# Das neue Datenschutzgesetz und Datenschutzverordnung

## Datenschutzerklärung

Informationen zur Beschaffung, Zweck und Weitergabe von Personendaten. Die Erklärung muss insbesondere enthalten:

- Wer ist für die Datenbearbeitung verantwortlich und wie kann der Kontakt erfolgen?
- Für welchen Zweck oder für welche Zwecke werden die Personendaten bearbeitet?
- Wer sind allfällige Empfänger der bearbeiteten Personendaten und in welchen Ländern/Regionen befinden sich diese?
- Wie wird ein allfälliger Daten-Export abgesichert?
- Welche Rechte haben die betroffenen Personen im Zusammenhang mit dem Datenschutz?

## Richtlinien für die Datenbearbeitung erstellen

(hilfreich für behördliche Anfragen oder allfälligen Rechtsverfahren)

- Wer hat Zugriff auf welche Daten
- Wer darf welche Daten bearbeiten
- Wo müssen die Daten gespeichert werden
- Wie/wann werden Daten wieder gelöscht
- Welche Daten dürfen nur verschlüsselt verschickt werden
- Welche Regeln gelten mit dem Umgang mit Daten (Verwendung von Passwörtern, Clean Desk usw.)

## Verzeichnis aller Datenbearbeitungen

Unternehmen mit weniger als 250 Beschäftigte ➔ **Kein Verzeichnis**
**Ausnahme:** hohes Risiko für die betroffenen Personen (Personendaten über Religion, Politik, Gesundheit usw.)
Eine einfache Excel- oder Wordliste genügt.

## Auskunftsbegehren

Betroffene Personen (Kunden, Websitebesucher usw.) können ein Auskunfts- oder Löschbegehren stellen. Solche Begehren müssen innerhalb kurzer Frist (in der Regel innerhalb 30 Tagen) beantwortet werden.

## Prozess Meldung Verletzung Datenschutzes

Eine Datenschutzverletzung liegt vor, wenn Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht vernichtet, verändert, unbefugten Personen offengelegt oder zugänglich gemacht werden.
Solche Verletzungen, die ein hohes Risiko für die Beeinträchtigung der Persönlichkeit oder der Grundrechte der Betroffenen darstellen, müssen umgehend (innerhalb von 72 Stunden in der EU) dem Eidgenössischen Datenschutzbeauftragten EDÖB gemeldet werden. Bei geringem Risiko kann die Meldung freiwillig erfolgen. Um die betroffene Person zu schützen, sollte sie bei einem hohen Beeinträchtigungsrisiko informiert werden. Auftragsbearbeiter, einschließlich externer Dienstleister, müssen alle Verletzungen der Datensicherheit unverzüglich dem Verantwortlichen melden.

## Verträge mit Subunternehmen / Dienstleister überprüfen

Für viele Funktionen werden Dienste von Dritten eingesetzt, zum Beispiel für den E-Mail- und Newsletter-Versand, Buchhaltungssoftware in der Cloud, Software-as-a-Service-Anbieter oder für Video-Konferenzen. Die Auslagerung der Datenbearbeitung an Subunternehmen ist unter folgenden Voraussetzungen möglich:

- Es werden keine Geheimhaltungspflichten verletzt
- Der Beauftragte darf die Daten nur so bearbeiten, wie es der Auftraggeber selbst darf. Zweckänderung sind nicht erlaubt
- Der Beauftragte muss in der Lage sein, die Datensicherheit zu gewährleisten
- Die Unter-Auftragsbearbeitung darf nur mit vorgängiger Genehmigung erfolgen

Verträge mit Subunternehmern sind zu überprüfen, ob die Sicherheit der Daten gewährleistet ist.

## 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. Daten sind korrekt gelöscht, wenn sie nicht ohne unverhältnismässigen Aufwand wiederhergestellt werden können.

## Datenübermittlung ins Ausland

Die meisten Cloud- und Software-as-a-Service-Anbieter (Buchhaltungssoftware, E-Mail Newsletters, CRM usw.) haben Server ausserhalb der Schweiz. Personendaten dürfen ins Ausland bekanntgegeben werden, wenn die Gesetzgebung des betreffenden Staates (oder das internationale Organ) einen angemessenen Schutz gewährleistet.

## IT Infrastruktur

Je nach Risiko der Daten müssen entsprechende technische und organisatorische Massnahmen ergriffen werden. Personendaten aus der Personalabteilung sind besonders heikel und sollten mit Vorsicht bearbeitet werden. Für sensitiven Kundendaten sollte der Datensicherheit einen hohen Stellenwert eingeräumt werden.

Um die Datensicherheit zu gewährleisten, empfehlen wir, die IT Infrastruktur durch einen externen

Spezialisten prüfen zu lassen. Dieser testet, ob

- organisatorische Massnahmen vorhanden sind (z.B. interne Richtlinien, Passwortrichtlinien, Passwortmanager, Schulung/Sensibilisierung der Mitarbeitenden usw.)
- alle Software auf dem neuesten Stand sind mit allen sicherheitsrelevanten Updates
- ob alle Geräte mit modernen Virenscanner geschützt sind
- ob aktuelle Firmware im Einsatz sind
- ob Firewall korrekt konfiguriert ist
- ob Daten Back-up korrekt durchgeführt werden.

**Besonders schützenswerte Personendaten**

Besonders schützenswerte Personendaten sollte man auch besonders schützen und auch immer nur verschlüsselt übermitteln. Unter diese fallen unter anderem:

- personenbezogene Daten, aus denen rassische oder ethnische Herkunft, politische Meinungen,
- religiöse oder weltanschauliche Überzeugungen einer Person hervorgehen
- Gewerkschaftszugehörigkeit
- genetische Daten, biometrische Daten, die ausschließlich zur eindeutigen Identifizierung einer natürlichen Person verarbeitet werden
- Gesundheitsdaten
- Daten zum Sexualleben oder zur sexuellen Orientierung einer Person.
- Daten über verwaltungs- oder strafrechtliche Verfolgungen und Sanktionen
- Daten über Massnahmen der sozialen Hilfe

Lohndaten gehören nicht zu besonders schützenswerte Personendaten. Eine Bestätigung, dass diese Daten aber unverschlüsselt verschickt werden dürfen, ist dennoch empfehlenswert.

**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 heraus zu verlangen oder einem Dritten übertragen zu lassen. Vorausgesetzt ist, dass die Daten automatisiert und mit der Einwilligung der betroffenen Person oder in unmittelbarem Zusammenhang mit einem Vertrag bearbeitet wird.

**Datenschutz-Folgenabschätzung**

Unternehmen müssen 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. Wenn eine Bearbeitung voraussichtlich hohe Risiken mit sich bringt, verlangt das revDSG, dass der Verantwortliche Risiken im Rahmen einer Datenschutz-Folgenabschätzung (DSFA) beurteilt und dokumentiert.

Ob hohe Risiken vorliegen, ist nicht immer einfach zu beurteilen. Eine DSFA sollte aber jedenfalls dann durchgeführt werden, wenn besonders schützenswerte Personendaten in grösserem Umfang bearbeitet werden. Davon ist aber nicht schon dann die Rede, wenn Mitarbeiterdaten bearbeitet werden, auch wenn diese besonders schützenswerte Personendaten enthalten.