Das totalrevidierte Datenschutzgesetz der Schweiz

Datenschutz: Eine Übersicht zum neuen Gesetz

Gemäss dem Bundesamt für Justizsoll das neue Datenschutzgesetzt am 1. September 2023 in Kraft treten. Der dafür notwendige Entscheid des Bundesrats muss allerdings noch erfolgen.

Dirk Spiegel / Rolf Aeberhard, AvelaLaw AG, Fraumünsterstrasse 15, 8001 Zürich, www.avelalaw.com 15. März 2022

Die Änderungen auf einen Blick

- Das revidierte Datenschutzgesetz (revDSG) bringt **neue Informations- und Dokumentationspflichten**. Sobald Personendaten erhoben werden, müssen die davon betroffenen Personen über folgende Punkte informiert werden:
  a) Identität und Kontaktdaten des Datenverarbeiters;
  b) Zweck der Verarbeitung;
  c) alle Empfänger denen Personendaten mitgeteilt werden bekannt gegeben werden.
- **Juristische Personen** werden durch das Datenschutzgesetz **nicht mehr geschützt**.
- Die **Liste der streng vertraulichen Personendaten wird im revDSG erweitert** und umfasst neu auch (i) genetische Daten und (ii) biometrische Daten.
- Die **automatisierte Verarbeitung von Personendaten**, um bestimmte Aspekte einer natürlichen Person zu beurteilen (sog. **Profiling**) wird im revDSG **aus der europäischen Gesetzgebung (DSGVO) übernommen**.
- **Für die Datenverarbeitung wird in der Regel eine Vereinbarung erforderlich sein**.
- Die Datenverarbeitung muss so gestaltet sein, dass **Datenschutzvorschriften und Verarbeitungsgrundsätze zu allen Zeiten beachtet und eingehalten werden können (Datenschutz durch Technikeinstellungen)**. Die Standardeinstellungen müssen so gestaltet sein, dass die **Verarbeitung von Personendaten auf das für den Verwendungszweck benötigte Minimum beschränkt wird**.
- Das revDSG führt eine **Meldepflicht bei Datenverlusten und sonstigen Sicherheitspannen ein**. Diesbezüglich muss ein entsprechender Prozess eingeführt werden.
- Das **revDSG ist nicht strenger als die europäische Gesetzgebung (DSGVO)**, aber auch nicht identisch. Hier gilt es, die Unterschiede zu erkennen und Differenzen zu prüfen.

Ausgangslage

Es ist vorgesehen, dass das neue Datenschutzrecht auf den 1. September 2023 in Kraft gesetzt wird. Der dafür notwendige Bundesratsentscheid steht noch aus.

Die neue Gesetzgebung soll insbesondere den Entwicklungen auf Ebene des Europarates und der Europäischen Union Rechnung tragen. Dies bedeutet, dass das revidierte Datenschutzgesetz massgeblich von der Datenschutz-Grundverordnung der Europäischen Union (DSGVO) beeinflusst wurde.

Das revDSG bezweckt den Schutz der Persönlichkeit und der Grundrechte von natürlichen Personen, die sich in der Schweiz befinden und deren Daten durch Private oder vom Staat bearbeitet werden. Das unter bisherigem Recht bestehende Regelungskonzept wird durch die Revision nicht verändert. Weiterhin gilt, dass für die Bearbeitung von Personendaten weder eine Einwilligung noch die Angabe eines Rechtfertigungsgrund erforderlich ist. Ein Rechtfertigungsgrund ist nur dann notwendig, wenn entweder die Bearbeitungsgrundsätze des revDSG nicht eingehalten werden, die betroffene Person der Bearbeitung widersprochen hat oder einem Dritten besonders schützenswerte Personendaten mitgeteilt werden sollen. Dies ist der wichtigste Unterschied zur DSGVO, wo Personendaten erst dann bearbeitet werden dürfen, wenn eine angemessene «Rechtsgrundlage» besteht.

