Merkblatt zum neuen Datenschutzgesetz

Stand: 1.09.2023

Das neue Datenschutzgesetz ist am 1. September 2023 in Kraft getreten und ab sofort einzuhalten. Prüfen Sie mit unserer Checkliste auf Seite 4, wo Ihr Unternehmen beim Thema Datenschutz steht[1].

Wichtige Begriffe kurz erklärt:

Was sind Personendaten?

Alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen.
Bsp.: Name, Adresse, E-Mail-Adresse, Telefonnummer, IP-Adresse

Was bedeutet bearbeiten?

Jeder Umgang mit Personendaten. Beispiele: Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten

Was muss ich als Unternehmer:in tun?

1) Überblick verschaffen (Datenbearbeitungsverzeichnis)

Verschaffen Sie sich einen Überblick über die Datenbearbeitung, die in Ihrem Unternehmen stattfindet. Vergessen Sie dabei nicht, dass jeder Umgang mit Daten, die sich auf bestimmte oder bestimmbare Personen beziehen, eine Datenbearbeitung darstellt.
Halten Sie in einem schriftlichen Verzeichnis (Datenbearbeitungsverzeichnis) fest, welche Kategorien von Daten Sie für welche Zwecke bearbeiten, wo Sie die Daten speichern und wann Sie diese löschen. Bewahren Sie das Verzeichnis auf und aktualisieren Sie es regelmässig. Das Verzeichnis dient Ihnen als Übersicht und muss nicht veröffentlicht werden.

[1]Dieser Beitrag soll zu einer ersten Orientierung und Selbsteinschätzung dienen. Unsere Empfehlungen erheben keinen Anspruch auf Vollständigkeit und erfolgen ohne Gewähr. Ob Ihr Unternehmen tatsächlich alle gesetzlichen Anforderungen erfüllt, verlangt nach einer einzelfallorientieren Beurteilung.

2) Informieren (Datenschutzerklärung)

Informieren Sie die betroffenen Personen in einer Datenschutzerklärung darüber, welche Datenkategorien Sie zu welchem Zweck bearbeiten und an welche Kategorie von Empfängern Sie Personendaten weitergeben. Informieren Sie betroffene Personen, wenn Sie deren Daten ins Ausland transferieren – denken Sie z.B. an Cloud-Lösungen oder IT-Dienstleistungen mit Servern im Ausland. Stellen Sie den Betroffenen Ihre Kontaktdaten zur Verfügung, sodass diese Sie bei Fragen oder Anliegen zum Datenschutz kontaktieren können.

3) Datensicherheit gewähren

Überlegen Sie sich anhand Ihres Datenbearbeitungsverzeichnisses, wo Risiken für die betroffenen Personen bestehen (z.B. Kund:innen und Mitarbeiter:innen) und wie Sie diese Risiken mit angemessenen und Ihnen zumutbaren technischen und organisatorischen Massnahmen minimieren können. Bsp.: Passwort- und Virenschutz, Berechtigungskonzept, Datenverschlüsselung, interne Datenschutzrichtlinien, Anpassung von Verträgen etc.. Sobald eine Datenbearbeitung ein hohes Risiko für die Betroffenen darstellen könnte, ist eine Datenschutz-Folgenabschätzung (Risikoanalyse) durchzuführen.

4) Berechtigungs- und Löschkonzept erstellen

Erstellen Sie ein geeignetes Berechtigungs- und Löschkonzept. Beachten Sie jedoch gesetzliche Aufbewahrungspflichten und Ihre berechtigten Interessen an der Aufbewahrung (z.B. zur Abwehr von Forderungen).

5) Verträge anpassen und erstellen

Prüfen Sie, im Rahmen welcher Abläufe Sie Daten an Dritte weitergeben (z.B. Outsourcing) und verpflichten Sie die Empfänger mit sog. Auftrags-bearbeitungsverträgen zur Einhaltung des Datenschutzes.

6) Einhalten der Grundprinzipien

Bei jedem Umgang mit Personendaten (Bearbeiten) sind die Grundprinzipien des DSG zu beachten (Art. 6 und 8 DSG). Es müssen alle Grundprinzipien eingehalten werden. Im Zentrum für die Mitarbeitenden stehen aber die Zweckmässigkeit und die Verhältnismässigkeit. Das Prinzip der Zweckmässigkeit besagt, dass die Beschaffung und Bearbeitung von Personendaten nur zu einem bestimmten Zweck erfolgen darf. Sie müssen die Betroffenen über den Zweck informieren und die Daten grundsätzlich nach Zweckerreichung löschen. Das Prinzip der Verhältnismässigkeit lässt sich am einfachsten mit dem Grundsatz der Datenminimierung erklären. Bearbeiten Sie so wenig Daten wie möglich. Dies gilt mit Blick auf die Menge der Daten (wenig in Bezug auf Volumen), auf die Speicherdauer (wenig in Bezug auf Zeit) oder auf die Menge der bearbeitenden Personen (wenig in Bezug auf Zugriffsberechtigte = "Need-to-Know"). Entsprechend ist wie unter Ziffer 5 erwähnt, ein Berechtigungskonzept und ein Löschkonzept umzusetzen. Speziell zu erwähnen ist auch das Prinzip der Datensicherheit, welches verlangt, dass eine dem Risiko angemessene Datensicherheit garantiert wird.

7) Datensicherheit im Ausland garantieren

Prüfen Sie, ob Sie Daten ins Ausland transferieren und ob in diesem Land ein angemessener Datenschutz garantiert ist (i.d.R. trifft dies auf die EU zu). Sollten Sie Daten in andere Staaten weitergeben, so sind weitergehende Massnahmen wie z.B. der Einsatz von Standardvertragsklauseln notwendig.

8) Meldeverfahren einhalten

Sollte der Fall eintreten, dass die Datensicherheit verletzt wird (z.B. E-Mail an falschen Empfängerkreis versendet, Cybercrime, Datenverlust etc.), prüfen Sie so schnell wie möglich, ob eine Meldung an den EDÖB oder an die betroffenen Personen nötig und sinnvoll ist.

9) Einhaltung der allgemeinen Bearbeitungsgrundsätze

- Bearbeiten Sie nur so viele Daten wie nötig und löschen Sie die Daten, sobald sie diese nicht mehr benötigen.
- Bearbeiten Sie Daten nur zum im Voraus kommunizierten Zweck.
- Kommunizieren Sie transparent darüber, welche Daten Sie zu welchem Zweck bearbeiten, an wen und in welche Länder Sie diese weitergeben.
- Bewahren Sie Daten sicher auf.

Checkliste zum neuen Datenschutz

Stand: 1.9.2023

Schritt 1: Projektierung

- Bestandesaufnahme und Bearbeitungsverzeichnis
- Datensicherheit (technische und organisatorische Massnahmen)

Schritt 2: Extern wirksame Massnahmen

- Erstellung einer Datenschutzerklärung (Informationspflicht)
- Sicherstellung der Betroffenenrechte
- Ausarbeitung eines Löschkonzepts
- Regelung vom Datentransfer ins Ausland

Schritt 3: Intern wirksame Massnahmen

- Erstellung eines Auftragsbearbeitungsvertrags
- Einführung von Reglementen und Mitarbeiterschulungen
- Vornahme einer Datenschutz-Folgenabschätzung
- Erstellung eines Prozesses zur Meldepflicht
- Erstellung eines Prozesses zur Datenübertragbarkeit / Speicherbegrenzung