usercentrics

Das Schweizer Bundesgesetz über den Datenschutz (DSG): Wissenswertes

Übersicht

- Es tritt am 1. September 2023 in Kraft, keine Nachfrist für Datenschutzkonformität.
- Die Einwilligung zur Datenerfassung/-verarbeitung ist nicht unter allen Umständen erforderlich.
- Es gilt für natürliche Personen (nicht mehr für juristische Personen) sowie kommerzielle und nichtkommerzielle Organisationen, die die Daten von Schweizer Bürgern verarbeiten.
- Organisationen sind selbst dann für eine datenschutzkonforme Datenverarbeitung verantwortlich, wenn sie dazu Dritte (wie etwa Lieferanten) einsetzen.
- Alle Verarbeiter müssen angemessene organisatorische und technische Maßnahmen ergreifen, um den Datenschutz und die Sicherheit zu gewährleisten.
- Es gilt für Daten in Akten und elektronischen Dateien.
- Extraterritoriales Recht: Organisationen, die personenbezogene Daten verarbeiten, müssen ihren Sitz nicht in der Schweiz haben.
- Es verbietet die Übermittlung personenbezogener Daten aus der Schweiz in Länder, mit denen keine Angemessenheitsvereinbarung besteht, es sei denn, die ausdrückliche Einwilligung des Nutzers wurde eingeholt.

Einwilligungsanforderungen

Im Gegensatz zur DSGVO erlaubt das DSG Organisationen die Verarbeitung personenbezogener Daten ohne konkrete Rechtsgrundlage, es sei denn, die Verarbeitung erfüllt bestimmte Kriterien. Die Einwilligung ist in folgenden Fällen erforderlich:

- Bei der Verarbeitung sensibler personenbezogener Daten
- Bei der Verarbeitung im Rahmen einer Hochrisiko-Profilerstellung durch eine Privatperson
- Bei der Verarbeitung im Rahmen einer Profilerstellung durch eine Bundesbehörde (Regierung)
- Bei der Übermittlung von Daten in Drittländer, in denen kein angemessener Datenschutz besteht

Das DSG gestattet neben der Einwilligung andere Rechtsgrundlagen für die Verarbeitung (wie Gesetze oder das vorrangige öffentliche Interesse), jedoch in geringerem Umfang als die DSGVO. Wenn eine Einwilligung erforderlich ist, muss diese vor oder zum Zeitpunkt der Datenerfassung eingeholt werden. Wie auch bei der DSGVO muss die Einwilligung des Nutzers gemäß des DSG granular, informiert und freiwillig erfolgen.

Eine Consent Management Platform ermöglicht datenschutzkonforme Nutzerbenachrichtigungen, z. B. durch die Erstellung einer Datenschutzerklärung, sowie die datenschutzkonforme Erfassung und Speicherung von Einwilligungen. Es können mehrere Konfigurationen mit Geolokalisierung verwendet werden, um die Einhaltung verschiedener Verordnungen mit unterschiedlichen Anforderungen, wie z. B. DSGVO und DSG, je nach Standort des Nutzers sicherzustellen.

Benachrichtigungsanforderungen

Die betroffenen Personen müssen stets vor der Datenerfassung informiert werden, auch wenn für die beabsichtigte Datenverarbeitung keine Einwilligung erforderlich ist.

Unternehmen müssen den Nutzern die folgenden Informationen klar vermitteln, z. B. mithilfe einer Datenschutzerklärung auf der Webseite. Dies sind die gleichen Benachrichtigungskriterien, die auch für eine gültige Einwilligung erforderlich sind:

- Identität des Datenverantwortlichen, sowohl Unternehmen als auch Dritte
- Kontaktdaten des Datenverantwortlichen
- Identität des Datenempfängers und aller weiteren Parteien mit Zugang zur Datendatei
- Empfängerland, falls die Daten über die Landesgrenzen hinaus übermittelt werden
- Zweck(e) der Datenerfassung und -nutzung
- Kategorien erfasster Daten, sofern relevant
- Mittel der Datenerfassung, sofern relevant
- Die Rechtsgrundlage für die Verarbeitung, sofern erforderlich
- Nutzerrechte bezüglich ihrer personenbezogenen Daten gemäß des DSG, einschließlich des Rechts, die Einwilligung zu verweigern oder zu widerrufen

Rechte der betroffenen Personen

Betroffene Personen haben gemäß des DSG die folgenden Rechte:

- Das Recht, zu erfahren, ob Daten über sie verarbeitet werden oder wurden (das vorausgehende Informationsrecht bleibt davon unberührt)
- Das Recht, Zugang zu den erfassten Daten zu erhalten
- Das Recht, ihre Daten kostenlos und in physischer Form (gedruckt oder fotokopiert) zu erhalten
- Das Recht, ihre personenbezogenen Daten berichtigen zu lassen, wenn diese fehlerhaft oder unvollständig sind (dieses Recht kann eingeschränkt, abgelehnt oder aufgeschoben werden, insbesondere in Fragen der Sicherheit, zum Schutz strafrechtlicher Ermittlungen oder zum Schutz der Interessen vorrangiger Dritter)

Checkliste für DSG-Konformität

- ✓ Erstellen oder aktualisieren Sie Ihre Datenschutzerklärungen und stellen Sie sicher, dass sie an Ihr Unternehmen, Ihre Nutzer, die Verarbeitungszwecke und die von Ihnen verwendeten Daten angepasst wurden.
  - Betroffene Personen sind über die Verarbeitung stets zu benachrichtigen, auch wenn keine Einwilligung erforderlich ist.
  - Mit einer Consent Management Platform können Sie Ihre Datenschutzerklärung erstellen und anpassen sowie aktualisieren.
- ✓ Stellen Sie sicher, dass in den Benachrichtigungen auch darüber informiert wird, in welche Länder personenbezogene Daten übermittelt werden.
  - Wenn es keine Angemessenheitsvereinbarung mit den jeweiligen Ländern gibt, machen Sie dies deutlich und holen Sie die ausdrückliche Einwilligung für die Weitergabe der Daten ein.
- ✓ Falls erforderlich, beispielsweise zur Verarbeitung sensibler personenbezogener Daten, holen Sie die Einwilligung des Nutzers ein und speichern Sie diese auf sichere Art und Weise.
- ✓ Erstellen oder aktualisieren Sie interne Datenverarbeitungsrichtlinien und sorgen Sie dafür, dass diese angemessen kommuniziert werden.
- ✓ Richten Sie ein internes Register der Datenverarbeitungsaktivitäten ein und pflegen Sie es.
- ✓ Führen Sie ein Verfahren ein, mit dem die berechtigten Anliegen betroffener Personen (die Ausübung ihrer Rechte) effizient entgegengenommen, bestätigt und bearbeitet werden, z. B. Anfragen bzgl. Kopien, Berichtigung oder Löschung personenbezogener Daten.
  - Sorgen Sie dafür, dass die Daten in einem zugänglichen Format, etwa als Ausdruck oder in einem gebräuchlichen elektronischen Format, vorhanden sind.
- ✓ Führen Sie eine Datenschutz-Folgenabschätzung durch – vor allem dann, wenn das Unternehmen in großem Umfang sensible Daten verarbeitet.
- ✓ Führen Sie ein Verfahren zum Umgang mit Datenschutzverletzungen ein, einschließlich der unverzüglichen Benachrichtigung des EDÖB und der betroffenen Personen, falls erforderlich. Dieser Prozess muss auch für Dritte gelten, die auf Daten zugreifen oder diese verarbeiten.
- ✓ Überprüfen und aktualisieren Sie Verträge mit Dritten (wie etwa Lieferanten) und stellen Sie so sicher, dass die Anforderungen an Sicherheit und Datenschutz in angemessener Weise erfüllt werden. (Die rechtliche Verantwortung liegt dabei jedoch bei der Erstpartei.)
- ✓ Bewahren Sie die Daten nur so lange auf, wie es gemäß der angegebenen Benachrichtigung erforderlich ist, und ausschließlich für den angegebenen Verarbeitungszweck. Löschen oder anonymisieren Sie Daten, sobald sie für diesen Zweck nicht mehr benötigt werden.
- ✓ Ernennen Sie einen Datenschutzbeauftragten, der im Kontakt mit Nutzern und dem EDÖB steht und zudem Richtlinien und Verfahren verwaltet.
- ✓ Wenden Sie sich bezüglich der Pflichten Ihres Unternehmens im Rahmen des DSG und der Möglichkeiten, diesen nachzukommen, an einen qualifizierten Rechtsberater. Aktualisieren Sie sie stets. Usercentrics bietet keine Rechtsberatung, sondern lediglich Hinweise zu Informationszwecken.