SCHILLER RECHTSANWÄLTE

SCHILLER RECHTSANWÄLTE AG KASINOSTRASSE 2 POSTFACH 1507 CH-8401 WINTERTHUR
TELEFON 052 269 16 16 FAX 052 269 16 00 OFFICE@SCHILLERLEGAL.CH WWW.SCHILLERLEGAL.CH

NEUES SCHWEIZER DATENSCHUTZRECHT

1. Revision, Inkrafttreten

Am 25. September 2020 hat das Parlament das **revidierte Datenschutzgesetz (DSG)** verabschiedet. Von den Medien nicht gross vermeldet, hat das Parlament zahlreiche Angleichungen an die EU-Datenschutzgrundverordnung (DSGVO) beschlossen. Dennoch hat das Parlament ein Copy/Paste der zum Teil weit gehenden und komplizierten EU-Regeln vermieden. Das revidierte DSG behält die bisherige Struktur bei und weicht in einigen Punkten von der DSGVO ab.

Das Gesetz untersteht dem fakultativen Referendum. Nach Ablauf der 100-tägigen Referendumsfrist entscheidet der Bundesrat über das Inkrafttreten. Es ist zu erwarten, dass das revidierte DSG frühestens Anfang 2022, möglicherweise aber auch erst Mitte 2022 in Kraft treten wird. Weil das revidierte Gesetz **keine Übergangsfrist** vorsieht, ist es wichtig, sich frühzeitig auf die Änderungen vorzubereiten.

2. Wo gilt das neue DSG? Was ändert, was nicht?

Der räumliche Geltungsbereich bestimmt sich neu ausdrücklich nach dem sog. Auswirkungsprinzip. Das DSG ist auf Sachverhalte anwendbar, die sich **in der Schweiz auswirken**, auch wenn sie im Ausland veranlasst werden (Art. 3 Abs. 1 nDSG). Auch Unternehmen mit Sitz im Ausland haben die Vorschriften des DSG einzuhalten, wenn eine Bearbeitung von Personendaten sich in der Schweiz auswirkt. Für Schweizer Unternehmen gilt das DSG, soweit eine Datenbearbeitung sich in der Schweiz auswirkt; liefert ein Schweizer Unternehmen Produkte ins Ausland und bearbeitet es dabei Daten ausländischer Kunden, ist hingegen (auch) das ausländische Datenschutzrecht zu beachten, in der EU die DSGVO.

Neu erfasst das DSG die Bearbeitung von Daten juristischer Personen nicht mehr. Wie die DSGVO gilt auch das DSG künftig nur noch für Personendaten **natürlicher Personen**.

Anders als in der EU braucht es in der Schweiz für die Bearbeitung von Personendaten **auch künftig keine ausdrückliche Einwilligung**. Die Zustimmung zur Verwendung von Cookies beim Besuch von Webseiten, die alle

nervt und – weil auf allen Seiten aufpoppend und von niemandem gelesen – nur wenig hilfreich ist, bleibt uns in der Schweiz erspart (jedenfalls soweit eine Datenbearbeitung sich nicht im Ausland auswirkt). Eine ausdrückliche Einwilligung ist erforderlich für die Bearbeitung besonders schützenswerter Personendaten und das Profiling mit hohem Risiko (Art. 6 Abs. 7 nDSG).

Doch was **bedeutet das revidierte DSG für Unternehmen**? Welche Vorbereitungen sind nötig, damit der Betrieb und die Website "fit" für das neue Recht sind? Mit den folgenden Informationen möchten wir einen einfachen Überblick für ein durchschnittliches KMU geben. Je nach Grösse des Unternehmens, Tätigkeitsgebiet und der Art der Daten, die bearbeitet werden, sind weitere Abklärungen zu empfehlen.

3. Die wichtigsten Neuerungen

Wichtig ist zunächst einmal: Die **allgemeinen Grundsätze** der Datenbearbeitung (Transparenz, Verhältnismässigkeit und Datensicherheit) gelten weiter.

