epartners Rechtsanwälte AG
Puls 5 | Hardturmstrasse 11 | CH-8005 Zürich
T +41 43 268 8777 | F +41 43 268 8779
www.epartners.ch

epartners
Rechtsanwälte
Attorneys-at-Law

Dr. Urs Egli und Marius Vischer
Januar 2022

e:1.22

DAS REVIDIERTE DATENSCHUTZGESETZ – EINE ÜBERSICHT ÜBER NEUERUNGEN UND ZU ERGREIFENDE MASSNAHMEN

Die Schweiz wird demnächst ein neues, revidiertes Datenschutzgesetz (DSG) einführen. Für Unternehmen, welche noch kein Compliance-Programm zur europäischen Datenschutzgrundverordnung (DSGVO) durchlaufen haben, erfordert die Revision einen Ausbau ihrer Governance. Zudem sollten alle Unternehmen ihre Datenschutzerklärungen überprüfen. Am Schluss dieses Beitrages liefern wir eine Checkliste mit zu ergreifenden Massnahmen im Hinblick auf die Revision. Die Verletzung einiger Bestimmungen des DSG kann Bussen für die handelnden Personen zur Folge haben.

Revision des Datenschutzgesetzes

Am 25. Mai 2018 ist die europäische Datenschutzgrundverordnung (DSGVO) in Kraft getreten. Dies und die technologische Entwicklung seit der letzten grösseren Revision 2008 haben den schweizerischen Gesetzgeber veranlasst, das eidgenössische Datenschutzgesetz (DSG) umfassend zu revidieren. Das DSG gilt für private Unternehmen sowie die Bundesbehörden. Für die kantonalen Behörden und Institutionen gelten die kantonalen Datenschutzgesetze.

Das DSG hat zwingend Geltung, die Betroffenen können also nicht mittels Vereinbarung davon abweichen. Es schreibt einerseits vor, welche Regeln bei der Bearbeitung von Personendaten einzuhalten sind und regelt andererseits die Rechte derjenigen Personen, deren Daten bearbeitet werden. Einzelne Vorschriften des DSG sind als Straftatbestände ausgestaltet, d.h. der Verstoss hat auch eine Bestrafung zur Folge.

Das revidierte DSG wird am 1. September 2023 in Kraft treten. Das DSG wurde im Rahmen der Revision umfassend überarbeitet und neu gegliedert. Die Grundprinzipien des geltenden DSG bleiben dabei erhalten, das Gesetz wird jedoch in weiten Teilen der DSGVO angeglichen. Im Folgenden werden die wesentlichen Neuerungen des DSG dargestellt, soweit sie für private Unternehmen mit einem Geschäftssitz in der Schweiz relevant sind. Für Bundesbehörden gelten teilweise zusätzliche Bestimmungen, auf welche in diesem Fokus-Beitrag jedoch nicht eingegangen wird.

Neue Terminologie

Der bisherige "Inhaber der Datensammlung" wird neu als "Verantwortlicher" bezeichnet und die Person, deren Daten bearbeitet werden, als "betroffene Person". Unternehmen, welche im Auftrag des Verantwortlichen Personendaten bearbeiten, sind "Auftragsbearbeiter" (unter der DSGVO "Auftragsverarbeiter"). Der

Vertrag zwischen dem Verantwortlichen um dem Auftragsbearbeiter wird unter der DSGVO als "Auftragsdatenverarbeitungsvertrag" ("*Data Processing Agreement*") bezeichnet; ob sich diesbezüglich in der Schweiz die Bezeichnung "Auftragsdatenbearbeitungsvertrag" durchsetzen wird, wird sich zeigen.

Wichtige Regeln zum Datenschutz, die weiterhin gelten

Auch unter dem revidierten DSG (nachfolgend revDSG) gilt weiterhin, was folgt:

Geschützt durch das DSG sind nur Personendaten, d.h. Daten, die sich auf eine bestimmte oder bestimmbare Person beziehen. Pseudonymisierte oder verschlüsselte Daten sind nur für diejenigen Verantwortlichen oder Auftragsbearbeiter Personendaten, welche den Personenbezug herstellen können. Deshalb ist eine Übergabe verschlüsselter Daten an einen Auftragsbearbeiter im Ausland auch kein Datenexport, solange der Auftragsbearbeiter keinen Zugang zum Schlüssel hat.

