LEGAL

Data processing agreement

Agreement on the processing of data on behalf of the Client under Art. 28 GDPR, with the appendices on subprocessors, technical and organizational measures and types of personal data.

Last updated: October 30, 2026

CONTENTS

Preamble
1. Subject matter and purpose of the processing
2. General Provision
3. Subject Matter of the Processing
4. Rights and Obligations of the Client
5. General Obligations of the Contractor
6. Data Protection Coordinator of the Contractor
7. Reporting Obligations of the Contractor
8. Cooperation Obligations of the Contractor
9. Audit and Inspection Rights
10. Subcontracting Relationships
11. Confidentiality Obligation
12. Safeguarding Data Subject Rights
13. Technical and Organisational Measures
14. Term and Termination
15. Consequences of Termination
16. Place of Jurisdiction
17. Final Provisions
Appendix 1: Subprocessors
Appendix 2: Technical and Organizational Measures (TOMs)
Appendix 3: Types of Personal Data

Preamble

This Data Processing Agreement (“DPA”) applies between Prodlane GmbH, Löhrstraße 15, 04105 Leipzig, Germany (“Contractor”), and the customer using MAIA in the course of its professional, business or organizational activities (“Client”). It supplements the agreement on the use of MAIA (“Usage Agreement”) and governs the processing of personal data that the Contractor carries out in that context on behalf of the Client.

The DPA is agreed by being expressly incorporated into an offer accepted by the Client, an order or the Usage Agreement, including by electronic acceptance on behalf of the Client, for example when placing an online order. It may also be signed separately. A separate signature is not required where the DPA is otherwise effectively incorporated.

From the date it is agreed, the DPA applies to all processing carried out on behalf of the Client in the course of using MAIA, including trial and pilot phases. It is to be agreed before such processing begins.

1. Subject matter and purpose of the processing

The Client's order to the Contractor includes the following work and/or services:

As part of this contract, the Contractor shall provide the Client with the cloud-based SaaS solution "MAIA". MAIA enables the use of various large language models (LLMs) in a data protection-compliant environment, in particular chatting with an AI assistant, analysing and searching documents provided by the Client, connecting the Client's external data sources, creating files and running workflows. The service description sets out the scope of services in detail.

2. General Provision

2.1 The Contractor processes personal data on behalf of the Client within the meaning of Article 4(8) and Article 28 of Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR). This Agreement governs the rights and obligations of the Parties in connection with the processing of personal data.

2.2 Where the terms “data processing” or “processing” (of data) are used in this Agreement, they shall have the meaning assigned to “processing” in Article 4(2) GDPR.

2.3 Where the processing for the Client is subject to the Swiss Federal Act on Data Protection (FADP), the Contractor shall also perform its obligations under this Agreement in accordance with the FADP, in particular Article 8 FADP (data security), Article 9 FADP (processing by processors) and Articles 16 et seq. FADP (disclosure abroad). In that case, references to the GDPR include the corresponding provisions of the FADP. The authorisation of subprocessors under Clause 10 constitutes prior authorisation within the meaning of Article 9(3) FADP.

3. Subject Matter of the Processing

3.1 The subject matter of the processing relates to all personal data that the Client provides to the Contractor for processing, in particular via the chat interface, document upload and integrated interfaces. Where the Client provides such data by another channel, in particular by e-mail, via file sharing services or by post, so that the Contractor processes it, such data is also subject to this Agreement. In the context of interface integration, this includes both the integrations provided by MAIA and those developed in-house by the Client and connected via the application programming interface (API). Integration is understood here as any technical interface that enables bidirectional data exchange between MAIA and third-party systems. Integrations, including servers connected via the Model Context Protocol (MCP), access third-party systems with the permissions granted by the Client or its users, in particular by signing in to the third-party system or by consent of an administrator. Read and write operations in third-party systems are performed on the Client’s instructions (Clause 4.3). Operators of third-party systems that the Client uses on the basis of its own contracts and connects to MAIA are not subprocessors of the Contractor. The Client is itself responsible for the processing in such third-party systems in its relationship with their operators. The processing in MAIA of data retrieved from third-party systems is subject to this Agreement.

3.2 Irrespective of the content provided by the Client, certain categories of personal data are processed by the Contractor on behalf of the Client when the MAIA platform is used, which are technically or organizationally necessary for the provision, operation and security of the platform (in particular data relating to the setup and administration of user accounts, authentication, and the logging of access and activities). These categories of data are described in Appendix 3 (Types of Personal Data). The Contractor shall be entitled to update this Appendix in the event of changes to the platform or its technical requirements. The Contractor shall inform the Client without undue delay of any such updates.