Ausgebaut wurde die **Informationspflicht** bei der Beschaffung von Personendaten (Art. 19 Abs. 1 nDSG). Wer Personendaten beschafft, muss die betroffene Person darüber informieren. Er muss ihr mindestens die Identität und die Kontaktdaten des Verantwortlichen, den Bearbeitungszweck und gegebenenfalls die Empfänger, denen Personendaten bekannt gegeben werden, mitteilen (Art. 19 Abs. 1 und 2 nDSG). Damit wird die **Datenschutzerklärung** faktisch zur Pflicht. Die Datenschutzerklärung wird üblicherweise auf der Website aufgeschaltet; viele Unternehmen weisen zudem in ihren Verträgen, AGB oder anderen Dokumenten darauf hin. Art. 20 nDSG statuiert Ausnahmen von der Informationspflicht. Eine Information ist zum Beispiel nicht nötig, wenn die Bearbeitung gesetzlich vorgesehen ist (z.B. Führen eines Personaldossiers).

Erforderlich ist neu ein **Verzeichnis der Bearbeitungstätigkeiten** (Art. 12 nDSG). Das Gesetz definiert den Mindestinhalt. Im Verzeichnis ist insbesondere festzuhalten, welche Daten zu welchem Zweck bearbeitet werden (z.B. für die Abwicklung eines Vertrags, für die Lohnbuchhaltung), wer dafür verantwortlich ist, wer die Daten empfängt (z.B. Muttergesellschaft, externer Dienstleister, Behörden), wie lange die Daten aufbewahrt werden (z.B. solange eine Kundenbeziehung besteht, gesetzliche Aufbewahrungsfrist) und welche Massnahmen ergriffen werden, um die Datensicherheit zu gewährleisten. Zusätzliche Angaben sind nötig, wenn Daten ins Ausland bekannt gegeben werden. Der Umfang eines solchen Verzeichnisses wird sehr unter-

schiedlich sein, in vielen Fällen dürfte eine (mehr oder weniger lange) Excel-Tabelle genügen. Es ist auch zu erwarten, dass der Bundesrat Erleichterungen für KMU vorsehen wird (Art. 12 Abs. 5 nDSG). Das Verzeichnis der Bearbeitungstätigkeit wird häufig Grundlage der Datenschutzerklärung sein. Zur Vorbereitung auf das neue Recht ist allen Unternehmen, die das nicht bereits getan haben, zu empfehlen, rechtzeitig ein Verzeichnis zu erstellen. Es spricht nichts dagegen, schon jetzt damit zu beginnen. Mit Verzeichnis der Bearbeitungstätigkeiten verfügt das Unternehmen auch über eine Grundlage für die Datenschutzerklärung.

Wer Personendaten von einem Dritten (sog. Auftragsbearbeiter; z.B. externer IT-Support oder externe Lohnbuchhaltung) bearbeiten lässt, kann dies tun, wenn der **Auftragsbearbeiter** die Daten so bearbeitet, wie der Verantwortliche selbst es tun dürfte. Weiter muss sich der Verantwortliche vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit zu gewährleisten (Art. 9 Abs. 1 und 2 nDSG). Im Ergebnis muss der Verantwortliche mit dem Auftragsbearbeiter einen Vertrag schliessen und sich diesbezügliche Garantien geben lassen.

Kann eine Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen, ist der Verantwortliche verpflichtet, eine **Datenschutz-Folgenabschätzung** zu erstellen (Art. 22 nDSG). In der Datenschutz-Folgenabschätzung sind die Risiken der Bearbeitung (z.B. Kreditkartendaten könnten missbraucht werden; eine Verwechslung von Adressen könnte dazu führen, dass der Arztbericht an den falschen Patienten geschickt wird) und die getroffenen Massnahmen zu beschreiben und zu bewerten. Im Grunde handelt es sich um eine Selbst-Evaluation. Ergibt sich aus der Datenschutz-Folgenabschätzung, dass die geplante Bearbeitung trotz der vorgesehenen Massnahmen noch ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person zur Folge hat, ist die Stellungnahme des Eidgenössischen Datenschutzbeauftragten (EDÖB) einzuholen (Art. 23 Abs. 1 nDSG).

