Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB
Préposé fédéral à la protection des données et à la transparence PFPDT
Incaricato federale della protezione dei dati e della trasparenza IFPDT
Incumbensà federal per la protecziun da datas e per la transparenza IFPDT

Das neue Datenschutzgesetz aus Sicht des EDÖB

Inhaltsverzeichnis

I. Einleitung

In der Herbstsession 2020 hat das Eidgenössische Parlament das totalrevidierte Bundesgesetz über den Datenschutz (DSG) sowie weitere, geänderte Erlasse zum Datenschutz verabschiedet. Die Referendumsfrist ist am 14. Januar 2021 ungenutzt abgelaufen. Die Bundesverwaltung ist aktuell daran, die dazugehörigen Vollzugsverordnungen auszuarbeiten, welche der Bundesrat voraussichtlich im zweiten Semester des Jahres 2022 zusammen mit dem neuen DSG in Kraft setzen wird.

Bis zum Inkrafttreten werden die Privatwirtschaft und die Bundesbehörden die Bearbeitung von Personendaten an die neuen Bestimmungen anzupassen haben. Vorliegend weist der EDÖB auf die wichtigsten Neuerungen hin, welche sie dabei beachten müssen.

II. Vorgeschichte und Ziele der Revision

Das erste Bundesgesetz über den Datenschutz vom 19. Juni 1992 trat Mitte 1993 in Kraft – zu einem Zeitpunkt also, in welchem das Internet noch nicht kommerziell genutzt wurde und die heutige, vom Umgang mit dem allgegenwärtigen Smartphone geprägte, digitale Realität noch nicht absehbar war. Nach einer Teilrevision im Jahr 2008, deren Ziel es war, die Bevölkerung besser über die Bearbeitung ihrer Daten zu informieren, sollte sich schon bald zeigen, dass die rasante, technologische Entwicklung weitere Anpassungen notwendig machte. Inzwischen ist für das Gros der Bevölkerung ein Leben ohne jederzeitigen Internetzugang sowie intelligente und mit berührungssensiblen Bildschirmen ausgerüsteten Geräten kaum mehr vorstellbar. Um der Bevölkerung in einem Alltag, der von Cloud-Computing, Big Data, Sozialen Netzwerken und Internet der Dinge geprägt ist, einen zeitgemässen Datenschutz zu garantieren, wurde eine umfassende Erneuerung des DSG unausweichlich.

Im Herbst 2017 verabschiedete der Bundesrat den Entwurf zu einer Totalrevision des DSG, den er mit der dazugehörenden Botschaft an die eidgenössischen Räte überwies. Ziel dieser Revision war es, den Datenschutz an die veränderten technologischen und gesellschaftlichen Verhältnisse anzupassen. Das neue DSG muss damit dem Anspruch gerecht werden, die informationelle Selbstbestimmung sowie die Privatsphäre der Bürgerinnen und Bürger zu stärken und damit möglichst langfristig zu gewährleisten.

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

Anfang 2018 beschloss das Parlament, die Revision in zwei Etappen aufzuteilen: Zwecks Beachtung staatsvertraglicher Umsetzungsfristen wurden in einer ersten Etappe vorab die Bestimmungen zu Datenbearbeitungen angepasst, die für Bundesorgane wie das fedpol gelten, welche die angepasste EU-Richtlinie 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten im Bereich des Strafrechts anwenden, weil diese Teil des sog. Acquis zum Schengener Assoziierungsübereinkommen sind. Diese Arbeiten mündeten im sog. Schengen-DSG bzw. SDSG. In einem zweiten Schritt erfolgte dann die Totalrevision des DSG als Ganzes.

1. Etappe 1: Schengen-Teil

Das SDSG trat am 1. März 2019 in Kraft. Neben dem SDSG, dessen Geltungsdauer bis zum Inkrafttreten der Totalrevision begrenzt ist, wurden sodann weitere Gesetze angepasst, die in den Bereich der Schengener Zusammenarbeit in Strafsachen fallen.

