This data processing agreement including all attachments (hereinafter jointly referred to as the "DPA") specifies the data protection obligations of the Parties under the underlying Order Form.

§ 1 Scope of application and definitions

(1) The following provisions shall apply to all data processing services within the meaning of Art. 28 GDPR provided by HYPATOS to Customer on the basis of the Order Form and to all activities in which personal data may be processed by HYPATOS.
(2) Insofar as the term data processing is used in this DPA for the processing of orders, this is generally to be understood as the use of personal data. Data processing means any operation or set of operations carried out with or without the aid of automated processes relating to personal data, such as collection, recording, organisation, sorting, recording, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, comparison or association, limitation, erasure or destruction.
(3) Reference is made to the other definitions in Art. 4 GDPR and in the Order Form.

§ 2 Subject and duration of data processing

(1) HYPATOS shall process personal data on behalf of and in accordance with instructions by Customer.
(2) The subject of this DPA is the digitisation, storage and further processing of documents, for example incoming invoices of Customer within the scope agreed with HYPATOS, in accordance with the Order Form.
(3) The duration of this DPA corresponds to the duration of the Order Form.

§ 3 Type and purpose of data processing

The type and purpose of data processing include the following activities and purposes:

- Training of the AI base models to the specific requirements of Customer during the project phase
- Automated and manual digitisation of documents
- Storage of documents and associated metadata in a document management system
- Implementation of release processes
- Enhancement of document data with posting accounts, cost centers and other attributes
- Provision of payment information in payment lists
- Export of data for further processing in the Customers' systems
- Providing customer support

§ 4 Categories of data subjects

The categories of persons affected by the handling of personal data under the Order Form can include:

- Employees of Customer
- Customer's suppliers or their employees
- Customers of Customer or their employees
- If applicable, other natural persons whose personal data are contained in the processed documents.

§ 5 Type of Personal Data

(1) The personal data are subject to two categories: personal data of Users ("Personal User Data") and personal data of persons mentioned in the documents processed by means of the Services ("Personal Document Data").
(2) The following data types are affected by data processing:

- Person master data, for example name, address (Personal User Data as well as Personal Document Data.)
- Communication data (e.g. telephone, e-mail) (Personal User Data as well as Personal Document Data.)
- Account master data (e.g. bank details) (Personal Document Data)
- Electronic communication data (e.g. IP address, operating system and browser, time and date) (Personal User Data)
- Log data (Personal User Data)
- Where applicable, other personal data of natural persons contained in the documents provided by the Customer (Personal Document Data).

§ 6 Rights and Duties of the Customer

(1) Customer is the data controller within the meaning of Art. 4 No. 7 GDPR.
(2) Customer is entitled to issue instructions on the type, scope and procedure of data processing. Oral instructions shall be confirmed immediately by HYPATOS in writing or in text form (e.g. by e-mail) at Customer's request.
(3) Insofar as Customer deems it necessary, persons authorized to issue instructions may be named. Customer shall notify HYPATOS of this in text form. In the event that these persons authorized to issue instructions change at Customer, HYPATOS shall be notified thereof in text form, naming the new person in each case.
(4) Customer shall inform HYPATOS immediately if errors or irregularities are detected in connection with the processing of personal data by HYPATOS.

§ 7 Obligations of HYPATOS

(1) Data processing
HYPATOS will process the personal data exclusively in accordance with this DPA and/or the underlying Order Form and in accordance with Customer's instructions, unless HYPATOS is legally required to do otherwise. In the latter case, HYPATOS will inform Customer of that legal requirement before processing.
(2) Data Subject Rights

a. HYPATOS shall support Customer in fulfilling the rights of the parties concerned, in particular with regard to rectification, restriction of processing and deletion, notification and provision of information, within the scope of its capabilities, insofar as HYPATOS is obliged to do so for compelling legal reasons. The obligation to provide support shall only apply in the case of enquiries by data subjects with regard to the data processed on behalf of the Customer as specified in this DPA.
b. If HYPATOS collects the personal data specified in this DPA on behalf of Customer and if this data is the subject of a justified claim to data portability pursuant to Art. 20 GDPR and if the person concerned is identified within the meaning of Art. 12 GDPR, HYPATOS shall notify Customer of the fact that the data has been processed on behalf of Customer in a structured, common and machine-readable format within a reasonable time.
c. At the instruction of Customer, HYPATOS shall correct, delete or restrict the processing of the personal data on behalf of Customer. The same shall apply if this DPA provides for the correction, deletion or limitation of the processing of data.

