Merkblatt revidiertes Datenschutzgesetz für KMU

1. Ausgangslage

Das revidierte Datenschutzgesetzt (DSG) gilt seit dem 01.09.2023 und schützt personenbezogene Daten vor Verlust und Missbrauch. Die neuen Regelungen sind deutlich restriktiver geworden. Unternehmen die in den EU-Raum exportieren oder personenbezogene Daten aus dem EU-Raum bearbeiten, müssen zudem die Bestimmungen des DSGVO einhalten. Dieses Merkblatt gilt nur für das neue, schweizerische Datenschutzgesetz.

2. Inhalt des DSG

Das DSG verpflichtet KMU zu folgenden Massnahmen:

- Bestimmung eines Datenschutzverantwortlichen in der Geschäftsleitung
- Geeignete technische und organisatorische Massnahmen zum Schutz personenbezogener Daten umsetzen
- Eine Datenschutzerklärung und ein Impressum zu erstellen und auf der Website zu veröffentlichen
- Auskunftsbegehren von Personen über Ihre gesammelten Daten innerhalb von 30 Tagen beantworten
- Anträge zur Berichtigung oder Löschungen von Daten bearbeiten und umzusetzen
- Mitarbeiter für die Belange personenbezogener Daten zu sensibilisieren
- Meldepflicht bei Verlust oder Missbrauch personenbezogener Daten

3. Erleichterungen für KMU

Für Unternehmen bis 250 Mitarbeiter gibt es wesentliche Erleichterungen, denn sie müssen im Regelfall kein Bearbeitungsverzeichnis führen (wo werden welche Daten wie lange und zu welchem Zweck gespeichert). Dies gilt für alle KMU, die keine «besonders schützenswerte» Personendaten im grösseren Umfang sammeln.

4. Was sind «besonders schützenswerte Personendaten?

Das DSG hat folgende Klassifizierung für besonders schützenwerte Personendaten festgelegt:

- Genetische oder biometrische Daten
- Gesundheitsdaten
- Rassische und ethnische Herkunft
- Politische Meinung
- Religionszugehörigkeit
- Weltanschauliche Überzeugung
- Sexualleben oder sexuelle Orientierung
- Strafrechtliche Verfolgung und Sanktionen
- Sozialhilfe Bezug
- Gewerkschaftszugehörigkeit
- Profiling mit hohem Risiko (Persönlichkeitsprofile)

5. Umsetzung der Massnahmen aus dem DSG

Wir empfehlen unseren Kunden folgende Vorgehensweise:

- Verschaffen Sie sich einen Überblick, welche personenbezogene Daten wo gespeichert werden. Typischerweise werden solche Daten im ERP, CRM sowie auf der Website (Cookies) und im Personalwesen gesammelt.
- Vergewissern Sie sich, dass keine besonders schützenswerte Daten im grösseren Umfang gesammelt werden (falls doch, müssen Sie ein Bearbeitungsverzeichnis erstellen)

- Bestimmen Sie einen Datenschutzverantwortlichen für Ihr Unternehmen. Wir raten von einem externen Datenschutzverantwortlichen ab, denn dieser hat gegenüber der Geschäftsleitung in Datenschutzthemen eine Weisungsbefugnis. Lassen Sie sich allenfalls von externen Spezialisten beraten.
- Erstellen Sie eine Datenschutzerklärung und ein Impressum und veröffentlichen Sie diese auf Ihrer Website. Vorlagen und Muster finden Sie im Internet oder Sie können diese auch bei uns kostenlos beziehen. Die Datenschutzerklärung muss folgende Fragen beantworten:
    - Wie wir Daten sammeln
    - Welche Daten wir erfassen
    - Warum wir diese Daten erfassen
    - An wen wir die Daten weitergeben
    - Wo die Daten gespeichert werden
    - Wie lange die Daten vorgehalten werden
    - Wie wir die Daten schützen
    - Auskunftsrecht
- Prüfen Sie, welche technische und organisatorische Massnahmen zum Schutz vor Verlust und Missbrauch der Daten umgesetzt werden müssen. Mit dem Aspekt von «Verlust und Missbrauch der Daten» wurde das Datenschutzgesetz und die IT-Sicherheit unzertrennlich vereint. Beachten Sie dazu unser Merkblatt über IT-Sicherheit in KMU.
- Falls Sie auf Ihrer Website nicht nur technisch notwendige Cookies einsetzen, müssen Sie aktiv eine Zustimmung von Ihren Besuchern einholen (Cookie-Banner).
- Erstellen Sie Vorlagen für die Beantwortung von Auskunftsbegehren. Sie finden im Internet entsprechende Muster oder Sie können diese bei uns kostenlos beziehen.
- Informieren, sensibilisieren und schulen Sie Ihre Mitarbeiter in Bezug auf das DSG und der IT-Sicherheit

6. Sanktionen

Bei Missachtung der Massnahmen drohen Bussen bis maximal CHF 250'000. Diese Sanktionen treffen nicht die betroffenen Unternehmen, sondern den Datenschutzverantwortlichen oder ein leitendes Mitglied der Geschäftsleitung. Bussen ab CHF 5'000 führen zu einem Eintrag im Strafregister. Strafbar ist nur vorsätzliches (oder eventualvorsätzliches) Handeln oder Unterlassen.