2. Etappe 2: Ganzes Gesetz

In der Herbstsession 2019 nahm sich der Nationalrat der Totalrevision des ganzen Gesetzes als Erstrat an, welche die eidgenössischen Räte am 25. September 2020 nach Bereinigung aller Differenzen verabschiedet haben. Bei der Ausgestaltung des neuen DSG berücksichtigten Bundesrat und Parlament die von der Schweiz unterzeichnete Erweiterung der Europaratskonvention 108[1] sowie die Datenschutzgrundverordnung der Europäischen Union (DSGVO)[2]. Aufgrund ihres extraterritorialen Anwendungsbereichs wird Letztere seit ihrer Inkraftsetzung im Mai 2018 bereits von weiten Teilen der Schweizer Wirtschaft angewandt. Trotz dieser Anlehnung an das europäische Recht entspricht das neue DSG der schweizerischen Rechtstradition, indem es einen hohen Abstraktionsgrad ausweist und technologieneutral formuliert ist. Von der DSGVO hebt es sich nicht nur aufgrund seiner Kürze, sondern auch einer teilweise unterschiedlichen Terminologie ab. Allgemein wird davon ausgegangen, dass die Schweiz und die EU nach der Erneuerung ihrer Datenschutzgesetzgebungen gegenseitig die Gleichwertigkeit ihrer Datenschutzniveaus anerkennen werden, so dass der formlose Austausch von Personendaten über die Landesgrenzen weiterhin möglich bleibt. Die Erneuerung des aus dem Jahre 2000 stammenden Anerkennungsbeschlusses der EU gegenüber der Schweiz wird für das Frühjahr 2021 erwartet.

III. Wichtigste Neuerungen des totalrevidierten Datenschutzgesetzes

3. Nur noch Daten von natürlichen Personen

Das revidierte DSG bezweckt ausschliesslich den Schutz der Persönlichkeit von natürlichen Personen, über welche Personendaten bearbeitet werden. Daten von juristischen Personen wie kaufmännischen Gesellschaften, Vereinen oder Stiftungen werden vom neuen DSG nicht mehr erfasst, womit dessen Geltungsbereich mit jenem der DSGVO übereinstimmt. Unternehmen können sich nach wie vor auf den Persönlichkeitsschutz durch Art. 28 ZGB, den Schutz des Geschäfts- und Fabrikationsgeheimnis nach Art. 162 StGB sowie die einschlägigen Bestimmungen der Bundesgesetze über den unlauteren Wettbewerb und über Kartelle berufen.

4. Besonders schützenswerte Personendaten

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

5. Privacy by Design und by Default

Im revidierten DSG sind neu die Grundsätze «Privacy by Design» (Datenschutz durch Technik) und «Privacy by Default» (Datenschutz durch datenschutzfreundliche

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

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

Voreinstellungen) verankert. Sie verpflichten Behörden und Unternehmen, die Bearbeitungsgrundsätze des DSG bereits ab der Planung entsprechender Vorhaben umzusetzen, indem sie angemessene technische und organisatorische Schutzmassnahmen treffen. Der Datenschutz durch Technik verlangt, dass sie ihre Applikationen u.a. so ausgestalten, dass die Daten standardmässig anonymisiert oder gelöscht werden. Datenschutzfreundliche Voreinstellungen schützen die Nutzer von privaten Online-Angeboten, die sich weder mit Nutzungsbedingungen noch den daraus abzuleitenden Widerspruchsrechten auseinandergesetzt haben, indem nur die für den Verwendungszweck unbedingt nötigen Daten bearbeitet werden, solange sie nicht aktiv werden und weitergehende Bearbeitungen autorisieren. Um diesen Schutz des neuen Gesetzes zu gewährleisten, sollten Schweizer Unternehmen ihre Angebote rechtzeitig überprüfen und nötigenfalls durch Einsatz datenschutz- und kundenfreundlicher Programme Anpassungen vornehmen.

