

Vereinbarung über die Auftragsverarbeitung

gemäß Art. 28 Abs. 3 der Verordnung (EU) 2016/679 (DSGVO)

zwischen dem **Auftraggeber** (Kunde, wie im Bestellprozess bzw. Hauptvertrag angegeben) — nachfolgend „Verantwortlicher“ —

und **Sebastian Faujour (Entreprise individuelle)**, 10 Coat Moualch, 29233 Cléder, Frankreich, handelnd unter „Billhorse“ — nachfolgend „Auftragsverarbeiter“ —

§ 1 Gegenstand und Dauer

(1) Der Auftragsverarbeiter erbringt für den Verantwortlichen Leistungen zur Validierung und zum Parsen elektronischer Rechnungen (XRechnung, ZUGFeRD/Factur-X) über eine Programmierschnittstelle (API) gemäß Hauptvertrag bzw. den jeweils gültigen Nutzungsbedingungen.

(2) Die Dauer dieser Vereinbarung entspricht der Laufzeit des Hauptvertrags.

§ 2 Art, Zweck und Umfang der Verarbeitung

(1) Die Verarbeitung erfolgt ausschließlich zur synchronen Prüfung und Strukturierung der vom Verantwortlichen übermittelten Rechnungsdateien. Die Verarbeitung erfolgt flüchtig im Arbeitsspeicher; eine Speicherung, Protokollierung oder anderweitige Persistierung der Rechnungsinhalte durch den Auftragsverarbeiter findet nicht statt.

(2) **Art der Daten:** Rechnungsdaten, die personenbezogene Daten enthalten können, insbesondere Namen und Kontaktdaten von Ansprechpartnern, Adressdaten, Bankverbindungen, Kennungen (z. B. USt-IdNr., Leitweg-ID) sowie Leistungsbeschreibungen.

(3) **Kategorien betroffener Personen:** Ansprechpartner und Mitarbeiter des Verantwortlichen, seiner Kunden und Lieferanten.

(4) Die Verarbeitung findet ausschließlich auf Servern in Frankfurt am Main (Bundesrepublik Deutschland) statt. § 6 bleibt unberührt.

§ 3 Weisungsrecht

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen; die Nutzung der API stellt eine solche Weisung dar.

(2) Hält der Auftragsverarbeiter eine Weisung für rechtswidrig, informiert er den Verantwortlichen unverzüglich.

§ 4 Vertraulichkeit

Der Auftragsverarbeiter stellt sicher, dass sich alle zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO).

§ 5 Technische und organisatorische Maßnahmen

Der Auftragsverarbeiter trifft die in **Anlage 1** beschriebenen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO und passt sie dem Stand der Technik fortlaufend an, ohne das Schutzniveau zu unterschreiten.

§ 6 Unterauftragsverhältnisse

(1) Die in **Anlage 2** genannten Unterauftragsverarbeiter gelten als genehmigt.

- (2) Der Auftragsverarbeiter informiert den Verantwortlichen über beabsichtigte Änderungen mit angemessener Frist vorab; der Verantwortliche kann aus wichtigem Grund widersprechen.
- (3) Soweit ein Unterauftragsverarbeiter seinen Sitz in einem Drittland hat, erfolgt die Übermittlung nur bei Vorliegen geeigneter Garantien nach Kapitel V DSGVO (insbesondere EU-Standardvertragsklauseln).

§ 7 Unterstützungspflichten

Der Auftragsverarbeiter unterstützt den Verantwortlichen mit angemessenen Mitteln bei der Erfüllung der Rechte betroffener Personen (Art. 12–23 DSGVO) sowie der Pflichten aus Art. 32–36 DSGVO. Da Rechnungsinhalte nicht gespeichert werden, liegen beim Auftragsverarbeiter regelmäßig keine betroffenenbezogenen Daten vor, auf die sich Auskunfts-, Berichtigungs- oder Löschersuchen beziehen könnten.

§ 8 Meldung von Verletzungen

Der Auftragsverarbeiter meldet dem Verantwortlichen Verletzungen des Schutzes personenbezogener Daten unverzüglich nach Bekanntwerden (Art. 33 Abs. 2 DSGVO) und stellt die zur Erfüllung der Meldepflichten erforderlichen Informationen bereit.

§ 9 Löschung und Rückgabe

Rechnungsinhalte werden systembedingt unmittelbar nach Abschluss der jeweiligen Verarbeitung aus dem Arbeitsspeicher entfernt. Sonstige im Rahmen des Vertragsverhältnisses verarbeitete personenbezogene Daten (z. B. Kontodaten des Verantwortlichen) werden nach Vertragsende gelöscht, soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

§ 10 Nachweise und Kontrollen

Der Auftragsverarbeiter stellt dem Verantwortlichen alle zum Nachweis der Einhaltung dieser Vereinbarung erforderlichen Informationen zur Verfügung und ermöglicht angemessene Überprüfungen (Art. 28 Abs. 3 lit. h DSGVO), in der Regel durch Vorlage geeigneter Dokumentation.

§ 11 Schlussbestimmungen

- (1) Es gilt das Recht der Bundesrepublik Deutschland.
- (2) Sollten einzelne Bestimmungen unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.
- (3) Diese Vereinbarung wird in deutscher, englischer und französischer Sprache bereitgestellt. Bei Abweichungen oder Auslegungsfragen ist allein die deutsche Fassung maßgeblich.

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

Vertraulichkeit & Zugriffskontrolle: Betrieb in isolierten Umgebungen beim Hosting-Anbieter; Zugriff auf Produktionssysteme ausschließlich durch autorisierte Personen mittels personengebundener Schlüssel; Prinzip der minimalen Rechtevergabe.

Transportverschlüsselung: Sämtliche Kommunikation mit der API erfolgt ausschließlich über HTTPS/TLS; unverschlüsselte Verbindungen werden abgewiesen.

Datenminimierung durch Architektur: Verarbeitung ausschließlich flüchtig im Arbeitsspeicher; keine Persistierung, keine Protokollierung von Rechnungsinhalten; Betriebs-Logs enthalten ausschließlich Metadaten (Zeitpunkt, Endpoint, Status).

Verfügbarkeit: Automatische Überwachung (Health Checks), automatischer Neustart fehlerhafter Instanzen.

Standortkontrolle: Verarbeitung ausschließlich in der Region Frankfurt am Main; die Regionsbindung ist konfiguratив festgeschrieben.

Anlage 2 — Genehmigte Unterauftragsverarbeiter

Fly.io Inc., 2045 W Grand Ave Ste B, Chicago, IL 60612, USA — Leistung: Infrastruktur-Hosting der API (Rechenzentrumsregion Frankfurt am Main, Deutschland). Garantien: Auftragsverarbeitungsvertrag inkl. EU-Standardvertragsklauseln.

Ort, Datum: _____ Ort, Datum: _____

Verantwortlicher

Auftragsverarbeiter