d. If a data subject contacts HYPATOS directly for the purpose of correcting, deleting or restricting the processing of the personal data, HYPATOS shall forward this request to Customer immediately upon receipt.

(3) Control obligations

a. HYPATOS shall ensure by means of appropriate controls that the personal data collected, processed or used on behalf of Customer are processed exclusively in accordance with this DPA and/or the Order Form and/or the corresponding instructions.

b. HYPATOS shall set up its operating procedures in such a way that the data which it processes on behalf of Customer are secured to the extent necessary and protected from unauthorised access by third parties.

c. HYPATOS confirms that it has appointed a data protection officer and will monitor compliance with data protection and data security regulations, including the data protection officer.

(4) Duty to provide information

a. HYPATOS shall immediately draw Customer's attention to any instructions issued by Customer which, in its opinion, violate statutory provisions. HYPATOS is entitled to suspend the execution of the corresponding instruction until it has been confirmed or changed by the responsible person at Customer's.

b. HYPATOS shall assist Customer in complying with the obligations set out in Articles 32 to 36 GDPR, taking into account the type of processing and the information available to it.

(5) Place of data processing

The data processing takes place in principle on the territory of the Federal Republic of Germany or within the European Union or the states of the European Economic Area. Processing in other states is only permitted with the prior consent of the Customer and only if the special requirements of Art. 44, 45, 46 or 49 GDPR are fulfilled. The consent may only be refused for compelling reasons of data privacy law.

(6) Deletion of personal data after completion of the order

Upon termination of the Order Form, HYPATOS shall delete or destroy all personal data, documents and processing and usage results that have come into its possession and that are connected with the contractual relationship, in accordance with data protection regulations, insofar as the deletion of such data does not conflict with any statutory storage obligations. The deletion or destruction of such data must be documented and confirmed to Customer upon request.

§ 8 Control rights of Customer

(1) Customer shall be entitled, after timely prior registration during normal business hours and without disrupting the business operations of HYPATOS or endangering the security measures for other customers and at his own expense, to ensure compliance with the provisions on data protection and the contractual agreements in the necessary scope itself or by third parties. The controls can also be carried out by accessing existing HYPATOS certifications customary in the industry, current certificates or reports from an independent body (e.g. auditor, external data protection officer, auditor or external data protection auditor) or self-disclosure. HYPATOS will provide the necessary support to carry out the controls.

(2) HYPATOS shall inform Customer about the implementation of control measures by the supervisory authority, insofar as the measures or data processing which HYPATOS provides for Customer may be affected.

§ 9 Subprocessing relationships

(1) Customer authorizes HYPATOS to make use of further data processors in accordance this § 9. This authorization constitutes a general written approval within the meaning of Art. 28 para. 2 GDPR.

(2) HYPATOS currently cooperates with the subprocessors named in Appendix 2. Customer agrees to their assignment.

(3) HYPATOS shall be entitled to commission further subprocessors or to replace those already commissioned. HYPATOS shall inform Customer in advance of any intended change.

(4) Customer may object to an intended change. The objection to the intended change must be made to HYPATOS within two (2) weeks of receipt of the information about the change. In the event of an objection, HYPATOS may, at its own discretion, provide the service without the intended change or - if the provision of the service without the intended change is not reasonable for HYPATOS, e.g. due to disproportionate expenses for HYPATOS associated therewith – extraordinarily terminate this DPA and the Order Form.

(5) HYPATOS is obliged to conclude agreements in accordance with Art. 28 para. 4 GDPR with the subprocessors.

