WENGERPLATTNER

Handels- und Gesellschaftsrecht / IP & IT – März 2021

Das revidierte Schweizer Datenschutzgesetz (DSG): Neuerungen und Auswirkungen auf Unternehmen

Autoren: Dr. Tobias Meili, Melanie Müller, Dr. Martina Braun

Das Schweizer Parlament hat im Herbst 2020 die Totalrevision des Schweizer Datenschutzgesetzes (DSG) verabschiedet. Das revidierte DSG tritt voraussichtlich Mitte 2022 in Kraft. Mit der Totalrevision soll das DSG an den rasanten technologischen Wandel, die geänderten gesellschaftlichen Verhältnisse sowie an die im Jahr 2018 in Kraft getretene Datenschutz-Grundverordnung der Europäischen Union (DSGVO) angepasst werden.

Die wichtigsten Aspekte im Überblick:

- **Weitergeltung der bisherigen Grundsätze der Datenbearbeitung.**
- **Rechtzeitige Löschung oder Anonymisierung von Personendaten bleibt wichtig.**
- **Einführung der Pflicht zur Führung eines Datenbearbeitungsverzeichnisses.**
- **Ausbau der Informationspflicht bei der Beschaffung von Personendaten.**
- **Erweiterte Vorgaben betreffend Auftragsdatenbearbeitung.**
- **Datenschutzverstösse können neu mit Bussen bis CHF 250'000 geahndet werden.**

Das revidierte Schweizer Datenschutzgesetz (DSG): Neuerungen und Auswirkungen auf Unternehmen

Personendaten sind ein wertvolles Gut. Aufgrund der stetigen Weiterentwicklung der Technologien und den damit verbundenen Möglichkeiten sowie der Einführung der DSGVO wurde es erforderlich, das Schweizer Datenschutzrecht den aktuellen Gegebenheiten anzupassen. Das revidierte DSG verstärkt den Datenschutz teilweise in erheblicher Hinsicht, was auch bei Schweizer Unternehmen zu Handlungsbedarf in Bezug auf interne Abläufe und Sicherheitsvorkehrungen führen dürfte.

Dr. Tobias Meili
Partner der Business Group Handels- und Gesellschaftsrecht sowie Immaterialgüter- und Technologierecht, Rechtsanwalt
tobias.meili@wenger-plattner.ch

Melanie Müller
Associate im Team Life Sciences und Gesundheitsrecht sowie Immaterialgüter- und Technologierecht, Rechtsanwältin
melanie.mueller@wenger-plattner.ch

Dr. Martina Braun
Senior Associate im Team Immaterialgüter- und Technologierecht, Rechtsanwältin
martina.braun@wenger-plattner.ch

Einleitung

Eine frühzeitige Auseinandersetzung mit den neuen Regelungen ist unerlässlich, denn das revidierte DSG enthält mit wenigen Ausnahmen keine Übergangsbestimmungen. Die meisten Neuerungen werden bei Inkrafttreten der Revision sofort anwendbar sein. Ausnahmen gelten lediglich im Bereich der technischen Massnahmen zur Sicherstellung des Datenschutzes (Privacy by Design und Privacy by Default) sowie der Datenschutzfolgeabschätzung (Data Privacy Impact Assessment / DPIA).

Geltungsbereich

Das DSG gilt unverändert für alle Unternehmen, welche Sitz in der Schweiz haben oder deren Datenbearbeitung sich in der Schweiz auswirken, und zwar unabhängig von Grösse, Rechtsform oder Art der Geschäftstätigkeit.

Gültigkeit bisheriger Grundsätze

Die bisherigen Grundsätze bleiben bestehen. Namentlich gilt im privaten Bereich (im Gegensatz zur Bearbeitung durch Bundesorgane) weiterhin das Prinzip, dass für die Bearbeitung von Personendaten grundsätzlich weder eine Einwilligung noch ein sonstiger Rechtfertigungsgrund erforderlich ist, dies im Unterschied zur DSGVO. Zudem müssen Daten vernichtet (bzw. datenschutzkonform gelöscht) oder anonymisiert werden, sobald sie zum Zweck der Bearbeitung nicht mehr notwendig sind. Diese Grundsätze ergeben sich – wie bereits bis anhin – aus der Notwendigkeit der Verhältnismässigkeit der Datenbearbeitung.

