Mimirio FlexCo
Schönbrunner Strasse 63/30,
1050 Vienna, Austria
ATU81466904

Data Processing Agreement

Version 3.0 · Effective 1 September 2026 · Article 28 GDPR · Annex to the Mimirio Software and Services Terms version 3.0

1. Parties, subject matter and roles

1.1 This data processing agreement ("Agreement") is concluded between the customer identified below as controller ("Client") and Mimirio FlexCo, Schönbrunner Strasse 63/30, 1050 Vienna, Austria, company register FN 640289, as processor ("Mimirio").

Controller (Client)	
Address	
Company register number	
Data protection contact	
Address for breach notifications	

1.2 Mimirio's data protection contact: security@mimirio.com. Notices and requests under this Agreement may be sent to that address; support requests go to the support channel agreed in the Order Form.

1.3 The subject matter of the processing is the provision of the services agreed in the Order Form and the Mimirio Software and Services Terms: provision and operation of the Mimirio platform including the AI model service, connection of the source systems selected by the Client, support and error analysis. The nature, purpose and scope of the processing, the categories of data subjects and of personal data, and the retention periods are set out in Annex A.

1.4 The Client is the controller within the meaning of Article 4(7) GDPR and Mimirio is the processor within the meaning of Article 4(8) GDPR. Operating the infrastructure or holding administrative access does not make Mimirio a controller.

1.5 This Agreement applies irrespective of the deployment model: to the cloud service operated by Mimirio and equally to an installation operated by the Client itself or by a third party engaged by the Client. In a self-operated installation too, Mimirio is given access to the installation — for provisioning, updates, maintenance, support and error analysis — and thereby to the personal data processed in it; that access is processing on the Client's behalf and is covered by this Agreement. Which deployment model is agreed, and which components are operated by whom, is stated in the Order Form (Appendix A or Appendix B to the Terms).

1.6 On the subject of the processing of personal data this Agreement prevails over the Order Form and the Terms. In all other respects the Order Form and the Terms apply unchanged. Terms used in this Agreement have the meaning given to them in the GDPR.

2. Duration

2.1 This Agreement enters into force on signature by both parties and in any event before the processing of personal data begins, and runs for the duration of the contractual relationship.

2.2 It also covers processing of personal data that Mimirio carried out on the Client's behalf before this Agreement was concluded.

2.3 Obligations that extend beyond the end of the contractual relationship — in particular confidentiality, deletion and the evidence obligations under section 13 — remain in force until they have been fulfilled.

3. Instructions

3.1 Mimirio processes personal data only on the Client's documented instructions. This Agreement, the Order Form, the Terms and the platform configuration made by the Client constitute the initial instructions.

3.2 Individual instructions are given by the Client in writing or by email through the contacts named in section 1. Mimirio implements them within the agreed scope of services; any effort going beyond that scope is agreed separately.

3.3 Mimirio does not process the data for its own purposes. If Mimirio receives an order from an authority or a court to disclose the Client's data, Mimirio will — to the extent legally permitted — inform the Client without delay and refer the requesting body to the Client.

3.4 If Mimirio considers that an instruction infringes Union or Member State data protection law, Mimirio will inform the Client without delay and may suspend implementation of that instruction until the matter is resolved.

4. Confidentiality

4.1 Mimirio confirms with binding effect that every person involved in the processing has been bound to confidentiality before starting that activity, or is subject to an appropriate statutory duty of secrecy. The obligation continues after the activity ends and after the person leaves Mimirio.

4.2 Access to the Client's personal data is granted only to persons who need it to provide the agreed services, to the extent required, and is logged.

4.3 Personal data is disclosed to third parties only as provided in this Agreement, in particular to the sub-processors listed in Annex C, or where required by law.

5. Security of processing

5.1 Mimirio has implemented the technical and organisational measures required by Article 32 GDPR. They are described and documented in Annex B.

5.2 Mimirio may develop the measures further, in particular to keep pace with technical progress. The agreed level of protection must not be reduced as a result. Material changes are documented and communicated to the Client on request.

