Das Datenschutzgesetz und die Folgen für EVUs

Neues Datenschutzgesetz | Am 25. September 2020 haben im Parlament beide Räte dem Entwurf zur Totalrevision des Datenschutzgesetzes (DSG) zugestimmt.[1] Am 14. Januar 2021 ist die Referendumsfrist ungenutzt abgelaufen. Das neue DSG wird somit voraussichtlich 2022 in Kraft treten. In einem nächsten Schritt werden nun die Verordnungen ausgearbeitet und in die Vernehmlassung geschickt.

MICHÈLE BALTHASAR

Das DSG gilt für die Bearbeitung von Personendaten[1)] durch Bundesorgane und Private. Die Datenbearbeitung durch Kantone beziehungsweise kantonale Behörden wird hingegen in den kantonalen Datenschutzgesetzen geregelt. Soweit deshalb Elektrizitätsversorgungsunternehmen hoheitlich tätig sind und öffentliche Aufgaben wahrnehmen – wie etwa bei der Stromversorgung im nicht geöffneten Markt –, unterstehen sie nach wie vor den kantonalen Datenschutzgesetzgebungen. Daneben enthalten auch spezialgesetzliche Vorschriften Regelungen zum Datenschutz, etwa das Bundesgesetz über die Stromversorgung[2)] und die Stromversorgungsverordnung[3)].

Sinn und Zweck der Revision

Mit dem neuen DSG sollen hauptsächlich zwei Ziele verwirklicht werden:

- Einerseits sollen die Schwächen des bestehenden Datenschutzgesetzes behoben werden, die aufgrund der rasanten technologischen Entwicklung entstanden sind.
- Anderseits soll das Datenschutzgesetz den Entwicklungen in der Europäischen Union Rechnung tragen und der Europäischen Datenschutz-Grundverordnung (DSGVO) angeglichen werden. Diese gilt seit dem 25. Mai 2018.[2]

Noch immer ausstehend und mit Spannung zu erwarten ist die Erneuerung des Angemessenheitsbeschlusses der Europäischen Kommission, welcher ungehinderte Datentransfers aus der EU in die Schweiz ermöglicht. Die EU könnte die Schweiz bezüglich des

Bild: Chris Yang/unsplash

Inkrafttretens des neuen Schweizer Datenschutzgesetzes denn auch unter Druck setzen.

Eckpunkte des neuen DSG

Kein Schutz juristischer Personen Geschützt sind nach dem neuen DSG zukünftig nur noch die Daten natürlicher Personen, nicht mehr auch die Daten juristischer Personen wie jene einer AG, GmbH oder von Vereinen. Diesen verbleiben der Schutz durch das Firmenrecht sowie der Persönlichkeitsschutz nach ZGB.

Verantwortlicher und Auftragsbearbeiter Statt wie bisher vom Inhaber einer Datensammlung ist neu von Verantwortlichen und Auftragsbearbeiter die Rede. Verantwortliche sind private Personen oder Bundesorgane, die allein oder zusammen mit anderen über den Zweck und die Mittel der Bearbeitung entscheiden. Auftragsbearbeiter sind private Personen oder Bundesorgane, die im Auftrag des Verantwortlichen Personendaten bearbeiten, wie etwa IT Service Provider bei der Datenbearbeitung in einer Cloud. Der Auftragsbearbeiter hat die Daten so zu bearbeiten, wie der Verantwortliche es tun dürfte. Der Verantwortliche muss sich dabei vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit zu gewährleisten. Neu darf der Auftragsbearbeiter die Bearbeitung erst mit vorgängiger Genehmigung des Verantwortlichen einem Dritten übertragen (Vetorecht).[4] Allfällige Datensicherheitsverletzungen hat der Auftragsbearbeiter dem Verantwortlichen so rasch als möglich zu melden.[5]

Erweiterung des Katalogs besonders schützenswerter Daten Ferner wurde der Katalog der besonders schützenswerten Personendaten um biometrische und genetische Daten erweitert.[6] Zur Bearbeitung von besonders schützenswerten Daten gelten strengere Anforderungen als zur Bearbeitung von normalen Personendaten. Gegebenenfalls bedarf es hier für die Bearbeitung einer ausdrücklichen Einwilligung.

