Das revidierte Datenschutzgesetz

Am 1. September 2023 tritt das totalrevidierte Datenschutzgesetz in Kraft. Es bringt erhöhte Auskunfts-, Informations- und Meldepflichten sowie Sanktionen bei Nichteinhalten von Vorschriften mit sich. Vom neuen Datenschutzgesetz sind alle Unternehmen betroffen, ganz unabhängig von ihrer Grösse.

Von Klaus Krohmann
Leiter Rechtsberatung, Partner
BDO Zürich

Das revidierte Datenschutzgesetz gilt ab dessen Inkrafttreten am 1. September 2023; ohne weitere Übergangfristen. Es orientiert sich stark an den Grundsätzen der Datenschutz-Grundverordnung der EU (DSGVO), deren Regeln durch unser Parlament angepasst wurden.

Empfohlene Massnahmen

Unternehmen werden im Hinblick auf das totalrevidierte Datenschutzgesetz in einem 1. Schritt die interne Projektplanung regeln müssen. Es sind Fragen zu klären, wie man sich organisieren will, wer das Projekt leiten soll, wie viele Ressourcen in welchem Zeitraum zur Verfügung gestellt werden, was intern gelöst und wo externe Unterstützung beigezogen wird. Es ist empfehlenswert, einen groben Projektplan zu erstellen und möglichst früh ein Reporting bei den Verantwortlichen im Unternehmen einzuführen und über die wesentlichsten Schritte zu berichten.

In einem 2. Schritt sollte das Unternehmen eine Übersicht über seine Verfahren und Prozesse, bei denen Personendaten bearbeitet werden, gewinnen. Dazu ist ein Inventar zu erstellen. Dieses dient als Grundlage für die vorgeschriebene Risikobeurteilung. Die datenschutzrechtlichen Risiken der Prozesse sind entsprechend zu bewerten und es ist zu überlegen, welche technischen und organisatorischen Massnahmen (TOM) angemessen sind. Es ist zu bestimmen, wo Verbesserungen der Massnahmen aufgrund allfällig hoher Risiken in einem Prozess vorgenommen werden sollen, um das Risiko auf ein angemessenes Niveau zu senken.

Schliesslich sind einem weiteren 3. Schritt verschiedene Prozesse in der Organisation zu installieren oder anzupassen:

(a) Die interne Alarmierung bei Datenschutzvorfällen ist sicherzustellen. Innert rund 72 Stunden muss beurteilt werden können, ob eine allfällige Meldung an den Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) notwendig ist. Ebenso ist zu prüfen, ob die von einem Datenschutzvorfall betroffenen Personen zu informieren sind.
(b) Die korrekte Bearbeitung von Betroffenenrechten, also insbesondere von Auskunfts- und Löschbegehren, ist sicherzustellen. Eine Auskunft muss i.d.R. innert 30 Tagen erfolgen. Diese Frist erscheint auf den ersten Blick als einfach einzuhalten. Die Daten zu sammeln, zu prüfen und mitzuteilen, kostet jedoch Zeit. Ein entsprechend effizienter Prozess ist unerlässlich.
(c) Schliesslich muss sich ein Unternehmen in Zukunft Gedanken zum Datenschutz machen, wenn Prozesse mit Personendaten ändern oder neu eingeführt werden. Der Eintrag im Inventar ist zu überprüfen und allenfalls sind die TOM anzupassen. Sind grosse Mengen besonders schützenswerter Personendaten (z.B. Gesundheitsdaten) davon betroffen, so braucht es allenfalls eine formelle Datenschutz-Folgenabschätzung, die beim EDÖB einzureichen ist, sofern kein Datenschutzberater im Unternehmen bestellt wurde.

Neue Informationspflichten

Führungsorgane von Unternehmen, die ihren Informationspflichten bei der Beschaffung von Personendaten in Zukunft nicht genügend nachkommen, riskieren strafrechtliche Sanktionen und Bussen bis zu 250'000 Franken. Entsprechend ist die Datenschutzerklärung anzupassen und i.d.R. auszubauen: Bisher wurde in Datenschutzerklärungen auf Webseiten meist nur über die Bearbeitung von auf der Webseite gesammelten Daten informiert. Nachdem neu umfassend informiert werden muss, werden die Datenschutzerklärungen zukünftig weitere Informationen enthalten, wie z.B. die Identität und Kontaktdaten des Unternehmens, welches die Personendaten erhebt, über den Bearbeitungszweck, bei Weitergabe an Dritte die Empfänger, generell über die Bearbeitung von Kundendaten und allfällig weiteren Kategorien. Werden Personendaten ins Ausland bekanntgegeben, sind die Länder sowie allenfalls zur Anwendung gelangende Garantien zur Sicherstellung eines angemessenen Schutzes der Personendaten oder zur Anwendung gelangenden Ausnahmen mitzuteilen.

Was im ersten Moment als mühsame Bürde erscheinen mag, wird langfristig Vorteile bringen, denn die Auseinandersetzung mit den eigenen Prozessen lässt oftmals Ineffizienzen oder veraltete Abläufe zu Tage treten. Fest steht: Ein guter Datenschutz ist ein Qualitätsmerkmal.

Wo steht Ihr Unternehmen? Finden Sie es heraus: ***www.bdo.ch/dsgtest***
klaus.krohmann@bdo.ch

BDO-Seminare zum Thema Datenschutzgesetz: Seite 35