3.3 The Client is responsible for ensuring that the processing of the data it transmits is lawful. This also applies to special categories of personal data pursuant to Article 9 GDPR.

3.4 Personal data arising in the course of initiating, performing and administering the business relationship between the parties is processed by the Contractor as a controller in its own right within the meaning of Art. 4(7) GDPR and not on behalf of the Client. This includes in particular business contact details of contact persons, correspondence on support, invoicing, scheduling and contract administration, as well as status and incident reports. The Contractor informs the data subjects in accordance with Art. 13 GDPR and states the legal basis in its privacy notice. Where such communication contains personal data that the Client provides for processing, in particular as an attachment, embedded screenshot or extract, such data is subject to Section 3.1 and thus to this Agreement.

4. Rights and Obligations of the Client

4.1 The Client shall remain the controller within the meaning of Article 4(7) GDPR for the processing of personal data carried out by the Contractor on its behalf. Pursuant to Clause 5.5, the Contractor shall have the right to inform the Client if, in its opinion, any processing of personal data is unlawful or if an instruction issued by the Client is unlawful.

4.2 As controller, the Client shall be responsible for safeguarding the rights of data subjects. The Contractor shall inform the Client without undue delay if data subjects assert their rights against the Contractor.

4.3 The Client shall have the right to issue additional instructions to the Contractor at any time regarding the nature, scope and procedures of the processing of personal data. Instructions shall be issued in text form (e.g. by e-mail) or by using the configuration options of MAIA. Where the Client selects models, integrations or functions in MAIA or makes other settings, this constitutes a documented instruction within the meaning of Article 28(3)(a) GDPR.

4.4 Any provisions regarding compensation for additional expenses incurred by the Contractor as a result of supplementary instructions issued by the Client shall remain unaffected.

4.5 The Client may designate persons authorized to issue instructions. If such authorized persons are appointed or replaced, the Client shall notify the Contractor thereof in text form.

4.6 The Client shall inform the Contractor without undue delay if it becomes aware of any errors or irregularities in connection with the processing of personal data by the Contractor.

4.7 In the event that the Client is subject to an obligation to notify or inform third parties pursuant to Articles 33 and 34 GDPR or under any other statutory reporting obligation applicable to the Client, the Client shall be responsible for compliance with such obligations.

5. General Obligations of the Contractor

5.1 The Contractor shall process personal data exclusively within the scope of the agreements concluded and/or in compliance with any supplementary instructions issued by the Client. This shall not apply where Union or Member State law to which the Contractor is subject requires other processing. In such a case, the Contractor shall inform the Client of such legal requirements prior to processing, unless the relevant law prohibits such notification on important grounds of public interest. Otherwise, the purpose, nature and scope of the processing of personal data shall be governed exclusively by this Agreement and/or the Client’s instructions. Any processing deviating therefrom shall be prohibited unless the Client has expressly consented thereto in text form.

5.2 The Contractor undertakes to carry out processing of personal data on behalf of the Client only in Member States of the European Union (EU) or the European Economic Area (EEA), or in Switzerland. Any processing outside the EU, the EEA or Switzerland shall only be permitted with the prior consent of the

Client and subject to compliance with the requirements set out in Articles 44 et seq. GDPR. For personal data subject to the FADP, disclosure to a state outside Switzerland, the EU and the EEA shall only be permitted where the Swiss Federal Council has determined that the state provides adequate protection (Article 16(1) FADP), where appropriate safeguards pursuant to Article 16(2) FADP are in place, in particular standard contractual clauses with the adaptations recognised by the FDPIC, or where an exception under Article 17 FADP applies.

5.3 Within the scope of the agreed processing of personal data, the Contractor shall ensure the proper performance of all contractually agreed measures.

5.4 The Contractor shall structure its organization and operational processes in such a manner that the personal data processed on behalf of the Client are secured to the extent necessary and protected against unauthorized access by third parties. The Contractor shall coordinate in advance with the Client any changes to the organization of the commissioned processing that are significant for the security of the data.

5.5 The Contractor shall inform the Client without undue delay if, in its opinion, an instruction issued by the Client violates applicable statutory provisions.

5.6 The Contractor shall process the personal data processed on behalf of the Client separately from other data. Physical separation shall not be mandatory.

