Überblick

Nach langem Hin und Her hat das Schweizer Parlament nach Bereinigung der letzten Differenzen im Rahmen seiner Schlussabstimmung vom 25. September 2020 die Totalrevision des Schweizer Datenschutzgesetzes (DSG) verabschiedet. Gerne informieren wir Sie hiermit (nochmals) kurz über den Hintergrund der Gesetzesvorlage und vor allem über die wichtigsten Neuerungen.

Mit der Totalrevision sollte das in die Jahre gekommene Schweizer Datenschutzgesetz (datiert aus dem Jahr 1992) an die heutigen gesellschaftlichen und technologischen Verhältnisse angepasst und den jüngeren und moderneren Regelungen im europäischen Datenschutzumfeld (insb. EU-DSGVO) angenähert werden. Zentral waren dabei namentlich die folgenden vier Aspekte:

- Erhöhung der Transparenz und Stärkung der Rechte der betroffenen Personen;
- Förderung der Prävention und der Eigenverantwortung der Datenbearbeiter;
- Stärkung der Datenschutzaufsicht;
- Ausbau der Strafbestimmungen.

Aufgrund der Botschaft und des Vorentwurfs des Bundesrats waren einige gesetzlichen Verschärfungen zu befürchten, welche für viele Unternehmen zu Rechtsunsicherheit und grossem Mehraufwand bei der Bearbeitung von Personendaten geführt hätten. Deshalb hat sich der AGVS gemeinsam mit dem Schweizerischen Leasingverband (SLV) sowie mit seinen Partnerverbänden economiesuisse und dem Schweizerischen Gewerbeverband sgv für eine liberale und praxistaugliche Umsetzung der Gesetzesrevision eingesetzt, welche einerseits den Angemessenheitsbeschluss der EU und damit den Datentransfer aus der EU in die Schweiz nicht gefährdet, und andererseits auf unnötig strenge Regelungen verzichtet, welche über diejenigen der EU-DSGVO hinausgehen (sog. „Swiss Finishs"). Dies ist uns in weiten Teilen gelungen, so etwa bei der Ausnahme zur Führung eines Bearbeitungsverzeichnisses, sowie beim Auskunftsrecht und – zumindest teilweise – beim Profiling.

Gleichwohl werden in Zukunft bei der Bearbeitung von Personendaten **verschärfte Regelungen** zu beachten sein, mit welchen Sie sich frühzeitig auseinandersetzen sollten, um Ihr Datenschutz-Konzept bis zum Inkrafttreten des revidierten Gesetzes überprüfen und – wo nötig – anpassen zu können (z.B. Erstellen von Datenschutzerklärungen sowie ggf. Verzeichnissen der Bearbeitungstätigkeiten, Anpassung der Datenbearbeitungsprozesse, Ernennung eines Datenschutzbeauftragten, Abschluss von Auftragsdatenbearbeitungsverträgen etc.).

Nach Ablauf der 100-tägigen Referendumsfrist wird der Bundesrat über das Inkrafttreten bestimmen. Das revidierte Datenschutzgesetz (nachfolgend „**revDSG**") wird dementsprechend wohl nicht vor dem 1. Januar 2022 in Kraft treten, zumal auch noch die entsprechende Verordnung (DSGV) anzupassen ist. Wir werden Sie frühzeitig über den Beschluss des Bundesrats informieren.

AGVS/UPSA
Wölflistrasse 5, 3006 Bern
Telefon 031 307 15 15, Fax 031 307 15 16
info@agvs-upsa.ch, www.agvs-upsa.ch

Wichtige Neuerungen

Bitte beachten Sie, dass wir im Rahmen dieser Mitgliederinformation nicht sämtliche neuen oder angepassten Gesetzesbestimmungen im Detail erläutern können. Wir beschränken uns daher auf die aus unserer Sicht wichtigsten Neuerungen gegenüber dem geltenden Recht:

- **Kein Schutz von Daten juristischer Personen:** Während das geltende DSG auf Daten sowohl natürlicher als auch juristischer Personen anwendbar ist, beschränkt das revDSG den Geltungsbereich – gleich wie die EU-DSGVO – auf Daten natürlicher Personen.
- **Besonders schützenswerte Personendaten:** Das revDSG erweitert die Auflistung von Daten, welche als besonders schützenswert gelten und damit an qualifizierte Rechtsfolgen knüpfen (u.a. bei der Einwilligung, der Datenschutz-Folgenabschätzung, der Bekanntgabe an Dritte sowie der Kreditwürdigkeitsprüfung). So werden genetische Daten sowie biometrische Daten (z.B. Fingerabdruck), die eine natürliche Person eindeutig identifizieren, neu ebenfalls als besonders schützenswert qualifiziert.
- **Profiling und Profiling mit hohem Risiko:** Ob nebst „gewöhnlichem" Profiling ein „Profiling mit hohem Risiko" ins Gesetz aufgenommen werden soll, war die am heftigsten umstrittene und meist diskutierte Frage der gesamten Vorlage. Schliesslich folgten die Räte – entgegen unseren Empfehlungen – den Anträgen der Einigungskonferenz, wonach Profiling mit hohem Risiko gesetzlich definiert und speziell geregelt werden soll. So muss bei einem Profiling mit hohem Risiko eine allenfalls erforderliche Einwilligung *ausdrücklich* sein. Zudem entfallen das berechtigte Interesse des Verantwortlichen und damit sein Rechtfertigungsgrund für eine Persönlichkeitsverletzung, wenn seine Datenbearbeitungen zur Prüfung der Kreditwürdigkeit ein Profiling mit hohem Risiko beinhaltet.

  Profiling mit hohem Risiko soll vorliegen, wenn Personendaten automatisiert bearbeitet werden und eine Verknüpfung von Daten die Beurteilung „wesentlicher Aspekte der Persönlichkeit" erlaubt. Die gesetzliche Definition ist sehr offen und eine Abgrenzung zu „normalem" Profiling wird in der Praxis nicht einfach sein. Allenfalls wird hierzu die Verordnung noch weitere Klärung bringen.

  Jedenfalls bedeutet diese Änderung, dass für eine Kreditfähigkeitsprüfung, bei welcher ein Profiling mit hohem Risiko eingesetzt wird, in Zukunft sichergestellt sein muss, dass sämtliche Bearbeitungsgrundsätze eingehalten werden oder ein anderer Rechtfertigungsgrund (insb. Einwilligung durch die betroffene Person) vorliegt.
- **Verhaltenskodizes:** Das revDSG ermöglicht unter anderem Berufs-, Branchen- und Wirtschaftsverbände, die nach ihren Statuten zur Wahrung der wirtschaftlichen Interessen ihrer Mitglieder befugt sind, dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) Verhaltenskodizes vorzulegen. Damit soll die Entwicklung

der Selbstregulierung und die Eigenverantwortung der Verantwortlichen gefördert werden. Der EDÖB nimmt dann zu den Kodizes öffentlich Stellung. Zwar lassen sich aus einer positiven Stellungnahme keine Rechte ableiten.

Es kann diesfalls aber immerhin davon ausgegangen werden, dass ein dem Kodex entsprechendes Verhalten keine Verwaltungsmassnahmen nach sich zieht. Zudem können Verantwortliche, welche die Kodizes einhalten, unter bestimmten Voraussetzungen auf die Durchführung einer Datenschutz-Folgenabschätzung verzichten. Der AGVS trägt – wie Sie bereits wissen – das „Grundbekenntnis der Schweizer Wirtschaft zu einem verantwortungsvollen Umgang mit Daten“ mit (der Verhaltenskodex ist abrufbar unter nachfolgendem Link: https://www.economiesuisse.ch/de/datenwirtschaft).

