Bild Archiv

Revidierte Verordnung zum Datenschutzgesetz

Bereits viele Jahre wurde uns das neue Datenschutzgesetz versprochen. Immer wieder wurde es nach hinten verschoben. Nach vierjährigem Gesetzgebungsprozess wurde es Ende September 2020 vom Parlament verabschiedet. In Kraft ist es jedoch noch nicht, es fehlt die Verordnung dazu. Darin werden die Details geregelt.

Am 23. Juni 2021 war es dann so weit, der Bundesrat hat den Vorentwurf zur totalrevidierten Verordnung zum schweizerischen Datenschutzgesetz (E-VDSG), den dazugehörigen erläuternden Bericht und eine Vergleichstabelle veröffentlicht.

ZUM AUTOR

Andreas Wisler, Dipl. Ing FH
goSecurity AG
Schulstrasse 11
CH-8542 Wiesendangen

T +41 (0)52 511 37 37
www.goSecurity.ch
wisler@gosecurity.ch

Aufbau

Das E-VDSG ist in folgende Bereiche unterteilt:

- Datensicherheit (Art. 1 bis 5 E-VDSG)
- Bearbeitung durch Auftragsbearbeiter (Art. 6 und 7 E-VDSG)
- Bekanntgabe von Personendaten ins Ausland (Art. 8 bis 12 E-VDSG)
- Pflichten des Verantwortlichen und des Auftragsbearbeiters (Art. 13 bis 19 E-VDSG)
- Rechte der betroffenen Person (Art. 20 bis 24 E-VDSG)
- Besondere Bestimmungen zur Datenbearbeitung durch private Personen (Art. 25 und 26 E-VDSG)
- Besondere Bestimmungen zur Datenbearbeitung durch Bundesorgane (Art. 27 bis 36 E-VDSG)
- Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (Art. 37 bis 45 E-VDSG)
- Schlussbestimmungen (Art. 46 bis 48 E-VDSG)

Das Risiko bestimmt die Massnahmen

Das E-VDSG verfolgt den bisherigen Risiko-basierten Ansatz weiter. Dies wird schon im ersten Teil sichtbar: die für die IT-Sicherheit zuständige Person muss sich um die minimalen Vorgaben an die IT-Sicherheit kümmern.

Im erläuternden Bericht steht dazu: «Da bereits im Gesetz der Ansatz einer risikobasierten Datensicherheit verfolgt wird und sich keine allgemeingültigen Mindestanforderungen für jegliche Branchen festlegen lassen, wurde im E-VDSG auf ein starres Regime von Mindestanforderungen verzichtet. Der Ansatz des E-VDSG beruht vielmehr darauf, dass es in erster Linie in der Verantwortung des Verantwortlichen liegt, die im Einzelfall notwendigen Massnahmen zu bestimmen und zu ergreifen. Diese sind stark einzelfallbezogen und abhängig vom jeweiligen Risiko zu bestimmen. So stellen sich etwa in einem Spital, wo regelmässig besonders schützenswerte Personendaten bearbeitet werden, in aller Regel erhöhte Anforderungen im Vergleich zur Bearbeitung von Kunden- oder Lieferantendaten in einer Bäckerei, Metzgerei oder …).»

In Art. 2 werden die folgenden Schutzziele angesprochen (momentan in Art. 9):

- Zugriffskontrolle
- Zugangskontrolle
- Datenträgerträgerkontrolle (vorher Personendatenträgerkontrolle)
- Speicherkontrolle
- Benutzerkontrolle
- Bekanntgabekontrolle
- Wiederherstellung*
- Verfügbarkeit*
- Zuverlässigkeit*
- Datenintegrität*
- Erkennung*

Weggefallen sind die Transport- und die Eingabekontrolle. Die mit * markierten sind neu erwähnt. In Art. 2j steht dazu: «Es wird gewährleistet, dass alle Funktionen des Systems zur Verfügung stehen (Verfügbarkeit), auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit) und gespeicherte Personendaten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität).» Jedes Unternehmen sollte diesen Punkt erfüllen. Die verschiedenen Ausfälle und negativen Nachrichten zeigen aber ein anderes Bild. Dazu kommt Art. 2k: «Erkennung: Verletzungen der Datensicherheit können rasch erkannt und Massnahmen zur Minderung oder Beseitigung der Folgen eingeleitet werden.» Ein Monitoring ist also Pflicht. Jedoch nicht eines, das einfach vor sich hin loggt, sondern Alarm schlägt, sollte etwas nicht mehr rund laufen. Sollte ein unerwünschtes Ereignis eintreten, müssten bereits Massnahmen zur Bewältigung vorbereitet sein. Stichwort Busi-