Wichtige Neuerungen im Überblick

Allgemein

Bisher ist das DSG auf natürliche und auf juristische Personen anwendbar. Neu wird sich dessen Geltungsbereich auf Daten natürlicher Personen beschränken, wie dies auch unter der DSGVO der Fall ist.

Datenschutzerklärung

Viele Unternehmen haben bereits unter der DSGVO eine Datenschutzerklärung ausgearbeitet. Aufgrund der erweiterten Informationspflichten wird eine solche auch unter dem revidierten DSG unerlässlich. Im Rahmen der DSGVO formulierte Datenschutzerklärungen sind meist sehr umfangreich, können aber mit entsprechenden Anpassungen verwendet werden. Neu wird gesetzlich vorgegeben, dass den betroffenen Personen bei Beschaffung von Personendaten folgende Angaben mitgeteilt werden müssen: Identität und Kontaktdaten des Verantwortlichen, Bearbeitungszweck, ggfs. Kategorien der Empfänger und der Daten sowie, bei Bekanntgabe der Personendaten ins Ausland, die Empfängerstaaten und ggfs. Schutzvorkehrungen (vgl. unten). Die Datenschutzerklärung kann z.B. auf der Unternehmenswebseite aufgeschaltet werden.

Brauche ich einen Data Protection Officer (DPO) in meinem Unternehmen?

Ein DPO oder Datenschutzbeauftragter (neu «Datenschutzberater») kann in gewissen Unternehmen notwendig sein, wenn z.B. die Datenbearbeitung zur Kerntätigkeit zählt. In der Schweiz kann ein Unternehmen einen Mitarbeiter oder Dritten als DPO bezeichnen. Wird ein DPO ernannt, ist dieser dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) zu melden und in der Datenschutzerklärung aufzuführen. Meist wird in einem Unternehmen eine Person damit betraut, sich generell um Fragen des Datenschutzes zu kümmern, diese gilt jedoch nicht automatisch als DPO.

Nach neuem Recht ist der Anreiz zur Ernennung eines DPO jedoch gering: Zwar muss ein Datenbearbeitungsvorhaben, welches nach erfolgter Datenschutzfolgeabschätzung noch immer ein «hohes Risiko» aufweist, nicht dem EDÖB vorgelegt werden, sofern der DPO für das Bearbeitungsvorhaben zuständig ist. Solche Fälle sind in der Praxis aber selten. Der bisherige Vorteil, dass durch die Ernennung eines DPO die Unternehmen ihre ansonsten registrierungspflichtigen Datensammlungen nicht mehr dem EDÖB melden müssen, entfällt unter dem revidiertem DSG.

Für Unternehmen, auf welche die DSGVO Anwendung findet, die aber nicht über eine Niederlassung in der EU verfügen, besteht i.d.R. eine Pflicht, einen Datenschutzvertreter in einem EU-Mitgliedsstaat zu ernennen. Dies, um den Aufsichtsbehörden eine faktische Zugriffsmöglichkeit auf die Datenbearbeitung bzw. das Unternehmen innerhalb der EU zu ermöglichen. Nach revidiertem DSG besteht teilweise auch für ausländische Unternehmen die Pflicht der Ernennung eines Vertreters in der Schweiz.

Betroffenenrechte

Auch unter dem revidierten DSG haben betroffene Personen das Recht, Auskunft über ihre Daten und Korrekturen derselben zu verlangen sowie einer Bearbeitung zu widersprechen. Die Ausübung der Betroffenenrechte ist grundsätzlich kostenlos. Bei einem Auskunftsersuchen muss das Unternehmen innert 30 Tagen antworten, die Abgabe einer Vollständigkeitserklärung ist jedoch nicht vorausgesetzt. Zudem sieht das revidierte DSG ein Recht auf Datenherausgabe oder -übertragung («Datenportabilität») vor, d.h. die betroffene Person kann unter gewissen Bedingungen die Herausgabe bzw. Übertragung ihrer Personendaten in einem gängigen elektronischen Format verlangen.

