

Vertrag zur Auftragsverarbeitung (AVV) nach Art. 28 DSGVO

Vorlage. Diese Vereinbarung regelt die Verarbeitung personenbezogener Daten, die der Verantwortliche (Betrieb) mithilfe der Anwendung Offerion verarbeitet. Vor produktivem Einsatz rechtlich prüfen lassen; Platzhalter [] ausfüllen.

1. Parteien

Verantwortlicher (Auftraggeber):

[Firmenname des Betriebs], [Inhaber/Vertretungsberechtigte/r], [Straße und Hausnummer], [PLZ Ort]

Auftragsverarbeiter (Auftragnehmer):

Arne Mehrens Solutions, Inhaber Arne Mehrens, Dorfstraße 23, 24256 Stoltenberg, E-Mail: offerion@arnemehrenssolutions.de

2. Gegenstand, Art und Zweck der Verarbeitung

- Gegenstand: Bereitstellung der SaaS-Anwendung Offerion zur Angebotserstellung (Sprachnotiz/Fotos zu Transkription, Positionsliste, PDF/Versand).
- Art der Verarbeitung: Erheben, Erfassen, Speichern, Auslesen, Verändern, Übermitteln an eingebundene Dienstleister, Löschen.
- Zweck: ausschließlich die vertragsgemäße Nutzung der Anwendung durch den Verantwortlichen.

3. Dauer

Die Verarbeitung erfolgt für die Laufzeit des Nutzungsverhältnisses und endet mit dessen Beendigung (Ziffer 9).

4. Art der personenbezogenen Daten

- Stammdaten der Endkunden des Betriebs (Name, Anschrift, ggf. Kundennummer, E-Mail/Telefon, soweit erfasst).
- Angebots- und Leistungsdaten (Positionen, Preise, Betreff, Leistungszeitraum).
- Sprachnotizen (Audio) und Fotos samt erzeugter Transkripte, soweit hochgeladen.

5. Kategorien betroffener Personen

- Endkunden / Auftraggeber des Verantwortlichen.
- ggf. Ansprechpartner und Mitarbeitende dieser Endkunden.

6. Pflichten des Auftragsverarbeiters (Art. 28 Abs. 3 DSGVO)

Der Auftragsverarbeiter

- verarbeitet die Daten nur auf dokumentierte Weisung des Verantwortlichen (die Nutzung der Anwendung gilt als Weisung) und weist auf rechtswidrige Weisungen hin;
- verpflichtet die zur Verarbeitung befugten Personen zur Vertraulichkeit;
- trifft die erforderlichen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO (Anlage 1);
- nimmt weitere Auftragsverarbeiter nur nach Ziffer 7 in Anspruch;
- unterstützt bei der Erfüllung von Betroffenenrechten (Art. 12 bis 23);
- unterstützt bei der Einhaltung der Art. 32 bis 36 DSGVO (Sicherheit, Datenpannen, Folgenabschätzung);
- löscht oder gibt die Daten nach Vertragsende zurück (Ziffer 9);
- stellt die zum Nachweis erforderlichen Informationen bereit und ermöglicht Überprüfungen.

7. Unterauftragsverarbeiter

Der Verantwortliche genehmigt allgemein die Beauftragung der folgenden Unterauftragsverarbeiter. Die Verarbeitung erfolgt in der EU; etwaige Drittlandbezüge sind über EU-Standardvertragsklauseln (Art. 46 DSGVO) abgesichert:

- Vercel Inc. - Hosting/Auslieferung - EU; US-Mutter (SCC).
- Supabase - Datenbank, Authentifizierung, Datei-Speicher - EU-Region; US-Mutter (SCC).
- Mistral AI - Transkription (Voxtral) und KI-Extraktion - Frankreich (EU).

Über Änderungen informiert der Auftragsverarbeiter vorab; der Verantwortliche kann aus wichtigem datenschutzrechtlichem Grund widersprechen.

8. Ort der Verarbeitung / Drittländer

Die Verarbeitung der Inhaltsdaten erfolgt innerhalb der EU/des EWR. Übermittlungen in Drittländer nur unter den Voraussetzungen der Art. 44 ff. DSGVO.

9. Löschung und Rückgabe nach Vertragsende

Nach Abschluss der Verarbeitung löscht der Auftragsverarbeiter die Daten oder gibt sie nach Wahl des Verantwortlichen zurück, sofern keine gesetzliche Aufbewahrungspflicht besteht. Sprachnotizen (Audio) werden bereits im laufenden Betrieb automatisch nach 30 Tagen gelöscht.

10. Schlussbestimmungen

Es gilt deutsches Recht. Unwirksame Bestimmungen berühren die Wirksamkeit des Übrigen nicht. Änderungen bedürfen der Textform.

Ort, Datum: _____

Verantwortlicher

Auftragsverarbeiter

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

- Vertraulichkeit: Mandantentrennung über Datenbank-Sicherheitsregeln (Row-Level-Security); Zugriff nur für befugte Personen.
- Integrität: verschlüsselte Übertragung (TLS); etablierte Cloud-Dienstleister mit anerkannten Sicherheitsstandards.
- Verfügbarkeit: Hosting mit redundanter Infrastruktur und regelmäßigen Backups.
- Datensparsamkeit: automatische Löschung von Audiodateien nach 30 Tagen; die Kundenkartei wird nicht an die KI übergeben.
- Belastbarkeit/Prüfung: Rate- und Kostenlimits gegen Missbrauch; regelmäßige Aktualisierung der Komponenten.