5.7 The Contractor hereby designates the following persons as authorized to receive instructions from the Client:

- Management of Prodlane GmbH, compliance@getmaia.ai

5.8 In the event of any change to the persons authorized to receive instructions, the Contractor shall notify the Client thereof in text form.

6. Data Protection Coordinator of the Contractor

6.1 The external Data Protection Officer of Prodlane GmbH is: heyData GmbH, Schützenstraße 5, 10117 Berlin, Germany, www.heydata.eu, datenschutz@heydata.eu

6.2 The internal Data Protection Coordinator of Prodlane GmbH is its management, compliance@getmaia.ai

6.3 The Contractor shall notify the Client in writing of any change to the Data Protection Coordinator or the appointment of a Data Protection Officer.

7. Reporting Obligations of the Contractor

7.1 The Contractor shall notify the Client without undue delay of any breach of applicable data protection laws, of the contractual agreements concluded, and/or of any instructions issued by the Client, occurring in the course of the processing of personal data by the Contractor or by any persons engaged by the Contractor in such processing. The same shall apply to any personal data breach affecting personal data processed by the Contractor on behalf of the Client.

7.2 The Contractor shall further inform the Client without undue delay if a supervisory authority, pursuant to Article 58 GDPR, takes action against the Contractor and such action may also relate to or affect the processing activities carried out by the Contractor on behalf of the Client.

7.3 The Contractor acknowledges that the Client may be subject to notification obligations pursuant to Articles 33 and 34 GDPR, including the obligation to notify the competent supervisory authority within 72

hours of becoming aware of a personal data breach. The Contractor shall support the Client in fulfilling such notification obligations insofar as personal data processed by the Contractor on behalf of the Client are concerned. In particular, the Contractor shall notify the Client of any unauthorized access to personal data processed on behalf of the Client without undue delay and, in any event, no later than 48 hours after becoming aware of such access. The notification by the Contractor shall include, in particular: a description of the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned; a description of the measures taken or proposed to be taken by the Contractor to address the personal data breach and, where appropriate, measures to mitigate its possible adverse effects.

8. Cooperation Obligations of the Contractor

8.1 The Contractor shall assist the Client in fulfilling its obligation to respond to requests for the exercise of data subject rights pursuant to Articles 12 to 23 GDPR. Clause 12 of this Agreement shall apply.

8.2 The Contractor shall assist the Client in the preparation of the records of processing activities insofar as they relate to personal data processed by the Contractor on behalf of the Client. The Contractor shall provide the Client with the information required for this purpose in an appropriate manner.

8.3 The Contractor shall support the Client, taking into account the nature of the processing and the information available to the Contractor, in complying with the obligations set out in Articles 32 to 36 GDPR.

9. Audit and Inspection Rights

9.1 The Client shall have the right, in coordination with the Contractor, to verify at any time, to the extent necessary and reasonable, compliance with applicable data protection laws, the contractual provisions agreed between the Parties, and the Client’s instructions by the Contractor.

9.2 The Contractor shall provide the Client with all information necessary to carry out the audit within the meaning of paragraph 9.1.

9.3 The Client may request access to the personal data processed by the Contractor on behalf of the Client, as well as to the data processing systems and programs used for such processing.

9.4 Following prior notice with reasonable advance notice, the Client may conduct an audit within the meaning of paragraph 9.1 at the Contractor’s business premises during normal business hours. The Client shall ensure that such audits are conducted only to the extent necessary and in a manner that does not disproportionately disrupt the Contractor’s business operations.

9.5 In the event of measures taken by a supervisory authority pursuant to Article 58 GDPR against the Client, the Contractor shall provide the Client with the necessary information, in particular with regard to information and audit obligations, and shall enable the competent supervisory authority to conduct on-site inspections. The Contractor shall inform the Client of any such planned measures without undue delay.

10. Subcontracting Relationships

10.1 The Contractor shall list all subprocessing relationships already existing at the time of conclusion of this Agreement in Appendix 1 (Subprocessors).

10.2 The Contractor shall carefully select the subprocessor and, prior to engaging it, verify that the subprocessor is capable of complying with the agreements concluded between the Client and the Contractor.

10.3 The Contractor shall obtain confirmation from the subprocessor that it has appointed a Data Protection Officer pursuant to Article 37 GDPR. If no Data Protection Officer has been appointed, the Contractor shall inform the Client accordingly and provide evidence demonstrating that the subprocessor is not legally required to appoint a Data Protection Officer.

10.4 The Contractor shall ensure that the provisions agreed in this Agreement and any supplementary instructions issued by the Client also apply vis-à-vis the subprocessor.