Bearbeitungsverzeichnis

Wie gemäss DSGVO, wird neu auch unter dem revidierten DSG die Führung eines Verzeichnisses im Sinne eines Inventars verlangt, welches die unterschiedlichen Bearbeitungstätigkeiten erfasst. Wurde bereits ein Verzeichnis gemäss den Vorgaben der DSGVO errichtet, genügt dies auch den Voraussetzungen nach revidiertem DSG. Wie das Verzeichnis formal ausgestaltet wird, ist dabei den Unternehmen überlassen, z.B. genügt eine Excel-Tabelle. Der Mindestinhalt des Verzeichnisses wird dahingegen vom Gesetz vorgegeben. Das Verzeichnis hat für jede Datenbearbeitung mind. folgende Angaben zu enthalten: Identität des Verantwortlichen und ggfs. Auftragsdatenbearbeiters, Zweck der Bearbeitung, Kategorien der betroffenen Personen und der bearbeiteten Personendaten, Kategorien der Empfänger, Aufbewahrungsdauer oder Datenschutzmassnahmen und ggfs. Empfängerstaaten und Angaben betreffend Schutzmassnahmen.

Auslandtransfer

Gemäss revidiertem DSG dürfen Personendaten ins Ausland bekannt gegeben werden, wenn die Gesetzgebung des betreffenden Staates ein angemessenes Schutzniveau gewährleistet. Ein Datentransfer in sog. «unsichere» Drittstaaten ist lediglich zulässig, wenn anderweitig ein gleichwertiger Datenschutz sichergestellt wird. Dies entspricht im Grundsatz der bisherigen Regelung. Neu legt der Bundesrat und nicht mehr der EDÖB fest, welche Länder als sicher gelten. Bezüglich der möglichen Schutzmassnahmen bei Bekanntgabe in «unsichere Länder», entspricht das revidierte DSG weitgehend der DSGVO. Als anerkannte besondere Schutzvorkehrungen gelten z.B. die vom EDÖB genehmigten Standard-Vertragsklauseln oder konzernweite sog. Binding Corporate Rules (BCR).

Auftragsbearbeitung

Wer als Verantwortlicher einem Dritten (z.B. Dienstleister) die Bearbeitung von Personendaten überträgt, muss mit diesem einen Vertrag abschliessen. Ein solcher Vertrag muss die Weisungsrechte und Kontrollrechte des Auftraggebers gegenüber dem betreffenden Dritten sowie die Gewährleistung der Datensicherheit regeln. Neu ist der Beizug eines Unterauftragsbearbeiters nur mit Genehmigung des Auftraggebers zulässig.

Data Breach Notification

Nach revidiertem DSG haben Verantwortliche dem EDÖB eine Datenschutzverletzung so rasch als möglich zu melden, sofern ein hohes Risiko für die Betroffenen besteht. Zusätzlich müssen sie die Betroffenen informieren, wenn dies zu deren Schutz erforderlich ist. Es empfiehlt sich, eine konkrete Stelle im Unternehmen zu bestimmen, an welche Mitarbeiter Vorfälle melden müssen.

Sicherheitsmassnahmen

Die bereits unter der DSGVO anwendbaren Prinzipien Datenschutz durch Technik (Privacy by Design) und datenschutzfreundliche Voreinstellungen (Privacy by Default) sind neu ausdrücklich im revidierten DSG verankert, d.h. der Verantwortliche muss – wie bis anhin – bemüht sein, angemessene technische und organisatorische Datenschutzmassnahmen zu treffen.

«Die erforderlichen Massnahmen, um Ihr Unternehmen den Neuerungen des DSG anzupassen, sollten möglichst frühzeitig in Angriff genommen werden, da nach Inkrafttreten des revidierten DSG nur hinsichtlich einzelner neuen Pflichten eine Übergangsfrist vorgesehen ist.»

