Data processing agreement (Art. 28 GDPR)

Non-binding translation. Only the German version (Auftragsverarbeitungsvertrag) is legally binding.

1. Subject matter and basis

This data processing agreement (DPA) specifies the obligations of the parties under Art. 28 GDPR. It applies to the processing of personal data that the **processor** (FHC+P GmbH, Würmstraße 55, 82166 Gräfelfing) carries out on behalf of the **controller** (customer or user of the service "sichere-erechnung.de") in the course of the use of the service.

1a. Company groups (multiple sender companies)

If a customer creates further sender companies (**group companies**) in its account (**main account**), each group company is a separate controller within the meaning of Art. 4(7) GDPR for the personal data processed in its area of the service. This agreement applies with each group company as a separate controller.

The holder of the main account concludes this agreement at the same time on behalf of each group company that the holder creates. The holder warrants to be authorised to do so by each group company and proves the authorisation in text form at the request of the processor.

Instructions for a group company (section 4) are given by the holder of the main account and the persons to whom the holder gives access to the team of the main account; each group company recognises these persons as authorised to give instructions. Notices from the processor under this agreement are sent to the contact address of the main account and are thereby deemed to have been received by each group company.

The data of each group company is stored separately (section 6). Data is processed between group companies of the same company group only to the extent that the main account initiates this or the service provides for it as a function of the company group: incoming invoices addressed to another group company are assigned to that company; the block list of suspicious bank details is evaluated jointly for all group companies; the group overview and the full export combine the data of all group companies for users who are permitted to see all invoices. The group companies themselves are responsible for the permissibility of this processing in their relationship to one another.

The remaining provisions of this agreement, in particular the sub-processors under section 8, apply unchanged to each group company.

2. Subject matter, nature, purpose and duration

Subject matter and purpose: Creation, validation and management of electronic invoices (ZUGFeRD/Factur-X in accordance with EN 16931) as well as related account, customer and invoice management. **Nature:** Collection, storage, alteration, retrieval, transmission (PDF/XML), erasure. **Duration:** for the term of the usage relationship; thereafter in accordance with section 7.

3. Type of data and categories of data subjects

Types of data: Master data (company or name, address, VAT ID or tax number, contact details), invoice and payment data (amounts, IBAN/BIC, line items), account and access data of the user. **Data subjects:** Employees and contact persons of the controller, its customers or invoice recipients, and suppliers. In a company group (section 1a), these categories apply separately to each group

company; the account and access data of the users and team members is kept once for the company group at the main account.

4. Obligation to follow instructions

The processor processes the data exclusively on documented instructions from the controller (including the entries made via the application), unless it is required by law to process the data. If it considers an instruction to be unlawful, it informs the controller. Instructions can be given in writing, in text form or through documented configurations in the application. The processor archives all instructions for the duration of the contractual relationship and makes them available to the controller on request.

5. Confidentiality

Persons engaged in the processing are bound to confidentiality and have been instructed accordingly (Art. 28(3)(b), Art. 29, Art. 32(4) GDPR).

6. Technical and organisational measures (Art. 32 GDPR)

- **Transport encryption:** TLS/HTTPS for all connections; HSTS.
- **Encryption at rest:** particularly sensitive stored values (including OAuth access tokens and two-factor secrets) are protected by authenticated encryption (libsodium/XSalsa20-Poly1305); offsite backups are additionally AES-256 encrypted.
- **Access control:** personal accounts, password hashing, separation of roles and admin rights, automatic IP blocking in case of abuse (firewall).
- **Physical access control at the data centre:** physical access controls by the hosting provider (Hetzner, data centre in Germany).
- **Client separation:** account-based data separation; customer data is isolated per account, in a company group per group company. Only the main account and its team have access to several group companies; membership of the company group is checked on every access.
- **Availability and recoverability:** daily, integrity-checked backups with a periodically tested restore procedure and automated monitoring of the backup status (alerting in case of failure).
- **Logging:** security-relevant events; error and access logs.
- **Data minimisation:** no special categories of data (Art. 9 GDPR) are collected.

7. Erasure and return

After completion of the service, the processor deletes the data or returns it (at the choice of the controller), unless statutory retention obligations prevent this. Invoices can be exported (PDF/XML) at any time.

An individual group company is not deleted in the service but deactivated; its data remains stored so that statutory retention obligations and the continuity of invoice numbers are preserved. If a group company instructs the processor in text form to delete its data, the processor deletes the personal content of that group company, unless statutory retention obligations prevent this. The deletion of the main account covers all group companies.

8. Sub-processors

The controller approves the use of the following sub-processors. A change of sub-processor will be notified to the controller at least 30 days before the planned change. The controller may reject the

change in text form within 14 days of notification if facts justify the assumption that the new sub-processor does not meet the requirements of Art. 28 GDPR.

Service provider	Purpose	Location
Hetzner Online GmbH	Hosting / data centre	Germany
Stripe Payments Europe, Ltd.	Payment processing (credit purchases)	EU/Ireland
Mistral AI SAS	AI-assisted mapping (only when the optional AI function is used)	EU/France
ALL-INKL.COM, Neue Medien Münnich	Offsite backup (encrypted only, the provider has no access to the plain text)	Germany
Microsoft Ireland Operations Limited	Connection of Microsoft 365 mailboxes via Microsoft Graph (only when used)	EU/Ireland, transfer to the USA possible
Cloudflare, Inc.	Turnstile bot protection on registration and login, only when active (IP address and browser data of visitors, no invoice data)	USA (Standard Contractual Clauses or Data Privacy Framework)
European Commission (VIES)	Validity check of VAT IDs (only the number is transmitted)	EU

Hetzner, ALL-INKL.COM, Stripe and Mistral process the data within the EU. For Microsoft and Cloudflare, a transfer to a third country is possible; it relies on the Standard Contractual Clauses or the EU-US Data Privacy Framework. Should a sub-processor in a third country be used in the future, the Standard Contractual Clauses adopted by the European Commission will be agreed for this purpose and, before the first transfer, a transfer impact assessment will be carried out together with the necessary supplementary technical and organisational measures; the results will be made available to the controller on request.

9. Assistance, data subject rights, data breaches

The processor assists the controller, as far as possible, in fulfilling data subject rights (Art. 12 to 23) and obligations under Art. 32 to 36. It reports personal data breaches without undue delay after becoming aware of them.

10. Evidence and audits

The processor provides the information necessary to demonstrate compliance and allows for appropriate audits (Art. 28(3)(h)).

11. Final provisions

German law applies. Should individual provisions be invalid, the remainder of the agreement remains valid.