

# DATENSCHUTZ

## 01 LISTE DER DATEN-BEARBEITUNGEN

**Art. 12** Erstellen Sie eine Liste mit den Prozessen und Aktivitäten, bei denen Ihre Organisation(en) Personendaten bearbeiten (z.B. Verkauf, Cookies, Marketing, Aftersales, Vermietung, Pannenhilfe, Buchhaltung, Personalverwaltung, E-Shop, Videoüberwachung). **Die Liste enthält:** mind. Bearbeitung, Zweck, Kategorie-Personen, Kategorie-Daten, Empfänger / Auftragsbearbeiter, Speicherdauer. Evtl. weitere Informationen nach Bedarf.

## 02 DATENSCHUTZERKLÄRUNG - DSE

**Art. 19** Immer, wenn Sie Personendaten, die gesetzlich nicht erforderlich sind, erfassen od. bearbeiten, müssen Sie vor der Bearbeitung transparent in der DSE informieren. Am besten stellen Sie die DSE auf die Webseite, Links auf diese bei Videokameras, in Verträgen (Verweis auf DSE). Für Bewerber und Mitarbeiter, empfiehlt sich eine separate DSE im Mitarbeiterreglement.

**Die DSE enthält:** Ihre Kontaktdaten, Zweck der Datenbearbeitung, Kategorien von Empfängern, Auslandsübertragung (Länder), Rechte der Betroffenen.

## 03 AUFTRAGSBEARBEITERVERTRAG - ABV

**Art. 9** Die meisten Unternehmen geben oder überlassen den Zugriff auf Daten auch Dritten, so z.B. IT-Provider, Marketing etc. Der Auftragsbearbeiter darf nur tun, was wir auch tun dürfen. **Mit Dritten muss daher ein „ABV“ geschlossen werden, ein Vertrag, der Ihre Datenhoheit festhält und den Dritten zum Datenschutz und zur Datensicherheit verpflichtet.** Ein ABV nach EU-Recht mit einem Verweis auf das DSG genügt (Vorlage: z.B. bei der Datenschutzstelle Liechtenstein).

## 04 DATENSICHERHEIT - TOMs & DSFA

**Art. 8** Personendaten schützen wir durch technische und organisatorische Massnahmen. **Technisch:** Zugang nur mit persönlichem Account und „MFA“, Zugriff von Dritten nur auf Anfrage und mit Audit-Trail, Firewalls, Antiviren-Software, Backups. **Organisatorisch:** Clean-Desk, Need-to-Know, Verpflichtung zum Datenschutz und Schulungen, Schreddern, etc. **Meldepflicht Art. 24:** Wenn Daten verloren gegangen sind, muss eine Meldung an den EDÖB (edoeb.admin.ch) und ggf. auch eine Meldung an Betroffene geprüft werden.

**Art. 22** Wenn die Organisation viele, sehr sensitive oder besonders schützenswerte Personendaten bearbeitet und Fehler oder sonstige Risiken für den Betroffenen risikoreich sein könnten, ist eine Datenschutz-Folgenabschätzung - DSFA (Risiko-Assessment) zu erstellen und zu dokumentieren. Mit der DSFA **werden die betroffenen Massnahmen zum Schutz der Personendaten vertieft und auf ihre tatsächliche Eignung geprüft.**

## 05 AUSLANDSÜBERMITTLUNG

**Art. 16** Kein unsicheres Ausland und daher **Länder in die Personendaten übermittelt werden können:** die EU, UK, der EWR und einzelne weitere Länder der Länderliste. Denken Sie daran, dass die Länder in der DSE zu nennen sind. In anderen Ländern dürfen Daten bearbeitet werden, wenn dies im Einzelfall in einem Vertrag erforderlich und festgehalten ist, falls der Betroffene auf einen separaten Schutz verzichtet hat oder **es liegen sog. SCC also Standardvertragsklauseln der EU mit Hinweis auf die Schweiz** vor.

## 06 BETROFFENENRECHTE

**Art. 25ff** Wir geben den Betroffenen die in der DSE genannten Rechte auf **Auskunft** über ihre eigenen Personendaten (nicht Dokumente) und auf Wunsch weitere Informationen. Das Gesetz räumt für die kostenlose Auskunft eine Frist von 30 Tagen ein. Zuvor müssen wir die Auskunftersuchende Person identifizieren. Achtung: eine falsche bzw. unvollständige Auskunft ist strafbar. Der Zweck der Auskunft muss dem Persönlichkeitsschutz dienen. Weitere Rechte sind: **Berichtigung** falscher Daten. **Löschung** kann nur verlangt werden, wenn wir keinen besseren Grund haben oder eine gesetzliche Pflicht. Bei einer **vollautomatischen Entscheidung, Art. 21**, entscheidet auf Verlangen auch noch ein Mensch.

## 07 DATENSCHUTZGRUNDSÄTZE

**Art. 6** Wir setzen in unseren Prozessen in der Organisation die Grundsätze zum Datenschutz um: **Rechtmässigkeit, Treu und Glauben, Zweckbindung, Löschgebot, Richtigkeit, Transparenz und Datensicherheit.** Diese Grundsätze und die Verfahren zur Einhaltung der Sorgfaltspflichten dokumentiert die Organisation.

## 08 PRIVACY BY DEFAULT

**Art. 7** Wenn wir einem Betroffenen eine Auswahl geben, sollen die Datenschutz- und die Sicherheitseinstellungen eines Systems, einer Anwendung oder eines Produkts **standardmässig auf die sichersten oder datenschutzfreundlichsten** Optionen eingestellt werden.

## 09 KLEINES BERUFSGEHEIMNIS

**Art. 62** Personendaten, die der Organisation übergeben wurden, sind vertraulich zu halten, sofern dem Betroffenen nichts anders mitgeteilt wurde.

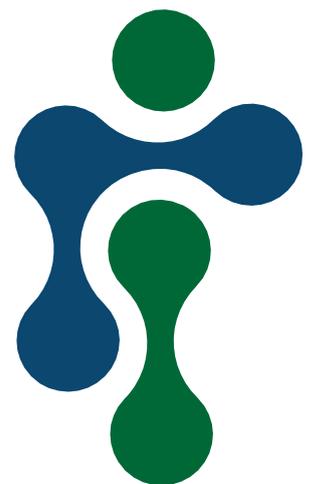
## 10 SCHULUNG DER MITARBEITER

Bei der Umsetzung und Einhaltung des Datenschutzes sind die Mitarbeiter sehr wichtig. Es gibt viele Gründe, warum die Mitarbeiter im Datenschutz zu schulen sind:

**Strafen vermeiden:** Verstösse gegen Datenschutzgesetze können zu erheblichen persönlichen Strafen von bis zu CHF 250'000 führen.

**Datensicherheit:** Ausgebildete Mitarbeiter sind besser darauf vorbereitet, potenzielle Sicherheitsrisiken zu erkennen und zu vermeiden, wie Phishing-Angriffe, unsichere Passwörter und andere Sicherheitsprobleme.

**Vertrauen der Kunden:** Kunden vertrauen eher Unternehmen, die ihre Daten schützen. Eine gute Datenschutzpraxis kann zur Kundenzufriedenheit beitragen.



Dies ist eine stark verkürzte Information zum neuen Datenschutzgesetz und keine Rechtsberatung.

10 Schritte zum neuen revidierten Datenschutzgesetz. Vorsätzliche Verletzungen der **rot** markierten Artikel sind strafbewehrt. Andere Vorgaben können zivilrechtlich eingeklagt werden.