DAS REVIDIERTE DSG - “PRIVACY BY DESIGN”

EINFÜHRUNG/HINTERGRUND

Das Schweizer Parlament hat am 25. September 2020 das totalrevidierte Datenschutzgesetz (revDSG) angenommen. Es ersetzt den bisherigen Erlass aus dem Jahre 1992 und trägt somit der dramatischen technischen Entwicklung und den Anforderungen der EU-Datenschutzgrundverordnung (DSGVO) Rechnung. Das Inkrafttreten des Gesetzes wird im Verlauf von 2022 erwartet.

Welche Datensätze sind betroffen?

Das revDSG regelt zukünftig ausschließlich den Datenschutz von natürlichen Personen und nicht mehr die Daten von juristischen Personen (z.B. GmbH, AG, Vereine). Im Mittelpunkt stehen hierbei persönlich identifizierbare Informationen (PII) anhand derer die Identität einzelner Personen abgeleitet werden kann. Die Liste der besonders schützenswerten Personendaten wird um Daten über die Ethnie, genetische und biometrische Daten (z.B. Fingerabdruck), die eine natürliche Person eindeutig identifizieren, erweitert.

Das Gesetz unterscheidet zwischen Profiling und Profiling mit hohem Risiko. Unter Profiling von Personendaten versteht man die automatisierte Bearbeitung von Daten zur Bewertung von bestimmten persönlichen Aspekten einer natürlichen Person. Profiling mit hohem Risiko liegt dann vor, wenn Personendaten automatisiert bearbeitet werden und eine Verknüpfung von Daten die Beurteilung wesentlicher Aspekte der Persönlichkeit erlaubt. Bei Profiling mit hohem Risiko muss immer eine Einwilligung ausdrücklich erfolgen.

Welche Grundsätze der Datensicherheit treffen zu?

Zunächst hat der Verantwortliche Datenbearbeiter sicher zu stellen, dass die Bearbeitung der Personendaten rechtmäßig ist. Hierzu ist ein Wissen und Überblick über die Gesamtheit der Datensätze im Unternehmen unabdingbar. Das revDSG verlangt daher ein Verzeichnis sämtlicher Datenbearbeitungen („Verzeichnis der Datenbearbeitungen“) von den Unternehmen. Mithin ist dies die Voraussetzung eines effektiven Datenschutzes.

Weiterhin gilt, dass der Verantwortliche die Datenbearbeitung ab der Planung so gestalten muss, dass die Datenschutzvorschriften und insbesondere die Bearbeitungsgrundsätze eingehalten werden (Privacy by Design). Weiter müssen die Voreinstellungen so eingestellt sein, dass die Bearbeitung von Personendaten auf das für den Verwendungszweck notwendige Mindestmaß beschränkt ist, soweit die betroffene Person nicht etwas anderes bestimmt (Privacy by Default).

Werden die Datensätze nicht mehr zur Bearbeitung benoetigt, sind diese zu vernichten oder zu anonymisieren.

Weiter ist der Verantwortliche verpflichtet, eine Datenschutz-Folgenabschätzung vorzunehmen, wenn eine Datenbearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann. Dabei sind die geplante Bearbeitung, die entstehenden Risiken sowie geeignete Maßnahmen dagegen zu beschreiben.

Was ist im Falle einer Verletzung des Datenschutzes zu tun?

Bei einer Datenschutzverletzung hat der Verantwortliche dem EDÖB (Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter) so schnell wie möglich Meldung zu erstatten, wenn große Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Personen bestehen. Zudem müssen in der Regel auch die Betroffenen informiert werden, sofern dies zu ihrem Schutz erforderlich ist. Auch der Auftragsbearbeiter (z.B. ein Outsourcing-Unternehmen) muss eine Verletzung der Datensicherheit so schnell wie möglich dem Verantwortlichen melden, der dann die weiteren Schritte einzuleiten hat.

Neu im revDSG ist, dass natürliche Personen bei vorsätzlicher Verletzung der Informations- und Auskunftspflichten sowie der Sorgfaltspflichten neu mit Buße bis CHF 250'000 bestraft werden können!

Wie datenbezogener Datenschutz helfen kann

Die umfassenden Datenschutzanforderungen des revidierten DSG sind hier nur angerissen worden, aber es wird schnell deutlich, dass eine Menge Arbeit auf die betroffenen Unternehmen zukommt. Um Personendaten effektiv schützen zu können, muss man wissen welche Daten vorliegen und wo diese zu finden sind (‚Bearbeitungsverzeichnis'). Im ersten Schritt ist eine Ermittlung und Klassifizierung der vorliegenden Daten durchzuführen. Danach ist festzulegen wie die Daten am besten zu schützen sind. Herkömmliche Datenschutzmethoden wie z.B. die Verschlüsslung von Speichermedien greifen hier meist zu kurz.

Eine effektive Maßnahme, um Personendaten zu schützen, ist die Tokenisierung von sensitiven Daten. Bei der Tokenisierung werden sensitive Daten (z.B. Kreditkartennummer, Sozialversicherungsnummer, Mobiltelefonnummer, etc.) mit einem Algorithmus unkenntlich gemacht und durch einen Token ersetzt. Dieser Token hat das gleiche Format wie der ursprüngliche Datensatz und kann ohne weiteres von nachgelagerten Anwendungen verwendet werden. Der Token hat für einen Hacker keinen monetären Wert.

Diese Verfahrensweise ermöglicht es den Anwendern, den Anforderungen von Datenschutzgesetzen gerecht zu werden und sich vor Datenmissbrauch im Falle eines Angriffs zu schützen.

SCHLUSSBEMERKUNG

Auch wenn das revDSG erst im Jahr 2022 in Kraft treten wird, sind alle Bearbeiter von Personendaten angehalten, die Regelungen des revDSG bereits heute umzusetzen.

Bis zum Inkrafttreten des revDSG ist Unternehmen zu empfehlen, dass sie zunächst eine Bestandsaufnahme ihrer Datenbearbeitungen (Personendaten) durchführen, um anschliessend im Rahmen einer Gap-Analyse den datenschutzrechtlichen Handlungsbedarf festzustellen.

Für weiterführende Informationen zu den technisch möglichen Lösungen rund um den Datenschutz, lesen Sie bitte die Kurzfassung von comforte's Datenschutzlösungen.

MEHR ERFAHREN