Profiling und Profiling mit hohem Risiko Neu wird der Begriff des Profilings eingeführt.[7] Er ersetzt den Begriff des Persönlichkeitsprofils. Dabei wird unterschieden zwischen normalem Profiling und Profiling mit hohem Risiko. Profiling ist jede Art der automatisierten Bearbeitung von Personendaten, die darin besteht, dass diese Daten verwendet werden, um bestimmte persönliche Aspekte zu bewerten[8]. Profiling mit hohem Risiko bringt ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich, indem es zu einer Verknüpfung von Daten führt, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt. Auch hier gelten zu deren Bearbeitung strengere Voraussetzungen.

Keine Änderung an den Grundprinzipien Unverändert bleiben im neuen DSG die Grundprinzipien der Datenbearbeitung. Auch das Schweizer Konzept, wonach Datenbearbeitungen unter Berücksichtigung der Datenschutzgrundsätze (Rechtmässigkeit, Verhältnismässigkeit, Treu und Glauben etc.) grundsätzlich zulässig sind und nur in gewissen Situationen ein besonderer Rechtfertigungsgrund erforderlich ist, bleibt erhalten.[9]

Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen Der Verantwortliche ist verpflichtet, bei der Planung der Datenbearbeitung diese technisch und organisatorisch so auszugestalten, dass die Datenschutzvorschriften eingehal-

Bild: Markus Hein/pixelio

Die Regeln, was EVUs mit den Daten über ihre Kunden tun dürfen, wurden verschärft.

ten werden (Data Protection by Design). Ferner ist der Verantwortliche verpflichtet, mittels geeigneter Voreinstellungen sicherzustellen, dass die Bearbeitung der Personendaten auf das für den Verwendungszweck notwendige Mindestmass beschränkt ist, soweit die betroffene Person nicht etwas anderes bestimmt (Data Protection by Default).[10] Diese Verpflichtungen sind nicht neu im eigentlichen Sinne, da sie bereits heute gelten; sie wurden nun allerdings gesetzlich verankert.

Pflicht zum Führen eines Bearbeitungsverzeichnisses Neu müssen sowohl der Verantwortliche als auch der Auftragsbearbeiter ein Verzeichnis der Bearbeitungstätigkeiten führen. Wie der zukünftigen Datenschutzverordnung zu entnehmen sein wird, sind gewisse Unternehmen, die weniger als 250 Mitarbeitende beschäftigen und deren Datenbearbeitung nur ein geringes Risiko mit sich bringt, von dieser Pflicht befreit. Da die Erfüllung fast aller Datenschutzpflichten einer gewissen Übersicht über die Datenbearbeitung im Unternehmen bedarf, dürfte es sich, praktisch gesehen, für jede Organisation, unabhängig von einer entsprechenden Pflicht, lohnen, ein entsprechendes Verzeichnis zu führen.[11]

Erweiterte Informationspflicht Von gewissen Ausnahmen abgesehen werden Verantwortliche verpflichtet sein, betroffene Personen bei der Datenbeschaffung über verschiedene Aspekte der Datenbearbeitung zu informieren, wie Identität und Kontaktdaten des Verantwortlichen, Bearbeitungszweck, allfällige Empfängerinnen und Empfänger oder Kategorien von Empfängerinnen und Empfängern, denen Personendaten bekannt gegeben werden, sowie bei Bekanntgabe ins Ausland zusätzlich auch der Staat oder das internationale Organ und gegebenenfalls die Garantien zum Schutz der Personendaten. Derzeit beschränken sich solche Informationspflichten weitgehend auf die Beschaffung besonders schützenswerter Personendaten und Persönlichkeitsprofile.[12]