Je nachdem sind weitere Vorschriften zu beachten: Personendaten dürfen grundsätzlich nur dann **ins Ausland** bekanntgegeben werden, wenn das betreffende Land einen angemessenen (Daten-)Schutz gewährt (Art. 16 Abs. 1 nDSG). Ist das nicht der Fall, sind spezielle Garantien oder Schutzklauseln zur Gewährleistung des Datenschutzes oder die ausdrückliche Einwilligung der betroffenen Person erforderlich. Kommt es zu einer **Verletzung der Datensicherheit** (z.B. Datenverlust, Hackerangriff), die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt, ist eine Meldung an den EDÖB zu machen (Art. 24 nDSG). Wie bisher kann jede Person vom Verantwortlichen **Auskunft** betreffend

über sie bearbeitete Daten verlangen (Art. 25 nDSG). Neu wird ein Anspruch auf **Datenportabilität** im Gesetz verankert: Jedermann kann die Herausgabe seiner Personendaten in einem gängigen Format verlangen (z.B. der Patient vom Spital die von ihm erhobenen Gesundheitsdaten in elektronischer Form; der Kunde vom Musikstreamingdienst die von ihm angelegten Playlists), ebenso kann verlangt werden, dass der Verantwortliche die Daten direkt auf einen anderen Verantwortlichen überträgt (Art. 28 nDSG). Schliesslich besteht bei einer **automatisierten Entscheidung** (z.B. automatisierte Kreditvergabe) eine besondere Informationspflicht (Art. 21 nDSG).

4. Sanktionen

Bei der Verletzung bestimmter Pflichten sieht das revidierte DSG als Sanktion eine **Busse von bis zu CHF 250'000.--** vor (Art. 60 ff. nDSG). Während sich die Busse gemäss DSGVO gegen das jeweilige Unternehmen richtet, wird die Busse nach dem nDSG grundsätzlich der verantwortlichen natürlichen Person und nur ausnahmsweise dem Unternehmen auferlegt. Allerdings ist eine solche Busse nicht für alle, sondern nur für bestimmte Verstösse vorgesehen, etwa bei vorsätzlich falschen Angaben in einer Datenschutzerklärung oder der Übertragung der Datenbearbeitung an einen Auftragsbearbeiter, der die Datensicherheit nicht gewährleistet. Keine Sanktion ist hingegen vorgesehen, wenn ein Verantwortlicher es unterlässt, ein Verzeichnis der Bearbeitungstätigkeiten zu erstellen oder eine Datenschutz-Folgenabschätzung vorzunehmen.

5. Fazit

Mit dem revidierten Datenschutzgesetz treten einige Neuerungen in Kraft. Jedes Unternehmen ist gut beraten, sich rechtzeitig darauf einzustellen. Wer jetzt schon beginnt, ein Verzeichnis der Bearbeitungstätigkeiten zu erstellen, kann rechtzeitig die Datenschutzerklärung entwerfen oder anpassen und ist für allfällige weitere Schritte gerüstet. Wer sich bisher bereits an der europäischen DSGVO orientiert und deren Vorgaben eingehalten hat, kann die entsprechenden Erklärungen und Vereinbarungen grundsätzlich übernehmen und punktuell anpassen. Am einen oder anderen Ort lässt das schweizerische Recht auch Raum für eine einfachere Regelung. Gerne beraten wir Sie, wenn in Ihrem Unternehmen Fragen hierzu auftauchen.

_____