Das revDSG bezweckt die Verbesserung der Transparenz der Bearbeitung von Daten und stärkt die Kontrollmöglichkeiten der betroffenen Personen über ihre Daten. Ausserdem soll das Verantwortungsbewusstsein der für die Bearbeitung verantwortlichen Personen erhöht werden, die Bekanntgabe von Daten ins Ausland erleichtert und die Entwicklung neuer Wirtschaftszweige im Bereich der Digitalisierung der Gesellschaft gefördert werden. Die neuen Informations- und Meldepflichten des revDSG verpflichten Organisationen inskünftig, betroffenen Individuen über die Bearbeitung ihrer Personendaten zu informieren.

Das revDSG kennt keine wesentlichen Übergangsfristen. Aufgrund dessen empfiehlt es sich, sich bereits heute mit den neuen Anforderungen auseinanderzusetzen.

Geltungsbereich

Das revDSG ist auf Sachverhalte anwendbar, die sich auf die Schweiz auswirken. Demnach ist die neue Gesetzgebung auch auf Unternehmen mit Sitz im Ausland anwendbar, die Daten in der Schweiz bearbeiten.

Neue und erweiterte Begriffe

(a) Verantwortlicher und Auftragsbearbeiter

Das revDSG führt die Begriffe «Verantwortlicher» und «Auftragsbearbeiter» ein. Es handelt sich dabei um die wichtigsten Rollen, auf welchen das revDSG beruht.

Unter dem Verantwortlichen versteht das revDSG, wer allein oder zusammen mit anderen «über den Zweck und die Mittel der Bearbeitung entscheidet». Im bisherigen Datenschutzgesetz wurde vom «Inhaber der Datensammlung» gesprochen. Es handelt sich damit um diejenige Person, welche die datenschutzrechtlichen Parameter einer Datenbearbeitung festlegt.

Als Auftragsbearbeiter gilt, wer eine Datenbearbeitung lediglich nach Weisung ausführt, auch wenn er gewisse Entscheidungen diesbezüglich selbst treffen kann.

(b) Personendaten

Der Begriff «Personendaten» wird von der DSGVO übernommen. Dabei handelt es sich gemäss Art. 5 revDSG um «alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen».

(c) Kein Schutz mehr von Personendaten juristischer Personen

Das revDSG verzichtet auf den Schutz der Daten von juristischen Personen, da dieser von nur geringer praktischer Bedeutung ist. Damit wird ein zentraler Unterschied zum europäischen Recht beseitigt. Das revDSG ist somit nur noch auf die Bearbeitung von Personendaten natürlicher Personen anwendbar. Damit hat eine juristische Person kein Auskunftsrecht mehr. Juristische Personen sind aber nach wie vor durch Art. 28 ZGB geschützt.

Ausserdem soll damit die Bekanntgabe von Daten an Empfänger in ausländischen Staaten, deren Gesetzgebung keinen Schutz von Daten juristischer Personen vorsieht, erleichtert werden.

(d) Profiling

Das bisherige Recht kannte den Begriff des «Persönlichkeitsprofils», für welchen dieselben Regelungen galten, wie für besonders schützenswerte Personendaten. Neu wird der Begriff des «Profiling» eingeführt und die Legaldefinition der DSGVO übernommen. Beim Profiling handelt es sich um «jede Art der automatisierten Bearbeitung von Personendaten, die darin besteht, dass diese Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen».[1]

Wichtig ist, dass die Interpretation automatisiert zu erfolgen hat, d.h. nicht manuell vorgenommen wird.

(e) Profiling mit hohem Risiko

Art. 5 lit. g revDSG führt den Begriff des «Profiling mit hohem Risiko», ein, welcher definiert ist als «Profiling, das ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringt, indem es zu einer Verknüpfung von Daten führt, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt». Es handelt sich dabei eigentlich um den aus dem bisherigen DSG stammenden Begriff des «Persönlichkeitsprofils».