10.5 The Contractor shall conclude a data processing agreement with the subprocessor that complies with the requirements of Article 28 GDPR. Furthermore, the Contractor shall impose on the subprocessor the same data protection obligations as those agreed between the Client and the Contractor. A copy of the data processing agreement shall be provided to the Client upon request.

10.6 The Contractor shall ensure by contractual arrangements that the audit rights set out in Clause 9 of this Agreement and the powers of supervisory authorities also apply to the subprocessor. It shall further be contractually stipulated that the subprocessor is obliged to allow such audits and any on-site inspections.

10.7 Services used by the Contractor from third parties purely as ancillary services in order to conduct its business activities shall not be considered subprocessing within the meaning of paragraphs 10.1 to 10.6. This includes, for example, cleaning services, telecommunications services without a specific connection to the services provided by the Contractor to the Client, postal and courier services, transport services and security services. Nevertheless, the Contractor shall ensure that appropriate safeguards and technical and organizational measures are implemented to protect personal data even where ancillary services are provided by third parties. The maintenance and servicing of IT systems or applications shall constitute a subprocessing relationship requiring prior authorization pursuant to Article 28 GDPR where such maintenance concerns IT systems used in connection with the provision of services to the Client and where access to personal data processed on behalf of the Client cannot be excluded.

10.8 The Contractor shall be entitled to engage additional subprocessors or replace existing subprocessors (“general authorization” within the meaning of Article 28(2) GDPR). The Contractor shall inform the Client at least 14 calendar days prior to the intended engagement or replacement by e-mail and by updating the list in Appendix 1 (Subprocessors). The Client may object within 14 calendar days of receipt of the notification on reasonable data protection grounds. Purely economic or technical reasons shall not constitute valid grounds for objection.

10.9 Upon receipt of an objection, the Contractor shall examine reasonable alternatives, such as alternative processing solutions, deactivation of affected functionalities, engagement of a different subprocessor or use of another region, insofar as technically and economically feasible. If no reasonable alternative is available, the Client’s sole remedy shall be to terminate the affected service with effect as of the date of change without penalty. Any prepaid fees for the affected service shall be refunded on a pro rata basis.

10.10 Where the immediate replacement of a subprocessor is mandatory, for example to maintain security or availability, the Contractor may carry out the replacement without prior notice and shall inform the Client without undue delay. The rights set out in paragraphs 10.8 and 10.9 shall apply accordingly.

11. Confidentiality Obligation

11.1 When processing personal data for the respective other Party, each Party shall be obliged to maintain the confidentiality of all data received or becoming known to it in connection with this Agreement. The Parties undertake to observe the same confidentiality obligations as are binding upon the disclosing Party. Each Party shall inform the other Party of any specific confidentiality requirements applicable to it.

11.2 The Parties represent and warrant that they are aware of the applicable statutory data protection provisions and are familiar with their application. The Parties further represent and warrant that they have made their employees aware of the data protection provisions applicable to them and have bound them to confidentiality. The Parties further warrant that, in particular, the employees involved in the performance of the services have been bound to confidentiality and have been informed of the instructions of the respective other Party.

11.3 Upon request, the Contractor shall provide the Client with evidence of the confidentiality obligations of its employees pursuant to paragraph 2.

12. Safeguarding Data Subject Rights

12.1 Notwithstanding the commissioning of the processing activities, the Client shall remain responsible for safeguarding data subject rights. The Contractor shall nevertheless support the Client in fulfilling its obligation to respond to requests from data subjects pursuant to Articles 12 to 23 GDPR. In particular, the Contractor shall ensure that any information required for this purpose is provided to the Client without undue delay so that the Client can comply with its obligations under Article 12(3) GDPR.

12.2 Where the cooperation of the Contractor is necessary for the Client to safeguard data subject rights, in particular rights of access, rectification, restriction of processing or erasure, the Contractor shall take the necessary measures in accordance with the Client's instructions. The Contractor shall, where possible, support the Client with appropriate technical and organizational measures in fulfilling its obligation to respond to requests for the exercise of data subject rights.

13. Technical and Organisational Measures

13.1 The Contractor shall implement and maintain the technical and organisational measures required to comply with the applicable data protection laws. This shall include, in particular, compliance with the requirements set out in Article 32 GDPR.

