Auftragsverarbeitungsvertrag (Art. 28 DSGVO)

1. Gegenstand und Grundlage

Dieser Auftragsverarbeitungsvertrag (AVV) konkretisiert die Pflichten der Parteien aus Art. 28 DSGVO. Er gilt für die Verarbeitung personenbezogener Daten, die der **Auftragsverarbeiter** (FHC+P GmbH, Würmstraße 55, 82166 Gräfelfing) im Auftrag des **Verantwortlichen** (Kunde/Nutzer des Dienstes „ZUGFeRD-API") im Rahmen der Nutzung des Dienstes durchführt.

2. Gegenstand, Art, Zweck und Dauer

Gegenstand/Zweck: Erzeugung, Prüfung und Verwaltung elektronischer Rechnungen (ZUGFeRD/Factur-X nach EN 16931) sowie zugehörige Konto-, Kunden- und Rechnungsverwaltung. **Art:** Erheben, Speichern, Verändern, Auslesen, Übermitteln (PDF/XML), Löschen. **Dauer:** für die Laufzeit des Nutzungsverhältnisses; danach gemäß Ziffer 7.

3. Art der Daten und Kategorien betroffener Personen

Datenarten: Stammdaten (Firma/Name, Anschrift, USt-IdNr./Steuernummer, Kontaktdaten), Rechnungs-/Zahlungsdaten (Beträge, IBAN/BIC, Positionen), Konto-/Zugangsdaten des Nutzers. **Betroffene:** Beschäftigte und Ansprechpartner des Verantwortlichen, dessen Kunden/Rechnungsempfänger und Lieferanten.

4. Weisungsbindung

Der Auftragsverarbeiter verarbeitet die Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen (einschließlich der über die Anwendung getätigten Eingaben), es sei denn, er ist gesetzlich zur Verarbeitung verpflichtet. Hält er eine Weisung für rechtswidrig, informiert er den Verantwortlichen.

5. Vertraulichkeit

Zur Verarbeitung eingesetzte Personen sind auf Vertraulichkeit verpflichtet und entsprechend unterwiesen (Art. 28 Abs. 3 lit. b, Art. 29, 32 Abs. 4 DSGVO).

6. Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

- **Transportverschlüsselung:** TLS/HTTPS für alle Verbindungen; HSTS.
- **Zugangs-/Zugriffskontrolle:** persönliche Konten, Passwort-Hashing, Rollen-/Admintrennung, automatische IP-Sperren bei Missbrauch (Firewall).
- **Mandantentrennung:** kontobezogene Datentrennung; Kundendaten sind je Konto isoliert.
- **Verfügbarkeit/Wiederherstellbarkeit:** regelmäßige, integritätsgeprüfte Backups; Wiederherstellungsverfahren.
- **Protokollierung:** sicherheitsrelevante Ereignisse; Fehler-/Zugriffslogs.
- **Datenminimierung:** es werden keine besonderen Kategorien (Art. 9 DSGVO) erhoben.

7. Löschung und Rückgabe

Nach Abschluss der Leistung löscht der Auftragsverarbeiter die Daten oder gibt sie zurück (Wahl des Verantwortlichen), soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen. Der Export von Rechnungen (PDF/XML) ist jederzeit möglich.

8. Unterauftragsverarbeiter

Der Verantwortliche genehmigt den Einsatz folgender Unterauftragsverarbeiter; ein Wechsel wird mit angemessener Frist mitgeteilt und kann begründet abgelehnt werden:

Dienstleister	**Zweck**	**Ort**
Hostinger International Ltd	Hosting / Rechenzentrum	Deutschland
Stripe Payments Europe, Ltd.	Zahlungsabwicklung (Credit-Kauf)	EU/Irland
OpenRouter, Inc.	KI-gestützte Zuordnung (nur bei Nutzung der optionalen KI-Funktion)	USA / Drittland

9. Unterstützung, Betroffenenrechte, Datenpannen

Der Auftragsverarbeiter unterstützt den Verantwortlichen im Rahmen des Möglichen bei der Erfüllung von Betroffenenrechten (Art. 12–23) sowie bei Pflichten nach Art. 32–36. Er meldet Verletzungen des Schutzes personenbezogener Daten unverzüglich nach Bekanntwerden.

10. Nachweise und Kontrollen

Der Auftragsverarbeiter stellt die zur Einhaltung erforderlichen Informationen bereit und ermöglicht angemessene Überprüfungen (Art. 28 Abs. 3 lit. h).

11. Schlussbestimmungen

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