(f) Ergänzung der Definition besonders schützenswerte Personendaten

Die Aufzählung der besonders schützenswerten Personendaten wird im revDSG mit der expliziten Nennung der «genetischen Daten» und der «biometrischen Daten» ergänzt. Dabei werden unter genetischen Daten sämtliche Informationen über das Erbgut einer Person verstanden, die durch eine genetische Untersuchung gewonnen werden können. Bei biometrischen Daten handelt es sich um Daten, welche durch ein spezifisches technisches Verfahren zu den physischen, physiologischen oder verhaltenstypischen Merkmalen eines Individuums gewonnen werden und die eine eindeutige Identifizierung der betreffenden Person ermöglichen oder bestätigen (bspw. ein Fingerabdruck, Gesichtsbild mit Iris Scan etc.). Die Aufnahme dieser zusätzlichen besonders

[1] vgl. Art. 5 lit. f revDSG.

schützenswerten Daten im revDSG erfolgte zwecks Angleichung an die DSGVO.

Einwilligung

Das revDSG hat keinen neuen Standard für Einwilligungen eingeführt. Entsprechend wird sich materiell nichts ändern. Das revDSG geht damit weniger weit als die DSGVO.

Nach Art. 6 Abs. 7 revDSG muss die Einwilligung ausdrücklich erfolgen für:

a) die Bearbeitung von besonders schützenswerten Personendaten;
b) ein Profiling mit hohem Risiko durch eine private Person; oder
c) ein Profiling durch ein Bundesorgan.

Wichtig ist, dass je mehr Risiken eine Datenverarbeitung für die betroffene Person birgt, umso höher sind die Anforderungen an die Gültigkeit der Einwilligung.

Zweckbindung

Das revDSG führt neu das Konzept der «Vereinbarkeit» eines Bearbeitungszwecks ein. Art. 6 Abs. 3 revDSG statuiert, dass Personendaten nur für einen bestimmten Zweck beschafft werden dürfen. Ausserdem dürfen sie nur so bearbeitet werden, dass dies mit dem Zweck vereinbar ist.

Keine Übernahme des Verbotsprinzips

Grundsätzlich erlaubt das revDSG die Bearbeitung von Personendaten, sofern sie datenschutzkonform, d.h. unter Einhaltung der allgemeinen Bearbeitungsgrundsätze erfolgt. Als Unterschied zur DSGVO gilt damit das Verbotsprinzip nicht, d.h. es muss nicht für jede Bearbeitung ein Rechtfertigungsgrund (wie bspw. die Einwilligung, Gesetz etc.) vorliegen.

Pflichten des Datenbearbeiters

(a) Einhaltung der Bearbeitungsgrundsätze

Die in Art. 6 DSG genannten Bearbeitungsgrundsätze wurden im Rahmen der Revision nur wenig umformuliert. Wie erwähnt ist auch unter dem revDSG keine Rechtfertigung für eine Datenbearbeitung erforderlich, falls die Bearbeitungsgrundsätze eingehalten werden bzw. soweit keine besonders schützenswerten Personendaten von Dritten offenbart werden.

(b) Verstärkte Informationspflichten

Die Informationspflicht wird im revDSG ausgebaut. Dies bedeutet, dass Unternehmen eine Datenschutzerklärung haben müssen, aufgrund welcher sie gewisse Pflichtinformationen über die von ihnen durchgeführten Datenbeschaffungen den betroffenen Personen zugänglich machen müssen. Dies geschieht normalerweise auf der eigenen Webseite mit Links auf entsprechende Informationsbroschüren oder mittels spezifischer Verträge.

Gemäss Art. 14 DSG besteht eine Informationspflicht lediglich im Hinblick auf die Beschaffung bzw. Bearbeitung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen. Das revDSG statuiert bei jeder Beschaffung von Personendaten eine Informationspflicht. Somit entsteht eine Informationspflicht sowohl bei der direkten als auch bei der indirekten Beschaffung von Personendaten (d.h. wenn die Daten bei Drittpersonen erhoben werden).

