Revision des Schweizer Datenschutzgesetzes: Wichtige Änderungen und allfällige zu treffende Vorkehrungen im Hinblick auf die neuen Anforderungen

1. Einleitung

Am 25. September 2020 haben National- und Ständerat den Schlussabstimmungstext des revidierten Datenschutzgesetzes (DSG) angenommen. Nach Ablauf der 100-tägigen Referendumsfrist hat der Bundesrat, anlässlich seiner Sitzung vom 31. August 2022, den Zeitpunkt des Inkrafttretens des revidierten DSG auf den 1. September 2023 festgesetzt. Mit der Umsetzungsfrist von einem Jahr haben die Datenschutzverantwortlichen in der Wirtschaft genügend Zeit erhalten, um die notwendigen Vorkehrungen für die Umsetzung des neuen Datenschutzrechts zu treffen.

Allgemein ist zu erwähnen, dass sich das revidierte DSG sehr stark an der europäischen Datenschutz-Grundverordnung (DSGVO) orientiert, wobei punktuelle Unterschiede zwischen dem EU- und Schweizer Recht bestehen bleiben. Die folgenden Ausführungen beziehen sich ausschliesslich auf das revidierte DSG. Die Überprüfung, ob gewisse Geschäftsbereiche eines Schweizer Unternehmens dem Anwendungsbereich der DSGVO unterstehen und welche Differenzen im Einzelnen bestehen, liegt in der Verantwortung des jeweiligen Unternehmens. Ist die Anwendbarkeit der DSGVO zu bejahen, sind die entsprechenden Bestimmungen zwingend zu berücksichtigen und umzusetzen. Für weitergehende Informationen zum Thema DSGVO und deren Anwendbarkeit auf Schweizer Unternehmen verweisen wir gerne auf folgenden Link: Tipps zur DSGVO.

Abschliessend möchten wir ausdrücklich darauf hinweisen, dass das vorliegende Dokument eine allgemeine Übersicht über einige wichtige Neuerungen betreffend die Revision des Schweizer Datenschutzgesetzes vermitteln und als Orientierungshilfe hinsichtlich allfälliger zu treffender Vorkehrungen dienen soll. Es werden nicht sämtliche Neuerungen erwähnt. Für die Vollständigkeit und Richtigkeit übernimmt der VöV keine Gewähr.

2. Wichtige Änderungen im revidierten DSG

Der Schlussabstimmungstext ist **hier** abrufbar.

Persönlicher Geltungsbereich

Das revidierte Datenschutzgesetz gilt neu nur noch für die Bearbeitung von Personendaten natürlicher Personen (vgl. Art. 2 revDSG). Das aktuelle DSG erfasst dagegen auch die Bearbeitung von Personendaten juristischer Personen (vgl. Art. 2 DSG).

Verantwortlicher und Auftragsbearbeiter

Neu wird zwischen den Rollen des Verantwortlichen und des Auftragsbearbeiters unterschieden. Als Verantwortlicher wird eine private Person oder ein Bundesorgan qualifiziert, die oder das allein oder zusammen mit anderen über den Zweck und die Mittel der Bearbeitung entscheidet (vgl. Art. 5 Bst. j revDSG). Auftragsbearbeiter kann eine private Person oder ein Bundesorgan sein, die oder das im Auftrag des Verantwortlichen Personendaten bearbeitet (vgl. Art. 5 Bst. k revDSG).

Profiling / Profiling mit hohem Risiko

Nebst dem Profiling wird neu auch das Profiling mit hohem Risiko im Gesetz geregelt. Letzteres 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 (vgl. Art. 5 Bst. f und g revDSG). Bei einem Profiling mit hohem Risiko muss die Einwilligung der betroffenen Person ausdrücklich erfolgen. Bei einem Profiling durch ein Bundesorgan wird

immer die ausdrückliche Einwilligung benötigt, unabhängig davon, ob ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person besteht (vgl. Art. 6 Abs. 7 revDSG).

Anmeldung von Datensammlungen

Unter Datensammlungen wird jeder Bestand von Personendaten verstanden, der so aufgebaut ist, dass die Daten nach betroffenen Personen erschliessbar sind (vgl. Art. 3 Bst. g DSG). Diese Datensammlungen müssen private Personen bei Vorliegen von gewissen Voraussetzungen beim Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) anmelden (vgl. Art. 11a Abs. 3 DSG). Künftig entfällt diese Anmeldepflicht beim EDÖB.

