BLOG

MATTIG SUTER & PARTNER

info@mattig.ch
www.mattig.swiss

Claudia Mattig
dipl. Lm.-Ing. ETH,
Master of Arts HSG in Accounting and Finance,
dipl. Wirtschaftsprüferin
E-MAIL: claudia.mattig@mattig.ch

Das neue Datenschutzgesetz – das Wichtigste in Kürze

© iStock.com/ greenbutterfly

Das revidierte Datenschutzgesetz («revDSG») tritt – ohne Übergangsfristen – am 1. September 2023 in Kraft und gilt insbesondere für private Personen, die physische und/oder elektronische Personendaten bearbeiten. Das heisst, es findet auch auf alle Unternehmen, unabhängig ihrer Rechtsform, Anwendung. Bei Verstössen gegen das revDSG drohen den bearbeitenden Personen und nicht zwingend den Unternehmen strafrechtliche Bussen.

Frage
Was sind die wichtigsten Änderungen und Grundsätze des revidierten Datenschutzgesetzes, welche eine Unternehmerin bzw. ein Unternehmer kennen und umsetzen muss?

Antwort
Welche Daten sind betroffen?
In den Geltungsbereich des revDSG fallen neu nur noch die Daten von natürlichen Personen. Als Personendaten gelten alle Informationen über Personen, welche namentlich genannt werden oder welche aus anderen Gründen einer bestimmten oder bestimmbaren Person zugeordnet werden können (z.B. Name, Geschlecht, Geburtsdatum, E-MailAdresse, Bankkonto von Kunden oder Mitarbeitenden). Als Bearbeitung gilt jeglicher Umgang mit Personendaten wie z.B. das Beschaffen, Aufbewahren, Speichern und Weitergeben. Personendaten können auch besonders schützenswerte, sensitive Daten sein (z.B. biometrische Daten, genetische Daten, Gesundheitsdaten). Im Fall der Bearbeitung solcher Daten gelten strengere Anforderungen.

Privacy by Design (Datenschutz durch Technik) and by Default (Datenschutz durch datenschutzfreundliche Voreinstellung)
Der Grundsatz von Privacy by Design and by Default hält fest, dass der Datenschutz durch Technik und durch datenschutzfreundliche Voreinstellungen sicherzustellen ist. Das bedeutet, dass die Bearbeitung auf das für den Verwendungszweck notwendige Mindestmass beschränkt ist, sofern die betroffene Person nicht etwas anderes akzeptiert. In der Praxis wird dies unter anderem bei den Voreinstellungen der Webseiten, durch Multi-Faktor-Authentifizierung bei Systemzugriffen oder durch professionelle Lösungen zur Verschlüsselung von Mails umgesetzt (werden).

Datensicherheit
Die Datensicherheit ist durch geeignete technische und organisatorische Massnahmen sicherzustellen. Die Massnahmen müssen dabei dem Risiko angemessen sein. Das bedeutet, je grösser das Risiko einer Verletzung der Datensicherheit ist, umso höher sind die Anforderungen der zu treffenden Massnahmen. Konkret soll das Ziel dieser Massnahmen sein, Verletzungen der Datensicherheit (d.h. jede Verletzung der Sicherheit die ungeachtet der Absicht oder der Widerrechtlichkeit dazu führt, dass Personendaten verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt bzw. zugänglich gemacht werden) zu vermeiden. Sofern dabei der Stand der Technik nicht berücksichtigt wird, kann die Verletzung der Datensicherheit gegebenenfalls zu einer Sorgfaltspflichtverletzung und damit zu einer strafrechtlichen Sanktion führen.

Auftragsbearbeitung
Die Bearbeitung von Personendaten kann vertraglich oder gesetzlich auf einen Dritten (Auftragsbearbeiter) übertragen werden, sofern der Auftragsbearbeiter die Daten so bearbeitet, wie es der Verantwortliche selbst tun dürfte; dies aber nur sofern keine gesetzlichen oder vertraglichen Geheimhaltungspflichten die Übertragung verbietet. Der Verantwortliche muss jedoch in jedem Fall die Datensicherheit gewährleisten. Der Auftragsbearbeiter darf die Bearbeitung nur mit vorgängiger Genehmigung des Verantwortlichen an einen Dritten übertragen. Die Genehmigung

muss zwar nachweisbar sein, ist aber an keine besondere Form gebunden. Die Genehmigung kann spezifischer oder allgemeiner Art sein, wobei allgemeine Art bedeutet, dass der Auftragsbearbeiter über jede Änderung informiert, damit Einspruch erhoben werden könnte. Bei der Bekanntgabe von Personendaten ist zudem zu beachten, dass diese nur ins Ausland bekanntgegeben werden dürfen, wenn ein angemessener Schutz der Personendaten im Ausland gewährleistet ist.

Der Verantwortliche muss mit jedem Auftragsbearbeiter einen Auftragsbearbeitungsvertrag abschliessen, indem u.a. Gegenstand und Dauer der Bearbeitung, Art und Zweck der Bearbeitung, die Art der Personendaten und auch die Gewährleistungen der Datensicherheit geregelt werden.

Obschon das revDSG den Begriff bzw. die Rolle der gemeinsamen Verantwortlichkeit im Gesetz nicht vorsieht, existiert das Konzept wohl auch im Schweizer Recht. Obschon einige Unklarheiten hinsichtlich der gemeinsamen Verantwortung bestehen, ist klar, dass eine gemeinsame Verantwortung häufig bei Gruppengesellschaften vorliegt, die dieselben Lösungen (z.B. für das Mitarbeitermanagement oder Kunden- bzw. Dokumentenmanagement) verwenden. Da das revDSG dieses Konzept nicht explizit vorsieht, besteht auch keine Verpflichtung zum Abschluss von entsprechenden Verträgen. Dennoch ist der Abschluss solcher Verträge sinnvoll, um die Zuständigkeiten und Verantwortlichkeiten hinsichtlich der Datenschutzpflichten intern klar abzugrenzen.