Die von einer Datenbearbeitung betroffenen Personen sollen wissen, was mit ihren Daten geschieht. Das revDSG führt eine zweistufige Informationspflicht ein.

Proaktive Informationspflicht

Die für die Datenverarbeitung verantwortlichen Personen haben von sich aus, m.a.W. proaktiv über eine Datenverarbeitung zu informieren.

Nach geltendem Recht bestand diese Pflicht lediglich bei der Beschaffung von besonderes schützenswerten Personendaten und Persönlichkeitsprofilen. Neu wird diese Pflicht generell – mit einigen wenigen Ausnahmen - für die Beschaffung von Personendaten eingeführt. Dieser Pflicht wird normalerweise mittels einer Datenschutzerklärung («Privacy Statement») nachgekommen. Damit wird die Information für sämtliche Datenverarbeitungen der verantwortlichen Person in einem einzigen Dokument erteilt. Gemäss Entwurf der Verordnung des revDSG (VrevDSG) ist die Datenschutzerklärung in «präziser, verständlicher und leicht zugänglicher» Form zu erlassen.[2] In der Datenschutzerklärung sind insbesondere diejenigen Informationen bekannt zu geben, die erforderlich sind, damit die betroffene Person ihre Rechte nach dem Datenschutzgesetz geltend machen kann und womit eine transparente Datenbearbeitung gewährleistet ist. Folgende Informationen sind mindestens mitzuteilen:

a) Die Identität und die Kontaktdaten der verantwortlichen Person;
b) der Bearbeitungszweck;
c) gegebenenfalls die Empfänger der Daten sowie

[2] vgl. Art. 13 E-VrevDSG.

d) ob die Daten ins Ausland bekannt gegeben werden und welche Sicherheiten getroffen werden, falls das Zielland nicht über einen angemessenen Datenschutz verfügt.

Im Gegensatz zur europäischen Gesetzgebung verzichtet das revDSG auf die Angabe eines Rechtfertigungsgrundes, d.h. gemäss revDSG bedarf es keinerlei Rechtfertigung, um Personendaten zu bearbeiten, es sei denn, die Bearbeitung verletzt die Persönlichkeit der betroffenen Person.[3] Das revDSG statuiert, dass die Persönlichkeit der betroffenen Person dann verletzt ist, wenn die Datenbearbeitung nicht an die datenschutzrechtlichen Grundsätze hält. Als besonderes wichtige datenschutzrechtliche Grundsätze gelten dabei bspw. die Erkennbarkeit des Zwecks im Moment der Datenbeschaffung und der Zweckbindung der zukünftigen Bearbeitung. Dies bedeutet, dass Personendaten ausschliesslich im Einklang mit dem bei der Datenbeschaffung angegebenen Zweck bearbeitet werden dürfen.

Informationen auf Anfrage

Auf ein Auskunftsbegehren sind einer betroffenen Person gemäss Art. 25 Abs. 2 revDSG diejenigen Informationen zu liefern, «die erforderlich sind, damit sie ihre Rechte nach diesem Gesetz geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist.»

Rechte der betroffenen Personen

(a) Ausgebautes Auskunftsrecht

Das Auskunftsrecht im revDSG ergänzt die Informationspflicht. Das Auskunftsrecht führt dazu, dass die betroffene Person zusätzliche Informationen zu denjenigen, die im Rahmen der Datenschutzerklärung offengelegt werden, erhält. Auf ein Auskunftsbegehren sind einer betroffenen Person gemäss Art. 25 Abs. 2 revDSG diejenigen Informationen zu liefern, «die erforderlich sind, damit sie ihre Rechte nach diesem Gesetz geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist.» Damit kann jede natürliche Person verlangen, dass ihr der Verantwortliche offenlegt, ob er Personendaten von ihr bearbeitet und wenn ja, welche. Auf Verlangen der natürlichen Person sind folgende Informationen offenzulegen:

