
Kurz und knapp erklärt:
Auftragsverarbeitung

[Anforderung] Was sagt das Gesetz?

Das Outsourcing – in der Regel „Auftragsverarbeitung“ – wird in der DSGVO umfassend geregelt:

Artikel 28:

„Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.“ [Absatz 1]

„Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags [...], der [...] den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet [...]“ [Absatz 3]

[Maßnahmen] Was ist zu tun?

Im Rahmen der **Auswahl** eines Dienstleisters sind demnach geeignete Sicherheitsmaßnahmen nachzuweisen (Verantwortung trägt der Auftraggeber). Dies kann wie folgt sichergestellt werden:

- » Prüfung eines IT-Sicherheitskonzepts des Dienstleisters durch den Auftraggeber
- » Ausfüllen eines Selbstauskunftsbogen des Auftraggebers durch den Dienstleister
- » Nachweis eines Sicherheits-Zertifikats durch den Dienstleister (z. B. ISO 27001)

Ferner ist ein **Vertrag** mit dem Dienstleister abzuschließen, der bestimmte Pflichtinhalte aufweisen muss, um DSGVO-konform zu sein.

Hinweis: Trotz der Pflicht für **beide** Parteien, vollständige Verträge abzuschließen, nehmen wir dennoch teils unvollständige Verträge zur Kenntnis. Daher: Prüfung stets durch Datenschutz-Experten vornehmen lassen. Der Datenschutzbeauftragte kann hierbei weiterhelfen.

Hinweis: Beachten Sie die besonderen Anforderungen bei Dienstleister außerhalb der EU (One Pager „Drittlandtransfer“).

[Nutzen] Was bringt mir das?

Die Prüfung der Sicherheitsmaßnahmen und klare Vertragsinhalte hat verschiedene Vorteile:

- » Verbesserung der Qualität von Sicherheitsmaßnahmen durch klare Vorgaben;
- » Reduzierung von durch Dienstleister verursachte Datenpannen (beachte: Vorfälle, die durch Auftragsverarbeiter verschuldet werden, sind oftmals auch Imageproblem für Auftraggeber)
- » Höhere Transparenz der Datenverarbeitung, der Sicherheit und der Verantwortlichkeiten

[UIMC] Wie hilft die UIMC?

Die UIMC hat nicht nur **Templates** für verschiedene Vertragskonstellationen, sondern auch eine umfassende Expertise im Rahmen der Vertragsprüfung (Juristen) und Auditierung von IT-Dienstleistern (Informationssicherheitsexperten). Unsere Berater sind nicht nur gewissenhaft, sondern auch effizient und lösungsorientiert.

[Anlage] Definition von Auftragsverarbeitung

Eine Auftragsverarbeitung ist die Inanspruchnahme von externen Dienstleistungsfunktionen durch den Verantwortlichen.

Der Auftraggeber bleibt für die Einhaltung der Vorschriften über den Datenschutz verantwortlich.

Abgrenzung zur Übermittlung

Für eine Übermittlung und damit für eine Verarbeitung oder Nutzung zu eigenen Zwecken des Auftragnehmers sprechen:

- die den bloßen Verarbeitungsvorgängen zugrunde liegenden Aufgaben oder Geschäftszwecke werden ganz oder teilweise mit abgeben;
- die Übertragung von Nutzungsrechten an den übermittelten Daten;
- eine vereinbarte Dienstleistung, die deutlich über die Ausführung von praktisch-technischen Bearbeitungen hinausgeht;
- die fehlende Kontrollmöglichkeit des Auftraggebers;
- die Verantwortlichkeit für die Zulässigkeit und Richtigkeit der Daten;
- das Eigeninteresse des Vertragspartners an den Daten (nicht an der Auftragserfüllung);
- eine direkte Kontaktaufnahme des Auftragnehmers mit dem Betroffenen.

Beispiele für eine Übermittlung sind (Einzelfallprüfung erforderlich):

- Beauftragung eines Anwalts im Rahmen eines Rechtsstreits;
- Beauftragung eines Inkassobüros zum Eintreiben säumige Zahlungen (Forderungsverkauf).

Es ist vor der Übermittlung an den Auftragnehmer die Zulässigkeit der Übermittlung zu prüfen, da die auftraggebende Stelle die Verantwortung hierfür trägt. Auch ist der Nutzungszweck schriftlich festzulegen und darauf zu beschränken.