13.2 The technical and organisational measures in place at the time of conclusion of this Agreement are set out in Appendix 2 (Technical and Organizational Measures). The Parties agree that modifications to such measures may become necessary in order to adapt to technical or legal developments. The Contractor shall coordinate in advance with the Client any substantial changes that may adversely affect the integrity, confidentiality or availability of personal data. Measures that involve only minor technical or organisational modifications and do not adversely affect the integrity, confidentiality or availability of personal data may be implemented by the Contractor without prior coordination with the Client. The Client may request an updated version of the technical and organisational measures at any time.

13.3 The Contractor shall regularly, and where appropriate on an ad hoc basis, review and assess the effectiveness of the technical and organisational measures implemented. Where any need for optimisation or modification is identified, the Contractor shall inform the Client accordingly.

14. Term and Termination

14.1 This Agreement shall enter into force upon conclusion and shall be concluded for an indefinite term.

14.2 Ordinary termination of this Agreement is excluded for as long as the Contractor processes personal data on behalf of the Client within the Usage Agreement or a trial. This Agreement shall terminate automatically once the Usage Agreement and any trial have ended. Its obligations shall continue to apply until the data has been returned or deleted in accordance with Clause 15.

14.3 The Parties may terminate this Agreement at any time for good cause without notice in the event of a serious breach of applicable data protection laws, of obligations under this Agreement, or of comparable contractual obligations. In particular, the Client may terminate this Agreement for good cause if the Contractor is unable or unwilling to comply with an instruction issued by the Client, or if the Contractor unlawfully refuses access for the Client or for the competent supervisory authority. Termination for good cause shall be excluded where the grounds for termination are attributable to the Client. In such case, the Contractor shall instead be entitled to terminate this Agreement in accordance with this paragraph.

15. Consequences of Termination

15.1 Upon termination of this Agreement, the Contractor shall, at the Client's discretion, return to the Client or delete all documents, data, and any processing or usage results that have come into its possession in connection with the contractual relationship. Such return or deletion shall take place within 30 days of termination of this Agreement, unless the Client instructs a longer retention or a longer retrieval period is provided for by law, for example when switching provider under Chapter VI of Regulation (EU) 2023/2854 (Data Act). The deletion shall be documented in an appropriate manner. Any statutory retention obligations or other legal obligations to store the data shall remain unaffected. With regard to data carriers, where deletion is requested by the Client, such data carriers shall be destroyed in a manner ensuring that the data are rendered permanently irrecoverable. The destruction shall be documented. Copies in backup systems shall be deleted in the course of the regular rotation no later than 100 days after deletion from the production system. Until then, they shall be retained solely for recovery purposes.

15.2 The Client shall have the right to verify the complete and contractually compliant return and deletion of the data by the Contractor. Such verification may also include an inspection of the data processing systems at the Contractor's business premises. Any on-site inspection shall be announced by the Client with reasonable prior notice.

16. Place of Jurisdiction

This Agreement shall be governed by the laws of the Federal Republic of Germany, including the GDPR. The exclusive place of jurisdiction for all disputes arising out of or in connection with this Agreement shall be Leipzig, Germany. Mandatory provisions of the FADP remain unaffected.

17. Final Provisions

17.1 Should the Client's property at the Contractor be endangered by measures taken by third parties, such as attachment or seizure, by insolvency proceedings, or by any other events, the Contractor shall inform the Client without undue delay. The Contractor shall promptly inform the relevant creditors that the data concerned are personal data processed on behalf of the Client.

17.2 No oral side agreements have been entered into between the Parties prior to the conclusion of this Agreement.

17.3 Should any provision of this Agreement be or become invalid, this shall not affect the validity of the remaining provisions of this Agreement.

17.4 Only the German version of this Agreement is legally binding. This English translation is provided for information purposes only. The German version is available here.

Appendix 1: Subprocessors

Overview of the subprocessors. The detailed entries below prevail.

SUBPROCESSOR	SERVICES	PROCESSING LOCATION	TRANSFER MECHANISM
Hetzner Online GmbH	Cloud infrastructure and hosting of the platform, including GPU inference	EU	Not required (processing in the EU)
Microsoft Azure	Cloud infrastructure and AI services, including LLMs	EU	Not required (processing in the EU)
Amazon AWS	Cloud infrastructure and AI services, including LLMs	EU	Not required (processing in the EU)
Google Cloud	Cloud infrastructure and AI services, including LLMs	EU	Not required (processing in the EU)
AKI.IO GmbH	Provision of LLMs for use in the platform	Germany	Not required (processing in the EU)
PostHog	Product analytics based on pseudonymized usage and event data	EU	EU-US Data Privacy Framework; EU standard contractual clauses (module 2)

Hetzner Online GmbH

- **Provider:** Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Germany
- **Data protection contact:** data-protection@hetzner.com

The Processor obtains extensive infrastructure from Hetzner, consisting of multiple servers, networks, and load balancing. Within this environment, the main servers are active, which are responsible for both providing the MAIA web application and secure data storage.

