Data Processing Agreement pursuant to Art. 28 GDPR

between the Licensee of the software "fetchtax" (hereinafter the "Controller") and HeyPragmatic GmbH, Kolonnenstr. 8, 10827 Berlin, Germany (hereinafter the "Processor"), jointly referred to hereinafter as the "Parties"

This Data Processing Agreement is a translation of the German original ("Vertrag zur Auftragsverarbeitung"). In the event of any discrepancy or contradiction between the German and English versions, the German version shall prevail.

Preamble

The Processor provides services to the Controller in connection with the software "fetchtax" on the basis of the Terms of Service concluded between the Parties (hereinafter the "Main Agreement"). In the course of providing such services, the Processor processes personal data on behalf of the Controller within the meaning of Art. 4 No. 8 and Art. 28 of Regulation (EU) 2016/679 (General Data Protection Regulation, hereinafter "GDPR"). This Data Processing Agreement (hereinafter "DPA") governs the data protection rights and obligations of the Parties in connection with such processing.

Upon conclusion of the Main Agreement between the Parties, this DPA automatically becomes part of the contract without requiring separate acceptance by the Controller.

§ 1 Subject Matter, Duration, and Specification of Data Processing

(1) The subject matter, nature, and purpose of the processing, the types of personal data, and the categories of data subjects are set out in Annex 1 to this DPA.

(2) The duration of the data processing (term) corresponds to the duration of the Main Agreement, unless the provisions of this DPA give rise to obligations beyond that term.

§ 2 Scope and Responsibility

(1) The Processor processes personal data on behalf of the Controller. This covers activities specified in the Main Agreement and in Annex 1.

(2) Within the scope of this DPA, the Controller is solely responsible for compliance with the statutory provisions of data protection law, in particular for the lawfulness of the transfer of data to the Processor and the lawfulness of data processing ("Controller" within the meaning of Art. 4 No. 7 GDPR).

(3) The Controller's instructions are initially set out in the Main Agreement and this DPA and may thereafter be amended, supplemented, or replaced by the Controller through individual instructions given in writing or in text form to the contact point designated by the Processor (individual instructions). Oral instructions must be confirmed in writing or in text form without undue delay.

§ 3 Obligations of the Processor

(1) The Processor processes personal data exclusively within the scope of the agreements concluded and in accordance with documented instructions of the Controller, unless the Processor is required to process the data under the law of the European Union or of a Member State to which it is subject. In such a case, the Processor shall inform the Controller of these legal requirements before processing, unless the law in question prohibits such information on grounds of important public interest.

(2) The Processor will inform the Controller without undue delay if the Processor is of the opinion that an instruction of the Controller violates data protection provisions. The Processor is entitled to suspend the execution of the respective instruction until it is confirmed or amended by the Controller.

(3) The Processor warrants that the persons entrusted with the data processing have been obliged to confidentiality or are subject to an appropriate statutory obligation of secrecy. This obligation continues after termination of their activity.

(4) The Processor implements the measures in accordance with § 6 of this DPA.

(5) The Processor supports the Controller, to the extent possible, in fulfilling requests and claims of data subjects under Chapter III of the GDPR and in complying with the obligations set out in Art. 32 to 36 GDPR.

(6) The Processor has appointed a data protection officer or has verified that no obligation to appoint one exists. The contact details will be provided to the Controller upon request.

(7) The processing of personal data takes place in principle within the territory of the European Union or the European Economic Area. Any transfer to a third country may only take place if the specific requirements of Art. 44 et seq. GDPR are met.

§ 4 Obligations of the Controller

(1) The Controller shall inform the Processor without undue delay and completely if the Controller identifies errors or irregularities in the processing results with regard to data protection provisions.

(2) The Controller is obliged to treat confidentially all knowledge of trade secrets and data security measures of the Processor obtained in the course of the contractual relationship. This obligation continues after termination of this contract.

(3) Upon request, the Controller shall designate a contact person for the Processor for data protection matters.

§ 5 Requests and Rights of Data Subjects

(1) The Processor will assist the Controller, to the extent possible, with appropriate technical and organizational measures in fulfilling the Controller's obligations under Art. 12 to 22 as well as Art. 32 and 36 GDPR.

(2) If a data subject contacts the Processor directly with claims for rectification, deletion, access, restriction of processing, or data portability, the Processor will refer the data subject to the Controller, to the extent assignment to the Controller is possible.

(3) The Processor may disclose information on personal data processed on behalf only after prior instruction or consent of the Controller.

§ 6 Technical and Organizational Measures

(1) The Processor takes the technical and organizational measures pursuant to Art. 32 GDPR to ensure a level of protection appropriate to the risk. The measures implemented at the time of conclusion of the contract are described in Annex 2.

(2) The technical and organizational measures are subject to technical progress and further development. The Processor is therefore permitted to implement alternative adequate measures. The level of security of the agreed measures must not be reduced thereby. Material changes must be documented.

§ 7 Sub-Processors

(1) The Controller grants the Processor general authorization to engage further processors (hereinafter "Sub-Processors") within the meaning of Art. 28 para. 2 sentence 1 GDPR. The Sub-Processors engaged at the time of conclusion of the contract are listed in Annex 3.