(6) At the request and instruction of Customer, HYPATOS will exercise all rights against a subprocessor, including but not limited to audit rights, which HYPATOS itself is entitled to under the respective data processing agreement and which concern the processing for Customer. HYPATOS is not entitled to any scope of assessment; HYPATOS exercises such rights as if they were Customer's rights.

§ 10 Technical and Organizational Measures

(1) The technical and organisational measures described in Appendix 1 shall be agreed. HYPATOS may update and modify these measures provided that such updates and/or modifications do not significantly reduce the level of protection and are documented.

(2) HYPATOS shall observe the principles of proper data processing pursuant to Art. 32 in connection with Art. 5 para. 1 GDPR. It is obliged to the contractually agreed and legally prescribed data security measures. It will take all necessary, appropriate technical and organizational measures to secure the data and/or the security of the processing, in particular also taking into account the state of the art, the implementation costs and the nature, scope, circumstances and purposes of Customer data as well as to mitigate possible adverse consequences for data subjects. The measures to be taken include in particular measures to protect the confidentiality, integrity, availability and resilience of the systems and measures to ensure the continuity of the processing after incidents. guarantee. HYPATOS will regularly evaluate the implemented measures and make any necessary adjustments in order to be able to guarantee an appropriate level of processing security at all times.

Appendix 1 to DPA

Technical and organizational measures to ensure the security of data processing

HYPATOS warrants that it has taken the following technical and organizational measures:

A. Encryption measures
Measures or processes in which a clearly readable text/information is converted into an illegible, i.e. not easily interpretable, character string (ciphertext) with the aid of an encryption procedure (cryptosystem):

Hypatos has implemented encryption measures in compliance with ISO 27001:2013 Annex A.10. These are documented as part of Hypatos Information Security Management System (ISMS) under Cryptography Policy and include:
- All web traffic transmitted over the Internet between Hypatos and its Customers is encrypted using TLS 1.2+
- Customer data stored at Cloud Infrastructure as a Service (IaaS) providers, documented as sub-processors in Appendix 2 to this DPA, is encrypted at rest using AES-256
- Hard drives of employees' devices are encrypted using AES-256
- Encryption keys and secrets are stored in secure cloud locations, accessible only by Engineering team members, in accordance with least privilege and need-to-know principles
- Implemented encryption measures are monitored by automated security solutions and alerts are sent to relevant stakeholders within Hypatos in case violations are detected

B. Measures to ensure confidentiality (Art. 32 para. 1 lit. b GDPR)

1. Physical access control
Measures physically preventing unauthorised persons from gaining access to IT systems and data processing equipment processing personal data and to confidential files and data carriers:

Description of the access control system:
The Cloud Infrastructure as a Service (IaaS) providers, documented as sub-processors in Appendix 2 to this DPA, maintain physical access control over the cloud infrastructure data processing facilities. Independent external audits review the respective physical security mechanisms in relation to ISO/IEC 27001, PCI DSS and other applicable standards and regulations.
Physical access to Hypatos facilities is controlled in compliance with ISO 27001:2013 Annex A.11. Physical security controls implemented by Hypatos are documented as part of the Information Security Management System (ISMS) under Physical Security Policy
- Entrance to office facilities (main entrance, designated office space) only accessible either with keycard or PIN-code in combination with transponder system for authorized employees or freelancers and service staff (for example cleaning personnel);
- External Security Service regularly controls building and premise
- Central administration and documentation of issue and withdrawal of key cards to employees, contractors and service providers
- Check-in/registration of visitors with office management and documentation of the check-in, access to office premises only possible if employees invite and accompany visitor for the duration of the visit

2. Logical access control
Measures to prevent unauthorised persons from processing or using data protected by data protection law.
Measures to ensure that the persons authorised to use data processing procedures have access only to the personal data subject to their right of access, so that data cannot be read, copied, altered or removed without authorisation during processing, use and storage.