Privacy-by-Design und -by-Default

Der Verantwortliche ist neu ab der Planung verpflichtet, die Datenbearbeitung technisch und organisatorisch so auszugestalten, dass die Datenschutzvorschriften, insbesondere die Grundsätze gemäss Art. 6 revDSG eingehalten werden (vgl. Art. 7 Abs. 1 revDSG; sog. «Privacy-by-Design»). Weiter ist der Verantwortliche verpflichtet, mittels geeigneter Voreinstellungen (bspw. bei Websites oder Apps) sicherzustellen, dass die Bearbeitung der Personendaten auf das für den Verwendungszweck nötige Mindestmass beschränkt ist, soweit die betroffene Person nicht etwas anderes bestimmt (vgl. Art. 7 Abs. 3 revDSG; sog. «Privacy-by-Default»).

Datenschutzberaterin oder -berater

Private Verantwortliche können eine Datenschutzberaterin oder einen Datenschutzberater ernennen. Diese Person ist Anlaufstelle für die betroffenen Personen und für die Behörden, die in der Schweiz für den Datenschutz zuständig sind. Sie hat den privaten Verantwortlichen in Fragen des Datenschutzes zu schulen und zu beraten sowie bei der Anwendung und Umsetzung der Datenschutzvorschriften mitzuwirken (vgl. Art. 10 revDSG).

Verzeichnis der Bearbeitungstätigkeit

Künftig müssen die Verantwortlichen und Auftragsbearbeiter ein Verzeichnis über ihre Bearbeitungstätigkeit führen (vgl. Art. 12 Abs. 1 revDSG). Der Mindestinhalt dieser Verzeichnisse wird in Art. 12 Abs. 2 und 3 revDSG aufgeführt. Für Unternehmen mit weniger als 250 Mitarbeiterinnen und Mitarbeitern, deren Datenbearbeitung nur ein geringes Risiko für Verletzungen der Persönlichkeit der betroffenen Personen darstellen, sieht der Bundesrat Ausnahmen vor (vgl. Art. 12 Abs. 5 revDSG).

Erweiterte Informationspflicht

Bisher musste eine betroffene Person nur dann aktiv über die Beschaffung von Personendaten informiert werden, wenn es sich um besonders schützenswerte Personendaten und/oder Persönlichkeitsprofile handelte (vgl. Art. 14 Abs. 1 DSG). Künftig hat der Verantwortliche betroffene Personen bei jeder Bearbeitung von Personendaten angemessen zu informieren, selbst dann, wenn er die Daten nicht bei dieser Person direkt beschafft (vgl. Art. 19 Abs. 1 revDSG). Der Mindestinhalt dieser Informationspflicht wird in Art. 19 Abs. 2 revDSG geregelt. Weitere Bestimmungen im Zusammenhang mit der Beschaffung von Personendaten bei Dritten sowie der Bekanntgabe von Daten ins Ausland sind in Art. 19 Abs. 3 – 5 revDSG enthalten. Ausnahmen von der Informationspflicht und Einschränkungen regelt Art. 20 revDSG.

Datenschutz-Folgenabschätzung

Kann eine Bearbeitung von Personendaten ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen, hat der Verantwortliche künftig vorgängig eine Datenschutz-Folgenabschätzung zu erstellen (vgl. Art. 22 revDSG). Das hohe Risiko ergibt sich insbesondere bei Verwendung neuer Technologien, aus der Art, dem Umfang, den Umständen und dem Zweck der Bearbeitung. Art. 22 Abs. 2 revDSG zählt einige Beispiele auf. Was eine Datenschutz-Folgenabschätzung enthalten muss und unter welchen Voraussetzungen davon abgesehen werden kann, wird in Art. 22 Abs. 3 – 5

revDSG geregelt. Wann im Zusammenhang mit einer Datenschutz-Folgenabschätzung beim EDÖB eine Stellungnahme einzuholen ist, kann Art. 23 revDSG entnommen werden.

