Data Processing Agreement

pursuant to Art. 28(3) of Regulation (EU) 2016/679 (GDPR) — courtesy translation; the German version prevails (see § 11(3))

between the **customer** (as specified during ordering or in the main agreement) — hereinafter the “Controller” —

and **Sebastian Faujour (entreprise individuelle)**, 10 Coat Moualch, 29233 Cléder, France, trading as “Billhorse” — hereinafter the “Processor” —

§ 1 Subject matter and duration

(1) The Processor provides services to the Controller for the validation and parsing of electronic invoices (XRechnung, ZUGFeRD/Factur-X) via an application programming interface (API) in accordance with the main agreement or the applicable terms of use.

(2) The duration of this agreement corresponds to the term of the main agreement.

§ 2 Nature, purpose and scope of processing

(1) Processing takes place exclusively for the synchronous validation and structuring of invoice files submitted by the Controller. Processing is transient and in-memory only; the Processor does not store, log or otherwise persist invoice contents.

(2) **Types of data:** invoice data which may contain personal data, in particular names and contact details of contact persons, address data, bank details, identifiers (e.g. VAT ID, Leitweg-ID) and service descriptions.

(3) **Categories of data subjects:** contact persons and employees of the Controller, its customers and suppliers.

(4) Processing takes place exclusively on servers in Frankfurt am Main (Federal Republic of Germany). § 6 remains unaffected.

§ 3 Right to issue instructions

(1) The Processor processes personal data only on documented instructions from the Controller; use of the API constitutes such an instruction.

(2) If the Processor considers an instruction unlawful, it shall inform the Controller without undue delay.

§ 4 Confidentiality

The Processor ensures that all persons authorised to process the data have committed themselves to confidentiality or are under an appropriate statutory obligation of secrecy (Art. 28(3)(b) GDPR).

§ 5 Technical and organisational measures

The Processor implements the technical and organisational measures described in **Annex 1** pursuant to Art. 32 GDPR and adapts them continuously to the state of the art without falling below the agreed level of protection.

§ 6 Sub-processors

(1) The sub-processors listed in **Annex 2** are deemed approved.

(2) The Processor shall inform the Controller of intended changes with reasonable advance notice; the Controller may object for good cause.

(3) Where a sub-processor is established in a third country, transfers only take place subject to appropriate safeguards under Chapter V GDPR (in particular EU Standard Contractual Clauses).

§ 7 Assistance obligations

The Processor supports the Controller with appropriate means in fulfilling the rights of data subjects (Art. 12–23 GDPR) and the obligations under Art. 32–36 GDPR. As invoice contents are not stored, the Processor generally holds no data-subject-related data to which access, rectification or erasure requests could refer.

§ 8 Notification of breaches

The Processor shall notify the Controller of personal data breaches without undue delay after becoming aware of them (Art. 33(2) GDPR) and shall provide the information required to fulfil notification obligations.

§ 9 Deletion and return

By design, invoice contents are removed from memory immediately after the respective processing is completed. Other personal data processed in the course of the contractual relationship (e.g. the Controller's account data) will be deleted after the end of the contract, unless statutory retention obligations require otherwise.

§ 10 Evidence and audits

The Processor shall make available to the Controller all information necessary to demonstrate compliance with this agreement and shall allow for reasonable audits (Art. 28(3)(h) GDPR), as a rule by providing suitable documentation.

§ 11 Final provisions

(1) This agreement is governed by the laws of the Federal Republic of Germany.

(2) Should individual provisions be invalid, the validity of the remaining provisions shall remain unaffected.

(3) This agreement is provided in German, English and French. In the event of discrepancies or questions of interpretation, the German version alone shall prevail.

Annex 1 — Technical and organisational measures (Art. 32 GDPR)

Confidentiality & access control: operation in isolated environments at the hosting provider; access to production systems exclusively by authorised persons using personal keys; principle of least privilege.

Transport encryption: all communication with the API takes place exclusively via HTTPS/TLS; unencrypted connections are rejected.

Data minimisation by architecture: processing is transient and in-memory only; no persistence, no logging of invoice contents; operational logs contain metadata only (timestamp, endpoint, status).

Availability: automatic monitoring (health checks), automatic restart of failed instances.

Location control: processing exclusively in the Frankfurt am Main region; the region binding is fixed in configuration.

Annex 2 — Approved sub-processors

Fly.io Inc., 2045 W Grand Ave Ste B, Chicago, IL 60612, USA — service: infrastructure hosting of the API (data centre region Frankfurt am Main, Germany). Safeguards: data processing agreement incl. EU Standard Contractual Clauses.

Place, date: _____ Place, date: _____

_____ _____

Controller Processor