Auftragsverarbeitungsvertrag (AVV)

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag nach **Art. 28 DSGVO**.

i Muster zum Prüfen. Dieses Dokument bildet die Struktur ab, die Sie vor Auftragserteilung einsehen und prüfen können. Der verbindliche Vertrag wird pro Auftrag individuell ausgefüllt (Parteien, konkrete Verarbeitungen, Anlagen) und von beiden Seiten unterzeichnet.

 Als PDF herunterladen

Zwischen

Verantwortlicher (Auftraggeber) — im individuellen Vertrag einzutragen:
[Firma / Name] · [Anschrift] · [vertreten durch]

— nachfolgend „Verantwortlicher" —

Auftragsverarbeiter (Auftragnehmer):
Pascal Kozlowski (Kozlowski IT) · Abteistraße 30/6, 88416 Ochsenhausen · pk@kozlowski-it.de

— nachfolgend „Auftragsverarbeiter" —

§ 1 Gegenstand, Dauer und Weisungsgebundenheit

(1) Gegenstand ist die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Rahmen der beauftragten IT-Betreuungs- und Entwicklungsleistungen (z. B. Administration, Wartung, Backup, Betrieb von Anwendungen). Umfang und Zweck ergeben sich aus dem Hauptvertrag.

(2) Die Verarbeitung erfolgt ausschließlich auf dokumentierte Weisung des Verantwortlichen, auch hinsichtlich der Übermittlung in Drittländer. Ist der Auftragsverarbeiter rechtlich zu einer weitergehenden Verarbeitung verpflichtet, teilt er dies dem Verantwortlichen vor der Verarbeitung mit (sofern gesetzlich zulässig).

(3) Die Dauer entspricht der Laufzeit des Hauptvertrags.

§ 2 Art der Daten und Kategorien betroffener Personen

Art der Daten und betroffene Personen ergeben sich aus der konkreten Beauftragung (Anlage 2). Typischerweise handelt es sich um Stamm- und Kontaktdaten von Mitarbeitenden, Kunden oder Mandanten/Patienten des Verantwortlichen, soweit für die IT-Leistung technisch berührt. Der Auftragsverarbeiter greift auf Systeme und deren Konfiguration zu; ein Zugriff auf inhaltliche Nutzdaten erfolgt nur, soweit für die konkrete Aufgabe erforderlich, nach Absprache und dokumentiert.

§ 3 Pflichten des Auftragsverarbeiters

(1) **Vertraulichkeit:** Der Auftragsverarbeiter verarbeitet die Daten vertraulich. Mit der Verarbeitung befasste Personen sind auf Vertraulichkeit verpflichtet (Art. 28 Abs. 3 lit. b, Art. 29, 32 Abs. 4 DSGVO).

(2) **Technische und organisatorische Maßnahmen (TOM):** Der Auftragsverarbeiter trifft die nach Art. 32 DSGVO erforderlichen Maßnahmen (Anlage 1) und passt sie dem Stand der Technik an.

(3) **Unterstützung:** Er unterstützt den Verantwortlichen bei der Beantwortung von Betroffenenanfragen (Art. 12–23), bei der Einhaltung der Art. 32–36 (Sicherheit, Meldung von Verletzungen, Datenschutz-Folgenabschätzung) sowie bei Anfragen der Aufsichtsbehörde — im Rahmen des Zumutbaren und der ihm vorliegenden Informationen.

(4) **Meldepflicht:** Verletzungen des Schutzes personenbezogener Daten meldet er dem Verantwortlichen unverzüglich nach Bekanntwerden.

(5) **Nachweis und Kontrolle:** Er stellt dem Verantwortlichen die zum Nachweis der Einhaltung erforderlichen Informationen bereit und ermöglicht Überprüfungen

(Audits) mit angemessener Vorankündigung, auch durch beauftragte Prüfer.

(6) **Rückgabe/Löschung:** Nach Abschluss der Leistungen gibt er alle Daten zurück oder löscht sie nach Wahl des Verantwortlichen, sofern keine gesetzliche Aufbewahrungspflicht entgegensteht. Backups werden im Rahmen der regulären Rotation gelöscht.

(7) Er informiert den Verantwortlichen, wenn eine Weisung nach seiner Auffassung gegen Datenschutzrecht verstößt.

§ 4 Unterauftragsverarbeiter

(1) Der Verantwortliche stimmt dem Einsatz der in **Anlage 3** genannten Unterauftragsverarbeiter zu. Beabsichtigte Änderungen zeigt der Auftragsverarbeiter rechtzeitig an; der Verantwortliche kann widersprechen.

(2) Der Auftragsverarbeiter erlegt Unterauftragsverarbeitern dieselben Datenschutzpflichten vertraglich auf (Art. 28 Abs. 4 DSGVO).

§ 5 Schlussbestimmungen

Änderungen bedürfen der Textform. Sollten einzelne Bestimmungen unwirksam sein, bleibt der Vertrag im Übrigen wirksam. Es gilt deutsches Recht.

Anlage 1 — Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

- **Vertraulichkeit:** Zugriff nur für befugte Personen; Rollen-/Rechtekonzept, starke Authentisierung (MFA/Schlüssel), verschlüsselte Zugänge (SSH/TLS), Netzsegmentierung, Least-Privilege.
- **Integrität:** Nachvollziehbarkeit von Änderungen (Logging, dokumentierte Konfigurationsänderungen), Schutz vor unbefugter Veränderung.
- **Verfügbarkeit & Belastbarkeit:** regelmäßige, verschlüsselte Backups, außer Haus gelagert, mit *getesteter* Wiederherstellung; Monitoring; Updates/Härtung.
- **Verschlüsselung:** Transport verschlüsselt (TLS); Backups verschlüsselt.
- **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung** der Wirksamkeit der Maßnahmen; Orientierung am BSI-IT-Grundschutz.

- **Trennungskontrolle:** getrennte Verarbeitung von Daten unterschiedlicher Auftraggeber.

Anlage 2 — Art der Verarbeitung / Daten / Betroffene

Wird pro Auftrag konkretisiert: Zweck, Art der Verarbeitung, Datenarten, Kategorien betroffener Personen, Ort der Verarbeitung.

Anlage 3 — Genehmigte Unterauftragsverarbeiter

- **Hetzner Online GmbH**, Industriestr. 25, 91710 Gunzenhausen (Deutschland) — Hosting/Rechenzentrum Falkenstein (Deutschland). Zweck: Server-/Infrastruktur-Betrieb.
- Weitere werden hier je nach Auftrag ergänzt (z. B. konkret genutzte Dienste).

Stand: 2026 · Kozlowski IT · Dieses Muster ersetzt keine Rechtsberatung. Vor dem verbindlichen Einsatz empfiehlt sich eine juristische Prüfung im Einzelfall.

Zurück zum Kontakt