Meldepflicht für Verletzungen der Datensicherheit

Führt eine Verletzung der Datensicherheit voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person, hat der Verantwortliche diese dem Beauftragten (EDÖB) so rasch als möglich zu melden (vgl. Art. 24 Abs. 1 revDSG). Der Mindestinhalt dieser Meldung ist in Art. 24 Abs. 2 revDSG geregelt. Der Verantwortliche informiert die betroffene Person, sofern es zu ihrem Schutz erforderlich ist oder der Beauftragte (EDÖB) es verlangt (vgl. Art. 24 Abs. 4 revDSG). Ausnahmen hiervon werden in Art. 24 Abs. 5 revDSG aufgeführt.

Auskunftsrecht

Das Auskunftsrecht wurde im revidierten DSG in einigen Punkten angepasst und konkretisiert (vgl. Art. 25 ff. revDSG). Neu hat die betroffene Person das Recht auf Datenherausgabe und -übertragung, sofern die entsprechenden Voraussetzungen erfüllt sind (vgl. Art. 28 revDSG), wobei der Verantwortliche die Herausgabe und Übertragung der Personendaten aus den in Art. 26 Abs. 1 und 2 revDSG genannten Gründen verweigern, einschränken oder aufschieben kann (vgl. Art. 29 Abs. 1 revDSG).

Prüfung der Kreditwürdigkeit als Rechtfertigungsgrund

Eine Persönlichkeitsverletzung ist widerrechtlich, wenn sie nicht durch Einwilligung der betroffenen Person, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt ist. Ein überwiegendes Interesse des Verantwortlichen an der Bearbeitung von Personendaten fällt u.a. dann in Betracht, wenn er Personendaten zur Prüfung der Kreditwürdigkeit der betroffenen Person bearbeitet (vgl. Art. 13 Abs. 1 und 2 Bst. c DSG). Diese Bestimmung wurde im revidierten DSG konkretisiert. Die Daten dürfen bspw. nicht älter als zehn Jahre sein (vgl. Art. 31 Abs. 2 Bst. c revDSG).

Kompetenzen der Aufsichtsbehörde

Der EDÖB erhält mit dem revidierten DSG neue Kompetenzen. Künftig eröffnet er Untersuchungen von Amtes wegen oder auf Anzeige hin, sofern genügend Anzeichen dafür bestehen, dass eine Datenbearbeitung gegen die Datenschutzvorschriften verstossen könnte (vgl. Art. 49 revDSG). Kommen die beteiligten Personen ihren Mitwirkungspflichten nicht nach, kann der EDÖB Anordnungen treffen (vgl. Art. 50 revDSG). Weiter kann er bei einer Verletzung von Datenschutzvorschriften anstelle der bisherigen Empfehlungen verbindliche Verwaltungsmassnahmen mittels Verfügung erlassen (vgl. Art. 51 revDSG).

Strafrechtliche Sanktionen

Die strafrechtlichen Sanktionen wurden verschärft und der Katalog der strafbaren Handlungen erweitert. Neu können natürliche Personen bei einer Verletzung bestimmter Vorschriften (teilweise auf Antrag) mit bis zu CHF 250'000.00 gebüsst werden (vgl. Art. 60 ff. revDSG). Bei Widerhandlungen in Geschäftsbetrieben kann die Behörde von einer Verfolgung der natürlichen Person absehen und an ihrer Stelle den Geschäftsbetrieb zur Bezahlung der Busse verurteilen, sofern eine Busse von höchstens CHF 50'000.00 in Betracht fällt und die Ermittlung nach der strafbaren Person Untersuchungsmassnahmen bedingen würde, die im Hinblick auf die Strafe unverhältnismässig wären (vgl. Art. 64 revDSG).

3. Zu treffende Vorkehrungen im Hinblick auf die neuen Anforderungen gemäss revidiertem DSG

Unternehmensorganisation

Es ist zu klären, wer für den Datenschutz verantwortlich ist (allenfalls Ernennung eines Datenschutzberaters) und wie dieser Bereich geregelt ist, mithin wie die Einhaltung der Datenschutzvorgaben gewährleistet wird. Dieser Bereich ist laufend zu überprüfen, notfalls sind Anpassungen vorzunehmen. Allenfalls sind Audits vorzusehen und interne Weisungen zu erstellen / anzupassen.