The main infrastructure is located in the EU. Backups and snapshots are replicated to a second data center in the EU.

- **Processing location:** EU
- **Transfer mechanism:** Not required (processing in the EU)
- **GDPR compliance agreements:**
  - DPA: Hetzner Data Processing Agreement

Microsoft Azure

- **Provider:** Microsoft Ireland Operations Ltd, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland
- **Data protection contact (Europe):** Microsoft Ireland Operations Limited, Attn: Data Protection Officer, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland; telephone: +353 1 706 3117; contact form

Microsoft Azure provides the Processor with GPT in a data protection compliant environment. The GPT models are used as deployments of type DataZone EU, so that prompts and outputs are processed only in the EU. The processed data is not used for training AI models.

Additionally, Microsoft provides the Processor with dedicated servers specifically designed for running AI models. These servers are operated in the EU, and serve exclusively for document preprocessing.

- **Processing location:** EU (Azure OpenAI deployments of type DataZone EU)
- **Transfer mechanism:** Not required (processing in the EU)
- **GDPR compliance agreements:**
  - SCC: Microsoft: EU Standard Contractual Clauses
  - DPA: Microsoft Products and Services Data Protection Addendum (DPA)

Amazon AWS

- **Provider:** Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855 Luxembourg
- **Data protection contact (Europe):** Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855 Luxembourg; data protection officer: aws-EU-privacy@amazon.com

Amazon AWS provides the Processor with Large Language Models in a data protection compliant environment. The associated infrastructures are operated exclusively in Europe.

The processed data is not used for training AI models.

- **Processing location:** EU (Amazon Bedrock EU cross-region inference)
- **Transfer mechanism:** Not required (processing in the EU)
- **GDPR compliance agreements:**
  - DPA: AWS Data Processing Addendum (DPA)

Google Cloud

- **Provider:** Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Dublin, Ireland
- **Data protection contact:** Cloud Data Protection Team, contact form

Google Cloud provides the Processor with Large Language Models in a data protection compliant environment. The associated infrastructures are operated exclusively in Europe.

The processed data is not used for training AI models.

- **Processing location:** EU
- **Transfer mechanism:** Not required (processing in the EU)
- **GDPR compliance agreements:**
  - DPA: Google Cloud Data Processing Addendum

AKI.IO GmbH

- **Provider:** AKI.IO GmbH, Marienburger Str. 1, 10405 Berlin, Germany
- **Data protection contact:** privacy@aki.io

AKI.IO provides the Processor with Large Language Models in a data protection compliant environment. The associated infrastructures are operated exclusively in Europe.

The processed data is not used for training of AI models.

- **Processing location:** Germany, own GPU servers in co-location data centres
- **Transfer mechanism:** Not required (processing in the EU)

PostHog

- **Provider:** PostHog Inc., 2261 Market Street #4008, San Francisco, CA 94114, USA
- **Data protection contact:** privacy@posthog.com

The Processor uses PostHog for the technical analysis of the operation, errors and performance of its web applications. PostHog enables data protection compliant tracking and real-time analysis. PostHog receives no prompts, model outputs or document contents. Events are pseudonymized: they are linked to an internal user ID, not to names or e-mail addresses.

The collected data is used exclusively for the technical analysis of the operation, errors and performance of the MAIA platform.

To comply with GDPR requirements, the Processor exclusively uses PostHog Cloud EU, which is operated in the EU.

- **Processing location:** EU
- **Transfer mechanism:** PostHog Inc. is established in the USA: EU-US Data Privacy Framework (PostHog is self-certified); in addition, EU standard contractual clauses (module 2) under the data processing agreement with PostHog of 6 January 2025
- **GDPR compliance:**
  - PostHog Cloud EU
  - PostHog: GDPR compliance

Appendix 2: Technical and Organizational Measures (TOMs)

1. Confidentiality

1.1 Physical Access Control

Technical Measures

- Mechanical locking system for the office premises
- Keys issued to authorized personnel only

Organizational Measures

- Key register with documented issue and return of keys
- Visitor register
- Policy on handling visitors
- Visitors must be accompanied by an employee at all times
- Regular training and awareness programs
- Policies for secure working in office and remote work environments
- Regular review of physical access rights

We rely on cloud providers for operating our IT infrastructure and providing systems for the processing of personal data. We do not operate any on-premises server infrastructure in the office.