5.3 Responsibility for security measures follows operational responsibility: Mimirio is responsible for the components Mimirio operates and for its own access paths; the Client is responsible for identities, permissions, the connected source systems and any infrastructure the Client operates itself (Appendix B to the Terms).

6. Place of processing

6.1 Personal data is processed exclusively within the European Union or the European Economic Area. The specific region is stated in the Order Form.

6.2 Processing in a third country — including access for support or maintenance purposes — does not take place without prior agreement with the Client and without a basis under Articles 44 et seq. GDPR.

6.3 Mimirio's own access to the platform likewise takes place from within the EU or EEA and through the access method agreed in the Order Form.

7. AI-specific commitments

7.1 Mimirio expressly warrants that the Client's personal data is not used to train or fine-tune AI models. That commitment applies equally to the sub-processors listed in Annex C.

7.2 Mimirio processes inputs (prompts), conversations, content and the outputs generated from them exclusively to provide the agreed services. Model services are used in a configuration in which inputs and outputs are not used for training and are not stored beyond the period required to provide the service.

7.3 Mimirio does not take automated decisions about data subjects. Outputs of the Software are proposals; the Client is responsible for their use and for any decision taken. Article 22 GDPR is for the Client to observe as controller.

7.4 Mimirio processes usage and telemetry data to provide the service, to keep it secure, for capacity planning and for troubleshooting. Any use for Mimirio's own purposes, such as product improvement, takes place exclusively in anonymised form with no link to an identifiable person.

8. Assistance with data subject rights

8.1 Mimirio assists the Client, by appropriate technical and organisational measures, in fulfilling the rights of data subjects under Chapter III GDPR (information, access, rectification, erasure, restriction, data portability, objection and automated decision-making in individual cases) within the statutory time limits, and provides the Client with the information and functionality required for that purpose.

8.2 If a data subject addresses a request directly to Mimirio, Mimirio forwards it to the Client without delay, informs the data subject accordingly and does not answer the request itself.

8.3 Mimirio does not rectify, erase or restrict the processing of personal data on its own initiative, but only on the Client's documented instructions. Functions that the Client or its users perform in the Software themselves are unaffected.

9. Personal data breaches

9.1 Mimirio notifies the Client of a personal data breach without undue delay and in any event within 48 hours of becoming aware of it, to the notification address given in section 1. Where the assessment is not complete within that period, an initial notification within 48 hours with the information then available satisfies this section, and the remaining information is supplied without undue delay. Substantiated suspected breaches are also notified.

9.2 The notification contains, as available:

- a description of the nature of the breach and of the categories and approximate number of data subjects and records concerned,
- the name and contact details of the contact point at Mimirio,
- a description of the likely consequences,
- a description of the measures taken or proposed to address the breach and to mitigate its possible adverse effects.

9.3 If not all of this information is available within the deadline, the notification is made with the information available and the remaining details follow without delay. Missing detail does not extend the deadline.

9.4 Mimirio assists the Client in complying with Articles 32 to 36 GDPR, in particular with notifications to the supervisory authority, with communication to data subjects and with a data protection impact assessment, and documents incidents including the measures taken. Mimirio makes a notification on the Client's behalf only on the Client's instructions.

9.5 Mimirio also notifies the Client without delay of material disruptions to the services, of breaches of this Agreement and of inspections or measures by supervisory authorities to the extent they relate to the processing carried out for the Client.

10. Evidence and audits

10.1 Mimirio makes available to the Client the information necessary to demonstrate compliance with the obligations under Article 28 GDPR, in particular:

- the documentation of the technical and organisational measures (Annex B) in its current version,
- the record of processing activities under Article 30(2) GDPR, to the extent it relates to the processing carried out for the Client,
- current certificates and audit reports of the hosting and model providers used,
- responses to reasonable data protection and security questionnaires from the Client.

10.2 Where that evidence is not sufficient in an individual case, the Client is entitled to verify compliance with this Agreement itself or through appointed third parties bound to confidentiality who are not competitors of Mimirio. Such verification takes place to a reasonable extent, with reasonable advance notice — as a rule 14 days — during normal business hours, without avoidable disruption to Mimirio's operations, and as a rule once a year. Verification beyond that is permitted where there is specific cause, in particular after a personal data breach or on the order of a supervisory authority.

