)** sind vielen Fällen auch für Schweizer Unternehmen, die Daten von EU-Bürgern bearbeiten oder ihre Dienstleistungen in der EU anbieten, unmittelbar anwendbar. Wir haben dazu umfassende Informationen auf unserer Internetseite zusammengetragen sowie einen detaillierten **Leitfaden** erstellt, der sowohl über die neuen Pflichten für Unternehmen informiert als auch über die Rechte für Privatpersonen zum Schutz ihrer Privatsphäre (Kap. 3.2).

Öffentlichkeitsprinzip

Zur **Beschleunigung des Schlichtungsverfahrens** und zum Abbau von Pendenzen führte der EDÖB im Jahr 2017 einen Pilotversuch durch. Der Auswertungsbericht zeigt nun, dass mit den ergriffenen Massnahmen die gesetzten Ziele erreicht wurden und der Pilotversuch erfolgreich war. Angesichts der positiven Resultate wird er in den ordentlichen Betrieb überführt (Kap. 2.3.1).

Der Verordnungsentwurf zum neuen Nachrichtendienstgesetz enthielt anfangs eine Bestimmung, mit der praktisch sämtliche Dokumente des **Nachrichtendienstes des Bundes (NDB)** vom Öffentlichkeitsgesetz ausgenommen worden wären. Die von uns kritisierte Bestimmung wurde im Anschluss an die Vernehmlassung gestrichen (Kap. 2.4.1).

Der EDÖB hatte sich in der letzten Berichtsperiode bei der Vorlage zur **Organisation der Bahninfrastruktur (OBI)** gegen die Einschränkung des Öffentlichkeitsprinzips ausgesprochen (Kap. 2.3.1 des 24. Tätigkeitsberichts). Das Bundesgericht hat entschieden, dass die in einer Datenbank des Bundesamts für Verkehr (BAV) verzeichneten Gefährdungen und Störungen im öffentlichen Verkehr bekannt gegeben werden müssen und die Beschwerde der Behörde abgewiesen, die einem Journalisten die Einsicht verweigern wollte (Kap. 2.4.2 des aktuellen Berichts). Ende Mai hat das Parlament beschlossen, Aufsichtstätigkeiten des Bundesamts für Verkehr (BAV) im Sicherheitsbereich vom Öffentlichkeitsgesetz ausnehmen.

Der Jahresbericht ist über das Internet integral abrufbar (www.derbeauftragte.ch – Dokumentation – Tätigkeitsberichte) oder kann beim BBL, Vertrieb Publikationen, 3003 Bern bestellt werden: Art. Nr. 410.025.d Bestellung per Internet: <http://www.bundespublikationen.admin.ch>