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 „sichere-erechnung.de") im Rahmen der Nutzung des Dienstes durchführt.

1a. Firmengruppen (mehrere Absenderfirmen)

Legt ein Kunde in seinem Konto (**Hauptkonto**) weitere Absenderfirmen an (**Gruppenfirmen**), ist jede Gruppenfirma für die personenbezogenen Daten, die in ihrem Bereich des Dienstes verarbeitet werden, eigene Verantwortliche im Sinne von Art. 4 Nr. 7 DSGVO. Dieser Vertrag gilt mit jeder Gruppenfirma als eigenem Verantwortlichen.

Der Inhaber des Hauptkontos schließt diesen Vertrag zugleich im Namen jeder Gruppenfirma ab, die er anlegt. Er sichert zu, von jeder Gruppenfirma dazu bevollmächtigt zu sein, und weist die Vollmacht auf Verlangen des Auftragsverarbeiters in Textform nach.

Weisungen für eine Gruppenfirma (Ziffer 4) erteilen der Inhaber des Hauptkontos und die Personen, denen er Zugang zum Team des Hauptkontos gibt; jede Gruppenfirma erkennt diese Personen als weisungsberechtigt an. Mitteilungen des Auftragsverarbeiters nach diesem Vertrag gehen an die Kontaktadresse des Hauptkontos und gelten damit jeder Gruppenfirma als zugegangen.

Die Daten jeder Gruppenfirma werden getrennt gespeichert (Ziffer 6). Zwischen Gruppenfirmen derselben Firmengruppe werden Daten nur verarbeitet, soweit das Hauptkonto es veranlasst oder der Dienst es als Funktion der Firmengruppe vorsieht: Eingangsrechnungen, die an eine andere Gruppenfirma adressiert sind, werden dieser zugeordnet; die Sperrliste verdächtiger Bankverbindungen wird für alle Gruppenfirmen gemeinsam ausgewertet; die Gesamtsicht und der Gesamtexport fassen die Daten aller Gruppenfirmen für Nutzer zusammen, die alle Rechnungen sehen dürfen. Für die Zulässigkeit dieser Verarbeitung im Verhältnis der Gruppenfirmen zueinander sind die Gruppenfirmen selbst verantwortlich.

Die übrigen Regelungen dieses Vertrags, insbesondere die Unterauftragsverarbeiter nach Ziffer 8, gelten für jede Gruppenfirma unverändert.

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. In einer Firmengruppe (Ziffer 1a) gelten diese Kategorien für jede Gruppenfirma gesondert; die Konto- und Zugangsdaten der Nutzer und

Teammitglieder werden einmal für die Firmengruppe am Hauptkonto geführt.

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. Weisungen können schriftlich, in Textform oder durch dokumentierte Konfigurationen in der Anwendung erteilt werden. Der Auftragsverarbeiter archiviert alle Weisungen für die Dauer des Vertragsverhältnisses und macht sie dem Verantwortlichen auf Anfrage zugänglich.

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.
- **Speicherverschlüsselung:** besonders sensible gespeicherte Werte (u. a. OAuth-Zugangstoken, Zwei-Faktor-Geheimnisse) werden durch authentifizierte Verschlüsselung (libsodium/XSalsa20-Poly1305) geschützt; Offsite-Datensicherungen sind zusätzlich AES-256-verschlüsselt.
- **Zugangs-/Zugriffskontrolle:** persönliche Konten, Passwort-Hashing, Rollen-/Admintrennung, automatische IP-Sperren bei Missbrauch (Firewall).
- **Zutrittskontrolle Rechenzentrum:** physische Zutrittskontrollen durch den Hosting-Dienstleister (Hetzner, Rechenzentrum Deutschland).
- **Mandantentrennung:** kontobezogene Datentrennung; Kundendaten sind je Konto isoliert, in einer Firmengruppe je Gruppenfirma. Auf mehrere Gruppenfirmen greifen nur das Hauptkonto und dessen Team zu; die Zugehörigkeit zur Firmengruppe wird bei jedem Zugriff geprüft.
- **Verfügbarkeit/Wiederherstellbarkeit:** tägliche, integritätsgeprüfte Backups mit periodisch getestetem Wiederherstellungsverfahren sowie automatisierter Überwachung des Sicherungsstatus (Alarmierung bei Ausfall).
- **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.