10.3 Mimirio provides the necessary information, demonstrates processes and grants the necessary insight. Other clients' data, source code and other trade and business secrets are excluded; for data centres, verification follows the options and evidence made available by the provider concerned.

10.4 Each party bears its own costs of a verification, except that the Client bears Mimirio's reasonable costs of support going beyond the evidence package under section 10.1, and the costs of any verification carried out more than once in a twelve-month period where there is no specific cause. Section 9.9 of the Terms applies to those costs.

11. Sub-processors

11.1 The Client consents to the engagement of the sub-processors listed in Annex C. Annex C names every possible sub-processor; which of them are actually engaged for the Client's deployment follows from Annex C read with the Order Form.

11.2 Mimirio informs the Client of its intention to add a further sub-processor or to replace an existing one at least 30 days in advance, stating the service, the establishment and the place of processing.

11.3 The Client may object to the change within 14 days of the notification on reasonable data protection grounds. In that case the parties will seek a mutually acceptable solution. If none is reached, the Client may terminate the affected service with effect from the date of the change without incurring any early-termination charge; services already provided up to that date remain payable.

11.4 Mimirio concludes an agreement under Article 28(4) GDPR with every sub-processor imposing the same obligations as those Mimirio has under this Agreement. If a sub-processor fails to fulfil its data protection obligations, Mimirio remains liable to the Client as for its own conduct.

11.5 Services that involve no access to the Client's personal data — such as telecommunications, postal services or cleaning — do not constitute processing on behalf of the Client. Where access cannot be ruled out, Mimirio binds the service provider to confidentiality and monitors compliance.

12. Obligations of the controller

12.1 The Client is responsible for the lawfulness of the processing, in particular for the existence of a legal basis, for meeting information obligations and for obtaining any consent required. The Client decides which source systems are connected, which content is processed and which permissions are granted.

12.2 Special categories of personal data under Article 9 GDPR and data under Article 10 GDPR are not covered by this Agreement unless expressly agreed together with any additional measures required. The Client informs Mimirio before connecting a source that contains such data.

12.3 The Client maintains its own record of processing activities and, where required, carries out a data protection impact assessment; Mimirio assists as set out in section 9.

12.4 The Client administers its user accounts and permissions and deactivates the accounts of users who have left without delay.

12.5 If a third party or an authority brings a claim against Mimirio caused by an instruction of the Client, by a missing legal basis or by a breach of the Client's obligations under this section 12, the Client indemnifies and holds Mimirio harmless. This does not apply to the extent that Mimirio is itself responsible for the infringement.

13. Deletion and return

13.1 On termination of the contractual relationship Mimirio returns the personal data or deletes it, at the Client's choice. Appendix C to the Terms (data export) applies to the return, with the formats and exclusions set out there.

13.2 The data remains available for retrieval for at least 30 calendar days after termination and is then deleted within a further 30 days, including copies in backup cycles once the cycle concerned has elapsed. A different period requires agreement in text form.

13.3 The retention periods for the individual categories of data during the term of the contract are set out in Annex A.

13.4 Copies retained as required by law remain stored under protection and are not used for any other purpose.

13.5 Mimirio confirms deletion in text form on request.

14. Liability

14.1 Section 10 of the Terms applies to this Agreement in full, including the limitation of liability and the exclusions set out there. Claims between the parties arising out of or in connection with this Agreement — including recourse and apportionment under Article 82(5) GDPR, administrative fines, and the cost of notification, remediation, forensic investigation, or credit monitoring — count towards and are limited by the caps in section 10 of the Terms and are subject to the exclusions there in the same way as any other claim. This does not affect liability towards data subjects under Article 82 GDPR, liability for personal injury, liability for intent, or any other liability that may not be limited by mandatory law.

14.2 Each party is responsible for the area of responsibility allocated to it (section 5.3). Engaging a sub-processor does not relieve Mimirio of responsibility for the service concerned.