ness Continuity Plan (BCP). Verschärft wurde auch die Protokollierung (Neu Art. 3, Alt Art. 10). Wenn aus der Datenschutz-Folgenabschätzung (DSFA) herauskommt, dass trotz Massnahmen ein erhöhtes Risiko für die Persönlichkeit oder deren Grundrechte besteht, sind das Speichern, Verändern, Lesen, Bekanntgeben, Löschen oder Vernichten zu protokollieren. Dazu gibt der Punkt 3 klare Anweisungen, wie die Protokollierung zu erfolgen hat: «Die Protokollierung gibt Aufschluss über die Art des Bearbeitungsvorgangs, die Identität der Person, die die Bearbeitung vorgenommen hat, die Identität der Empfängerin oder des Empfängers sowie den Zeitpunkt, an dem die Bearbeitung erfolgt ist.» Während die Logdaten während eines Jahres aufbewahrt werden mussten, sind es nun deren zwei. Und zwar getrennt vom System, auf welchem die Daten erhoben wurden. Dies macht auch Sinn, sollte ein System ausfallen, sind die Logdaten dennoch verfügbar. Wichtig ist auch, dass diese Daten nur für Personen zugänglich sind, denen die Überwachung der Datenschutzvorschriften oder die Wiederherstellung der Daten obliegen. Eine Trennung von Funktionen ist daher im Organigramm/Stellenbeschreibung unbedingt vorzusehen.

Bearbeitung Personendaten

Neu dazugekommen ist die Pflicht ein Bearbeitungsreglement zu erstellen, wenn umfangreich besonders schützenswerte Personendaten bearbeitet werden oder ein Profiling mit hohem Risiko durchgeführt wird. In Art. 4, Punkt 2 sind die Mindestangaben an dieses Reglement aufgelistet. Dieses gilt es regelmässig zu aktualisieren und der datenschutzverantwortlichen Person zur Verfügung stehen.

Das Führen von Verzeichnissen der Bearbeitungstätigkeiten ist Pflicht. Hier gibt es in Artikel 26 aber eine Ausnahme. Unternehmen mit weniger als 250 Mitarbeitende sowie natürliche Personen sind davon befreit, wenn sie nicht umfangreich besonders schützenswerte Personendaten bearbeiten oder kein Profiling mit hohem Risiko durchführen.

Wird die Bearbeitung von Personendaten einem Auftragsbearbeiter übertragen, bleibt der Verantwortliche weiterhin zuständig. Er muss sicherstellen, dass die Daten vertrags- oder gesetzesgemäss bearbeitet werden. Untersteht der Auftragsbearbeiter dem nDSG nicht, so muss sich der Verantwortliche vergewissern, dass andere gesetzliche Bestimmungen einen gleichwertigen Datenschutz gewährleisten. Andernfalls muss er diesen auf vertraglichem Wege sicherstellen.

Im Artikel 25 werden die Aufgaben der Datenschutzberaterin und des -beraters konkretisiert. Dazu gehören:

- Prüfung der Bearbeitung von Personendaten, inkl. deren Voraussetzung
- Empfehlung von Korrekturmassnahmen, wenn eine Vorschrift verletzt wird/wurde
- Wirkt bei der Erstellung von Datenschutz-Folgenabschätzungen mit

Dazu ist es notwendig, dieser Person die notwendigen Ressourcen zur Verfügung zu stellen sowie Zugang zu allen Auskünften, Un-

terlagen, Verzeichnissen der Bearbeitungstätigkeiten und Personendaten gewähren.

Der Artikel 8 geht dann auf die Bekanntgabe von Personendaten ins Ausland oder eines internationalen Organs ein. Dazu werden fünf Punkte aufgelistet, unter anderem internationale Verpflichtungen, die Achtung der Menschenrechte, geltende Gesetzgebung zum Datenschutz, Rechtsschutz der Betroffenen und dem Funktionieren von unabhängigen Behörden. Bei Unsicherheit kann dabei auf die Staatenliste (https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2017/04/staatenliste.pdf.download.pdf/staatenliste.pdf) des EDÖB zurückgegriffen werden.

Neu sind die Standarddatenschutzklauseln (Art. 10), die der EDÖB vorgibt: Der EDÖB veröffentlicht eine Liste von Standarddatenschutzklauseln, die er genehmigt, ausgestellt oder anerkannt hat. Zusätzlich definiert Artikel 11, dass verbindliche unternehmensinterne Datenschutzvorschriften für alle Unternehmen, die zum selben Konzern gehören, gelten.

