

Selbstcheck revDSG



Das müssen Sie ab dem 01.09.2023 beachten!

Ein Auszug der wichtigsten Anforderungen des revidierten Schweizer Datenschutzgesetzes.

Haben Sie alle Prozesse in Ihrem Unternehmen dokumentiert, bei denen Personendaten bearbeitet werden? Führen Sie ein Verzeichnis der Bearbeitungstätigkeiten?



Nach dem neuen Schweizer Datenschutzgesetz gibt es zwar keine allgemeine Pflicht zur Dokumentation, dennoch müssen Sie vermutlich ein Verzeichnis der Bearbeitungstätigkeiten führen. Art. 12 revDSG regelt die Mindestinhalte. Wenn Sie besonders schützenswerte Personendaten in grossem Umfang automatisiert bearbeiten, müssen Sie zudem ein Bearbeitungsreglement vorhalten können.

Sind die von Ihnen bearbeiteten Personendaten ausreichend geschützt?



Nach Art. 8 revDSG sowie Art. 1ff. DSV müssen Personendaten vor geplanten Zugriffen und unbeabsichtigten Beeinträchtigungen geschützt werden. Dies bedeutet, dass Sie durch geeignete technische und organisatorische Massnahmen (TOM) für eine dem Risiko angemessene Datensicherheit sorgen müssen. Haben Sie bspw. ein Berechtigungskonzept, eine Firewall, VPN oder Backups? Haben Sie eine TOM-Beschreibung Ihres Unternehmens? Ist Ihre IT auf dem aktuellen Stand der Technik?

Was ist mit Ihrer Webseite – haben Sie bereits eine Datenschutzerklärung? Berücksichtigen Sie bei der Newsletter-Anmeldung das Double-Opt-In-Verfahren? Gibt es Hinweise auf die Widerruflichkeit der Einwilligung?



Neu ist, dass Verantwortliche betroffene Personen bereits bei Beschaffung von Personendaten über die geplante Bearbeitung informieren müssen. Nach Art. 19 revDSG und Art. 13 DSV sind insbesondere die Bearbeitungszwecke und Empfänger*innen zu nennen, sowie ob eine Bekanntgabe ins Ausland erfolgt. Dies gilt auch für Ihren Online-Auftritt. Sie müssen die Nutzer über die Datenbearbeitung auf Ihrer Webseite informieren. Wenn Sie einen Newsletter versenden möchten, müssen Sie vorab eine Einwilligung einholen und auf das Widerrufsrecht hinweisen.

Haben Sie Auftragsbearbeitungsverträge mit Ihren Dienstleistern geschlossen?



Werden Buchhaltung und Gehaltsabrechnungen von einem externen Dienstleister ausgeführt oder haben Sie Ihre IT (teilweise) outgesourced? Dann müssen Sie einen schriftlichen Vertrag mit den Anforderungen aus Art. 9 revDSG sowie Art. 7 DSV mit Ihrem Vertragspartner schliessen. Zudem müssen Sie auch die technischen und organisatorischen Massnahmen des Auftragnehmers prüfen.

Können Sie einer Betroffenenanfrage auf Auskunft, Datenübertragbarkeit und Löschung gerecht nachkommen?



Das revDSG sieht einige Rechte für betroffene Personen vor. Ihre Kunden und Interessenten können z.B. eine Bestätigung verlangen, ob Sie deren Personendaten bearbeiten. Ist dies der Fall, so haben Betroffene darüber hinaus ein Auskunftsrecht über Bearbeitungszwecke, Herkunft, Aufbewahrungsdauer, Empfänger*innen, etc. Sofern keine gesetzlichen Aufbewahrungspflichten bestehen, können sie auch verlangen, dass ihre Personendaten gelöscht werden. Gibt es in Ihrem Unternehmen hier schon einen Workflow, wie mit Betroffenenanfragen umzugehen ist?

Werden Personendaten auch ins Ausland übermittelt?



Art. 16 ff. revDSG regelt die Bekanntgabe von Personendaten ins Ausland. Diese dürfen nur in Länder übermittelt werden, die ebenfalls ein angemessenes Datenschutzniveau bieten. Alternativ kann ein geeigneter Datenschutz auch dadurch gewährleistet werden, dass z.B. Standarddatenschutzklauseln in die jeweiligen Verträge mit einbezogen werden. Sind Sie sich dessen bewusst und haben Sie dies in Ihren Verträgen berücksichtigt?

Haben Sie eine*n Datenschutzberater*in bestellt?



Nach Art. 10 revDSG können Schweizer Unternehmen eine* Datenschutzberater*in ernennen. Dies bietet gewisse Vorteile, z.B. besteht dann bei Erstellung einer Datenschutz-Folgenabschätzung keine Vorlagepflicht beim EDÖB mehr. Haben Sie intern oder extern bereits eine*n Datenschutzberater*in ernannt oder besteht Interesse daran?

Rot und gelb im Selbstcheck?

Dann besteht dringender Handlungsbedarf für Ihr Unternehmen.

Wir unterstützen Sie gern beim Aufbau einer Datenschutzorganisation und Umsetzung der Anforderungen des revDSG.