15. Final provisions

15.1 Notices, instructions and amendments to this Agreement require text form; email between the designated contacts is sufficient unless mandatory law requires another form.

15.2 If changes in the law or requirements of a supervisory authority make an amendment to this Agreement necessary, the parties will agree the required amendments without delay and in good faith.

15.3 If individual provisions of this Agreement are or become invalid, the remaining provisions remain in force. Invalid provisions are to be replaced by mutual agreement with provisions that come as close as possible to the intended purpose.

15.4 Austrian substantive law applies, excluding its conflict-of-law rules. The competent courts in Vienna have exclusive jurisdiction over disputes arising from this Agreement. Mandatory provisions of the GDPR and the competence of the supervisory authorities remain unaffected.

15.5 This Agreement is available in an English and a German version. The version the parties sign governs. If both language versions are signed for the same engagement, the German version governs. The Terms are concluded in English and the English text governs.

15.6 Annexes A, B and C form part of this Agreement.

The controller (Client)	**Mimirio FlexCo**
Place, date	Place, date
Name, role	Name, role

Annex A — Details of the processing

A1. Purpose of the processing

A1.1 Mimirio processes personal data in order to provide the agreed services: provision and operation of the Mimirio platform, operation of the AI model service, connection and indexing of the sources selected by the Client, answering user requests and generating outputs, support and error analysis, and maintaining the security, stability and capacity of the service.

A1.2 Processing follows a strict need-to-know basis and privacy-friendly defaults: the extent of the data accessible, the duration and the depth of the intervention are limited to what is necessary for the purpose concerned.

A2. Categories of data subjects

A2.1 Employees and contractors of the Client who use or administer the Software, and the contact persons named by the Client.

A2.2 Persons whose personal data is contained in the content connected or uploaded by the Client — for example as author, editor, recipient or as a person named in a document. Which persons these are is determined by the Client through its choice of sources and content.

A3. Categories of personal data

Category	Description
Account data	Name, email address, account UUID, role and permissions. No passwords — authentication takes place through the Client's identity system.
Content and knowledge data	Content and metadata of the connected sources and uploaded files (content, author, last editor, creation and modification date, storage location, permission information). The scope is determined by the integrations the Client activates.
Inputs and outputs	Text inputs (prompts), conversations and the corresponding responses and outputs, including generated documents.
Usage and telemetry data	Consumption, tokens, quality and accuracy values, request metadata, timestamps and technical identifiers.
Log data	Access, security and error logs.
Support data	Requests, correspondence and the diagnostic information provided by the Client.

A3.1 Special categories of personal data under Article 9 GDPR are not the subject of the processing unless expressly agreed under section 12.2.

A4. Nature of the processing operations

- collection from the connected sources, storage and organisation,
- indexing and linking for retrieval within the user's permissions,
- querying, evaluating and generating outputs,
- logging, backup and restoration,
- analysis for troubleshooting and security purposes on a need-to-know basis,
- deletion and return in accordance with section 13.

A5. Retention

Category	Retention
Account data	For the term of the contract; deletion in accordance with section 13.
Content and knowledge data	For as long as the source concerned remains connected; once the source is disconnected the copies and index entries are removed.
Inputs, conversations and outputs	Until deleted by the user or the Client, otherwise for the term of the contract.
Usage and telemetry data	12 months, then deleted or anonymised.
Log data	90 days, unless a longer period is agreed in the Order Form or required by law.
Backups	As agreed in the Order Form; by default 30 days on a rolling basis.
Support data	24 months from closure of the request.

A6. Place of processing

A6.1 Exclusively EU or EEA. The specific region and hosting provider are stated in the Order Form; which sub-processors are used follows from Annex C. In an installation operated by the Client, the place of processing is the environment chosen by the Client; Mimirio's access takes place from within the EU or EEA.