Eine Anonymisierung von Daten kann nicht oder nur noch mit unverhältnismässigen Mitteln wieder aufgehoben werden, deshalb sind auch anonymisierte Daten keine Personendaten, denn auch hier fehlt der Personenbezug. Das Anonymisieren von Daten ist datenschutzrechtlich letztlich mit dem Löschen von Daten gleichzusetzen.

Datenbearbeitungen im privaten Bereich sind grundsätzlich zulässig und es braucht dafür weder eine Einwilligung noch einen anderen Rechtfertigungsgrund. Im Unterschied zur Regelung unter der DSGVO, wo immer ein Rechtfertigungsgrund erforderlich ist, braucht es in der Schweiz einen solchen erst dann, wenn entweder die Bearbeitungsgrundsätze oder die Bestimmungen zur Datensicherheit nicht eingehalten werden oder wenn die betroffene Person der Bearbeitung widerspricht. In diesem Fall handelt es sich bei der Datenbearbeitung um eine Persönlichkeitsverletzung, die nur mit Vorliegen eines Rechtfertigungsgrundes rechtmässig erfolgen kann.

Die Bearbeitungsgrundsätze sind (Art. 6 revDSG):

- Rechtmässigkeit;
- Verhältnismässigkeit;
- Zweckbindung und Erkennbarkeit der Datenbearbeitung; sowie
- Datenrichtigkeit.

Die Rechtfertigungsgründe sind (Art. 31 revDSG):

- Einwilligung;
- überwiegendes privates Interesse des Verantwortlichen; oder
- überwiegendes öffentliches Interesse.

Die betroffene Person hat das Recht, vom Verantwortlichen Auskunft darüber zu verlangen, ob und welche Personendaten über sie bearbeitet werden. Art. 25 revDSG beschreibt den Inhalt der Auskunft ausführlicher als unter dem bisherigen Recht. Die Auskunft kann verweigert werden, wenn das Begehren querulatorisch oder offensichtlich unbegründet ist, d.h. einen datenschutzwidrigen Zweck verfolgt. Mit dieser Präzisierung ist fraglich, ob das Datenschutzrecht weiterhin zur Beweismittelbeschaffung missbraucht werden kann, wie das unter dem bisherigen Recht aufgrund der bundesgerichtlichen Rechtsprechung dazu der Fall war,

welche den Auskunftsrechten der betroffenen Person eine grosse Bedeutung einräumt.

Die betroffene Person hat ein Widerspruchsrecht gegen die Bearbeitung ihrer Daten (Art. 30 Abs. Bst. b revDSG). Mit der Ausübung des Widerspruchs wird die weitere Bearbeitung ihrer Personendaten unzulässig, es sei denn, der Verantwortliche habe einen Rechtfertigungsgrund. Dieses Widerspruchsrecht ist gleichzeitig auch die schweizerische Umsetzung des gemäss DSGVO vorgesehenen Rechtes auf Vergessen.

Die betroffene Person hat einen Berichtigungsanspruch hinsichtlich unrichtiger Daten sowie einen Löschungsanspruch (Art. 32 revDSG).

Datenschutzerklärung

Die Informationspflichten bei der Beschaffung von Personendaten werden im neuen DSG erheblich ausgebaut (Art. 19 revDSG). Sie bestehen nunmehr generell und nicht mehr nur bei der Beschaffung von besonders schützenswerten Personendaten. Informiert werden muss neben der Information über die Beschaffung selbst über die Identität und die Kontaktdaten des Verantwortlichen, den Bearbeitungszweck, die Empfänger von Personendaten sowie beim Datenexport ins Ausland über den Staat, in welchem die Datenbearbeitung erfolgt. Mit Empfänger sind Dritte gemeint, die auf Daten Zugriff erhalten, wobei es ausreicht, diese als Kategorie zu bezeichnen (z.B. Bekanntgabe an Auftragsbearbeiter oder Konzerngesellschaften). Die Form der Information ist nicht vorgeschrieben. In der Regel wird der Informationspflicht mit einer generellen oder mehreren spezifischen Datenschutzerklärungen genüge getan. Datenschutzerklärungen sind über die Webseite verfügbar zu machen und in AGB oder anderen Unterlagen kann mittels eines Links darauf verwiesen werden.