Datenbearbeitungsverzeichnis
Ein Verzeichnis der Bearbeitungstätigkeiten wird in der Schweiz für Unternehmen mit 250 und mehr Mitarbeitenden oder für kleinere Unternehmen, die in grossem Umfang besonders schützenswerte Daten bearbeiten oder Profiling (automatisierte Bearbeitung personenbezogener Daten) mit besonders hohem Risiko durchführen, obligatorisch.

Informationspflicht
Bei jeder Beschaffung von Personendaten muss die betroffene Person angemessen informiert werden. Der Verantwortliche muss der betroffenen Person daher mindestens die Identität sowie die Kontaktdaten des Verantwortlichen, den Bearbeitungszweck und gegebenenfalls die Empfänger oder Kategorien von Empfängern der Personendaten bekannt geben. Sofern Personendaten ins Ausland bekanntgegeben werden, sind zudem die Garantien für ein angemessenes Datenschutzniveau oder die Anwendung einer Ausnahme mitzuteilen. Ferner bestehen weitere Informationspflichten bei automatisierten Einzelentscheidungen.

Meldepflichten
Verletzungen der Datensicherheit, die voraussichtlich zu einem hohen Risiko für die Persönlichkeitsrechte oder die Grundrechte der betroffenen Personen führen, müssen so rasch als möglich dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) gemeldet werden. Jedoch ist eine sofortige Meldung mit Blick auf die Bussen zu beachten. Man kann sich dabei an der 72 Stundenfrist aus der europäischen Gesetzgebung orientieren.

Rechte der betroffenen Personen
Den betroffenen Personen steht ein Auskunftsrecht zu, welches der Verantwortliche einzuhalten hat. Mittels eines Auskunftsbegehrens können die betroffenen Personen Informationen über die sie betreffenden Datenbearbeitung verlangen, um beispielsweise die Rechtmässigkeit der Datenbearbeitung zu überprüfen. Neben dem Auskunftsrecht haben die Betroffenen weitere Rechte. Das sind insbesondere das Recht auf Datenherausgabe und -übertragung, das Recht auf Berichtigung, das Recht auf einen Bestreitungsvermerk, das Recht auf Löschung und das Recht auf Sperrung.

Strafbestimmungen
Neben den erweiterten Kompetenzen des EDÖB, sieht das revDSG auch strafrechtliche Sanktionen vor. Konkret kann die vorsätzliche Verletzung von Informations-, Auskunfts- und Mitwirkungspflichten, Sorgfaltspflichten sowie beruflichen Schweigepflichten auf Antrag mit Bussen bis zu CHF 250’000 bestraft werden. Dieselbe Strafandrohung gilt auch für das Missachten von Verfügungen des EDÖB. Obschon Ausnahmen zur Strafbarkeit von privaten Personen bestehen können, ist grundsätzlich jeweils die natürliche Person und nicht das Unternehmen strafbar.

Was bedeutet dies für mein Unternehmen?
Wir empfehlen Ihnen, die Zeit bis zur Einführung des revDSG zu nutzen und insbesondere die nachstehenden Punkte bei der Umsetzung der neuen datenschutzrechtlichen Anforderungen zu beachten und zu dokumentieren:

- Verschaffen Sie sich eine Übersicht über die Personendaten, welche bearbeitet werden. Das heisst, alle Daten von Mitarbeiterdaten über Kundendaten zu Lieferantendaten sowie anderen unternehmensspezifischen Daten.
- Bearbeiten Sie Daten nicht heimlich. Informieren Sie die Betroffenen, wozu die Daten verwendet werden und halten Sie sich daran. Überprüfen Sie Ihre Datenschutzerklärung und passen diese, wo nötig, an.
- Bearbeiten Sie nur so viele Daten wie zwingend notwendig und definieren Sie Löschprozesse.
- Löschen Sie Daten, die nicht mehr gebraucht werden (vorbehältlich der gesetzlichen Aufbewahrungsfristen).
- Erarbeiten und implementieren Sie interne Datenbearbeitungsrichtlinien und -prozesse.
- Falls Betroffene selbst Einstellungen vornehmen können, richten Sie diese so ein, dass ohne Zutun der Betroffenen möglichst wenig Daten bearbeitet werden. Überprüfen Sie Ihre Cookie-Richtlinien bzw. Banner und passen Sie diese, wo nötig, an.

- Wenn Sie Auftragsverarbeiter sind oder mit Auftragsverarbeitern zusammenarbeiten, überprüfen Sie diese Verträge und passen diese, wo nötig, an. Prüfen Sie diese auch hinsichtlich allfälliger Transfers von Personendaten ins Ausland und ergänzen Sie – sofern notwendig – die implementierten Garantien zur Sicherstellung des Datenschutzniveaus bei Datentransfers ins Ausland.
- Überprüfen Sie Ihre Verträge mit Ihren Kunden und passen Sie diese, wo nötig, an.
- Implementieren Sie Massnahmen für die Gewährleistung der Datensicherheit.
- Schulen Sie Ihre Mitarbeitenden regelmässig in einem angemessenen Mass hinsichtlich des Umgangs mit Daten.

Tags: Wirtschaftsberatung, Datenschutz, Datensicherheit, Datenschutzerklärung, revDSG