Was ist ein Vertrag zur Auftragsdatenverwaltung (AV)?

Was ist ein AV-Vertrag?

Ein **AV-Vertrag** (auch Auftragsverarbeitungsvertrag genannt) ist ein **rechtlich bindender Vertrag** zwischen zwei Parteien:

- **Dem Verantwortlichen** (z. B. ein Unternehmen, das Kundendaten verarbeitet)
- **Dem Auftragsverarbeiter** (z. B. ein Dienstleister, der Daten im Auftrag verarbeitet – etwa ein Cloud-Anbieter oder eine externe Buchhaltung)

Er regelt, **wie personenbezogene Daten verarbeitet werden dürfen**, welche **Sicherheitsmaßnahmen** einzuhalten sind und welche **Rechte und Pflichten** die Beteiligten haben.

Wann ist ein AV-Vertrag erforderlich?

Ein AV-Vertrag ist **verpflichtend**, wenn personenbezogene Daten von einem externen Dienstleister **im Auftrag verarbeitet werden** – also im Namen und unter der Weisung des Auftraggebers.

Typische Beispiele:

- **Cloud-Dienste** (z. B. Google Workspace, Microsoft 365)
- **E-Mail-Marketing** (z. B. Mailchimp, CleverReach)
- **Webhosting**
- **Externe Lohnabrechnung oder Steuerberatung**
- **WhatsApp Business**, **wenn es für die Kundenkommunikation genutzt wird**

⚠ **Speziell bei WhatsApp:**

WhatsApp ist **kein klassischer Auftragsverarbeiter**, sondern agiert oft selbstständig. Daher ist die Nutzung von **WhatsApp (insbesondere der Standard-App)** für die geschäftliche Kommunikation mit Kundendaten **problematisch** im Sinne der DSGVO.
Die **Business-API von WhatsApp**, betrieben über Dienstleister wie Twilio oder 360dialog, kann **datenschutzkonform** eingesetzt werden – **mit AV-Vertrag und geeigneten TOMs**.

Was sind TOMs?

TOMs = **Technische und organisatorische Maßnahmen**

Diese Maßnahmen müssen im AV-Vertrag **beschrieben und eingehalten** werden. Sie sollen die **Sicherheit der Datenverarbeitung** gewährleisten.

Beispiele für TOMs:

- **Zugriffsschutz** (Passwortschutz, Rollenverteilung)

- **Verschlüsselung** von Datenübertragungen
- **Datensicherung und Wiederherstellung**
- **Protokollierung** von Zugriffen
- **Vertraulichkeitspflichten** für Mitarbeitende
- **Datenschutz-Folgenabschätzungen**, wenn nötig

Warum ist der AV-Vertrag bindend?

Die **DSGVO (Art. 28)** schreibt ausdrücklich vor, dass für jede Auftragsverarbeitung ein Vertrag bestehen muss. Ohne AV-Vertrag handelt es sich um eine **nicht zulässige Datenweitergabe** – mit Risiko für **Bußgelder** von bis zu 20 Mio. Euro oder 4 % des Jahresumsatzes.

Zusammenfassung:

Ein AV-Vertrag ist Pflicht, wenn ein Dienstleister personenbezogene Daten im Auftrag verarbeitet. Auch bei der Nutzung von Tools wie WhatsApp Business sollte genau geprüft werden, ob eine datenschutzkonforme Nutzung möglich ist – inklusive AV-Vertrag und angemessenen TOMs.

Eindeutige ID: #1417
Verfasser: KP
Letzte Änderung: 2025-04-23 15:03