Ausweitung der Rechte betroffener Personen Die bisherigen Rechte der betroffenen Personen, Auskunft, Löschung oder die Sperrung (Einschränkung) ihrer Personendaten zu verlangen, bleiben erhalten und werden teilweise angepasst. Betroffene Personen haben neu Anspruch auf alle Informationen, die erforderlich sind, um ihre Rechte nach dem neuen DSG geltend zu machen und eine transparente Datenbearbeitung zu gewährleisten.[13]

Recht auf Datenportabilität Demnach kann jede Person von einem Verantwortlichen verlangen, sie betreffende und ihm vorgängig bekannt gegebene und auf Basis einer Einwilligung oder eines Vertrags automatisiert bearbeitete Personendaten in einem gängigen elektronischen Format herauszugeben oder diese Daten einem anderen Verantwortlichen zu übergeben. Die Auskunft ist grundsätzlich kostenlos und hat in der Regel innerhalb von 30 Tagen zu erfolgen.[14]

Automatisierte Einzelfallentscheidung Neu muss der Verantwortliche die betroffene Person über eine Entscheidung informieren, die ausschliesslich auf einer automatisierten Bearbeitung beruht und die für sie mit einer Rechtsfolge verbunden ist oder sie erheblich beeinträchtigt. Die betroffene Person muss dabei die Möglichkeit erhalten, ihren Standpunkt darzulegen und kann verlangen, dass die Entscheidung von einer natürlichen Person geprüft wird.[15]

Erstellen einer Datenschutz-Folgenabschätzung Ferner hat ein Verantwortlicher vorgängig eine Datenschutz-Folgenabschätzung zu erstellen, wenn eine Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann. Bei etwas heikleren Vorhaben wie der Einführung besonderer Applikationen besteht also eine Pflicht, eine formalisierte Risikoanalyse durchzuführen und zu dokumentieren.[16] Von der Erstellung einer Datenschutz-Folgenabschätzung ausgenommen sind private[17] Verantwortliche, wenn sie gesetzlich zur Bearbeitung der Daten verpflichtet sind.

RÉSUMÉ

La Loi sur la protection des données et ses implications pour les EAE

Nouvelle Loi sur la protection des données

Le 25 septembre 2020, les deux chambres du Parlement ont approuvé le projet de révision totale de la Loi sur la protection des données (LPD). La nouvelle Loi suisse sur la protection des données entrera ainsi en vigueur probablement en 2022. Dans une prochaine étape, les ordonnances vont maintenant être rédigées et mises en consultation.

La LPD s'applique au traitement de données personnelles par des organes fédéraux et des personnes privées. Le traitement des données par les cantons ou les autorités cantonales, en revanche, est réglé dans les législations cantonales. Dans la mesure où les entreprises d'approvisionnement en électricité exercent une activité étatique et assument des tâches publiques – comme par exemple pour l'approvisionnement en électricité dans le marché non libéralisé –, elles continuent d'être soumises aux législations cantonales sur la protection des données. Par ailleurs, des prescriptions relevant de législations spéciales contiennent aussi des réglementations sur la protection des données, par exemple la Loi fédérale sur l'approvisionnement en électricité et l'Ordonnance sur l'approvisionnement en électricité.

La nouvelle Loi sur la protection des données doit concrétiser principalement deux objectifs: d'une part, écarter les faiblesses de la Loi sur la protection des données existante qui sont nées de la vitesse de l'évolution technologique; d'autre part, tenir compte des évolutions au sein de l'Union européenne et être harmonisée avec le Règlement européen sur la protection des données (RGPD), en vigueur depuis le 25 mai 2018.