(2) The Processor will inform the Controller of any intended change regarding the engagement or replacement of Sub-Processors in an appropriate manner, no later than 30 days before the engagement or change. The Controller has the right to object to such changes in text form within 14 days of receiving the notice. Such objection may only be raised for an important data protection reason, which must be substantiated to the Processor.

(3) If the Controller raises a substantiated objection within the deadline, the Parties are obliged to seek a mutually acceptable solution. If this is unsuccessful, either Party is entitled to terminate the Main Agreement and this DPA with the notice period provided for in the Main Agreement.

(4) The Processor shall impose on the Sub-Processor the same data protection obligations as set out in this DPA. For sub-processing relationships in a third country, the Processor shall ensure that the requirements of Art. 44 et seq. GDPR are met, in particular by concluding the Standard Contractual Clauses of the EU Commission.

(5) Ancillary services which the Processor obtains from third parties (e.g., telecommunications services, postal and transport services, maintenance and user service, cleaning staff, auditors, or disposal of data media) are not considered sub-processing relationships within the meaning of this provision. However, the Processor shall ensure that appropriate protective measures are taken to guarantee confidentiality also with regard to such ancillary services.

(6) Payment processing by Stripe (Stripe Payments Europe, Ltd.) does not constitute processing on behalf of the Controller within the meaning of this DPA. Stripe processes payment data as an independent controller. The Processor does not act on behalf of the Controller for such processing.

§ 8 Verification and Audit Rights

(1) The Processor shall demonstrate to the Controller by suitable means its compliance with the obligations set out in this DPA. This may in particular take place by submitting current attestations, reports, or report extracts from independent bodies (e.g., auditors, internal audit, data protection officer, IT security department) or by an appropriate certification pursuant to Art. 42 GDPR.

(2) Where, in individual cases, audits by the Controller or an auditor appointed by the Controller are necessary, such audits will be carried out during normal business hours without disruption of business operations, after timely advance notice with a reasonable notice period of at least 30 days. The Processor may make such audits conditional upon prior notification with a reasonable notice period and upon the signing of a confidentiality declaration regarding the data of other customers and the technical and organizational measures implemented.

(3) The Processor may demand reasonable remuneration for assistance with audits that go beyond one per calendar year or that require significant effort. This does not apply in the event of a concrete reason, in particular in the case of a personal data breach.

(4) If a data protection supervisory authority or another governmental supervisory authority of the Controller conducts an audit, the same rules as in paragraph 2 shall apply in principle. A confidentiality declaration need not be signed if the supervisory authority is subject to a professional or statutory obligation of secrecy.

§ 9 Notification in the Event of Processor Breaches

(1) The Processor supports the Controller in complying with the obligations regarding the security of personal data, data breach notification obligations, data protection impact assessments, and prior consultations set out in Art. 32 to 36 GDPR.

(2) The Processor shall inform the Controller without undue delay, and where possible within 48 hours, after becoming aware of a personal data breach. The notification shall contain at least the information pursuant to Art. 33 para. 3 GDPR, insofar as known to the Processor.

(3) The Processor shall take the necessary measures to secure the data and mitigate any possible adverse consequences for data subjects without undue delay, and shall coordinate with the Controller in this regard.

§ 10 Authority to Issue Instructions of the Controller

(1) The Controller shall confirm oral instructions in writing or in text form without undue delay.

(2) The Processor shall inform the Controller without undue delay if the Processor is of the opinion that an instruction violates data protection provisions. The Processor is entitled to suspend the execution of the respective instruction until it is confirmed or amended by the Controller.

§ 11 Deletion and Return of Personal Data

(1) Copies or duplicates of the data will not be created without the Controller's knowledge. Excluded from this are backup copies insofar as they are required to ensure proper data processing, as well as data required to comply with statutory retention obligations.

(2) After completion of the contractually agreed work, or earlier upon request by the Controller – at the latest upon termination of the Main Agreement – the Processor will delete all personal data that has come into its possession in accordance with the provisions of the Main Agreement. Deletion takes place in accordance with § 15 para. 3 of the Main Agreement within 100 days after the end of the contract from the production systems.

(3) Documentation that serves to demonstrate the contractual and proper processing of data must be retained by the Processor beyond the end of the contract in accordance with the respective retention periods. The Processor may hand such documentation over to the Controller at the end of the contract to discharge itself from the obligation.

§ 12 Liability

(1) The liability of the Parties is governed by the provisions of Art. 82 GDPR.

(2) In all other respects, the liability provisions of the Main Agreement apply accordingly, unless mandatory statutory provisions conflict therewith.

§ 13 Miscellaneous

(1) In the event of conflicts between provisions of this DPA and provisions of the Main Agreement, the provisions of this DPA shall prevail to the extent they relate to the processing of personal data.

(2) Should individual parts of this DPA be invalid, this shall not affect the validity of the remainder of the DPA.

(3) Amendments and additions to this DPA and all its components – including any warranties of the Processor – require text form and an express reference to the fact that they constitute

an amendment or addition to these terms. This also applies to the waiver of this form requirement.