1.2 System Access Control

Technical Measures

- Use of individual user accounts
- Login with username and password
- Centrally managed endpoints with anti-virus protection, disk encryption and password requirements
- Firewalls at client, server, and cloud level
- Encryption of storage media

- Automatic desktop lock
- Encryption of client devices
- Mandatory use of company-managed VPN for mobile work
- MFA (2FA) policies
- Mandatory use of centrally managed password manager
- Principle of least privilege
- Revocation or withdrawal of access upon departure or role change
- Protection of credentials through defined password requirements
- Access to sensitive systems only via approved and secured connections
- Company-managed laptops and workstations, including security requirements
- Access to company data only from approved or compliant devices

Organizational Measures

- Password policies
- Deletion / destruction policies
- Clean desk policy
- Clean office policy
- Desktop and mobile lock policy
- Training and awareness programs
- Onboarding procedures for provisioning new access
- Offboarding procedures for revoking access that is no longer required
- Regular review of permissions and access rights

1.3 Data Access Control

Technical Measures

- Paper shredder (P4, cross-cut)
- IAM systems
- Encryption of data in transit and at rest
- Principle of least privilege
- Administrative access to production systems is permitted exclusively via a secured VPN connection
- Non-console access to production infrastructure only with an individual SSH key or access key
- Role-based assignment of permissions
- Restriction of privileged access to specifically authorized personnel
- Traceability of administrative access through individual accounts
- Access restrictions for particularly sensitive data and systems
- Secured management of shared accounts via the password manager, where such exceptions are necessary

Organizational Measures

- Minimal number of administrators
- Management of user rights by administrators
- Regular access reviews for sensitive and critical systems
- Documented approval for elevated permissions
- Access rights granted on a need-to-know and least-privilege basis

- Documented modification of access rights upon role change

1.4 Separation Control

Technical Measures

- Separation of production, development, and test systems
- Separation of data by purpose and authorization
- Logical separation of environments and roles
- Restriction of the use of production data in test and development environments
- Protection of shared storage areas through permissions and roles

Organizational Measures

- Definition of database access rights
- Policies on the use of test data
- Release of only required data for defined purposes
- Defined responsibilities for data releases and environment separation

1.5 Pseudonymization

Technical Measures

- Pseudonymization in external systems, where the purpose of the processing permits
- Pseudonymization in logs
- Separation of mapping data in separately secured systems

Organizational Measures

- Policy requiring that data be pseudonymized during manual transfers so that identification is not possible

2. Integrity

2.1 Transfer Control

Technical Measures

- Use of approved and secured communication systems
- Encrypted transmission of confidential information over public networks
- Additional protective measures for external transmission of sensitive data
- Restriction of insecure transmission channels

Organizational Measures

- Transfer in anonymized or pseudonymized form, where the purpose of the transfer permits
- Transfer only to authorized recipients
- Guidelines for the secure external transmission of files and information
- No transmission of credentials or sensitive information over unprotected channels
- Assessment of necessity prior to external transfer

2.2 Input Control

Technical Measures

- Technical logging of data entry, modification, and deletion
- Manual review of logs
- Central collection or evaluation of logs where provided
- Alerting for critical security-relevant events where provided
- Logging of administrative activities on critical systems
- Monitoring of network traffic to the production environment with security tools

Organizational Measures

- Traceability of data entry, modification, and deletion through individual usernames
- Assignment of rights for data entry, modification, and deletion based on an authorization concept
- Clear responsibilities for deletions
- Regular review of relevant logs
- Documented responsibilities for monitoring and incident handling
- Documented approval and review of high-risk changes to production systems
- Secure development policy
- Change management procedure: changes to systems, network, security settings and infrastructure are documented, tested and approved
- Configuration and asset management for new and sensitive systems

3. Availability and Resilience

3.1 Availability Control

Technical Measures

- Fire and smoke detection systems
- Regular, automated backups and snapshots
- Secure storage of backups and backup data
- Backup procedures for production data, configurations, and relevant documentation
- Monitoring of critical systems and services
- Automated monitoring of uptime and availability
- High-availability configuration of systems, where appropriate
- Protective measures against malware and security-relevant disruptions
- Measures for timely restoration of availability in the event of incidents
- Remote lock and remote wipe for lost or stolen mobile devices

