

# Auftragsverarbeitungsvertrag (AVV)

nach Art. 28 DSGVO · Standard-Vorlage von adsbird

## Vertragsparteien

### Auftraggeber (Verantwortlicher):

[Firmenname]

[Anschrift]

[USt-ID / HRB]

### Auftragnehmer (Auftragsverarbeiter):

adsbird · Tim Vogel

Gustav-Pinkus-Straße 5

32457 Porta Westfalica

E-Mail: tim@adsbird.de

## § 1 — Gegenstand und Dauer der Verarbeitung

Gegenstand des Auftrags ist die Entwicklung und der Betrieb von Automatisierungs-Workflows, KI-Agents, Custom-CRMs oder vergleichbaren IT-Systemen gemäß separat geschlossenem Hauptvertrag. Die Verarbeitung personenbezogener Daten erfolgt ausschließlich im Rahmen dieses Hauptauftrags und nach dokumentierter Weisung des Auftraggebers. Die Dauer entspricht der Laufzeit des Hauptvertrags.

## § 2 — Art und Zweck der Verarbeitung

Art: Erhebung, Speicherung, Veränderung, Übermittlung und Löschung personenbezogener Daten im Rahmen der vereinbarten Workflows.

Zweck: Bereitstellung, Wartung und Weiterentwicklung der im Hauptvertrag definierten Software-Module.

## § 3 — Kategorien betroffener Personen und Daten

**Betroffene Personen:** Kunden, Interessenten, Mitarbeiter, Bewerber des Auftraggebers — je nach Use-Case projektspezifisch.

**Datenkategorien:** Kontaktdaten, Kommunikationsverläufe, Kundendaten, ggf. Profildaten und Verhaltensdaten gemäß Projekt-Scope.

## § 4 — Pflichten des Auftragnehmers

1. Verarbeitung nur auf dokumentierte Weisung des Auftraggebers.
2. Vertraulichkeit aller Personen mit Datenzugang nach Art. 28 (3) b DSGVO.
3. Umsetzung der in Anlage 1 dokumentierten technisch-organisatorischen Maßnahmen (TOMs).
4. Einhaltung der Bedingungen für die Inanspruchnahme weiterer Auftragsverarbeiter (Sub-Prozessoren) gemäß § 6.
5. Unterstützung des Auftraggebers bei der Erfüllung von Betroffenenrechten (Auskunft, Berichtigung, Löschung, Datenübertragbarkeit).
6. Unterstützung bei DSFA und Meldepflichten nach Art. 32-36 DSGVO.
7. Löschung oder Rückgabe sämtlicher personenbezogener Daten nach Ende der Verarbeitung — auf Wahl des Auftraggebers.

## § 5 — Technisch-organisatorische Maßnahmen (TOMs)

Vollständige TOMs sind in Anlage 1 dokumentiert. Kernelemente:

- **EU-Hosting** als Standard (Hetzner Falkenstein, Supabase EU-Frankfurt, Azure Germany West Central).
- **Verschlüsselung** at-rest (AES-256) und in-transit (TLS 1.2+).
- **Secret-Management** via Azure Key Vault / AWS Secrets Manager / n8n Credentials.
- **Audit-Logs** für alle Daten-Zugriffe, mind. 90 Tage Retention.
- **Backup-Strategie**: 7-Tage rollend + 30-Tage Wochen-Snapshots.
- **Zugriffskontrolle** rollenbasiert, MFA für Administratoren.
- **Lösch-Pfade** pro Workflow dokumentiert (User-Daten, Backups, Logs).

## § 6 — Sub-Prozessoren

Der Auftragnehmer setzt projektspezifisch folgende Sub-Prozessoren ein. Der Auftraggeber stimmt deren Einsatz mit Unterzeichnung dieses Vertrags allgemein zu. Eine projektspezifische Auswahl wird im Hauptvertrag oder Anlage 2 dokumentiert.

Anbieter	Standort	Zweck	DSGVO-Status
Anthropic	US / EU (Bedrock)	LLM-Inferenz	TADPF + DPA
OpenAI	US / Azure-OpenAI EU	GPT, Whisper	TADPF · EU via Azure
Supabase	EU-Frankfurt	PostgreSQL, Auth	EU-AVV
Hetzner Online	Falkenstein / Nürnberg (DE)	Hosting, n8n	DE-AVV
Microsoft Azure	Germany West Central	Container Apps, SignalR	EU-AVV
Cloudflare	EU-Edges	CDN, DNS, Workers	EU-AVV via TADPF
Make / Apify	EU	Workflow-Automation, Scraping	EU-AVV
Vercel	US / EU-Edges	Static Hosting (optional)	TADPF
Meta (WhatsApp BA)	US + Meta-EU-Cloud	WhatsApp Business API	EU-AVV via TADPF

*Hinweis: Änderungen an dieser Liste werden dem Auftraggeber mit mindestens 30 Tagen Vorlaufzeit angekündigt. Widerspruchsrecht besteht.*

## § 7 — Kontroll- und Auditrechte

Der Auftraggeber ist berechtigt, die Einhaltung der TOMs und gesetzlichen Anforderungen zu überprüfen. Audits sind mindestens 14 Tage vorher anzukündigen und finden zu üblichen Geschäftszeiten statt. Alternativ kann der Auftragnehmer auf eigene oder externe Zertifikate (z.B. ISO 27001 der Sub-Prozessoren) verweisen.

## § 8 — Mitteilungspflichten bei Verletzungen

Der Auftragnehmer informiert den Auftraggeber unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntnis, über Verletzungen des Schutzes personenbezogener Daten (Data Breach). Die Mitteilung enthält Art, Umfang, mögliche Folgen und ergriffene Gegenmaßnahmen.

## § 9 — Schlussbestimmungen

Es gilt deutsches Recht. Gerichtsstand ist der Sitz des Auftragnehmers. Sollten einzelne Bestimmungen unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Dieser Vertrag tritt mit Unterzeichnung beider Parteien in Kraft.

Ort, Datum: \_\_\_\_\_

Auftraggeber: \_\_\_\_\_

Auftragnehmer (Tim Vogel · adsbird): \_\_\_\_\_

*Diese Vorlage ist ein juristischer Standardentwurf von adsbird. Die finale, projektspezifisch angepasste und unterschriebene Version erhältst du vor Projektstart. Für Rückfragen: [tim@adsbird.de](mailto:tim@adsbird.de).*