



Das revidierte Datenschutzrecht – was ist zu tun?

Am 1. September 2023 tritt das revidierte Datenschutzrecht (neues DSG) ohne Übergangsfristen in Kraft. Das neue Gesetz orientiert sich zwar weitgehend an der EU-Datenschutzgrundverordnung (EU-DSGVO), dennoch gilt gewisse Besonderheiten zu beachten. Bei einer Verletzung des neuen DSG werden die Bussen grundsätzlich nicht wie bei der EU-DSGVO den Unternehmen, sondern den für das Unternehmen handelnden Personen auferlegt. Dieser Beitrag zeigt die wichtigsten Änderungen des neuen DSG und den damit verbundenen Handlungsbedarf auf.

Schutz der Daten von natürlichen Personen

Das neue DSG schützt nur noch Personendaten von natürlichen Personen. Es wird zwischen normalen Personendaten (alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen) und besonders schützenswerten Personendaten (z.B. unterschiedliche Daten über religiöse, politische oder gewerkschaftliche Ansichten oder Tätigkeiten, Gesundheitsdaten, biometrische Daten, Daten über verwaltungs- oder strafrechtliche Verfolgung, Daten über Sozialhilfemassnahmen) unterschieden.

Unterstellung von ausländischen Gesellschaften unter das neue DSG

Das neue DSG hat, wie die meisten modernen Datenschutzgesetze, eine extraterritoriale Wirkung. Es ist also nicht nur für Unternehmen mit Sitz in der Schweiz anwendbar, sondern gilt auch für ausländische Unternehmen, die bspw. Kunden in der Schweiz betreuen oder Mitarbeitende mit Wohnsitz in der Schweiz beschäftigen.

Zudem müssen ausländische Unternehmen einen Vertreter in der Schweiz bestellen, sofern die Bearbeitung der Personendaten im Zusammenhang mit dem Angebot von Waren und Dienstleistungen oder der Beobachtung des Verhaltens von Personen in der Schweiz steht, regelmässig und umfangreich Personendaten bearbeitet werden und die Bearbeitung ein hohes Risiko mit sich bringt.

Strafbestimmungen des neuen DSG

Bei einer Widerhandlung gegen das neue DSG kann die

handelnde Person mit einer Busse von maximal CHF 250'000 bestraft werden. Dies gilt auch, wenn die Widerhandlung beim Handeln für eine juristische Person oder im Rahmen von geschäftlichen oder dienstlichen Tätigkeiten begangen worden ist. Sollte es der Arbeitgeber vorsätzlich oder fahrlässig unterlassen, eine Widerhandlung der Mitarbeitenden zu verhindern, gelten die Strafbestimmungen des neuen DSG auch für den Arbeitgeber. Ist der Arbeitgeber eine juristische Person, haften die Organe, die Organmitglieder oder die Geschäftsleitung persönlich für die Widerhandlung gegen das neue DSG. Anstelle der Organe oder der Geschäftsleitung kann auch die Gesellschaft als Arbeitgeberin mit einer Busse bestraft werden, sofern die Busse maximal CHF 50'000 beträgt.

Um das Bussenrisiko für Unternehmen, Arbeitgeber und Organe zu minimieren, sollte mit geeigneten Massnahmen einer Verletzung des neuen DSG durch die Mitarbeitenden vorgebeugt werden. Zu empfehlen ist deshalb eine regelmässige Schulung der Mitarbeitenden, die Personendaten bearbeiten.

Weitere Pflichten des neuen DSG

a) Grundsätze der Bearbeitung

Werden Personendaten bearbeitet, so dürfen diese ausschliesslich rechtmässig, verhältnismässig sowie für einen bestimmten Zweck bearbeitet werden. Die Bearbeitungen sind technisch und organisatorisch derart auszugestalten, dass das Risiko für die betroffenen Personen angemessen ist, d.h. es ist für eine angemessene Datensicherheit zu sorgen.



**b) Information bei Beschaffung von Personendaten
(Art. 19 revDSG)**

Bei Erhebung der Personendaten müssen die betroffenen Personen angemessen über die Beschaffung der Daten, die Identität des Verantwortlichen sowie den Bearbeitungszweck informiert werden. Zudem dürfen die Daten nur zweckgebunden verwendet werden.