6. Datenschutzberater und Datenschutzberaterinnen

Private Unternehmen können nach Art. 10 revDSG eine Datenschutzberaterin oder einen Datenschutzberater ernennen. Diese können, müssen aber nicht in einem arbeitsvertraglichen Verhältnis zum Unternehmen stehen. In beiden Fällen sollte die Datenschutzberatung getrennt von übrigen Aufgaben des Unternehmens wahrgenommen werden. Auch empfiehlt es sich, die Geschäfte der Datenschutzberatung nicht mit jenen der übrigen Rechtsberatung und -vertretung zu vermischen. Weiter sollte Datenschutzberatern und -beraterinnen erlaubt sein, ihren Standpunkt bei Meinungsverschiedenheiten der Unternehmensleitung zur Kenntnis zu bringen. Im Gegensatz zur europäischen DSGVO ist die Ernennung von Beratern und Beraterinnen für Private stets fakultativ – nur Bundesorgane sind gesetzlich dazu verpflichtet. Sie sind nicht nur eine innerbetriebliche Anlaufstelle, sondern auch Bindeglied zum behördlichen Datenschutz und erste Ansprechpersonen für den EDÖB. Zu ihren Aufgaben gehören nebst der allgemeinen Beratung und Schulung des Unternehmens in Fragen des Datenschutzes die Mitwirkung beim Erlass und der Anwendung von Nutzungsbedingungen und Datenschutzvorschriften. Wird die interne Datenschutzberatung fachlich unabhängig und weisungsungebunden ausgeübt, und werden dort keine Aufgaben wahrgenommen, die mit der Funktion unvereinbar sind, kann ein Unternehmen nach Durchführung einer Datenschutz-Folgenabschätzung auch bei fortbestehend hohem Risiko einzig auf die interne Beratung abstellen, ohne darüber hinaus den EDÖB konsultieren zu müssen (s. dazu unten «Datenschutz-Folgenabschätzungen»).

7. Datenschutz-Folgenabschätzung

Datenschutz-Folgenabschätzungen sind im Schweizer Datenschutzrecht nicht neu – Bundesorgane sind bereits heute dazu verpflichtet. Wenn eine beabsichtigte Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann, müssen gemäss Art. 22 revDSG neu auch private Verantwortliche vorgängig eine Datenschutz-Folgenabschätzung erstellen. Das hohe Risiko ergibt sich – insbesondere bei Verwendung neuer Technologien – aus der Art, dem Umfang, den Umständen und dem Zweck der Bearbeitung. Insbesondere liegt ein hohes Risiko dann vor, wenn ein Profiling mit hohem Risiko oder umfangreiche Bearbeitungen besonders schützenswerter Personendaten geplant sind. Allgemein gehaltene Folgenabschätzungen vermögen nicht von erkennbaren Risiken zu dispensieren, die sie unerwähnt lassen. Ist ein Produkt, System oder eine Dienstleistung nach Art. 13 revDSG zertifiziert oder wird ein Verhaltenskodex nach Art. 11 revDSG eingehalten, der auf einer Datenschutz-Folgenabschätzung beruht, kann von der Erstellung einer solchen abgesehen werden. Ist aus einer Datenschutz-Folgenabschätzung erkennbar, dass die geplante Bearbeitung trotz der vom Verantwortlichen vorgesehenen Massnahmen noch ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen zur Folge hätte, muss dieser nach Art. 23 revDSG vorgängig die Stellungnahme des EDÖB einholen. Hat der EDÖB Einwände gegen die Folgenabschätzung selber, wird er dem Verantwortlichen entsprechende Präzisierungen oder Ergänzungen

