

Frage des Monats – Oktober 2022

Neues Schweizer Datenschutzgesetz - Was geht uns das an?

Die Antwort der Merki-Experten

Das neue Datenschutzgesetz wird am 1. September 2023 in Kraft treten.

Sämtliche Unternehmen in der Schweiz sind davon betroffen, unabhängig von ihrer Grösse oder Branche.

Zukünftig können auch gegen Einzelpersonen Bussen ausgesprochen werden bis zum Maximalbetrag von CHF 250'000.-. Nebst den Bussgeldern kann bei einem vorsätzlichen Verstoß gegen das neue DSG die verantwortliche Person (z.B. Geschäftsführer oder Verwaltungsrat) zur Rechenschaft gezogen werden.

Das neue Datenschutzgesetz enthält verschiedene Neuerungen;

1. **Nur noch die Daten natürlicher Personen sind künftig betroffen**, die von juristischen Personen nicht mehr.
2. **Genetische und biometrische Daten** werden in die Definition der besonders schützenswerten Daten aufgenommen.
3. **Die Grundsätze "Privacy by Design" und "Privacy by Default"** werden eingeführt.
4. **Folgenabschätzungen** müssen durchgeführt werden, sofern ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen besteht.
5. Die Informationspflicht wird ausgeweitet: Bei jeder Beschaffung von Personendaten – und nicht mehr nur von sogenannten besonders schützenswerten Daten – muss die betroffene Person vorgängig informiert werden.
6. **Ein Verzeichnis der Bearbeitungstätigkeiten** wird obligatorisch. Die Verordnung zum Gesetz sieht jedoch eine Ausnahme für KMU vor, deren Datenbearbeitung nur ein geringes Risiko von Verletzungen der Persönlichkeit von betroffenen Personen mit sich bringt.
7. **Eine rasche Meldung** ist erforderlich, wenn die Datensicherheit verletzt wurde. Sie ist an den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) zu richten.
8. **Der Begriff Profiling** (die automatisierte Bearbeitung personenbezogener Daten) wurde in das Gesetz aufgenommen.

Welche Anpassungen an das Datenschutzgesetz sind nötig?

Gerade KMU kämpfen mit neuen Anforderungen. Als Vorbereitung für die Anpassung an das neue DSG sollten die im Rahmen der Geschäftstätigkeit bearbeiteten Daten analysiert werden. Je mehr Daten besonders schützenswert sind (zum Beispiel im Zusammenhang mit Religion, Gesundheit, Betreibungen usw.), desto höher sind die Anforderungen.

Des Weiteren sollte überprüft werden, welche grundsätzlichen Risiken bei der Datensicherheit bestehen und ob diese durch technische und organisatorische Massnahmen (z.B. Zugriffskontrolle) minimiert werden.

Sobald ein Überblick über die Daten und Risiken verschafft wurde, können die wichtigsten Vorkehrungen getroffen werden.

Die Schweizer KMU müssen folgende zwölf Massnahmen umsetzen, um sich an das neue DSG anzupassen:

1. **Datenschutzerklärungen im Internet, in Werbe und Verkaufsdokumenten:** Erstellen oder überprüfen und anpassen
2. **Datenbearbeitungsrichtlinien:** Erstellen oder überprüfen und anpassen.
3. **Datenbearbeitungsverzeichnis:** Erstellen oder überprüfen und anpassen.
4. **Betroffenenrechte:** Implementieren eines Prozesses zur fristgerechten Bearbeitung.
5. **Datenschutzverletzungen:** Implementieren eines Prozesses zur fristgerechten Meldung.
6. **Datenschutz-Folgenabschätzung:** Implementieren eines Prozesses.
7. Verträge mit den Auftragsbearbeitern: Überprüfen und anpassen, insbesondere bezüglich Meldepflicht bei Datenschutzverletzungen, der Weitergabe an Unterauftragnehmer und der Datensicherheit.
8. **Personendaten:** Sicherstellen, dass diese gelöscht oder anonymisiert werden, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind.
9. **Personendaten:** Sicherstellen, dass diese nur an Länder bekanntgegeben werden und in Länder gespeichert werden (auch Cloud), die einen angemessenen Schutz gewährleisten. Der Bundesrat publiziert eine entsprechende Liste. Soweit die Länder nicht auf dieser Liste aufgeführt sind, dürfen Daten unter bestimmten Bedingungen dennoch exportiert werden, unter anderem mit dem ausdrücklichen Einverständnis der Betroffenen.
10. **Datensicherheit:** Sicherstellen durch geeignete technische und organisatorische Massnahmen. Da die Datenübermittlung per E-Mail unsicher ist, sollte zumindest bei besonders schützenswerten Personendaten eine E-Mail-Verschlüsselung zur Verfügung stehen. Der Bundesrat muss die Mindestanforderungen noch festlegen.
11. **Datenportabilität:** Sicherstellen der Datenherausgabe in einem gängigen elektronischen Format, wenn die Daten elektronisch und vor allem in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags bearbeitet werden.
12. **Datenschutzberater*in:** Ernennen eines Datenschutzberaters und dem EDÖB melden (empfohlen). Die Kontaktdaten müssen veröffentlicht werden. Gemäss DSGVO ist die Ernennung zwingend.

Quelle:

<https://www.kmu.admin.ch/kmu/de/home/faktentrends/digitalisierung/datenschutz.html>

(zuletzt aufgerufen am: 30.09.2022)

Allgemein kann festgehalten werden: analysiere und informiere darüber, welche Daten wie, wo, warum, mit wem und wie lange gesammelt werden. Implementiere und dokumentiere hierzu die notwendigen Prozesse.

Eine Datenschutzerklärung ist aufgrund der neuen Informationspflicht absolut notwendig.