Diese Informationen werden oftmals in den Datenschutzerklärungen auf den Webseiten der Unternehmen erwähnt. Folglich ist zu prüfen, ob sie mit der neuen Gesetzgebung übereinstimmen. Wird gegen die Informationspflicht verstossen, kann dies mit einer Busse von bis zu CHF 250'000 geahndet werden.

**c) Verzeichnis über die Bearbeitungstätigkeiten
(Art. 12 revDSG)**

Ab dem 1. September 2023 sind die Unternehmen grundsätzlich verpflichtet, ein sogenanntes Verzeichnis der Bearbeitungstätigkeiten zu führen. In diesem Verzeichnis sind sämtliche Arten von Datenbearbeitungen aufzuführen. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) hat ein Einsichtsrecht in das Datenbearbeitungsverzeichnis der Unternehmen und kann dessen Führung mit Verfügung unter Strafandrohung anordnen.

Eine Ausnahme besteht für Gesellschaften, die weniger als 250 Mitarbeitende beschäftigen und weder besonders schützenswerte Personendaten im grossen Umfang bearbeiten, noch ein Profiling mit hohem Risiko durchführen (Art. 24 revDSV).

Die Ausnahmen von der Pflicht zur Führung eines solchen Verzeichnisses sind sehr offen formuliert. Es ist daher im Einzelfall zu prüfen, ob eine solche Ausnahme besteht. Zudem ist es aus Compliance-Gründen sinnvoll, einen Überblick über die Bearbeitung von Personendaten im Unternehmen zu haben. Dies kann allerdings auch in einem einfacheren Datamapping festgehalten werden.

d) Auslagerung von Datenbearbeitungen an Dritte

Datenbearbeitungen dürfen nur an Dritte ausgelagert werden, wenn entweder hierfür eine gesetzliche oder eine vertragliche Grundlage besteht. Somit ist in der Regel bei jeglicher Auslagerung eine Datenbearbeitungsvereinbarung abzuschliessen. Gleichzeitig sind die Dritten verpflichtet, ein Bearbeitungsverzeichnis als Auftragsbearbeiter zu führen.

Als Beispiele solcher Datenbearbeitung durch Dritte können hier insbesondere eine externe Lohnverarbeitungstätigkeit, Webhosts oder IT-Support-Unternehmen aufgeführt werden.

Werden professionelle Dienstleistungsunternehmen mit Datenbearbeitungen ohne den Abschluss einer Datenbearbeitungsvereinbarung beauftragt, kann dies mit einer Busse von bis zu CHF 250'000 bestraft werden.

e) Datenbearbeitungen im Ausland

Im Rahmen von Datenbearbeitungen im Ausland ist sicherzustellen, dass der betreffende Staat entweder ein angemessenes Datenschutzniveau gewährleistet oder dass der Datenschutz durch weitere Massnahmen, bspw. Standarddatenschutzklauseln, gewährleistet wird.





Ob ein angemessenes Datenschutzniveau vorliegt, wird durch den Bundesrat festgelegt und periodisch überprüft. Über ein angemessenes Datenschutzniveau verfügen zurzeit EU-Staaten, EWR-Staaten, Andorra, Argentinien, Kanada (in gewissen Provinzen), Gibraltar, Guernsey, Isle of Man, Färöer, Israel, Jersey, Monaco, Neuseeland, Vereinigtes Königreich und Uruguay.

Werden Daten unter Verstoss gegen diese Bestimmungen ins Ausland bekannt gegeben, kann dies mit einer Busse von bis zu CHF 250'000 geahndet werden.

f) Datenschutz-Folgenabschätzung (Art. 22 revDSG)

Vor jeder neuen Bearbeitung von Personendaten ist zu prüfen, ob eine Datenschutz-Folgenabschätzung notwendig ist. Die Notwendigkeit einer Datenschutz-Folgenabschätzung besteht, wenn die beabsichtigte Datenbearbeitung mit einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen verbunden ist. Es ist zu empfehlen, einen Prozess betreffend die Einführung von neuen Datenbearbeitungstools zu definieren und die Datenschutz-Folgenabschätzung dort zu integrieren. Nach erfolgter Prüfung empfehlen wir, die Durchführung oder den Verzicht einer Durchführung im Datenverarbeitungsverzeichnis gemäss Buchstabe c) zu dokumentieren.