Description of the access control system:
Logical access to Hypatos systems is controlled in compliance with ISO 27001:2013 Annex A.9. Access controls implemented by Hypatos are documented as part of the Information Security Management System (ISMS) under Access Control Policy.
- Logical access to systems (including privileged access) is granted based on the principles of least privilege and need-to-know
- Monitoring and logging of logical access to Hypatos systems
- Review of user access rights on regular basis
- Use of centralized password management solution for all employees
- Central allocation of rights when employees join the company and withdrawal of rights when they leave, based on an authorisation concept; documentation of individual authorisations; maintenance of access lists
- Password-based authentication to systems, i.e. unique user credentials when logging on to systems
- Enforcement of strong password requirements, including minimum length, usage of special characters, etc.
- Depending on the system, single sign-on and/or two-factor authentication in addition to the password-based authentication
- Authentication attempts are logged. After a number of unsuccessful attempts credentials are suspended temporarily.

3. Separation requirement
Measures to ensure that data collected for different purposes are processed separately and are separated from other data and systems in such a way as to prevent unplanned use of such data for other purposes.

Description of the separation control process:
- Software-side user separation
- Logical separation of Customers
- Ensuring compliance with separate extinguishing periods through extinguishing concept
- Separation of development, test and production environments
- Ensuring the separation of data for the training of AI models

C. Measures to safeguard integrity (Art. 32 para. 1 lit. b GDPR)

1. Data integrity
Measures to ensure that stored personal data is not damaged by system malfunctions:

Description of data integrity:
Testing of new releases and patches to verify correctness of changed component. Components that fail these tests are not deployed to production environments
-Changes performed on production systems are planned, scheduled, documented and subject to prior approval
- Changes to production databases and other data storage locations are logged
- Established backup and recovery process in compliance with ISO 27001 Annex A.12.3. Backups are taken and tested regularly.

2. Transmission control
Measures to ensure that it is possible to verify and establish to which bodies personal data have been or may be transmitted or made available by means of data transmission facilities:

Description of the transmission control:
- Data transmission is governed by a process with individual responsibilities

3. Transport control
Measures to ensure that the confidentiality and integrity of personal data are protected when personal data are transmitted and when data media are transported:

Description of the transport control:
Transport control security controls are established in compliance with ISO 27001:2013 Annex A.13. and are documented as part of the Information Security Management System (ISMS) under Network Security Policy
- Sensitive data, including personal data is transported in encrypted form and/or via encrypted communication channels

4. Input control
Measures to ensure that it can be subsequently verified and established whether and by whom personal data have been entered into, modified in or removed from computer systems.

Description of the input control process:
- Activities performed by privileged users are logged and monitored
- Installation of software on production system is only performed by authorized IT personnel

D. Measures to ensure availability and resilience (Art. 32 para. 1 lit. b GDPR)

1. Availability control
Measures to ensure that personal data are protected against accidental destruction or loss.

Description of the availability control system:
Availability controls are established in compliance with ISO 27001:2013 Annex A.17. and are documented as part of the Information Security Management System (ISMS) under Business Continuity Policy
- Established backup and recovery process in compliance with ISO 27001 Annex A.12.3. Backups are taken and tested regularly
-In addition, the Cloud Infrastructure as a Service (IaaS) providers, documented as sub-processors in Appendix 2 to this DPA, maintain availability controls over the cloud infrastructure. Independent external audits review the respective availability mechanisms in relation to ISO/IEC 27001 and other applicable standards and regulations.

2. Rapid recoverability
Measures to ensure the ability to restore rapidly the availability of and access to personal data in the event of a physical or technical incident.

Description of the measures taken to ensure rapid recoverability:
- Established security incident management process compliant with ISO 27001 Annex A.16
- Backup and recovery process is regularly tested

3. Reliability
Measures to ensure that all functions of the system are available and that any malfunctions are reported:

Description of reliability measures:
Automated notifications in case production systems behave outside of defined normal conditions. In case malfunctions are reported, standardized communication and incident management processes are triggered.