nahelegen. Dies dürfte vor allem der Fall sein, wenn der Text so allgemein gehalten ist, dass er voraussehbare Risiken oder Massnahmen nur unzureichend beschreibt. Richten sich die datenschutzrechtlichen Einwände gegen die geplanten Bearbeitungen als solche, schlägt der EDÖB dem Verantwortlichen geeignete Massnahmen zu deren Modifizierung vor (s. dazu unten «Konsultationen»). Anders als bei den Verhaltenskodizes müssen die Stellungnahmen des EDÖB nicht publiziert werden. Als amtliche Dokumente unterstehen sie jedoch dem Bundesgesetz über das Öffentlichkeitsprinzip in der Verwaltung. Auf die Konsultation des EDÖB kann verzichtet werden, wenn die interne Datenschutzberatung konsultiert wurde (s. dazu oben «Datenschutzberater und Datenschutzberaterinnen»).

8. Verhaltenskodizes

In Art. 11 hat das neue DSG für Berufs-, Branchen- und Wirtschaftsverbände Anreize gesetzt, eigene Verhaltenskodizes zu entwickeln und diese dem EDÖB zur Stellungnahme vorzulegen. Dessen Stellungnahmen werden veröffentlicht. Sie können Einwände enthalten und entsprechende Änderungen oder Präzisierungen empfehlen. Positive Stellungnahmen des EDÖB begründen die gesetzliche Vermutung, dass das im Verhaltenskodex festgehaltene Verhalten datenschutzrechtskonform ist. Allgemein gehaltene Kodizes vermögen indessen nicht vor beliebigen Risiken zu dispensieren, die der Text nicht näher bezeichnet. Durch Unterwerfung unter einen Verhaltenskodex können die Mitglieder der Verbände davon entlastet werden, eigene Hilfestellungen und Vorgaben für die Anwendung des neuen DSG zu erarbeiten. Diese Form der Selbstregulierung bringt ihnen auch den Vorteil, dass sie keine eigenen Datenschutz-Folgenabschätzungen durchführen müssen, wenn sie einen Verhaltenskodex einhalten, der auf einer bereits durchgeführten und immer noch aktuellen Datenschutz-Folgenabschätzung beruht, Massnahmen zum Schutz der Persönlichkeit oder der Grundrechte vorsieht und dem EDÖB vorgelegt wurde.

9. Zertifizierungen

Gemäss Art. 13 revDSG können nebst den Betreibern von Datenbearbeitungssystemen oder -programmen neu auch deren Hersteller ihre Systeme, Produkte und Dienstleistungen zertifizieren lassen. Mittels Zertifizierung können Unternehmen z.B. nachweisen, dass sie dem Grundsatz von Privacy by Default gerecht werden und über ein angemessenes Datenschutzmanagementsystem verfügen. Wenn ein privater Bearbeitungsverantwortlicher ein System, Produkt oder eine Dienstleistung einsetzt, die zertifiziert ist, kann er von der Erstellung einer Datenschutz-Folgenabschätzung absehen. Weitere Vorschriften über das Zertifizierungsverfahren und Qualitätszeichen wird der Bundesrat auf dem Verordnungsweg regeln.

10. Verzeichnis der Bearbeitungstätigkeiten

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

11. Bekanntgabe von Personendaten ins Ausland

Das revidierte DSG hält in Art. 16 fest, dass Daten ins Ausland bekanntgegeben werden dürfen, wenn neu der Bundesrat festgestellt hat, dass die Gesetzgebung des Drittstaates einen angemessenen Schutz gewährleistet. Er wird zu diesem Zweck eine Liste publizieren, die nach dem bisherigen Recht vom EDÖB geführt wurde. Figuriert der betreffende Exportstaat nicht auf der Liste des Bundesrates, dürfen Daten wie nach bisherigen Recht trotzdem dorthin

geleitet werden, wenn ein geeigneter Datenschutz auf andere Weise gewährleistet wird. So durch einen völkerrechtlichen Vertrag, Datenschutzklauseln, die dem EDÖB vorgängig mitzuteilen sind, oder verbindliche unternehmensinterne Datenschutzvorschriften, sog. Binding Corporate Rules. Bereits unter der DSGVO genehmigte Standardklauseln der Europäischen Kommission werden vom EDÖB anerkannt.