Bearbeitungsverzeichnis

Verantwortliche müssen neu ein Verzeichnis der Bearbeitungstätigkeiten führen (Art. 12 revDSG; unter der DSGVO "Verarbeitungsverzeichnis" genannt). Unternehmen mit weniger als 250 Mitarbeitenden sind von dieser Pflicht ausgenommen, sofern sie nicht umfangreich besonders schützenswerte Personendaten bearbeiten oder ein Profiling mit hohem Risiko vornehmen.

Verzeichnisse, welche bereits unter der DSGVO erstellt wurden, können übernommen werden. Wie stark das Verzeichnis nach einzelnen Bearbeitungstätigkeiten aufgegliedert werden muss, schreibt das revDSG nicht vor. Es wird empfohlen, sachlich zusammenhängende Bearbeitungen zusammenzufassen (z.B. Personaladministration, Rekrutierung, Kundendatenverwaltung, Kundendienst, Onlineshop, Newsletter, Produkteentwicklung, Lieferantenverwaltung, Finanz- und Rechnungswesen, Auswertung der Webseitennutzung, Videoüberwachung, Gebäudemanagement, Finanz- und Rechnungswesen und E-Mail). Der Inhalt des Verzeichnisses ergibt sich aus Art. 12 Abs. 2 und 3 revDSG. Eine besondere Form des Verzeichnisses ist nicht vorgeschrieben. Es kann als Excel- oder Worddatei oder in der Form einer dedizierten IT-Lösung geführt werden.

Auch Auftragsbearbeiter müssen ein eigenes Verzeichnis führen. Als eine der Bearbeitungstätigkeiten sind dort die im Auftrag der Verantwortlichen ausgeführten Leistungen in allgemeiner Form aufzuführen (z.B. Erbringung von IT-Betriebsleistungen für Kunden).

Ausbau der Vorschriften zur Datensicherheit

Wie bisher müssen der Verantwortliche und allfällige Auftragsbearbeiter durch geeignete technische oder organisatorische Massnahmen eine dem Risiko angemessene Datensicherheit gewährleisten (Art. 8 revDSG). Die Mindestanforderungen an die Datensicherheit werden in einer Verordnung des Bundesrates beschrieben, welche erst im Entwurf vorliegt. Die Verordnung verlangt vom Verantwortlichen, diejenigen technischen und organisatorischen Massnahmen zu ergreifen, welche in Anbetracht des Zwecks der Datenbearbeitung, des Risikos, dem Stand der Technik und der Implementierungskosten erforderlich und angemessen sind. Die Verordnung führt einzelne Schutzziele auf (Zugriffskontrollen, Zugangskontrollen, Datenträgerkontrollen, Speicherkontrollen, Benutzerkontrollen etc.). Was eine angemessene Datensicherheit ist, müssen die betroffenen Unternehmen somit selbst entscheiden. Sie tun gut daran, ihre diesbezüglichen Überlegungen zu dokumentieren, insbesondere mit Blick auf die Strafbestimmung von Art. 61 Bst. c revDSG, welche die Nichteinhaltung der Mindestanforderungen unter Strafe stellt.

Auftragsbearbeitung

Die Auftragsbearbeitung ist nur zulässig, wenn sie vertraglich abgesichert ist (Art. 9 revDSG). Neu darf der Auftragsbearbeiter die Bearbeitung zudem nur mit vorgängiger Genehmigung des Verantwortlichen einem Unterbeauftragten übertragen (Art. 9 Abs. 3 revDSG). Beide Vorschriften wurden von der DSGVO übernommen und stellen auch in der Schweiz bereits weitgehend Standard dar.