E. Data protection through technology design and through data protection-friendly presettings
Privacy by Design means translated "data protection through technology design". The aim should be to ensure that suitable technical measures are implemented as early as the development of processing operations in order to make the planned processing operations compliant with data protection regulations.
Privacy by Default means translated "data protection through data protection-friendly default settings". This means that even the factory settings of a programme/software should be designed in a data protection-friendly manner. This is intended above all to protect the data of the user.
Compliance with data protection requirements and effective data structures in the selection and development of software

F. Measures for the regular evaluation of the security of data processing (Art. 32 para. 1 lit. d GDPR; Art. 25 para. 1 GDPR)

1. Review procedure
Measures to ensure that processing complies with data protection regulations and is secure.

Description of the verification procedures:
- Data protection management and data protection concept
- ISO 27001-certified Information Security Management System (ISMS)
- Formalised security risk management process

- Formalised order management
- Formalised processes for data protection incidents
- Regular control and, if necessary, adjustment of the technical and organisational measures on the basis of the state of the art
- External auditing service that regularly verifies compliance with data protection regulations.

2. Organisational control
Measures to ensure that employees are informed and sensitised to the requirements of data protection and that they are committed to compliance with data protection.

Description of organisational control measures:
- Obligation of all employees to maintain confidentiality
- Regular data protection training for employees
- Exclusion of business use of private equipment
- Written agreements on the use of the Internet and e-mail
- Written agreements on working from the home and mobile office

3. Order control
Measures to ensure that personal data processed on behalf of the Customer can only be processed in accordance with the instructions of the Customer:

Description of order control measures:
- Conclusion of commissioned processing contracts with contract processors in accordance with Art. 28 GDPR
- Keeping a register of Customers and processors
- Formalised order management
- Documentation of the Customers' written instructions
- Examination of technical and organisational measures prior to the conclusion of processing contracts with contract processors
- Ensuring the deletion/destruction of data after completion of the order by contractual agreement

Appendix 2 to DPA: Subcontracting relationships pursuant to § 9 of the DPA

HYPATOS currently cooperates with the following subcontractors in the fulfilment of the order, with whose assignment the Customer agrees.
If the data processing takes place outside the European Economic Area, the following overview also lists the measures and guarantees which ensure an adequate level of data protection in the processing in accordance with Art. 44 et seq. of the European Data Protection Act. GDPR (e.g. EU standard contract clauses, or adequacy decision of the EU Commission).

1. Amazon Web Services

Name/Company: Amazon Web Services EMEA SARL
Function/activity: Cloud Infrastructure as a Service (IaaS) Provider which offers cloud computing services including computing power, storage, and databases, necessary to deliver and maintain Hypatos' SaaS
Headquarters: 38 avenue John F. Kennedy, L-1855 Luxembourg
Type of data: Personal User Data, Personal Document Data
Location of data processing: European Union
Measures/guarantees to ensure an adequate level of data protection: Data Processing Agreement according to Art. 28 GDPR

2. Microsoft

Name/Company: Microsoft Ireland Operations Limited
Function/activity: Processing of customer document email uploads via Microsoft Exchange (part of Microsoft 365); Customer file storage and sharing via Microsoft SharePoint (part of Microsoft 365)
Headquarters: One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland
Type of data: Personal User Data, Personal Document Data
Location of data processing: European Union
Measures/guarantees to ensure an adequate level of data protection: Data Processing Agreement according to Art. 28 GDPR

3. Google Vision AI

Name/Company: Google Ireland Limited
Function/Activity: Cloud OCR provider, enabling extraction of text from customer-uploaded documents
Headquarters: Gordon House, Barrow Street Dublin 4, Ireland
Location of data processing: European Union
Type of data: Personal User Data, Personal Document Data
Measures/guarantees to ensure an adequate level of data protection: Data Processing Agreement according to Art. 28 GDPR

4. Atlas MongoDB

Name/Company: MongoDB, Inc.
Function/Activity: Managed database service within Hypatos' AWS environment, ensuring secure and scalable data storage and retrieval.
Headquarters: MongoDB Limited, Building Two, Number One Ballsbridge, Ballsbridge, Dublin 4, Ireland
Location of data processing: European Union
Type of data: Personal User Data
Measures/guarantees to ensure an adequate level of data protection: Data Processing Agreement according to Art. 28 GDPR

