## DSGVO Anforderungen

### Rechtsgrundlage (out of scope)

Es dürfen nur personenbezogene Daten verarbeitet werden, für die eine Rechtsgrundlage vorhanden ist. Rechtsgrundlage kann sein:

- Einwilligung des Betroffenen
- Vertragserfüllung
- Gesetzliche Verpflichtung
- Öffentliches Interesse
- Berechtigtes Interesse Dritter
- ...

### Zweckmäßigkeit (out of scope)

Personenbezogene Daten dürfen nur für den aus der Rechtsgrundlage hervorgehenden Zweck verarbeitet werden. Erheben von Name und Adresse für Zustellung eines Paketes (Rechtsgrundlage Vertragserfüllung) ist zulässig - Verarbeitung der Daten für Marketingzwecke nicht.

### Datenschutzbeauftragter (out of scope)

Ernennung eines Datenschutzbeauftragten ist notwendig wenn

- Kerntätigkeit ist die Verarbeitung personenbezogener Daten (regelmäßige und systematische Überwachung). Trifft zu auf Banken, Versicherungen, Berufsdetektive, etc)
- Kerntätigkeit ist die Verarbeitung sensibler personenbezogener Daten

### Inanspruchnahme von Subdienstleister (out of scope)

Auftragsverarbeiter muss sicherstellen, dass seine Subdienstleister für einen angemessenen Schutz der weitergegebenen personenbezogenen Daten sorgen. Generell muss die Verarbeitung in einem schriftlichen Vertrag (inklusive Rechte und Pflichten) festgehalten werden. Wichtig: Bei Sicherheitsvorfällen bei Dienstleistern herrscht eine solidarische Haftung mit dem Auftragsverarbeiter.

### Erfüllung der Betroffenenrechte

- Informationspflicht: Auftragsverarbeiter muss die Betroffenen über die Verarbeitung ihrer Daten informieren
- Auskunftspflicht: Jeder mögliche Betroffene (natürliche Personen) hat das Recht, falls eine Verarbeitung seiner Daten vorliegt, über diese informiert zu werden. Dazu gehört eine Auskunft über die konkreten personenbezogenen Daten, Rechtsgrundlage, Zweck, Übertragung an Dienstleister, Speicherfristen, etc.
- Recht auf Berichtigung: Jeder Betroffene hat das Recht, dass Daten berichtigt werden (z.B. bei Namensänderung usw)

- Recht auf Löschung: Personenbezogene Daten müssen gelöscht werden, wenn diese unzweckmäßig oder auf keiner Rechtsgrundlage (z.B. Wiederruf der Einwilligung) verarbeitet werden.
- Recht auf Einschränkung: Verarbeitung der Daten muss bei ausstehenden Prüfungen bis auf die Speicherung eingestellt werden
- Recht auf Datenübertragbarkeit: Personenbezogene Daten müssen dem Betroffenen in einem gängigen Format zur Verfügung gestellt werden.
- Widerspruchsrecht: Der Betroffene kann der Verarbeitung seiner Daten widersprechen falls keine Rechtsgrundlage vorhanden ist.

**Datensicherheit (Privacy by Design)**

- Pseudonymisierung
- CIA-Prinzip (Confidentiality, Integrity, Availability)
- Backup-Lösung
- regelmäßige Überprüfung, Bewertung und Evaluierung gesetzter Maßnahmen
- Umsetzung geeigneter Maßnahmen unter Berücksichtigung von
    - Stand der Technik
    - Implementierungskosten
    - Art/Umfang/Umstände des Verarbeitungszweckes
    - Eintrittswahrscheinlichkeit und Schwere einer Datenschutzverletzung für die Rechte und Freiheiten der Betroffenen

**Voreinstellungen (Privacy by Default)**

- Datensparsamkeit (nur die wirklich benötigten verarbeiten)
- Datenschutzfreundliche Voreinstellungen
- Speicherfristen
- Zugriff auf die Daten so weit wie möglich einschränken

**Verzeichnis der Verarbeitungstätigkeiten (out of scope)**

Auftragsverarbeiter müssen ein Verzeichnis führen, in dem alle Verarbeitungen inklusive Rechtsgrundlage, Zweck, Art der Daten, Ursprung, Dienstleister, Speicherfristen, usw aufgelistet sind.

**Meldepflicht (out of scope)**

Verletzungen und Vorfälle müssen ab Bekanntwerden innerhalb von 72 Stunden an die zuständige Behörde gemeldet werden

**Datenschutz Folgeabschätzung (out of scope)**

Notwendig bei der umfangreichen (Anzahl Betroffener, Datenmenge, Dauer) Verarbeitung von sensiblen Daten.

Ausnahme falls

- kein hohes Risiko für Betroffene
- gesetzliche Verpflichtung

- öffentliches Interesse
- auf white-list der Datenschutzbehörde (z.B: Patienten/Klienten/Kundenverwaltung bei Ärzten und Gesundheitsdiensteanbieter)

Datenschutzfolgeabschätzung muss beinhalten:

- Beschreibung der Vorgänge
- Beschreibung der Verarbeitungszwecke
- Bewertung der Notwendigkeit / Verhältnismäßigkeit
- Bewertung der Risiken
- geplante Maßnahmen

Falls ein hohes Risiko herauskommt, aber keine Maßnahmen gesetzt werden können muss eine Meldung an die Datenschutzbehörde erfolgen.

**Datenverkehr mit EU-Ausland**

Übermittlung ist nur zulässig wenn:

- Genehmigung durch die Datenschutzbehörde
    - EU-US Privacy Shield: Vereinbarung über den Schutz von personenbezogenen Daten in amerikanischen Unternehmen. Falls Unternehmen zertifiziert ist, ist eine Übertragung personenbezogener Daten ohne Genehmigung möglich (https://www.dsb.gv.at/eu-us-privacy-shield).
- Vorliegen geeigneter Garantien
- Ausnahmegrund
    - ausdrückliche Einwilligung
    - Vertragserfüllung
    - Rechtsansprüche
    - lebenswichtige Interessen Betroffener
    - öffentliches Interesse

**Nachweis über die Umsetzung der Maßnahmen um DSGVO-konform zu sein ist notwendig (z.B: Zertifizierung)**