TREUHAND|SUISSE

IST IHR UNTERNEHMEN BEREIT?

Das neue Datenschutzgesetz tritt auf 1. September 2023 in Kraft. Damit werden Unternehmen noch stärker verpflichtet, ihre Kunden-, Mitarbeiter-, Finanz- und anderen sensiblen Daten bestmöglich zu schützen. Eine Empfehlung, wie man Schritt für Schritt an diese Aufgabe herangeht.

Das neue Datenschutzgesetz betrifft uns alle.

Fast jedes Unternehmen erfasst und bearbeitet Daten, die vom Datenschutzgesetz betroffen sind. Diese zwölf Punkte helfen Ihnen bei der Analyse, wo Sie handeln müssen. Holen Sie sich dafür die Unterstützung Ihres IT- oder Treuhandpartners.

1. Datenschutzerklärung

Brauchen Sie eine Datenschutzerklärung für Ihre Website oder für die Kundenverträge? Sobald Sie Personendaten bearbeiten, haben Sie eine Informationspflicht. In der Datenschutzerklärung machen Sie den Betroffenen gegenüber transparent, was Sie mit den Daten genau tun. Mit Blick auf das neue Gesetz ist das Ausarbeiten einer Datenschutzerklärung eine Hauptaufgabe.

2. Richtlinien für die Datenbearbeitung

Wenn Sie Ihre Standards für die Datenbearbeitung festlegen, hilft Ihnen das intern (Handhabung, Ordnerstrukturen, Softwarelösungen), aber auch extern (behördliche Anfragen, Rechtsverfahren).

Patric von Reding
Leiter Institut Treuhand 4.0
Treuhand|Suisse

Sie klären damit relevante Fragen wie «Wer hat Zugriff auf welche Daten?», «Wo müssen die Daten gespeichert werden?», «Welche Daten dürfen nur verschlüsselt verschickt werden?».

3. Verzeichnis der Datenbearbeitungen

Für Unternehmen mit mehr als 250 Mitarbeitenden ist ein solches Verzeichnis der Bearbeitungstätigkeiten obligatorisch. Aber es empfiehlt sich auch für kleinere Firmen. Denn mit seiner Hilfe lässt sich verfolgen, welche Datenkategorien wann, von wem und wie bearbeitet wurden.

4. Auskunftsbegehren

Betroffene Personen (Kunden, Besucher der Website u.a.) haben zahlreiche Rechte im Zusammenhang mit der Bearbeitung ihrer Daten. Sie können ein Auskunfts- oder Löschbegehren stellen. Weil die Fristen kurz sind, empfiehlt es sich, vorausschauend eine Vorlage bereitzuhalten.

5. Meldeprozess bei Verletzungen

Eine Datenschutzverletzung liegt vor, wenn Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden. Es gibt in diesem Zusammenhang verschiedene Meldepflichten (im Unternehmen, an den Eidgenössischen Datenschutzbeauftragten). Hier sind organisatorische und technische Massnahmen (z. B. Verzeichnis der Datenbearbeitungen, Meldeformular) notwendig.

6. Verträge prüfen

Für viele Funktionen werden Dienste von Dritten eingesetzt: für den E-Mail- und Newsletter-Versand, die Buchhaltungssoftware in der Cloud, für Software-as-a-Service-Anbieter oder für Videokonferenzen. Sie müssen die Verträge mit Ihren Subunternehmern überprüfen, ob die Sicherheit der Daten gewährleistet ist. Ergänzen Sie Klauseln, die gewährleisten, dass diese Unternehmen die Voraussetzungen bezüglich Geheimhaltung, Datenbearbeitung oder Meldeverfahren erfüllen, für die Sie am Ende des Tages geradestehen müssen.

7. Wann müssen Daten gelöscht werden?

Personendaten, die nicht mehr benötigt werden und für deren Bearbeitung kein Rechtfertigungsgrund nachgewiesen werden kann, müssen vom Unternehmen gelöscht werden. Dies müssen Sie in Ihren Prozessen vorsehen (z.B. mittels Verzeichnis der Datenbearbeitungen).

8. Datenübermittlung ins Ausland

Die meisten Anbieter von Cloud- und Software-Services-Anbieter haben Server ausserhalb der Schweiz. Auf der Website des Eidgenössischen Datenschutzbeauftragten finden Sie eine Liste der «sicheren Drittstaaten», die unproblematisch sind. Bei allen anderen und auch bei den USA benötigt es zusätzliche und spezifische Vertragsklauseln.

9. IT-Infrastruktur

Lassen Sie Ihre IT-Infrastruktur überprüfen. Wo sind im Hinblick auf das neue Datenschutzgesetz zusätzliche Vorkehrungen nötig? Vergessen Sie aber nicht: Die Technik allein wird es nicht richten, die Schwachstelle beim Thema Cyberkriminalität ist oft der Mensch. Hier müssen Sie mit Information und organisatorischen Massnahmen (z. B. Passwortverwaltung) ansetzen.

10. Besonders schützenswerte Personendaten

Es gibt eine Reihe von Datenarten, die besonders heikel sind. Hierzu gehören beispielsweise Angaben zu Religion, Gesundheit, strafrechtlicher Verfolgung, Gewerkschaftszugehörigkeit, sexueller Orientierung oder biometrische Daten. Solche Daten müssen speziell geschützt und dürfen nur verschlüsselt übermittelt werden.

11. Datenportabilität

Mit dem Recht auf Datenherausgabe hat eine betroffene Person die Möglichkeit, ihre Personendaten, welche sie einem privaten Verantwortlichen bekanntgegeben hat, in einem gängigen elektronischen Format herauszuverlangen oder einem Dritten übertragen zu lassen. Welche Bedeutung dieses Recht in der Praxis erlangt, wird sich noch weisen müssen.

12. Datenschutz-Folgenabschätzung

Ein Unternehmen muss Risiken durch seine Bearbeitung von Personendaten in jedem Fall einschätzen. Oft genügt eine intuitive Risikoeinschätzung. Bestimmte Bearbeitungen sind aber heikler. Hier sind vertiefte Überlegungen notwendig. Ob hohe Risiken vorliegen, ist allerdings nicht immer einfach zu beurteilen.

Weitere Informationen
www.treuhandsuisse.ch/hilfe-services/cybersecurity