VERBAND

NEUES DSG: PRIVACY BY DESIGN & BY DEFAULT, TOMS

Im revidierten DSG (Art. 7) sind neu die Grundsätze «Privacy by Design» (Datenschutz durch Technik) und «Privacy by Default» (Datenschutz durch datenschutzfreundliche Voreinstellungen) verankert. Sie verpflichten Behörden und Unternehmen, die Bearbeitungsgrundsätze des DSG bereits ab der Planung entsprechender Vorhaben umzusetzen, indem sie angemessene technische und organisatorische Schutzmassnahmen treffen. Ferner finden sich in Art. 8 revDSG neue Bestimmungen zur Datensicherheit.

Privacy by Design

Der Datenschutz durch Technik kann beispielsweise beinhalten, dass eine Applikation so ausgestaltet wird, dass die Daten standardmässig anonymisiert oder gelöscht werden. Auf den ersten Blick ist die Idee nachvollziehbar: Datenschutzprobleme würden minimiert, wenn die genutzten Systeme *von Anfang an so ausgestaltet wären, dass der Datenschutz eingehalten werden muss*. In der praktischen Umsetzung zeigt sich aber rasch, dass die Anforderungen komplex und vielfältig sind. Der Grundsatz galt indes auch schon nach dem alten Datenschutzgesetz, wonach rechtzeitig Vorkehrungen zur Einhaltung des Datenschutzes getroffen werden mussten.

Welche Massnahmen muss der Verantwortliche treffen?
Welche Massnahmen der Verantwortliche treffen will, um Art. 7 zu erfüllen, ist ihm selbst überlassen. Ein erster Schritt wird in der Regel sein, alle wesentlichen datenschutzrechtlichen Parameter der Datenbearbeitung zu definieren. Weiter wird zu überlegen sein, wie die Bearbeitung stattfinden soll, damit alle Datenschutzvorschriften eingehalten werden.

Mögliche Mittel sind beispielsweise*:

- Datenschutzerklärungen
- Interne Weisungen
- Schaffung von Widerspruchsmöglichkeiten
- Self-Service Angebote für Betroffenenrechte
- Einsatz von Verschlüsselungen
- Interne Prozesse zur Beschränkung von Nutzungszwecken
- Vermeidung von Personendaten beim Applikationsdesign
- Automatisierung von Löschungen
- Verbote der Re-Identifikation
- Zuständigkeitsregeln
- Dokumentierte Prozesse
- Auswertung von Fehlerraten zwecks Qualitätssicherung
- Vermeidung von nicht synchronisierten Datenkopien
- Regelung der Aufbewahrungsdauer von Daten

*Quelle: David Rosenthal, Das neue Datenschutzgesetz, in: Jusletter 16. November 2020

Swico
Lagerstrasse 33
CH-8004 Zürich

Tel. +41 44 446 90 90
www.swico.ch
info@swico.ch

SWICO
Der Wirtschaftsverband
für die digitale Schweiz

Es geht um alle Prozesse, die die Datenbearbeitung tangieren (Abläufe, Zuständigkeiten, weitere Ressourcen etc.). Verlangt werden angemessene Massnahmen, die aber dem Stand der Technik entsprechen müssen, also dem, was sich in der Praxis als wirksam erwiesen hat.

Was passiert bei einer Verletzung des Grundsatzes?
Die Verletzung des Konzepts «Privacy by Design» ist im revDSG an sich nicht sanktioniert. Der EDÖB kann aber auf das allgemeine Mittel der Anordnung gegenüber dem verantwortlichen Unternehmen nach revDSG zurückgreifen.

Privacy by Default

Die Pflicht zu Privacy by Default ist im Gegensatz zu Privacy by Design neu. Datenschutzfreundliche Voreinstellungen schützen die Nutzer von privaten Online-Angeboten, die sich weder mit Nutzungsbedingungen noch mit den daraus abzuleitenden Widerspruchsrechten auseinandergesetzt haben. Dazu werden nur die für den Verwendungszweck unbedingt nötigen Daten bearbeitet, solange der Nutzer nicht weitergehende Bearbeitungen autorisiert. Um dieses Schutzniveau des neuen Gesetzes zu gewährleisten, sollten Schweizer Unternehmen ihre Angebote rechtzeitig überprüfen und nötigenfalls durch Einsatz datenschutz- und kundenfreundlicher Programme Anpassungen vornehmen.

Beispiel für Privacy by Default:

Sieht ein Unternehmen mittels eingesetzter Software mehrere Möglichkeiten vor, wie Personendaten bearbeitet werden können und kann eine Nutzerin diese Möglichkeiten selbst über Datenschutzeinstellungen anpassen, so muss die Standardeinstellung die am wenigsten weitgehende Einstellung vorsehen.

Die Bestimmung kommt dort an ihre Grenzen, wo der Verantwortliche dem Benutzer keine technische Wahlmöglichkeit anbietet, weil dort eben keine Voreinstellungen möglich sind. Art. 7 greift in diesem Fall nicht. Die Pflicht schreibt dem Verantwortlichen zudem nicht vor, dass er den Benutzern (z.B. einer App oder eines Geräts) Wahlmöglichkeiten anbieten muss. Wenn dies gemacht wird, muss die Voreinstellung aber auf das für die Verwendung nötige Mindestmass beschränkt sein.

Datensicherheit und TOMs

Gemäss Art. 8 revDSG haben Verantwortliche (und Auftragsdatenbearbeiter) mit technischen und organisatorischen Massnahmen (kurz: TOMs) für angemessene Datensicherheit zu sorgen. (Siehe hierzu Swico, Q&A zum revDSG, Kapitel 13).

Typische Massnahmen zur Erreichung angemessener Datensicherheit sind beispielsweise:

- Zugangskontrolle: Unbefugten wird zu den Orten, wo Personendaten bearbeitet werden, der Zugang verwehrt. Beispiel: Ein Serverraum, der nur Mittels Badge zugänglich ist.

- Speicherkontrolle: Personen ohne Befugnis können Daten nicht anpassen oder löschen. Beispiel: PCs von Mitarbeitenden sind mit Passwort und Zwei-Faktor Authentifizierung gesichert.
- Transportkontrolle: Bei Bekanntgabe oder Transport werden Daten vor unbefugtem Zugriff geschützt. Beispiel: Beim Versand von Personendaten per Mail verwenden wir Ende-zu-Ende Verschlüsselung.

- Systemsicherheit: Bekannte Lücken in Betriebssystemen und Software werden stets auf aktuellem Sicherheitsstandard gehalten. Bekannte Lücken werden geschlossen. Beispiel: Updates für das verwendete Betriebssystem werden umgehend installiert.

Das Gesetz schreibt keine bestimmten Massnahmen vor. Sie müssen keinen absoluten Schutz bieten, sondern bei einer objektiven Betrachtung dem Grundsatz standhalten.

Was passiert bei einer Verletzung der Datensicherheit?

Bei einer Verletzung sieht das Gesetz eine Meldepflicht vor. Die vorsätzliche Verletzung von Art. 8 revDSG kann mit einer Busse von bis zu CHF 250'000.- belegt werden.

Für Rückfragen:

Ivette Djonova
SWICO
Head Legal & Public Affairs
Direkt: +41 44 446 90 89