Inkrafttreten am 1. September 2023

Neues Bundesgesetz über den Datenschutz

Das 2010 lancierte Verfahren für die Revision des Datenschutzgesetzes (DSG) hat sich in die Länge gezogen. Das Gesetz wurde schliesslich im September 2020 verabschiedet und wird am 1. September 2023 in Kraft treten. Es verfolgt zwei Ziele: Erstens muss das bestehende Gesetz an das digitale Umfeld angepasst werden. Zweitens muss es sich der europäischen Gesetzgebung annähern. Angesichts der Zeit, die das Verfahren in Anspruch genommen hat, ist keine Übergangsfrist vorgesehen. Unternehmen müssen sich deshalb schon jetzt auf die Änderungen vorbereiten. Erklärungen zu dem, was sich ändert – und was unverändert bleibt.

Martina Guillod

Der vorliegende Artikel behandelt das eidgenössische Datenschutzgesetz (DSG), das auf die Bearbeitung von Daten durch Privatunternehmen anwendbar ist. Es sei allerdings darauf hingewiesen, dass jeder Kanton über sein eigenes Datenschutzgesetz verfügt, das auf den Umgang mit Daten durch den Kanton oder die Gemeinden anwendbar ist und das gemäss kantonaler Planung revidiert wird.

Es kann auch sein, dass gewisse Unternehmen bereits der europäischen Datenschutz-Grundverordnung (DSGVO) unterstehen, die im Mai 2018 in der Europäischen Union in Kraft getreten ist. Das ist der Fall für Unternehmen, die europäischen Konsumentinnen und Konsumenten Dienstleistungen (z. B. via einen Online-Shop) anbieten oder die das Verhalten der Kundinnen und Kunden in der EU beobachten. Für Unternehmen, die sich bereits an die DSGVO angepasst haben, bringt das neue Gesetz nur kleine Veränderungen.

Was unverändert bleibt

Die grundlegenden Prinzipien des Datenschutzes bleiben unverändert. Insgesamt sind es deren sechs: Treu und Glauben; Pflicht, im Hinblick auf das zu erreichende Ziel so wenig Daten wie möglich zu bearbeiten (Verhältnismässigkeit); Pflicht, über die Bearbeitung der Daten zu informieren (Information); Pflicht, ausschliesslich korrekte Daten zu bearbeiten und fehlerbehaftete Daten zu korrigieren (Richtigkeit); Pflicht, die gesammelten Daten nur für den Zweck zu verwenden, der bei deren Beschaffung angegeben wurde (Zweckbestimmung); Pflicht, Daten gesichert zu bearbeiten (Sicherheit).

Die Datenbearbeitung ist zulässig, wenn keiner der oben genannten Grundsätze verletzt wurde, die betroffene Person die Bearbeitung nicht ausdrücklich ablehnt und es sich nicht um sensible Daten handelt, die an einen Dritten weitergegeben werden. Wenn diese Voraussetzungen nicht erfüllt sind, muss die Person, welche die Daten bearbeiten will, einen Rechtfertigungsgrund haben (Gesetz, überwiegendes Interesse oder Einwilligung der betroffenen Person). Fehlt dieser, ist eine Bearbeitung der Daten nicht statthaft.

Neuerungen

- **Privacy by design und privacy by default:** Schon bei der Planung des Produkts oder der Dienstleistung muss das Unternehmen geeignete Massnahmen ergreifen, damit das Produkt DSG-konform ist. Die Daten müssen automatisch durch eine Standardeinstellung geschützt werden, ohne das der Benutzer diese aktivieren muss.

- **Verzeichnis der Bearbeitungstätigkeiten:** Unternehmen müssen ein internes Dokument führen, das insbesondere Auskunft gibt über die Kategorien der bearbeiteten Daten, die betroffenen Personen, den Zweck der Bearbeitung, die Kategorien von Empfängern, die Dauer, während der die persönlichen Daten aufbewahrt werden, sowie die getroffenen Sicherheitsmassnahmen. Unternehmen, die weniger als 250 Personen beschäftigen, sind von dieser Pflicht ausgenommen, es sei denn, die Bearbeitung erstrecke sich auf sensible Daten in grossem Ausmass (z. B. in einer Arztpraxis) oder beinhalte ein Profiling mit erhöhtem Risiko.

- **Informationspflicht:** Die Person, welche die Daten bearbeitet, muss informieren über Identität und Kontaktangaben der für die Bearbeitung verantwortlichen Person, über den Zweck der Bearbeitung und allenfalls über die Empfänger oder Empfängerkategorien, denen die persönlichen Daten übermittelt werden. Erfolgt eine Datenübermittlung von personenbezogenen Daten ins Ausland (dazu gehört auch die Speicherung von Daten in einer Cloud), muss die für die Bearbeitung verantwortliche Person über das Zielland und das angebotene Schutzlevel informieren. Diese Informationen können beispielsweise auf der Website des Unternehmens aufgeführt werden.

- **Informationspflicht bei einer automatisierten Einzelentscheidung:** Die betroffene Person muss informiert werden, wenn eine sie betreffende Entscheidung ausschliesslich auf der Grundlage einer automatisierten Bearbeitung (Algorithmus) ohne menschliches Zutun gefällt wurde. Sie hat anschliessend das Recht auf eine Überprüfung des Entscheids durch eine physische Person.

- **Folgenabschätzung:** Besteht ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person (beispielsweise bei der Bearbeitung von sensiblen Personendaten in grossem Ausmass), erstellt die für die Bearbeitung verantwortliche Person vorgängig eine Datenschutz-Folgenabschätzung. Bislang galt diese Verpflichtung nur für die Bearbeitung von sensiblen Daten. Neu ist sie auf alle personenbezogenen Daten anwendbar. Die Abschätzung muss eine Bewertung der Risiken enthalten und Schutzmassnahmen vorschlagen.

- **Meldung von Verletzungen der Datensicherheit:** Verletzungen der Datensicherheit, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit der betroffenen Personen führen, müssen dem eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) gemeldet werden.

- **Recht auf Datenherausgabe und -übertragung:** Die betroffene Person hat das Recht, von der für die Bearbeitung verantwortlichen Person die Herausgabe der Personendaten zu verlangen, die sie ihr elektronisch weitergegeben hatte. Sie kann zudem die Übergabe der Daten in einem gängigen elektronischen Format verlangen.

- **Strafbestimmungen:** Der EDÖB muss künftig von Amtes wegen eine Untersuchung eröffnen, wenn er eine Datenbearbeitung feststellt, die gesetzeswidrig ist. Er ist aber nicht berechtigt, administrative Bussen auszusprechen. Das DSG sieht bei vorsätzlicher Zuwiderhandlung Bussen bis zu einer Höhe von 250 000 Franken vor. Es ist wichtig zu wissen, dass es grundsätzlich die Person ist, die zur Verantwortung gezogen wird. Das Unternehmen wird nur dann bestraft, wenn die Identifizierung der verantwortlichen Person einen unverhältnismässigen Untersuchungsaufwand erfordern würde.