- Die Identität und Kontaktdaten des Verantwortlichen;
- die bearbeitenden Personendaten als solche;
- der Bearbeitungszweck;
- die Aufbewahrungsdauer der Personendaten oder, falls dies nicht möglich ist, die Kriterien zur Festlegung dieser Dauer;
- die verfügbaren Angaben über die Herkunft der Personendaten, soweit sie nicht bei der betroffenen Person beschafft werden;
- gegebenenfalls das Vorliegen eines rein automatisierten Entscheidungsprozesses, sofern dieser eine erheblich beeinträchtigende Rechtsfolge nach sich zieht (Einzelentscheidung), sowie die Logik, auf der diese Einzelentscheidung beruht und die Möglichkeiten zu deren Überprüfung;
- gegebenenfalls der Empfänger oder die Kategorien von Empfängern, denen Personendaten bekanntgegeben werden, sowie die Informationen nach Art. 19 Abs. 4 revDSG.

Die Auskunftsbegehren kann abgelehnt, zumindest eingeschränkt oder aufgeschoben werden, wenn das Gesuch der natürlichen Person «offensichtlich» unbegründet oder querulatorisch ist.[4] Offensichtlich unbegründet sind Auskunftsbegehren dann, wenn sie nicht der Geltendmachung von Datenschutzrechten oder der datenschutzrechtlich motivierten Schaffung von Transparenz dienen.

(b) Neues Recht auf Datenportabilität

Das revDSG führt ein Recht der Datenherausgabe und -übertragung ein, welches der Regelung der DSGVO nachgebildet ist. Die neue Regel greift dort, wo ein Verantwortlicher einer Datenbearbeitung zum Abschluss oder zur Abwicklung eines Vertrags mit der betroffenen Person, oder gestützt auf eine Einwilligung von ihr, Daten automatisiert bearbeitet. Die in diesem Zusammenhang von der betroffenen Person erhaltenen Personendaten, hat der Verantwortliche jederzeit auf Verlangen hin kostenlos herauszugeben.

Massnahmen zur Sicherstellung des Datenschutzes

(a) Privacy by Design

Art. 7 revDSG führt die Prinzipen (i) «Privacy by Design» (Datenschutz durch Technik) und (ii) «Privacy by Default» (Datenschutz durch datenschutzfreundliche Voreinstellungen) ein, welche heute bereits als «best practice» gelten.

Der Verantwortliche ist verpflichtet, die Datenbearbeitung technisch und organisatorisch so auszugestalten, dass die Datenschutzvorschriften eingehalten werden können.[5] Dies bedeutet, dass Personendaten durch Technik standardmässig

[3] Art. 30 f. revDSG.
[4] Art. 26 Abs. 1 lit. c revDSG
[5] Art. 7 revDSG

pseudonymisiert oder anonymisiert werden, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind oder dass sie regelmässig gelöscht werden. Ebenfalls gilt, dass nur solche Personendaten erhoben werden, welche zwingend für den Verwendungszweck benötigt werden und weitere Personendaten nur, wenn dies aktiv angewählt und damit autorisiert wird.

(b) Privacy by Default

Die Pflicht zur «Privacy by Default» wird durch das revDSG neu eingeführt. Sind in einem Service, in einer Software oder in einem Gerät mehrere Möglichkeiten vorgesehen, wie Personendaten bearbeitet werden können und kann der Benutzer diese Möglichkeiten über eine entsprechende Einstellung selbst anpassen, muss die Standardeinstellung, die am wenigsten weitgehende Einstellung aufzeigen.

Datenexporte

Die Grundsätze für Datenexporte bleiben im revDSG unverändert. Dies bedeutet, dass Datenexporte in Länder mit angemessenen Datenschutzgesetzen weiterhin zulässig sind. Datenexporte in einen Drittstaat bedürfen entweder der Rechtfertigung (z.B. Einwilligung, Vertragserfüllung, überwiegende öffentliche Interessen, Durchsetzung von Rechtsansprüchen) oder anderer Massnahmen zur Gewährleistung eines angemessenen Datenschutzniveaus.

