

IST IHR UNTERNEHMEN BEREIT?

Mit dem neuen Datenschutzgesetz sind Unternehmen noch stärker verpflichtet, ihre Kunden-, Mitarbeiter-, Finanz- und andere sensible Daten bestmöglich zu schützen.

Fast jedes Unternehmen erfasst und bearbeitet Daten, die vom Datenschutzgesetz betroffen sind. Das fängt beim Handwerksbetrieb an, auf dessen Website man sich für einen Newsletter registrieren oder Produkte bestellen kann. Und es betrifft erst recht Dienstleistungsfirmen. Das neue Datenschutzgesetz tritt am 1. September in Kraft. Diese zwölf Stichworte erleichtern es Ihnen, die Vorbereitungen anzupacken.

1. Datenschutzerklärung

Brauchen Sie eine Datenschutzerklärung für Ihre Website oder für die Kundenverträge? Sobald Sie Personendaten bearbeiten, haben Sie eine Informationspflicht. 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, aber auch extern (behördliche Anfragen, Rechtsverfahren). 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. Damit lässt sich nachverfolgen, welche Datenkategorien wann, von wem und wie bearbeitet wurden.

4. Auskunftsbeglehen

Betroffene Personen (Kunden, Website-nutzer) können ein Auskunfts- oder Löschbeglehen stellen. Weil die Fristen kurz sind, empfiehlt es sich, eine Vorlage bereitzuhalten.



Patric von Reding, TREUHAND|SUISSE

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 Meldepflichten, auf die man organisatorisch und technisch vorbereitet sein sollte.

6. Verträge prüfen

Für viele Funktionen (E-Mail- und Newsletter-Versand, Software in der Cloud, Videokonferenzen u.a.) werden Dienste von Dritten eingesetzt. Hier müssen Sie überprüfen, ob die Sicherheit der Daten gewährleistet ist. Ergänzen Sie in den Verträgen mit Ihren Subunternehmen Klauseln bezüglich Geheimhaltung, Datenbearbeitung oder Meldeverfahren.

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.

8. Datenübermittlung ins Ausland

Die meisten Anbieter von Cloud- und Software-Services-Anbieter haben Server aus-

serhalb 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 Angaben zu Religion, Gesundheit, strafrechtlicher Verfolgung, Gewerkschaftszugehörigkeit, sexueller Orientierung, biometrische Daten. Sie müssen speziell geschützt werden.

11. Datenportabilität

Mit dem Recht auf Datenherausgabe hat eine betroffene Person die Möglichkeit, ihre Personendaten zu verlangen. Welche Bedeutung dieses Recht in der Praxis erlangt, ist noch unklar.

12. Datenschutz-Folgenabschätzung

Ein Unternehmen muss Risiken durch seine Bearbeitung von Personendaten in jedem Fall einschätzen. Oft genügt eine intuitive Risikoeinschätzung. Für bestimmte Bearbeitungen sind aber vertiefte Überlegungen notwendig.

*Patric von Reding
leitet das Institut Treuhand 4.0 des
Schweizerischen Treuhänderverbands
TREUHAND|SUISSE*

WEITERE INFORMATIONEN

[www.treuhandswisse.ch/
hilfe-services/cybersecurity](http://www.treuhandswisse.ch/hilfe-services/cybersecurity)