Datenexport

Personendaten dürfen nach wie vor nur in Länder bekanntgegeben werden, deren Gesetzgebung einen angemessenen Datenschutz gewährleistet (Art. 16 revDSG). In andere Länder ist ein Datenexport nur mit flankierenden Massnahmen zulässig. Am einfachsten ist es, die vom Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) genehmigten Standardvertragsklauseln der Europäischen Kommission zu verwenden. Die Standardvertragsklauseln sind modular aufgebaut; je nach Konstellation sind andere Module zu verwenden. Werden Personendaten von einem Schweizer Verantwortlichen an einen ausländischen Auftragsbearbeiter bekanntgegeben, ist bspw. Modul 2 zu verwenden. Verwenden Parteien die Standardvertragsklauseln, entfällt die Pflicht zur Mitteilung des Datenexports an den EDÖB, wie sie noch unter dem bisherigen DSG vorgesehen war. Der EDÖB schreibt jedoch vor, dass jeweils im Einzelfall geprüft wird, ob die Standardvertragsklauseln eine genügende Sicherheit darstellen oder ob im Einzelfall darüberhinausgehende Regelungen notwendig sind (sog. *Transfer Impact Assessment*). Auch hier empfiehlt es sich, die entsprechenden Überlegungen zu dokumentieren.

Werden keine solchen genehmigten Standardvertragsklauseln verwendet, so muss der dem Export zugrunde liegende Vertrag dem EDÖB mitgeteilt werden (eine Genehmigung ist nicht erforderlich). Weiter besteht die Möglichkeit zum Erlass unternehmensinterner Datenschutzvorschriften (sog. *Binding Corporate Rules*), welche jedoch vom EDÖB vorgängig zu genehmigen sind. Und schliesslich darf ein Datenexport erfolgen, wenn er unmittelbar im Zusammenhang mit dem Vertragsabschluss oder der Vertragsabwicklung steht (z.B. Bekanntgabe des Zahlungsempfängers bei Banküberweisungen) oder die Zustimmung der betroffenen Person vorliegt (Art. 17 revDSG).

Datenschutz-Folgeabschätzungen

Wenn Verantwortliche Datenbearbeitungen planen, welche potentiell ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen können, müssen sie vorgängig eine Datenschutz-Folgeabschätzung durchführen. Beispiele für Datenbearbeitungen mit hohem Risiko sind die Einführung eines Flottenmanagementsystems mit einer Echtzeitüberwachung der Fahrzeugstandorte, der Aufbau einer Bewerberdatenbank mit potentiellen Stelleninteressenten durch eine HR-Abteilung oder der Unterhalt einer umfassenden Kundendatenbank durch einen Online-Händler. Bei der Datenschutzfolgeabschätzung handelt es sich um eine datenschutzrechtliche Selbstbeurteilung. Gegenstand sind eine Analyse der potentiellen negativen Folgen unter Berücksichtigung der Eintretenswahrscheinlichkeit, der möglichen Massnahmen zur Verhinderung der negativen Auswirkungen sowie der Einhaltung des DSG. Kann ein identifiziertes hohes Risiko mit Gegenmassnahmen nicht ausgeschlossen werden, muss das Vorhaben dem EDÖB (oder dem Datenschutzberater) zur Konsultation vorgelegt werden.

Meldepflichten für Verletzungen der Datensicherheit

Verletzungen der Datensicherheit muss der Verantwortliche dem EDÖB melden, wenn sie zu einem hohen Risiko für die Persönlichkeit oder der Grundrechte der betroffenen Person führen. Solche Verletzungen der Datensicherheit sind z.B. Hackerangriffe, E-Mail-Versand mit heiklen Daten an einen falschen Abnehmerkreis, Fehlmanipulationen, Systemfehler oder Zugriffe ausländischer Behörden auf Daten in der Cloud. Ob ein hohes Risiko besteht, muss der Verantwortliche im Einzelfall entscheiden. Beispiele für ein hohes Risiko sind der Diebstahl von Passwörtern bei einem Hackerangriff auf einen Online-Shop, die Entwendung von Kundendaten durch einen Bankmitarbeiter oder der Verlust eines Endgeräts mit Zugang zu vertraulichen Daten.

Die Meldepflicht betrifft den Verantwortlichen. Die Information des EDÖB hat raschestmöglich zu erfolgen. Eine besondere Frist besteht jedoch im Unterschied zur DSGVO (dort 72 Stunden) nicht.

Der Auftragsbearbeiter hat eine eigene, viel weitergehende Meldepflicht, denn er muss jede Verletzung der Datensicherheit melden, nicht nur solche mit hohem Risiko. Seine Meldepflicht besteht jedoch gegenüber dem Verantwortlichen und nicht gegenüber dem EDÖB. Es handelt sich um eine gesetzliche Pflicht, die vertraglich weder wegbedungen noch eingeschränkt werden kann.