5. Jira Service Management

Name/Company: Atlassian. Pty Ltd
Function/Activity: Service desk for customer support, processing the data that customers enter and attach to tickets, as well as all information related to such tickets
Headquarters: Level 6, 341 George Street, Sydney, NSW, 2000 Australia
Location of data processing: European Union
Type of data: Personal User Data
Measures/guarantees to ensure an adequate level of data protection: Data Processing Agreement according to Art. 28 GDPR

6. Mailjet

Name/Company: Mailjet SAS
Function/Activity: Email notification dispatch service for emails sent to Customer by Hypatos Cloud Services
Headquarters: 13-13 bis, rue de l'Aubrac, 75012 Paris, France
Location of data processing: European Union
Type of data: Personal User Data, Personal Document Data
Measures/guarantees to ensure an adequate level of data protection: Data Processing Agreement according to Art. 28 GDPR

7. OpenAI API

Name/Company: OpenAI Ireland Limited
Function/Activity: Natural language processing and generation of text-based outputs used for further document processing by Hypatos.
Headquarters: The Liffey Trust Centre 117-126, Sheriff Street, Upper, Dublin 1, Ireland, D01 YC43
Location of data processing: European Union
Type of data: Personal User Data, Personal Document Data
Measures/guarantees to ensure an adequate level of data protection: Data Processing Agreement according to Art. 28 GDPR

Optional:

8. LabelYourData

Name/Company: SupportYourApp, Inc. DBA Label Your Data
Function/Activity: Managed data annotation and labelling service provider
Headquarters: 1007 North Orange Street, 4th Floor, Suite 122, Wilmington, DE 19801, USA
Location of data processing: USA
Type of data: Personal Document Data
Measures/guarantees to ensure an adequate level of data protection: Certificate according to the EU-US Data Privacy Framework

9. CenterDevice

Name/Company: CenterDevice GmbH
Function/Activity: Cloud document management system (DMS) for GOBD archive service
Headquarters: Rheinwerkallee 3, 53227 Bonn, Germany
Location of data processing: European Union
Type of data: Personal User Data, Personal Document Data
Measures/guarantees to ensure an adequate level of data protection: Data Processing Agreement according to Art. 28 GDPR

10. DeepL

Name/Company: DeepL SE
Function/Activity: Provides automated translation services for customer documents in languages other than English
Headquarters: Maarweg 165, 50825 Cologne, Germany
Location of data processing: European Union
Type of data: Personal User Data, Personal Document Data
Measures/guarantees to ensure an adequate level of data protection: Data Processing Agreement according to Art. 28 GDPR

11. Wargitsch

Name/Company: Wargitsch & Comp. AG
Function/Activity: Implementation Partner
Headquarters: Ingolstädter Straße 92, 85276 Pfaffenhofen an der Ilm, Germany
Location of data processing: European Union
Type of data: Personal User Data, Personal Document Data
Measures/guarantees to ensure an adequate level of data protection: Data Processing Agreement according to Art. 28 GDPR

12. EY

Name/Company: EY GmbH & Co. KG Wirtschaftsprüfungsgesellschaft
Function/Activity: Implementation Partner
Headquarters: Graf-Adolf-Platz 15, 40213 Düsseldorf, Germany
Location of data processing: European Union
Type of data: Personal User Data, Personal Document Data
Measures/guarantees to ensure an adequate level of data protection: Data Processing Agreement according to Art. 28 GDPR

13. KPMG

Name/Company: KPMG Advisory N.V.
Function/Activity: Implementation Partner
Headquarters: (1186 DS) Laan van Langerhuize 1, Amstelveen, the Netherlands
Location of data processing: European Union
Type of data: Personal User Data, Personal Document Data
Measures/guarantees to ensure an adequate level of data protection: Data Processing Agreement according to Art. 28 GDPR