(4) The law of the Federal Republic of Germany applies to the exclusion of the UN Convention on Contracts for the International Sale of Goods and the conflict-of-law rules of private international law.

(5) The exclusive place of jurisdiction for all disputes arising from or in connection with this DPA is Berlin, provided the Controller is a merchant, a legal entity under public law, or a special fund under public law.

(6) This DPA is provided in German and English. In the event of contradictions or deviations between the German and English versions, the German version shall prevail.

Annex 1 – Description of the Processing

1. Subject Matter and Purpose of the Processing

Provision of the software "fetchtax" as Software-as-a-Service for the efficient management of commercial business transactions, in particular through the import of data from third-party systems, the processing and preparation of such data, and the provision of data to third-party systems.

2. Nature of the Processing

Collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, alignment or combination, restriction, erasure, or destruction of personal data in the course of providing and operating the Software.

3. Duration of the Processing

The duration of the processing corresponds to the duration of the Main Agreement. Upon termination of the Main Agreement, the data is deleted in accordance with § 11 of this DPA.

4. Types of Personal Data

The processing covers in particular the following types of data:

- Master data (e.g., name, address, company name)
- Contact data (e.g., email address, telephone number)
- Access credentials (e.g., username, encrypted passwords)
- Usage data (e.g., log data, IP addresses, timestamps)
- Data relating to business transactions (e.g., invoice and receipt data, payment information, VAT data)
- Other data processed in the course of business transactions, insofar as such data is personal data

The processing of special categories of personal data pursuant to Art. 9 GDPR is not subject to the agreement and should, as far as possible, be avoided by the Controller.

5. Categories of Data Subjects

- Employees, agents, and other users of the Controller who have access to the Workspace
- Customers, suppliers, and other business partners of the Controller (or of the companies managed by the Controller, e.g., clients of a tax advisor)

- Other persons whose data is processed in the course of the Controller's business transactions (e.g., invoice recipients, contact persons)

Annex 2 – Technical and Organizational Measures pursuant to Art. 32 GDPR

The Processor takes the following technical and organizational measures to protect personal data. The adequacy of the measures is reviewed regularly and adapted to the state of the art as necessary.

1. Confidentiality (Art. 32 para. 1 lit. b GDPR)

Physical access control: Protection against unauthorized physical access to data processing facilities, e.g., through locking systems, alarm systems, video surveillance, access authorization concepts, and visitor registration at hosting providers with appropriate certification (e.g., ISO 27001).

System access control: Protection against unauthorized system use through secure passwords, multi-factor authentication for administrative access, automatic lockout mechanisms, encryption of data storage media, firewall systems.

Data access control: Role and authorization concepts, restriction of access to data to what is necessary for the respective task (need-to-know principle), logging of access, secure deletion of data no longer required.

Separation control: Logical and physical separation of data of different tenants (multi-tenant architecture), separation of production, test, and development environments.

Pseudonymization: Use of pseudonymization and encryption where possible in view of the purpose of processing.

2. Integrity (Art. 32 para. 1 lit. b GDPR)

Transmission control: Transport encryption (TLS) during transmission of personal data, documentation of recipients, secured interfaces.

Input control: Logging of input, modification, and deletion of personal data, traceability through audit logs.

3. Availability and Resilience (Art. 32 para. 1 lit. b GDPR)

Availability control: Regular data backups, redundant systems, uninterruptible power supply (UPS) at the hosting provider, protection against malware, contingency plans.

Rapid recoverability: Defined recovery processes (disaster recovery) and regular tests of recoverability.

4. Procedures for Regular Review, Assessment, and Evaluation (Art. 32 para. 1 lit. d GDPR; Art. 25 para. 1 GDPR)

Data protection management and IT security management

Incident response management and documentation of security incidents

Privacy-friendly default settings (Privacy by Design / Default)

Regular training and obligation of staff to confidentiality and compliance with data protection provisions

Regular review and updating of these measures

5. Processing Control

Clear and unambiguous contract design, formalized order management, strict selection and regular review of Sub-Processors, written instructions, obligation of staff to confidentiality.

Annex 3 – Authorized Sub-Processors

At the time of conclusion of the contract, the Processor engages the following Sub-Processors in the course of providing services:

Sub-Processor	Service	Data	Place of Processing
Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855 Luxembourg	Cloud Hosting	Temporary processing of Customer Data, no permanent storage	EU
Lovable Labs AB, Box 190, 101 23 Stockholm, Sweden	Cloud Hosting	Computing resources and cloud storage for Customer Data	EU
Supabase, Inc., 65 Chulia Street #38-02/03, OCBC Centre, Singapore 049513	Cloud Hosting	Computing resources and cloud storage for Customer Data	EU
n8n GmbH, Novalisstr. 10, 10115 Berlin, Germany	Cloud Hosting	Processing of the Controller's business transactions	EU
Mailgun Technologies, Inc., 112 E Pecan St #1135, San Antonio, TX 78205, USA	Email Delivery	Email addresses and content of system and notification emails	EU

In the event of changes, the Processor will inform the Controller in accordance with § 7 of this DPA.