- **Verzeichnis über Datenbearbeitungen:** Das revDSG sieht – wie die EU-DSGVO – sowohl für den Verantwortlichen als auch für den Auftragsbearbeiter eine Pflicht zur Führung eines Verzeichnis ihrer jeweiligen Datenbearbeitungen vor. Das jeweilige Verzeichnis muss mindestens die vom Gesetz aufgeführten Angaben enthalten. Der Bundesrat sieht Ausnahmen für Unternehmen vor, die weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen und deren Datenbearbeitung ein geringes Risiko von Verletzungen der Persönlichkeit der betroffenen Personen mit sich bringt. Diese Ausnahmen sind in der Verordnung noch zu regeln.
- **Auftragsbearbeiter:** Gemäss revDSG kann ein Auftragsbearbeitungsverhältnis mittels Vertrag oder durch Gesetz begründet werden. Voraussetzung ist – gleich wie unter geltendem Recht – dass der Auftragsbearbeiter die Daten so bearbeitet, wie es der Verantwortliche selbst tun dürfte. Neu ist – wie in der EU – eine Übertragung der Datenbearbeitung an einen Unterauftragnehmer nur mit vorgängiger Genehmigung des Verantwortlichen zulässig, damit dieser (zumindest indirekt) die Kontrolle über die Datenbearbeitung behält, und, dass der Verantwortliche sich zu vergewissern hat, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit zu gewährleisten. Ansonsten ändert sich hier wenig. Insbesondere untersteht der Auftragsbearbeitungsvertrag weiterhin keinen besonderen Formvorschriften.
- **Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen:** Das revDSG enthält – wie die EU-DSGVO – die Grundsätze „Privacy-by-Design“ und „Privacy-by-Default“. Der Verantwortliche muss die Datenbearbeitung ab der Planung technisch und organisatorisch so ausgestalten, dass die Datenschutzvorschriften, insb. die Bearbeitungsgrundsätze, eingehalten werden (Privacy-by-Design). Zudem muss er die Voreinstellungen, bspw. bei Apps oder Websites, so ausgestalten, dass die Bearbeitung der Personendaten auf das für den Verwendungszweck nötige Mindestmass beschränkt ist (Privacy-by-Default).

- **Ausbau der Informationspflichten:** Gemäss revDSG müssen der betroffenen Person bei der Beschaffung von Personendaten neu folgende Mindestinformationen mitgeteilt werden:
    - Identität und Kontaktdaten des Verantwortlichen;
    - Bearbeitungszweck;
    - Ggf. Empfängerinnen und Empfänger oder Kategorien von Empfängerinnen und Empfängern, denen Personendaten bekanntgegeben werden.

  Falls die Personendaten ins Ausland bekanntgegeben werden, müssen der betroffenen Person auch der Staat oder das internationale Organ und ggf. die Garantien zum Schutz der Personendaten mitgeteilt werden.
- **Ausbau der Auskunftspflichten:** Das revDSG sieht gegenüber dem geltenden DSG erweiterte Auskunftspflichten vor. Neu beschränkt sich die Auskunftspflicht nicht mehr auf die abschliessend definierten Mindestinformationen (worunter neu auch Angaben über Aufbewahrungsdauer, Auslandtransfers und automatisierte Einzelentscheide fallen), sondern umfasst jede Information, welche für die betroffene Person erforderlich ist, um ihre Rechte nach revDSG geltend zu machen. Immerhin gilt für die Auskunft über die „bearbeiteten Personendaten" neu ebenfalls, dass diese Daten „als solche" mitzuteilen bzw. herauszugeben sind. Damit dürfte klargestellt worden sein, dass der datenschutzrechtliche Auskunftsanspruch kein Recht auf Urkundenedition bzw. Aktenherausgabe darstellt.
- **Recht auf Datenübertragbarkeit:** Das revDSG sieht ein Recht auf Datenherausgabe und -übertragung („Datenportabilität") vor. Demnach kann die betroffene Person vom Verantwortlichen – in der Regel kostenlos – die Herausgabe ihrer Personendaten in einem gängigen elektronischen Format bzw. deren Übertragung an einen anderen Verantwortlichen verlangen, wenn der Verantwortliche die Daten automatisiert bearbeitet und die Daten mit der Einwilligung der betroffenen Person oder in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrages bearbeitet werden.
- **Automatisierte Einzelfallentscheidung:** Das revDSG sieht vor, dass der Verantwortliche die betroffene Person über eine Entscheidung, die ausschliesslich auf einer automatisierten Bearbeitung beruht und die für sie mit einer Rechtsfolge verbunden ist oder sie erheblich beeinträchtigt, informieren muss. Die betroffene Person muss die Möglichkeit haben, ihren Standpunkt darzulegen und kann verlangen, dass die Entscheidung von einer natürlichen Person überprüft wird. Dies gilt nicht, wenn die Entscheidung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags zwischen dem Verantwortlichen und der betroffenen Person steht und ihrem Begehren stattgegeben wird oder die betroffene Person ausdrücklich eingewilligt hat, dass die Entscheidung automatisiert erfolgt.

