EU-Datenschutz-Grundverordnung (DSGVO): Verantwortlicher und Auftragsverarbeiter - (Überblick)

Wesentliche Pflichten des Verantwortlichen und des Auftragsverarbeiters

„**Verantwortlicher**" ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

„**Auftragsverarbeiter**" ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen bearbeitet.

Die DSGVO sieht **Pflichten** bei einer Datenverarbeitung für den **Verantwortlichen** – teilweise auch für **Auftragsverarbeiter** – vor:

- Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellung.
- Dokumentationspflicht (Verzeichnis von Verarbeitungstätigkeiten) – **betrifft auch den Auftragsverarbeiter**.
- Meldung von Datenschutzverletzungen (data breach notification).
- Datenschutz-Folgenabschätzung (bei Verarbeitungsvorgängen, die aufgrund der Art, des Umfanges, der Umstände und der Zwecke voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben).
- Vorherige Konsultation der Aufsichtsbehörde (wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte und der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft).
- Verpflichtender Datenschutzbeauftragter (wenn die Kerntätigkeit eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich macht oder in der umfangreichen Verarbeitung besonderer Kategorien von Daten oder von Daten über strafrechtliche Verurteilungen und Straftaten besteht) – **betrifft auch den Auftragsverarbeiter**.

Datensicherheitsmaßnahmen müssen sowohl vom Verantwortlichen als auch vom Auftragsverarbeiter vorgesehen werden.

> **Hinweis:**
> Der Verantwortliche muss sicherstellen und den Nachweis erbringen können, dass die Verarbeitung entsprechend der DSGVO erfolgt.

Den **Verantwortlichen** treffen weiters **Informationspflichten bei Erhebung von personenbezogenen Daten** und er ist **Adressat der Betroffenenrechte** (vor allem Auskunftsrecht, Recht auf Berichtigung, Recht auf Löschung – „Recht auf Vergessenwerden", Recht auf Einschränkung der Verarbeitung, Recht auf Datenübertragbarkeit, Widerspruchsrecht).

Was ist bei der Heranziehung eines Auftragsverarbeiters zu beachten?

- Es dürfen nur solche Auftragsverarbeiter herangezogen werden, die (insbesondere im Hinblick auf Fachwissen, Zuverlässigkeit und Ressourcen) **hinreichende Garantien** dafür bieten, dass technische und organisatorische Maßnahmen getroffen werden, die den Anforderungen der DSGVO genügen.
- Es ist ein **schriftlicher Vertrag** abzuschließen, der den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet. In diesem Vertrag müssen Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sein. Dieser Vertrag muss insbesondere Folgendes vorsehen:
  - Der Auftragsverarbeiter darf die personenbezogenen Daten nur auf dokumentierte **Weisung** des Verantwortlichen verarbeiten.
  - Der Auftragsverarbeiter verpflichtet sich zur **Vertraulichkeit** oder unterliegt einer angemessenen gesetzlichen Verschwiegenheitspflicht.
  - Der Auftragsverarbeiter ergreift alle erforderlichen **Datensicherheitsmaßnahmen**.
  - Der Auftragsverarbeiter nimmt **keinen weiteren Auftragsverarbeiter ohne** vorherige gesonderte oder allgemeine schriftliche **Genehmigung** des Verantwortlichen in Anspruch.
  - Der Auftragsverarbeiter **unterstützt den Verantwortlichen** in seiner Pflicht zur Erfüllung der Betroffenenrechte und sonstiger Verpflichtungen nach der DSGVO.
  - **Nach Abschluss** der Erbringung der Verarbeitungsleistungen werden alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder **gelöscht oder zurückgegeben**.
  - Der Auftragsverarbeiter stellt alle **Informationen zum Nachweis** der Einhaltung seiner Verpflichtungen zur Verfügung und ermöglicht diesbezügliche Prüfungen.

Geldstrafen

Bei Verstoß gegen die genannten Pflichten sind Geldbußen von bis zu 10 Mio EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres vorgesehen.

Relevante Artikel der DSGVO: Art 4, Art 24 – 43
Relevante Erwägungsgründe: 74ff

Stand: 11.03.2021