Das revDSG bringt allerdings eine bedeutende Neuerung mit sich:

- Der Bundesrat ist ermächtigt, nach dem Vorbild der EU verbindliche Angemessenheitsentscheide über das Datenschutzniveau anderer Staaten zu erlassen. Die bisherige Liste des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) von Staaten, die über einen angemessenen Datenschutz verfügen, entfällt;
- Die Notifikationspflicht bei der Verwendung von Standardklauseln entfällt;
- Das revDSG erlaubt Datenexporte in Drittstaaten zur Durchsetzung von Ansprüchen bei ausländischen Behörden (und nicht wie bisher nur bei ausländischen Gerichten);
- Die betroffene Person müssen darüber informiert werden, wohin ihre Daten exportiert werden und bei Exporten in Länder ohne angemessenes Schutzniveau auf welchen Rechtfertigungstatbestand sich der Verantwortliche stützt bzw. welche Schutzmassnahmen er getroffen hat.

Handlungsbedarf für Unternehmen

Im Hinblick auf die Einführung des revDSG sind Unternehmen gefordert, folgende Massnahmen zu ergreifen:

Überprüfung der Organisation: Unternehmen sollten einen Datenschutzbeauftragten ernennen. Es ist wichtig, die interne Zuständigkeit für den Datenschutz zu regeln.

Aktualisierung der Dokumentation: Es gilt die Datenschutzerklärungen auf die neuen Vorgaben hin zu überprüfen, anzupassen und gegebenenfalls neu zu erstellen, falls solche noch nicht vorhanden sind. Datenschutzerklärungen müssen so ausgestaltet sein, dass Mitarbeiter, Geschäftspartner und die Öffentlichkeit über die Datenverarbeitung informiert werden. Dies ist ein zentraler Aspekt der Datenschutz-Compliance.

Etwas aufwendiger ist die interne Prüfung, ob alle Fälle abgedeckt sind, über die das Unternehmen Personendaten beschafft. Nur mit diesen Angaben kann dann jedoch auch das neu vorgeschriebene Verzeichnis der Datenbearbeitungen erstellt werden.

Implementierung geeigneter Prozesse: Unternehmen müssen einen Prozess einführen zur Erfassung, Meldung und Bearbeitung von Verletzungen der Datensicherheit, wozu auch unbeabsichtigte Datenverluste und Fehlversendungen von Personendaten zählen,. Dabei gilt es zu beachten, dass mindesten eine Person im Unternehmen weiss, was in der konkreten Situation zu tun ist oder wie sie herausfindet, was zu tun ist bei Eintritt einer solchen Verletzung.

Überprüfung von Massnahmen zur Datensicherheit: Unternehmen müssen dafür sorgen, dass Personendaten angemessenen geschützt sind. Die getroffenen organisatorischen und technischen Massnahmen sind regelmässig zu überprüfen und gegebenenfalls zu aktualisieren.

AVELALAW AG ZÜRICH ist eine auf das Finanzmarktrecht (mit besonderem Schwerpunkt auf das Asset Management sowie Schweizer und ausländische kollektive Kapitalanlagen) spezialisierte Beratungsfirma mit Sitz in Zürich. AVELALAW deckt das gesamte Spektrum der Rechtsberatung, der Compliance und des Risikomanagements für ihre Klienten ab. Zu den Klienten von AVELALAW zählen Vermögensverwalter, Fondsmanager, Fondsleitungen, Anlageberater, Banken, Versicherungen und sonstige Finanzdienstleister aus dem In- und Ausland. Wir beraten Sie gerne in deutscher, englischer, spanischer und italienischer Sprache.

Der Inhalt dieses Dokuments stellt keine Rechts- oder Steuerauskunft dar und darf nicht als solche verwendet werden. Sollten Sie einen auf ihre Umstände bezogene Beratung wünschen, wenden Sie sich bitte an eine der oben aufgeführten Personen bei AVELALAW AG.