On attend encore, et avec impatience, le renouvellement de la « décision d'adéquation » de la Commission européenne, qui permet de transférer des données sans entraves de l'UE vers la Suisse. L'UE pourrait faire pression sur la Suisse concernant l'entrée en vigueur de la nouvelle Loi suisse sur la protection des données. MR

Wann ein hohes Risiko vorliegt, ergibt sich aus verschiedenen Umständen, so insbesondere bei der Verwendung neuer Technologien, aus der Art, dem Umfang, den Umständen und dem Zweck der Bearbeitung. Beispiele eines hohen Risikos können zum Beispiel die umfangreiche Bearbeitung besonders schützenswerter Personendaten oder die systematische umfangreiche Überwachung öffentlicher Bereiche sein.

Meldung von Verletzungen der Datensicherheit Zukünftig muss der Verantwortliche dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (und gegebenenfalls den betroffenen Personen) Verletzungen der Datensicherheit, welche voraussichtlich ein hohes Risiko für die betroffenen Personen darstellen, so rasch als möglich melden.[18] Darunter fallen etwa die Entwendung, Diebstahl durch interne oder externe Personen (zum Beispiel Hacker) oder die Zerstörung von Informationen, beispielsweise aufgrund eines Benutzerfehlers, technischen Fehlers, Viren oder Angriffe durch Hacker.

Verschärfung Strafbestimmungen Mit dem neuen DSG werden auch die Bussen wesentlich erhöht. Wer gewisse Pflichten des neuen DSG vorsätzlich (inklusive eventualvorsätzliche Inkaufnahme des sanktionierten Verhaltens) verletzt, muss mit einem Bussgeld von bis zu CHF 250 000 rechnen.[19] Im Gegensatz zur DSGVO zielen die Bussen nicht auf die Unternehmen, sondern auf den jeweils verantwortlichen Mitarbeitenden. Dies führt dazu, dass nach dem revidierten DSG Verantwortliche im Unternehmen wie CEOs, CFOs oder CIOs direkt sanktioniert werden können. Immerhin handelt es sich bei den meisten Strafbestimmungen um Antragsdelikte, ein Verstoss wird also nur verfolgt, wenn etwa die betroffene Person einen Strafantrag stellt.

Referenzen

[1] Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und Änderung weiterer Erlasse im Datenschutz, 15. September 2017.

[2] Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) in der aktuellen Version des ABl. L 119, 4. Mai 2016, ber. ABl. L 127, 23. Mai 2018, abrufbar unter www.eur-lex.europa.eu (Suchbegriff: L 119/1).

Autorin
Dr. **Michèle Balthasar** ist Head Data Privacy & Legal Consulting by Swiss Infosec.
→ Swiss Infosec, 8006 Zürich
→ michele.balthasar@infosec.ch

[1] Personendaten (Daten) sind alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen. Briefadressen sind typische Personendaten, ebenso Interessensprofile. Auch E-Mail-Adressen sind meist Personendaten, ob in Bezug auf den Domain-Namen-Inhaber, auf den angegebenen Namen oder weil sich eine Adresse über Aktivitäten im Internet leicht einer Person zuordnen lässt. Anonymisierte Daten (zum Beispiel die Daten in einer anonymen Statistik) sind dagegen keine Personendaten und unterliegen deshalb nicht dem Datenschutzgesetz.
[2] Stromversorgungsgesetz, StromVG; SR 734.7.
[3] StromVV; SR 734.71.
[4] Art. 9 nDSG.
[5] Art. 24 Abs. 3 nDSG.
[6] Art. 5 lit. c nDSG.
[7] Art. 5 lit. g nDSG.
[8] Insbesondere, um Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen.
[9] Art. 6 nDSG.
[10] Art. 7 nDSG.
[11] Art. 12 nDSG.
[12] Art. 19 f. nDSG.
[13] Art. 25 f. nDSG.
[14] Art. 28 nDSG.
[15] Art. 21 nDSG.
[16] Art. 22 nDSG.
[17] Im Gegensatz zu Bundesorganen.
[18] Art. 24 nDSG.
[19] Art. 49 nDSG.