

VERTRAG ZUR AUFTRAGSVERARBEITUNG NACH ART. 28 DSGVO

Dieser Vertrag regelt die Verarbeitung personenbezogener Daten im Auftrag eines Verantwortlichen (nachfolgend „Auftraggeberin“) durch einen Dienstleister (nachfolgend „Auftragnehmerin“). Die Parteien verpflichten sich zur Einhaltung der datenschutzrechtlichen Anforderungen gemäß der Datenschutz-Grundverordnung (DSGVO) und anderen einschlägigen Datenschutzvorschriften.

§ 1 Gegenstand und Dauer des Auftrags

- Die Auftragnehmerin verarbeitet personenbezogene Daten im Auftrag der Auftraggeberin zu den im Anhang 1 beschriebenen Zwecken.
- Die Verarbeitung erfolgt gemäß Art. 6 Abs. 1 DSGVO auf Grundlage der nachweisbaren Weisungen der Auftraggeberin.
- Der Vertrag tritt mit Zustimmung durch Setzen eines Häkchens auf der Webseite der Auftragnehmerin in Kraft.

§ 2 Weisungsrecht der Auftraggeberin

- Die Auftraggeberin ist für die Rechtmäßigkeit der Verarbeitung verantwortlich.
- Erhält die Auftragnehmerin eine unzulässige Weisung, informiert sie die Auftraggeberin unverzüglich.

§ 3 Technische und organisatorische Maßnahmen (TOMs)

- Die Auftragnehmerin verpflichtet sich, geeignete Sicherheitsmaßnahmen nach Art. 32 DSGVO umzusetzen.
- Wesentliche Änderungen sind der Auftraggeberin mitzuteilen.

§ 4 Pflichten der Auftragnehmerin

- Die Auftragnehmerin stellt sicher, dass sich ihre Mitarbeiter zur Vertraulichkeit verpflichten.
- Die Verarbeitung erfolgt nur im EWR, es sei denn, eine Drittlandverarbeitung ist genehmigt.

§ 5 Unterauftragsverhältnisse

- Die Auftragnehmerin darf Unterauftragnehmer nur mit Zustimmung der Auftraggeberin beauftragen.

§ 6 Kontrollrechte der Auftraggeberin

- Die Auftraggeberin hat das Recht, jährlich und anlassbezogen prüfen zu lassen, ob die Auftragnehmerin die Datenschutzvorschriften einhält.

§ 7 Beendigung des Auftrags

- Nach Beendigung der Auftragsverarbeitung löscht oder gibt die Auftragnehmerin alle Daten zurück.

§ 8 Haftung

- Die Haftungshöchstgrenze beträgt pro Schadensfall das dreifache Jahresvolumen des Vertrags.

§ 9 Schlussbestimmungen

- Vertragsänderungen bedürfen der Schriftform.
- Sollten einzelne Bestimmungen unwirksam sein, bleibt der Vertrag im Übrigen wirksam.

Anhang 1 – Liste der Unterauftragnehmer

Unterauftragnehmer	Sitz	Leistung
HelpScout Inc.	USA	Kundenservice- und Helpdesk-Software
noCRM.io	Frankreich	Vertriebsmanagement und Lead-Tracking
Calendly	USA	Terminbuchungssystem
Aircall	Frankreich	Cloud-Telefonie und VoIP
MailerLite	Litauen	E-Mail-Marketing
Zapier Inc.	USA	Automatisierung und Datenweiterleitung
Sentry	USA	Fehler- und Performance-Monitoring
Stripe Inc.	USA	Zahlungsabwicklung und Finanztransaktionen
D9D	Deutschland	IT-Dienstleistungen und Datenverarbeitung

Anhang 2 – Technische und organisatorische Maßnahmen (TOMs)

Zur Gewährleistung der Sicherheit personenbezogener Daten setzt die Auftragnehmerin die folgenden Maßnahmen um:

- **Zugriffskontrollen:**
Beschränkung des Zugangs zu personenbezogenen Daten durch passwortgeschützte Systeme.
- **Datenverschlüsselung:**
Speicherung und Übertragung von Daten nur in verschlüsselter Form (z. B. AES-256, TLS 1.2+).
- **Backup- und Wiederherstellungskonzepte:**
Regelmäßige Sicherung der Daten mit einer maximalen Wiederherstellungszeit von 24 Stunden.
- **Sicherheitsüberprüfungen:**
Regelmäßige Durchführung von Schwachstellenanalysen.
- **Datenschutzrichtlinien für Mitarbeiter:**
Vertraulichkeitsverpflichtungen und regelmäßige Schulungen.
- **Monitoring und Protokollierung:**
Überwachung der Systemaktivitäten zur frühzeitigen Erkennung von Sicherheitsvorfällen.

Stand: Februar 2025