Ist eine Bekanntgabe ins Ausland geplant – wozu auch die Speicherung auf ausländischen Systemen (Cloud) gehört – sind die Länder anzugeben, gleichgültig, ob diese einen angemessenen Datenschutz bieten. Hier geht das DSG weiter als die DSGVO. Anzugeben ist auch, welche Datenschutzgarantien gegebenenfalls zum Einsatz kommen (z.B. EU-Standardvertragsklauseln) oder auf welche Ausnahmen nach Art. 17 revDSG sich der Verantwortliche allenfalls bezieht; auch hier weicht das DSG von der DSGVO ab.

12. Ausgebaute Informationspflichten

In Erfüllung des Revisionsziels der Transparenz baut Art. 19 revDSG die Informationspflicht für Unternehmen aus. Neu gilt, dass ein privater Verantwortlicher bei grundsätzlich jeder beabsichtigten Beschaffung von Personendaten die betroffene Person vorgängig angemessen informieren muss, selbst wenn die Daten nicht direkt bei ihr beschafft werden. Im aktuellen DSG ist diese Informationspflicht bisher nur bei besonders schützenswerten Personendaten und Persönlichkeitsprofilen vorgeschrieben. Konkret sollen die Identität und Kontaktdaten des Verantwortlichen, der Bearbeitungszweck und gegebenenfalls die Empfänger von Personendaten bekanntgegeben werden. Anders als nach der DSGVO muss auch über den Empfangsstaat und die allfälligen Garantien zur Gewährleistung eines angemessenen Datenschutzniveaus informiert werden (s. oben, Bekanntgabe von Personendaten ins Ausland). Unternehmen werden somit ihre Datenschutzerklärungen entsprechend überprüfen und nachführen müssen. Ausgenommen von der Informationspflicht sind Personendaten, die nur nebenbei oder zufällig erfasst werden. Sodann wird die Informationspflicht durch die zahlreichen Einschränkungs- und Ausnahmegründe in Art. 20 revDSG beschränkt oder aufgehoben. Das ist beispielsweise der Fall, wenn betroffene bereits über die Information verfügen oder die Bearbeitung der Daten gesetzlich vorgesehen ist. Führen Bearbeitungen zu automatisierten Einzelentscheidungen, haben die Verantwortlichen nach Art. 21 revDSG neue Informationspflichten gegenüber der beschwerten Person wahrzunehmen und dieser die ihr zustehenden Anhörungs- und Überprüfungsrechte zu gewähren.

13. Auskunftsrecht der betroffenen Personen

Das Recht einer betroffenen Person, Auskunft darüber zu verlangen, ob Personendaten über sie bearbeitet werden, wurde im neuen DSG ausgebaut. Art. 25 revDSG enthält eine erweiterte Liste an Mindestinformationen, die vom Verantwortlichen herausgegeben werden müssen, beispielsweise die Aufbewahrungsdauer der über sie bearbeiteten Personendaten. Sodann sieht der Artikel vor, dass einer betroffenen Person generell alle Informationen zur Verfügung zu stellen sind, welche erforderlich sind, damit sie die ihr nach dem neuen DSG zustehende Rechte geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist. Wie nach altem Recht kann der Verantwortliche die Auskunft unter bestimmten Bedingungen verweigern, einschränken oder aufschieben.