Eine einzelne Gruppenfirma wird im Dienst nicht gelöscht, sondern stillgelegt; ihre Daten bleiben gespeichert, damit gesetzliche Aufbewahrungspflichten und die Lückenlosigkeit der Rechnungsnummern gewahrt bleiben. Weist eine Gruppenfirma den Auftragsverarbeiter in Textform an, ihre Daten zu löschen, löscht er die personenbezogenen Inhalte dieser Gruppenfirma, soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen. Die Löschung des Hauptkontos erfasst alle Gruppenfirmen.

8. Unterauftragsverarbeiter

Der Verantwortliche genehmigt den Einsatz folgender Unterauftragsverarbeiter. Ein Wechsel eines Unterauftragsverarbeiters wird dem Verantwortlichen mindestens 30 Tage vor dem geplanten Wechsel mitgeteilt. Der Verantwortliche kann den Wechsel innerhalb von 14 Tagen nach Mitteilung in Textform ablehnen, wenn Tatsachen die Annahme rechtfertigen, dass der neue Unterauftragsverarbeiter nicht die in Art. 28 DSGVO geforderten Voraussetzungen erfüllt.

Dienstleister	**Zweck**	**Ort**
Hetzner Online GmbH	Hosting / Rechenzentrum	Deutschland
Stripe Payments Europe, Ltd.	Zahlungsabwicklung (Credit-Kauf)	EU/Irland
Mistral AI SAS	KI-gestützte Zuordnung (nur bei Nutzung der optionalen KI-Funktion)	EU/Frankreich
ALL-INKL.COM, Neue Medien Münnich	Offsite-Datensicherung (nur verschlüsselt, der Anbieter hat keinen Zugriff auf den Klartext)	Deutschland
Microsoft Ireland Operations Limited	Anbindung von Microsoft-365-Postfächern über Microsoft Graph (nur bei Nutzung)	EU/Irland, Übermittlung in die USA möglich
Cloudflare, Inc.	Bot-Schutz Turnstile bei Registrierung und Anmeldung, nur wenn aktiv (IP-Adresse und Browserdaten der Besucher, keine Rechnungsdaten)	USA (Standardvertragsklauseln bzw. Data Privacy Framework)
Europäische Kommission (VIES)	Gültigkeitsprüfung von USt-IdNr. (nur die Nummer wird übermittelt)	EU

Hetzner, ALL-INKL.COM, Stripe und Mistral verarbeiten die Daten innerhalb der EU. Bei Microsoft und Cloudflare ist eine Übermittlung in ein Drittland möglich; sie stützt sich auf die Standardvertragsklauseln bzw. das EU-US Data Privacy Framework. Sollte künftig ein Unterauftragsverarbeiter in einem Drittstaat eingesetzt werden, werden hierfür die von der Europäischen Kommission erlassenen Standardvertragsklauseln vereinbart und vor der erstmaligen Übermittlung ein Transfer Impact Assessment nebst erforderlichen ergänzenden technischen und organisatorischen Maßnahmen durchgeführt; die Ergebnisse werden dem Verantwortlichen auf Anfrage zur Verfügung gestellt.

9. Unterstützung, Betroffenenrechte, Datenpannen

Der Auftragsverarbeiter unterstützt den Verantwortlichen im Rahmen des Möglichen bei der Erfüllung von Betroffenenrechten (Art. 12 bis 23) sowie bei Pflichten nach Art. 32 bis 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.