Übrige Melde- und Registrierungspflichten

Die Registrierungspflicht für Datensammlungen wurde abgeschafft. Ebenfalls abgeschafft wurde die Pflicht, den Export von Daten ins Ausland dem EDÖB immer dann zu melden, wenn das Zielland über keinen angemessenen Datenschutz verfügt. Hingegen müssen die verwendeten Standardvertragsklauseln dem EDÖB gemeldet werden, sofern sie von diesem nicht bereits genehmigt wurden, was bei den Standardvertragsklauseln der Europäischen Kommission jedoch der Fall ist.

Weiter müssen dem EDÖB die Ernennung eines Datenschutzberaters (was jedoch nicht zwingend erforderlich ist) oder gegebenenfalls eines Vertreters für ausländische Verantwortliche gemeldet werden. Zudem besteht unter Umständen eine

Konsultationspflicht des EDÖB im Zusammenhang mit Datenschutz-Folgeabschätzungen.

Einwilligung

Eine Einwilligung der betroffenen Person für die Datenbearbeitung durch Private ist in einigen Situationen erforderlich. Die zwei wichtigsten Konstellationen sind: Datenexport in ein Land ohne angemessenen Datenschutz, ohne dass gleichzeitig flankierende Massnahmen ergriffen werden (Art. 17 Abs. 1 Bst. a revDSG) und persönlichkeitsverletzende Datenbearbeitungen (Art. 31 Abs. 1 revDSG). Die Einwilligung muss ausdrücklich sein. Schriftlichkeit ist nicht erforderlich.

Allgemeine berufliche Schweigepflicht

Mit Art. 62 revDSG wurde eine allgemeine Schweigepflicht für sämtliche Berufstätigen eingeführt, welche von Personendaten in Ausübung ihres Berufes oder während der Ausbildung Kenntnis erhalten. Wer solche Personendaten vorsätzlich offenbart, wird bestraft.

Weitere Neuerungen

In Angleichung an die DSGVO enthält das DSG die folgenden weiteren Neuerungen, die aus heutiger Sicht vorerst noch eher wenig praktische Relevanz haben, resp. nur eine kleine Minderheit der Unternehmen betreffen:

Profiling ist eine automatisierte Datenbearbeitung, welche bestimmte Aspekte der Persönlichkeit bewertet. Erlaubt eine Verknüpfung solcher Daten die Beurteilung wesentlicher Aspekte der Persönlichkeit, dann liegt ein Profiling mit hohem Risiko vor, wofür es eine ausdrückliche Einwilligung braucht (Art. 6 Abs. 7 Bst. b revDSG).

Automatisierte Einzelentscheide sind Entscheidungen, die ausschliesslich von einer Maschine getroffen werden und welche die betroffene Person erheblich beeinträchtigen. Beispiele sind die automatische Bewerber-(Vor)Selektion oder die Kreditvergabe. Über solche Entscheidungen ist die betroffene Person zu informieren und es ist ihr die Möglichkeit zu geben, dass der getroffene Entscheid von einer natürlichen Person überprüft wird (Art. 21 revDSG).

Gemäss Art. 28 revDSG kann eine betroffene Person die Herausgabe von Daten verlangen, die vom Verantwortlichen automatisiert und in Abwicklung eines Vertrags mit der betroffenen Person bearbeitet werden. Das ursprüngliche Ziel dieser Bestimmung war, es den Nutzern von Social Media zu ermöglichen, zu einem anderen Anbieter zu wechseln. Wie sehr diese Regelung auch auf andere Sachverhalte Anwendung finden wird (z.B. klassischer Cloud Provider), wird sich zeigen.

Ein Datenschutzberater gemäss Art. 10 revDSG ist als Anlaufstelle für die betroffenen Personen und die Behörden gedacht. Er berät den Verantwortlichen bei Fragen des Datenschutzes und führt Schulungen durch. Anders als unter der DSGVO ist die Ernennung eines Datenschutzberaters gemäss revDSG für private Verantwortliche freiwillig. Der einzige konkret greifbare Vorteil eines Datenschutzberaters ist, dass die Konsultation des EDÖB entfällt, wenn sich aus einer Datenschutz-Folgeabschätzung ein hohes Risiko ergeben sollte.