14. Meldepflicht bei Verletzungen der Datensicherheit

Gemäss Art. 24 revDSG muss der Verantwortliche dem EDÖB neu Verletzungen der Datensicherheit melden, die für die Betroffenen zu einem hohen Beeinträchtigungsrisiko ihrer Persönlichkeit oder ihrer Grundrechte führen. Die Bestimmung gilt sowohl für private Verantwortliche als auch für Bundesorgane. Dabei hat die Meldung an den EDÖB so rasch wie möglich zu erfolgen. Vorher wird der Verantwortliche eine Prognose zu den möglichen Auswirkungen der Verletzung stellen und eine erste Beurteilung darüber vorzunehmen, ob Gefahr im Verzug sein könnte, ob die betroffenen Personen über das Ereignis zu informieren

sind und auf welche Weise dies geschehen könnte. Wenn der Verantwortliche das Risiko nicht als hoch einschätzt, hindert ihn dies nicht daran, freiwillig eine Meldung an den EDÖB abzusetzen. Gegenüber dem EDÖB meldepflichtig sind nur eingetretene Persönlichkeits- oder Grundrechtsverletzungen, nicht jedoch erfolgreich abgewehrte oder untaugliche Cyberangriffe. Auch die europäische DSGVO kennt eine entsprechende Meldepflicht und gibt für deren Wahrnehmung gegenüber den Datenschutzbehörden der EU konkrete Fristen vor. Zudem ist die Schwelle zur Meldepflicht nach dem europäischen Recht tiefer, da dieses lediglich ein einfaches Risiko voraussetzt.

15. Recht auf Datenportabilität

Mit dem Recht auf Datenherausgabe und -übertragung gemäss Art. 28 revDSG hat eine betroffene Person neu die Möglichkeit, ihre Personendaten, welche sie einem privaten Verantwortlichen bekanntgegeben hat, in einem gängigen elektronischen Format heraus zu verlangen oder einem Dritten übertragen zu lassen. Die Voraussetzungen hierzu sind, dass der Verantwortliche die Daten automatisiert und mit der Einwilligung der betroffenen Person oder in unmittelbarem Zusammenhang mit einem Vertrag bearbeitet. Das Recht kann kostenlos geltend gemacht werden, ausser wenn die Herausgabe oder Übertragung mit einem unverhältnismässigen Aufwand verbunden ist. Letzteres kann etwa der Fall sein, wenn bei Kommunikationsdaten eine aufwändige Triage zwischen den eigenen Äusserungen und jenen von Dritten nötig wird.

16. Untersuchung aller Verstösse gegen Datenschutzvorschriften

Der EDÖB wird in Zukunft alle Verstösse gegen das neue DSG durch Bundesorgane oder private Personen von Amtes wegen zu untersuchen haben (Art. 49 Abs. 1 revDSG). Im aktuellen DSG gilt noch die Einschränkung, wonach der EDÖB gegen Private nur dann von sich aus eine Untersuchung inklusive Sachverhaltsabklärungen durchführt, wenn die Bearbeitungsmethode geeignet ist, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen. Diese, als «Systemfehler» bezeichnete Interventionsschwelle fällt inskünftig weg. Bei Verletzungen der Datenschutzvorschriften von geringfügiger Bedeutung kann jedoch auch nach neuem Recht von der Eröffnung einer Untersuchung abgesehen werden (Art. 49 Abs. 2 revDSG). Auch kann der EDÖB wie bis anhin von der Eröffnung formeller Schritte absehen, wenn sich nach einer ersten Kontaktnahme mit dem Bearbeitungsverantwortlichen zeigt, dass dieser Mängel, auf die er aufmerksam gemacht wurde, anerkennt und innert nützlicher Zeit behebt. Aufgrund seiner beschränkten Ressourcen ist generell davon auszugehen, dass der EDÖB bei der Behandlung von Anzeigen auch nach Inkrafttreten des neuen Gesetzes nach Massgabe des Opportunitätsprinzips Prioritäten setzen wird.