g) Weitere Pflichten

Verletzung der Datensicherheit (Art. 24 revDSG)

Verletzungen der Datensicherheit sind dem EDÖB unverzüglich zu melden, wenn die Verletzung voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen führt. Intern sollten sämtliche Verletzungen gemeldet werden, sodass die intern verantwortliche Person eine Einschätzung vornehmen kann, ob eine Mitteilung an den EDÖB notwendig ist.

Technische und organisatorische Massnahmen (Art. 7 revDSG)

Datenbearbeitungen sind technisch und organisatorisch derart auszugestalten, dass die Anforderungen des Datenschutzgesetzes eingehalten werden. Dabei sind insbesondere Massnahmen zu definieren, die dem Stand der Technik sowie den jeweiligen Bearbeitungen angemessen sind. Der Bundesrat erlässt dabei Mindestanforderungen an die Datensicherheit. Der Verstoss gegen diese Mindestanforderungen ist mit einer Busse bis zu CHF 250'000 beahftet.

Auskunftsrecht (Art. 25 revDSG)

Jede betroffene Person hat ein Recht auf Auskunft bezüglich der Bearbeitung ihrer Daten. Die Auskunftserteilung hat i.d.R. innerhalb von 30 Tagen nach Einreichung des Auskunftsbegehrens zu erfolgen, widrigenfalls besteht ein Bussenrisiko. Damit das Auskunftsrecht gewahrt werden kann, sollten sämtliche Auskunftsgesuche zentral bearbeitet werden.

Recht auf Datenherausgabe (Art. 28 revDSG)

Jede betroffene Person kann grundsätzlich die kostenlose Herausgabe ihrer Personendaten in einem gängigen elektronischen Format verlangen, sofern die Daten automatisiert bearbeitet werden und die Daten mit Einwilligung der betroffenen

Person oder in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrages bearbeitet werden.

Löschung von Personendaten (Art. 32 revDSG)

Sobald die Personendaten zum Zweck der Bearbeitung nicht mehr erforderlich sind, müssen sie vernichtet oder anonymisiert werden. Entsprechend ist die Aufbewahrungsdauer und Löschung von Personendaten zu dokumentieren und die Löschung nach Ablauf der Aufbewahrungsdauer sicherzustellen.

Jede betroffene Person kann zudem die Löschung oder die Vernichtung ihrer Personendaten verlangen und gerichtlich durchsetzen. Ein generelles Löschkonzept hilft bei der Überprüfung, ob die Daten rechtmässig gelöscht werden.

h) Keine Pflicht zur Bestellung eines Datenschutzberaters

Das neue DSG sieht keine generelle Pflicht zur Bestellung eines Datenschutzberaters vor. Sollte jedoch ein solcher bestellt werden, kann auf die Konsultation des EDÖB bei einer Datenschutz-Folgenabschätzung verzichtet werden. Zudem ist dieser für die Schulung von Mitarbeitenden sowie für die Anwendung des Datenschutzrechts zuständig. Die Benennung eines Datenschutzberaters ist zu empfehlen, wenn im Unternehmen besonders viele (schützenswerte) Personendaten bearbeitet werden.

Fazit

Das neue DSG bringt Handlungsbedarf für die schweizerischen Unternehmen mit sich. Dieser kann sehr umfangreich sein und die Einführung diverser neuer Prozesse und Dokumentationen erfordern. Eine zeitnahe und zweckmässige Umsetzung der neuen Datenschutzanforderungen lohnt sich, um Bussen von bis zu CHF 250'000 zu vermeiden. Gerne unterstützt Sie unsere Rechtsabteilung sowohl bei der Überprüfung des Handlungsbedarfs als auch bei der Umsetzung des neuen DSG in Ihrem Unternehmen.



Selina Bruderer
LL.M. (Keio University, Tokyo),
Rechtsanwältin,
Mitglied des Kaders
Zürich



Gloria Eschenbach
lic.iur. Rechtsanwältin,
Partnerin
Zürich