Ausländische Verantwortliche ohne Sitz oder Wohnsitz in der Schweiz müssen unter bestimmten Umständen eine Vertretung in der Schweiz für Datenschutzfragen bezeichnen (Art. 14 revDSG).

Strafbestimmungen

Besonders wichtige Pflichten des revDSG geniessen auch strafrechtlichen Schutz. Wer gegen solche Bestimmungen verstösst, wird mit einer Busse bis zu CHF 250'000 bestraft. Die Strafen richten sich an die handelnden natürlichen Personen, z.B. an eine Führungsperson oder einen Datenschutzberater. Strafbar ist nur die vorsätzliche Tatbegehung. Das Unternehmen selber kann nur ausnahmsweise gebüsst werden, wenn die Ermittlung der verantwortlichen natürlichen Person mit unverhältnismässigem Aufwand verbunden wäre (Art. 64 revDSG).

Folgende Verletzungen des DSG stehen unter Strafe:

- Erteilung einer falschen oder unvollständigen Auskunft auf ein Auskunftsbegehren einer betroffenen Person;
- Unterlassung der Information der betroffenen Person bei der Datenbeschaffung oder bei automatisierten Einzelentscheidungen;
- Datenexport ins Ausland, ohne dass die Voraussetzungen dafür erfüllt sind;
- Übergabe von Daten an einen Auftragsbearbeiter, ohne dass die Voraussetzungen dafür erfüllt sind (insb. ohne Vertrag);
- Nichteinhaltung der Mindestanforderungen des Bundesrates für die Datensicherheit;
- Verletzung der beruflichen Schweigepflicht;
- Missachtung einer Verfügung des EDÖB, sofern diese einen Hinweis auf die Strafbarkeit enthält.

Übergangsregeln

Datenbearbeitungen, die bisher erlaubt waren, werden grundsätzlich auch nach dem Inkrafttreten des revDSG erlaubt sein. Es ist auch nicht notwendig, für bereits praktizierte Datenbearbeitungen bei Inkrafttreten des revDSG eine Datenschutz-Folgeabschätzung durchzuführen. Hingegen müssen die Datenschutzorganisation sowie die Datenschutzerklärung den neuen Anforderungen des DSG angepasst werden.

Die Vorgaben des revDSG sind unmittelbar mit dessen Inkrafttreten einzuhalten. Es wird keine Übergangsfrist geben.

Empfehlungen

Wir empfehlen privaten Unternehmen folgende Massnahmen im Hinblick auf das Inkrafttreten des revDSG:

- Überprüfung und Anpassung der Datenschutzerklärung(en);
- Bestimmung der organisatorischen Verantwortlichkeiten für den Datenschutz;
- Dokumentation der Massnahmen für die Gewährleistung der Datensicherheit;
- Erstellung eines Verarbeitungsverzeichnisses, sofern ein solches notwendig ist;
- Sicherstellung, dass alle Auftragsbearbeitungen vertraglich abgesichert sind;
- Sicherstellung, dass alle Datentransfers in unsichere Drittländer identifiziert und vertraglich abgesichert sind;
- Definition der Prozesse zur Bearbeitung von Auskunfts-, Berichtigungs- und Löschungsbegehren und von Widersprüchen zur Datenbearbeitung;

- Definition der Prozesse für Datenschutz-Folgeabschätzungen;
- Definition der Prozesse zur Meldung von Verletzungen der Datensicherheit;
- Definition der Prozesse zur Löschung und Archivierung von Daten;
- Information der betroffenen Mitarbeitenden über ihre berufliche Schweigepflicht.

Auch empfehlen wir privaten Unternehmen, die Verantwortlichkeiten und Prozesse im Zusammenhang mit dem Datenschutz in geeigneter Form zu dokumentieren (Reglement und/oder VR-Beschluss).

Für Unternehmen, welche ihre Organisation bereits der DSGVO angepasst haben, bringt das revDSG wenige Neuerungen mit sich, denn solche Unternehmen sollten diese Massnahmen bereits umgesetzt haben.

Wir unterstützen Sie gerne bei der Umsetzung der oben aufgeführten Massnahmen sowie bei der Durchführung von internen Schulungen zum Datenschutz.

epartners Rechtsanwälte AG