Das Kapitel 2 definiert die Pflichten des Verantwortlichen und des Auftragsbearbeiters. Diese teilen die Information über die Beschaffung von Personendaten in präziser, verständlicher und leicht zugänglicher Form mit. Wird dies mit Piktogrammen umgesetzt, die elektronisch dargestellt werden, so müssen diese maschinenlesbar sein. Ein sehr guter Ansatz stellt der Verein Privacy Icons unter https://privacyicons.ch/ in vier Sprachen zur Verfügung. Diese dürfen für die eigene Homepage kostenlos verwendet werden.

Literatur

- Erläuternder Bericht: https://www.bj.admin.ch/dam/bj/de/data/staat/gesetzgebung/datenschutzstaerkung/vdsg/vn-ber.pdf
- Vorentwurf: https://www.bj.admin.ch/dam/bj/de/data/staat/gesetzgebung/datenschutzstaerkung/vdsg/vorentw.pdf
- Vergleichstabelle E-VDSG – VDSG – nDSG: https://www.bj.admin.ch/dam/bj/de/data/staat/gesetzgebung/datenschutzstaerkung/vdsg/vergleichstabelle.pdf

Die BDO bietet unter www.bdo.ch/de-ch/dsg-compliance-test/datenschutz-test einen kurzen Compliance Test zum neuen Datenschutzgesetz an.

Recht der betroffenen Person

Der Artikel 9 befindet sich eine umfassende Auflistung der Datenschutzklauseln. Zusätzlich sind in Punkt k Rechte der betroffenen Person aufgezählt:

1. das Auskunftsrecht,
2. das Widerspruchsrecht,
3. das Recht auf Berichtigung, Löschung oder Vernichtung ihrer Daten,
4. das Recht, eine unabhängige Behörde, um Rechtsschutz zu ersuchen.

Datenschutz-Verletzung

Kommt es zu einer Verletzung der Datensicherheit, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt, so muss dies, analog zur DSGVO, so rasch als möglich dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) gemeldet werden. Folgendes ist dabei zu melden:

- die Art der Verletzung;
- soweit möglich den Zeitpunkt und die Dauer der Verletzung;
- soweit möglich die Kategorien und ungefähre Anzahl der betroffenen Personendaten;
- soweit möglich die Kategorien und ungefähre Anzahl der betroffenen Personen;
- die Folgen, einschliesslich der allfälligen Risiken, für die betroffenen Personen;
- welche Massnahmen getroffen wurden oder vorgesehen sind, um den Mangel zu beheben oder die Folgen zu mildern;
- den Namen und die Kontaktdaten einer Ansprechperson.

Der EDÖB

Das Kapitel 6 definiert die Rolle des EDÖB. Unter anderem dass sein Sitz in Bern ist, wie er/sie kommuniziert, wie Personendaten durch ihn/sie bearbeitet werden dürfen sowie die Selbstkontrolle und Verhaltenskodizes. Natürlich dürfen auch die Gebühren nicht fehlen. Der EDÖB wird nach Zeitaufwand bezahlt, mit einem Ansatz von CHF 150 bis 350, je nach Funktion und Komplexität. Ebenfalls wird in diesem Kapitel die Zusammenarbeit mit dem NCSC (Nationalen Zentrum für Cybersicherheit) erwähnt. Dies ist beispielsweise dann der Fall, wenn eine Verletzung der Datensicherheit an das NCSC zur Analyse übergeben wird.

Fazit

Alles in allem sind die geforderten Punkte für jedes Unternehmen umsetzbar. Bis zur endgültigen Verabschiedung wird es aber noch einige Diskussionen und Anpassungen geben. Der umfassende Rahmen ist aber mit der neuen Verordnung gegeben und zeigt die Anforderungen an den Datenschutz. Jedes Unternehmen sollte sich schon jetzt mit den neuen Anforderungen auseinandersetzen und sich darauf vorbereiten. Die öffentliche Vernehmlassung dauert noch bis am 14. Oktober 2021. Die VDSG soll gleichzeitig mit dem neuen DSG in der zweiten Jahreshälfte 2022 in Kraft treten. Der Bundesrat wird zu gegebener Zeit das genaue Datum festlegen. Im erläuternden Bericht wird erwähnt, dass gleichzeitig mit Inkrafttreten des neuen DSG auch die modernisierte Datenschutzkonvention 108 des Europarates ratifiziert wird.