Haftung

Untersuchungsverfahren wegen Verstössen gegen datenschutzrechtliche Bestimmungen richten sich gegen die für die betreffende Datenbearbeitung verantwortliche Person. Im Gegensatz zur DSGVO richten sich die Bussen nicht gegen das jeweilige Unternehmen. Die Strafbestimmungen wurden im revidierten DSG deutlich ausgebaut und der Bussenrahmen für Datenschutzverstösse wurde neu auf CHF 250'000.00 erhöht. Nach teilweise vertretener Auffassung können solche Bussen – aufgrund ihrer persönlichen Natur – weder versichert werden, noch darf das Unternehmen sie für die natürliche Person bezahlen.

Zu ergreifende Massnahmen

Um die neuen Massnahmen umzusetzen, ist in einem ersten Schritt im Sinne einer Auslegeordnung zu ermitteln, welche Personendaten, zu welchen Zwecken, wie, wo und von wem erhoben und bearbeitet werden. Auch sind die bestehenden Datenschutzmassnahmen und Prozesse zu dokumentieren. In einem nächsten Schritt ist zu prüfen, ob bzw. welche Lücken nach Massgabe des revidierten DSG bestehen. Sodann sind, anhand eines risikobasierten Ansatzes, die notwendigen Massnahmen zu ergreifen, beispielsweise:

- Umsetzung der Informationspflichten mittels Erstellung bzw. Anpassung von Datenschutzerklärungen;
- Erarbeitung eines Datenbearbeitungsverzeichnisses;
- Abschluss bzw. Anpassung von Verträgen mit Auftragsbearbeitern;
- Festlegung von internen Prozessen und Zuständigkeiten zur Sicherstellung der Betroffenenrechte (Recht auf Information, Auskunft, Berichtigung, Löschung und Widerspruch) und Ausarbeitung von internen Weisungen und allfälligen Mustervorlagen (z.B. zur Beantwortung einer Datenschutzanfrage);
- Implementierung von Verfahren und Zuständigkeiten bei Verletzungen des Datenschutzes.

Schliesslich sind die kontinuierliche Umsetzung und Aufrechterhaltung der implementierten Massnahmen und Prozesse sicherzustellen. Unabdingbar hierfür ist, (i) unternehmensintern verantwortliche Personen zu benennen, (ii) diese mit ausreichenden Ressourcen auszustatten und (iii) alle Mitarbeiter nach Massgabe ihres Aufgabenprofils und der damit einhergehenden «Nähe» zur Bearbeitung von Personendaten stufengerecht und praxisorientiert zu schulen und zu unterstützen.

Praktische Empfehlungen

Unternehmen müssen sich darauf einstellen, dass dem Datenschutz in Zukunft noch grössere Aufmerksamkeit zuteil werden wird. Nehmen Sie diese Gesetzesrevision zum Anlass, die Datenbearbeitungen Ihres Unternehmens risikobasiert auf deren Konformität mit dem revidierten DSG hin zu überprüfen. Beginnen Sie frühzeitig mit den Umsetzungsarbeiten, da nach Inkrafttreten des Gesetzes nur hinsichtlich einzelner neuen Pflichten eine Übergangsfrist besteht, und involvieren Sie von Anfang an die Fachverantwortlichen der relevanten Bereiche (namentlich IT, Marketing und HR), in welchen typischerweise Personendaten bearbeitet werden, sowie Vertreter von Legal & Compliance.

Basel: Aeschenvorstadt 55 | CH-4010 Basel | T +41 61 279 70 00 | basel@wenger-plattner.ch
Zürich: Seestrasse 39 | CH-8700 Küsnacht-Zürich | T +41 43 222 38 00 | zuerich@wenger-plattner.ch
Bern: Jungfraustrasse 1 | CH-3000 Bern 6 | T +41 31 357 00 00 | bern@wenger-plattner.ch

www.wenger-plattner.ch