Organizational Measures

- Backup & recovery concept
- Monitoring of the backup process
- Backups are stored separately from server locations
- Separate partitions for operating systems and data
- Restoration of backups to a non-production environment at least annually to verify their integrity
- Procedures for handling system outages and security incidents
- Business continuity and disaster recovery procedures
- Regular testing of the business continuity and disaster recovery plan, for example through tabletop exercises, with updates to the plan where needed
- Definition of responsibilities for restart and recovery

- Documentation and tracking of disruptions and recovery measures

4. Data Protection Measures

4.1 General Data Protection Measures

Technical Measures

- Central documentation of all data protection procedures and policies, accessible to employees as needed / by authorization (Confluence)
- Review of the effectiveness of technical protective measures is conducted at least annually
- Documented classification, retention, and deletion of data
- Documented rules for secure disposal and data destruction
- Network and application penetration test of the production environment by an external provider at least annually; critical and high-risk findings are tracked until resolved

Organizational Measures

- Internal Data Protection Coordinator (management); external Data Protection Officer: heyData GmbH (Clause 6.1)
- Employees trained and committed to confidentiality / data secrecy
- Monthly training and awareness programs:
  - Awareness activities
  - Discussion of new or amended policies
  - Information on potential threats
  - General knowledge transfer regarding data protection and data security
  - Discussion on how to further improve our processes
- The organization fulfills its information obligations under Art. 13 and Art. 14 GDPR
- A formalized process for handling data subject access requests is in place
- Regular review of the adequacy of key protective measures
- Information security policy and internal control policy; management reviews all security policies at least annually
- Formal risk assessment at least annually, with a risk register and risk treatment measures
- Organizational chart with clear responsibilities and lines of communication
- Disciplinary consequences for violations of security policies

4.2 Incident Response Management

Technical Measures

- Deployment of firewalls with regular updates
- Deployment of spam filters with regular updates
- Deployment of virus scanners with regular updates
- Support for incident handling through logging and traceability
- Unified communication channel toward customers
- Measures for containment, investigation, and recovery following security incidents
- Technical protective measures for handling lost or compromised devices

Organizational Measures

- Process for detecting and reporting security incidents / data breaches (including with regard to notification obligations toward the supervisory authority)
- Procedures for handling security incidents
- Documented roles and responsibilities in the incident response process
- Documented escalation and communication paths
- Post-incident review of security events and derivation of improvement measures
- Documented handling of device losses, unauthorized access, and data protection violations
- Transparent external communication via a status page where customers can track current system outages, affected services, remediation progress, and incident resolution
- Regular testing of the incident response plan, for example through tabletop exercises, with updates to the plan where needed

4.3 Privacy by Default

Technical Measures

- No more personal data is collected than is necessary for the respective purpose
- Easy exercise of the data subject's right of withdrawal through technical measures
- Privacy by Design
- Technical limitation of data access by role and purpose
- Privacy-friendly default configurations for systems and processes
- Restriction of storage locations and transmission channels for personal data
- Requirements for the use of managed storage locations and applications

4.4 Processor Control (Outsourcing to Third Parties)

Organizational Measures

- Prior review and documentation of security measures implemented by the processor
- Selection of the processor with due diligence (particularly regarding data protection and data security)
- Conclusion of the necessary data processing agreement or EU Standard Contractual Clauses
- Ongoing review of the processor and their level of protection during longer-term collaborations
- Risk-based classification of service providers prior to engagement
- Obtaining and reviewing appropriate evidence of data protection and information security, for example SOC 2 or ISO 27001 reports, at least annually
- Documented monitoring of critical or particularly high-risk service providers
- Policies for termination of collaboration and return or deletion of data
- Designation of internal contacts for service provider management

Appendix 3: Types of Personal Data

Data Subjects:

1. MAIA users
2. Individuals referenced in documents and data sources of MAIA users

User Data:

- First name

- Last name
- Email address
- Preferred software language

Document Contents:

- Text content
- Image content
- Document titles
- Document metadata (creation date, author, etc.)

Search Queries and Chat Messages:

- Text of search queries
- Content of chat messages

Authentication and User Management:

- Login timestamps
- Logout timestamps
- Token refresh timestamps
- Token revocation timestamps
- User email confirmation
- Password reset actions
- User registration data

Analytics and Audit Data (non-anonymized):

- IP addresses during authentication processes

Analytics and Audit Data (pseudonymized):

- Browser type and version
- Device type
- Operating system and version
- Initial and current referring URLs
- Event logs of software usage