Wird über den Abschluss eines Leasingvertrags also ausschliesslich automatisiert entschieden, muss dem Antragsteller eine Möglichkeit zur Stellungnahme gegeben werden und er kann verlangen dass eine natürliche Person den Entscheid prüft, ausser, der Leasingantrag wird bewilligt oder der Antragsteller hat ausdrücklich eingewilligt, dass die Entscheidung automatisiert erfolgt.

- **Datenschutz-Folgenabschätzung:** Gemäss revDSG ist der Verantwortliche verpflichtet, eine Datenschutz-Folgenabschätzung vorzunehmen, wenn eine Datenbearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann. Ein solch hohes Risiko kann sich aus der Art, dem Umfang, den Umständen und dem Zweck der Bearbeitung ergeben. In einer Datenschutz-Folgenabschätzung müssen die geplante Bearbeitung und die damit entstehenden Risiken sowie geeigneten Massnahmen, um letzteren zu begegnen, umschrieben werden. Ausnahmen sind unter Umständen möglich, wenn der Verantwortliche einen Verhaltenskodex einhält.
- **Meldung von Verletzungen des Datenschutzes:** Verantwortliche haben dem EDÖB gemäss revDSG im Falle einer Datenschutzverletzung so rasch als möglich Meldung zu erstatten, wenn ein grosses Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen besteht. Der Verantwortliche muss – vorbehältlich gewisser Ausnahmen – auch die betroffene Person darüber informieren, wenn es zu ihrem Schutz erforderlich ist oder der EDÖB es verlangt. Der Auftragsbearbeiter muss eine Verletzung der Datensicherheit dem Verantwortlichen (nicht dem EDÖB und/oder dem Betroffenen) so rasch als möglich melden.
- **Sanktionen:** Gemäss revDSG können natürliche Personen insbesondere bei einer vorsätzlichen Verletzung der Informations- und Auskunftspflichten sowie bei einer vorsätzlichen Verletzung der Sorgfaltspflichten, neu mit einer Busse von bis zu CHF 250'000.00 (bisher max. CHF 10‘000.00) bestraft werden. Fehlende Datenschutz-Compliance birgt künftig also nicht nur Reputationsrisiken für die Unternehmen, sondern kann auch einschneidende strafrechtliche Konsequenzen für die fehlbaren Mitarbeiter persönlich mit sich bringen.

Webinar

Gerne machen wir Sie darauf aufmerksam, dass das Datenschutz-Webinar (in allen Landessprachen), welches der AGVS gemeinsam mit dem SLV ausgearbeitet hat, demnächst auf der Webseite verfügbar sein wird. Es soll Ihnen eine Übersicht über die wichtigsten datenschutzrechtlichen Grundlagen sowie die (neuen) Pflichten bei der Datenbearbeitung verschaffen und enthält Links auf Musterdokumente.

Trotzdem kann dieses Webinar selbstverständlich keine Rechtsberatung ersetzen, welche für die Überprüfung und ggf. Anpassung Ihrer Datenschutz-Konzepte erforderlich sein wird.