17. Verfügungen

Nach Art. 51 Abs. 1 revDSG kann der EDÖB neu Verfahren nach dem Verwaltungsverfahrensgesetzes[3] durchführen und gegenüber Bundesorganen oder privaten Bearbeitungsverantwortlichen formell verfügen, eine Datenbearbeitung ganz oder teilweise anzupassen, zu unterbrechen oder gar einzustellen sowie Personendaten löschen oder vernichten zu lassen. So kann der EDÖB zum Beispiel verfügen, dass ein Unternehmen betroffene Personen über eine gemeldete Verletzung der Datensicherheit informieren muss. Bisher hatte der EDÖB lediglich die Kompetenz, Empfehlungen auszusprechen und bei deren Nichtbefolgung mit Klage an das Bundesverwaltungsgericht zu gelangen.

Gegen Verfügungen des EDÖB kann ein Adressat vor Bundesveraltungsgericht Beschwerde führen und danach weiter an das Bundesgericht gelangen. Beschwerdeentscheide des Bundesverwaltungsgerichts kann auch der EDÖB vor Bundesgericht anfechten (Art. 52 Abs. 3 revDSG).

[3] Bundesgesetz über das Verwaltungsverfahren (VwVG) vom 20. Dezember 1968, SR 172.021.

18. Konsultationen

Der EDÖB ist weder eine Genehmigungsbehörde noch eine Zulassungsstelle für Applikationen, Produkte, Regulierungen und Projekte. Das neue Gesetz sieht indessen an verschiedener Stelle vor, dass die Verantwortlichen den EDÖB vor dem definitiven Abschluss entsprechender Arbeiten und der Realisierung ihrer Vorhaben konsultieren müssen. So sind ihm Verhaltenskodizes und bei hohen Restrisiken auch Datenschutz-Folgenabschätzungen zur Stellungnahme vorzulegen. Angesichts der abstrakten Natur dieser Konsultationsgegenstände werden die Stellungnahmen des EDÖB in aller Regel keinen verfügenden Charakter haben und die von ihm empfohlen Massnahmen und Auflagen keine Beschwerdemöglichkeiten zulassen. Bleiben Letztere unbeachtet, müssen die Bearbeitungsverantwortlichen indessen damit rechnen, dass konkrete Datenbearbeitungen, die mit Empfehlungen des EDÖB im Zusammenhang stehen, später Gegenstand von Verfügungen werden. Diese können so weit gehen, Datenbearbeitungen als Ganzes zu untersagen, wogegen den Verantwortlichen dann aber die ordentlichen Rechtsmittel des Verwaltungsverfahrens offenstehen.

19. Spontane Stellungnahmen und Information der Öffentlichkeit

Abgesehen von den Stellungnahmen im Rahmen formeller Konsultationen steht es dem EDÖB weiterhin frei, sich spontan zu neuen Technologien, Phänomenen der Digitalisierung oder zu Bearbeitungspraktiken gewisser Branchen zu äussern und seine Meinungsäusserungen und Einschätzungen zu publizieren. In Fällen von allgemeinem Interesse informiert der EDÖB die Öffentlichkeit zudem – wie nach bisherigem Recht – über seine Feststellungen und Massnahmen. Gemäss Art. 57 Abs. 2 revDSG gilt dies auch für Feststellungen und Verfügungen, die im Rahmen formeller Untersuchungen des EDÖB ergangen sind.

20. Gebühren

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

21. Sanktionen

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

Im Gegensatz zu den europäischen Datenschutzbehörden kommen dem EDÖB auch nach neuem Recht keine Sanktionsbefugnisse zu. Die fehlbaren Personen werden durch die kantonalen Strafverfolgungsbehörden gebüsst. Der EDÖB kann zwar Anzeige erstatten und im Verfahren die Rechte einer Privatklägerschaft wahrnehmen (Art. 65 Abs. 2 revDSG), ein Strafantragsrecht steht ihm aber nicht zu. Anders als beim neuen DSG richten sich die Verwaltungssanktionen nach der DSGVO ausschliesslich gegen juristische Personen. Die Datenschutzbehörden in der EU können gegen fehlbare Unternehmen Bussen bis zu 20 Millionen Euro resp. 4 Prozent des weltweit erzielten Jahresumsatzes aussprechen.

EDÖB, 9. Februar 2021