Erkennen / Dokumentation von Datenbearbeitungen

Datenbearbeitungen sind unternehmensintern zu eruieren, zu analysieren und zu dokumentieren, auf die neuen Vorgaben hin zu überprüfen und allenfalls anzupassen. Dies gilt auch für Auslanddatentransfers. Wichtig ist zu beachten, dass unter den Begriff «Bearbeiten» jeder Umgang mit Personendaten fällt, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten (vgl. Art. 5 Bst. d revDSG).

Grundsätzlich ist neu ein Bearbeitungsverzeichnis über die Bearbeitung von Personendaten zu führen. Welche Angaben das Verzeichnis mindestens enthalten muss, wird in Art. 12 revDSG erwähnt. Für Unternehmen mit weniger als 250 Mitarbeiterinnen und Mitarbeitern sieht der Bundesrat Ausnahmen vom Führen eines formellen Verzeichnisses vor (diese Ausnahmeregelungen existieren aktuell noch nicht). Aber auch in diesen Fällen müssen Datenbearbeitungen dokumentiert werden. Da die Erstellung eines Bearbeitungsverzeichnisses mit einem nicht unerheblichen Aufwand verbunden sein kann, empfiehlt es sich, dieses Thema frühzeitig, folglich vor Inkrafttreten des neuen Datenschutzgesetzes anzugehen. So können auch allenfalls erforderliche Massnahmen im Zusammenhang mit dem Datenschutz rechtzeitig umgesetzt werden.

Wenn eine Bearbeitung von Personendaten ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringt, hat der Verantwortliche zudem im Vorfeld der Datenbearbeitung eine Datenschutz-Folgenabschätzung zu erstellen (vgl. Art. 22 revDSG).

Geeignete Prozesse definieren

Es ist zu prüfen, ob bereits effiziente Prozesse bestehen, welche die Einhaltung der DSG-Vorgaben gewährleisten können oder ob diese noch zu erarbeiten sind. Datenschutzvorfälle müssen schnellstmöglich erkannt werden können. In gewissen Fällen hat zudem so rasch als möglich eine Meldung beim EDÖB zu erfolgen (vgl. Art. 24 revDSG). Mitarbeitende sind für das Thema Datenschutz zu sensibilisieren und wo erforderlich zu schulen.

Weiter kann die betroffene Person Auskunft darüber verlangen, ob Personendaten über sie bearbeitet werden (vgl. Art. 25 Abs. 1 revDSG). Dieses Auskunftsbegehren muss in der Regel innerhalb von 30 Tagen bearbeitet werden können (vgl. Art. 25 Abs. 7 revDSG). Die fristgerechte und umfassende Beantwortung von Auskunftsbegehren muss folglich sichergestellt sein. Gleiches gilt für den Fall von behördlichen Anfragen.

Die Grundsätze der Bearbeitung von Personendaten gemäss Art. 6 revDSG müssen durch geeignete (technische) Prozesse sichergestellt werden. Daten müssen bspw. vernichtet / gelöscht oder anonymisiert werden, sobald sie zum Zweck der Bearbeitung nicht mehr benötigt werden (vgl. Art. 6 Abs. 4 revDSG).

Überprüfung und Aktualisierung von Dokumenten

Es gilt, sämtliche Dokumente, welche Berührungspunkte mit dem Bearbeiten von Personendaten haben, im Hinblick auf die rechtlichen Vorgaben gemäss dem revidierten DSG zu überprüfen und sofern erforderlich (einvernehmlich mit allfälligen Vertragspartnern) die notwendigen Anpassungen vorzunehmen. Dies gilt insbesondere für Datenschutzerklärungen und Verträge mit Auftragsbearbeitern (bspw. IT-Unternehmen, welches Personendaten im Auftrag des Unternehmens bearbeitet oder darauf Zugriff etc.).

Technische Vorkehrungen / Datensicherheit

Die Datenbearbeitung muss technisch und organisatorisch so ausgestaltet sein, dass die Datenschutzvorschriften eingehalten werden können (vgl. Art. 7 Abs. 1 revDSG). Betreffend Datensicherheit sind, sofern erforderlich, geeignete technische und organisatorische Massnahmen zu ergreifen. Diese müssen eine dem bestehenden Risiko angemessene Datensicherheit gewährleisten und die Vertraulichkeit, Verfügbarkeit und Integrität der Personendaten sicherstellen.