

Das revidierte Datenschutzgesetz – Handlungsbedarf für Unternehmen?

Das Schweizer Parlament hat im September 2020 das revidierte Datenschutzgesetz verabschiedet, welches voraussichtlich 2022 in Kraft treten wird. Daniela Fábíán Masoch, Rechtsanwältin und Datenschutzexpertin, erklärt, welche Pflichten auf Unternehmen zukommen und wie sich diese vorbereiten können.



Daniela Fábíán Masoch



Datenschutz hat in den vergangenen Jahren stark an Bedeutung gewonnen. Konsumenten, Kunden, Patienten und Arbeitnehmer, aber auch Führungskräfte und Behörden sind zunehmend sensibilisiert und haben hohe Erwartungen an den Schutz von Personendaten. Infolgedessen wurden die Datenschutzgesetze weltweit entsprechend verschärft.

Unter dem revidierten Schweizer Datenschutzgesetz (nDSG) bleibt die Bearbeitung von Personendaten grundsätzlich erlaubt. Unternehmen müssen aber in Zukunft eine ganze Reihe neuer oder erweiterter Vorschriften befolgen.

Welche neuen Pflichten kommen auf Unternehmen zu?

Erweiterte Informationspflicht: Künftig müssen Unternehmen betroffene Personen bei der Beschaffung von Personendaten informieren (bisher nur besonders schützenswerte Daten und Persönlichkeitsprofile), wobei das Gesetz Mindestangaben vorschreibt. Konkret bedeutet dies, dass Unternehmen ihre Datenschutzerklärungen überprüfen und ggf. anpassen oder komplett neu erstellen und den betroffenen Personen mitteilen müssen.

Privacy by Design (PbD): Unternehmen sind künftig verpflichtet, geplante Datenbearbeitungen so auszugestalten, dass die datenschutzrechtlichen Vorschriften und die Grundsätze der Datenbearbeitung eingehalten werden. PbD ist jedoch nicht bloss als neue Verpflichtung zu

verstehen, sondern vielmehr als Grundvoraussetzung für einen verantwortungsvollen und effektiven Datenschutz. Eine wirksame Umsetzung der Datenschutzgrundsätze setzt voraus, dass Unternehmen proaktiv handeln und potenzielle Risiken für die Privatsphäre von betroffenen Personen antizipieren.

Datenschutz-Folgenabschätzung: Unternehmen müssen künftig für Datenbearbeitungen, die ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen können, eine Datenschutz-Folgenabschätzung durchführen. Sie müssen die Risiken für die betroffene Person vorgängig bewerten und geeignete Massnahmen zum Schutz ihrer Persönlichkeit und Grundrechte ergreifen. Dies kann beispielsweise bei einer umfangreichen Bearbeitung von besonders schützenswerten Daten der Fall sein, aber auch bei der Verwendung neuer Technologien.

Verzeichnis der Bearbeitungstätigkeiten: Unternehmen sind neu grundsätzlich verpflichtet, ein Verzeichnis ihrer Bearbeitungstätigkeiten zu führen. Ein solches Verzeichnis kann, wenn es sorgfältig geführt und mit zusätzlichen Informationen ergänzt wird, durchaus einen Vorteil haben, nämlich als Grundlage für Konformitätsprüfungen und Datenschutz-Folgenabschätzungen dienen.

Meldung von Verletzungen der Datensicherheit: Wie bereits unter der EU-Datenschutz-Grundverordnung

(DSGVO) müssen Unternehmen in Zukunft Verstösse der Datensicherheit (wie z. B. unberechtigte Datenzugriffe) je nach Risiko dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) melden und die betroffenen Personen informieren.

Welche Sanktionen drohen Unternehmen, wenn sie die gesetzlichen Anforderungen nicht einhalten?

Im Unterschied zur DSGVO wird grundsätzlich nicht das Unternehmen, sondern die verantwortliche natürliche Person mit Bussgeldern von bis zu CHF 250 000 belegt. Strafbar macht sich insbesondere, wer gegen die Informations- oder Auskunftspflicht verstösst oder die Sorgfaltspflichten verletzt, namentlich die Mindestanforderungen an die Datensicherheit nicht einhält, Personendaten ins Ausland bekanntgibt oder die Datenbearbeitung einem Auftragsbearbeiter überträgt, ohne die gesetzlichen Anforderungen zu erfüllen. Bussen setzen allerdings eine vorsätzliche Handlung voraus und werden in den meisten Fällen nur auf Antrag verhängt.

Handlungsbedarf für Unternehmen?

Da das nDSG keine Übergangsfristen vorsieht, sollten Unternehmen frühzeitig prüfen, inwieweit ihre internen Regelungen und Prozesse betreffend Datenmanagement mit den neuen Anforderungen übereinstimmen.

Insbesondere müssen Konzepte wie Privacy by Design umgesetzt und Prozesse eingeführt werden, die eine gesetzeskonforme Löschung oder Vernichtung der Daten und die Datenportabilität unterstützen sowie die Durchführung von Datenschutz-Folgenabschätzungen und die rechtzeitige Meldung von Datensicherheitsverstössen sicherstellen. Datenschutzerklärungen müssen überprüft und gegebenenfalls an die Anforderungen des nDSG angepasst werden. Verzeichnisse, die derzeit Datensammlungen dokumentieren, müssen neu strukturiert werden, um zukünftig Bearbeitungsaktivitäten zu erfassen.

Über die Autorin

Daniela Fábíán Masoch ist Rechtsanwältin und Gründerin von Fabian Privacy Legal, einer Anwaltskanzlei mit Sitz in Basel, die sich auf internationales, europäisches und schweizerisches Datenschutzrecht spezialisiert hat.

Sie berät und unterstützt Schweizer und internationale Unternehmen mit einem pragmatischen Ansatz bei der Bewertung, Entwicklung, Umsetzung und Überwachung von Datenschutzstrategien, Governance-Modellen und globalen Datenschutzprogrammen sowie Datentransferstrategien, einschliesslich BCR.

Weitere Informationen:
www.privacylegal.ch