Annex B — Technical and organisational measures

B1. Basis and allocation of responsibility

B1.1 The Mimirio platform is provided in two deployment models: as a cloud service operated by Mimirio, and as an installation operated by the Client itself or by a third party engaged by the Client (section 1.5). The measures therefore operate at several levels:

- Data centre, physical security and platform services: for the cloud service the infrastructure provider named in Annex C; for a self-operated installation the Client or the provider engaged by the Client.
- Application, defaults, development and release processes: Mimirio, in both deployment models.
- Mimirio's access paths for provisioning, maintenance and support: Mimirio, in both deployment models, through the access method agreed in the Order Form.
- Identities, permissions and the connected source systems: the Client (section 5.3).

B1.2 In an installation operated by the Client, the measures below apply to the application, its defaults, the development and release processes, and to Mimirio's access. Measures concerning the infrastructure — in particular physical security (B3.5) and backup, monitoring and recoverability (B5) — are to that extent the Client's responsibility; Mimirio assists within the agreed scope of services and provides the information needed for that purpose.

B1.3 For the cloud service the platform runs on infrastructure of the providers named in Annex C read with the Order Form. Which certifications and audit reports — such as ISO/IEC 27001, ISO/IEC 27017 or SOC 2 — are held depends on the infrastructure provider selected in the Order Form and follows from Annex C. Mimirio provides the current evidence on request. For an installation operated by the Client, that evidence depends on the Client's own environment. Mimirio aligns its own information security management with these standards but does not currently hold a certification of its own.

B2. Pseudonymisation and encryption

- Transmission exclusively encrypted (TLS 1.2 or higher), including between platform components and to the connected source systems.
- Encryption at rest for databases, object storage and backups using the mechanisms of the infrastructure provider concerned, as a rule AES-256, to the extent the service concerned supports it. For an installation operated by the Client, encryption at rest depends on the Client's own environment (B1.2).
- Credentials and keys reside in configuration files on the respective host. Access to them is restricted to the system and administration accounts required for operation; the encryption at rest under B2.2 and the access controls under B3 apply.
- Where the purpose allows, analyses are carried out on pseudonymised or aggregated data; identifying attributes are held separately.

B3. Confidentiality

B3.1 **System access control.** Authentication through the Client's identity system or Microsoft Entra ID, multi-factor authentication for all administrative access, named personal accounts with no shared credentials, password and lockout policies.

B3.2 **Data access control.** Role-based permissions on a least-privilege basis, standard permission profiles on a need-to-know basis, a defined process for granting and withdrawing rights, and periodic review of administrative accounts in particular.

B3.3 **Tenant separation.** Each client's data is held logically separated and isolated by installation identifier; queries respect the permissions the user concerned has in the source system.

B3.4 **Support access.** Access to client data for support and troubleshooting only where there is a specific reason, to the extent necessary, logged, and through the access method agreed in the Order Form.

B3.5 **Physical security.** The infrastructure provider's data centres have access control, monitoring and visitor escorting. At Mimirio's own premises: locked entry, escorting of visitors and a clear desk / clear screen rule; client data is not stored on end-user devices.

B3.6 **Personnel.** Confidentiality undertaking before starting work, data protection and security training, and defined processes for joining, changing role and leaving, including immediate withdrawal of access.

B4. Integrity

B4.1 **Input control.** Logging of sign-ins, administrative changes and access to client data, with timestamp and the account acting.

B4.2 **Change control.** Version control, mandatory code review, protected main branches, automated tests, infrastructure as code and separate approval steps for production changes.

B4.3 **Transfer control.** Data transfers take place exclusively over encrypted, authenticated connections; exports only through the intended functions and to authorised recipients.

B5. Availability and resilience

B5.1 **Backup. For the cloud service, regular encrypted backups at the frequency and retention agreed in the Order Form, stored separately from the production systems; restores are tested. Scope, frequency, retention and any recovery objectives follow exclusively from the Order Form. For an installation operated by the Client, backup and recovery are the Client's responsibility unless the Order Form provides otherwise.**

B5.2 **Monitoring.** Monitoring of availability, load and security events with alerting; defined escalation paths outside business hours for critical events.

B5.3 **Protection against attack and loss.** Network segmentation, firewalls and a web application firewall, the provider's DDoS protection, system hardening, and malware protection on workstations.

B5.4 **Recoverability.** Documented recovery procedures; any agreed recovery objectives are stated in the Order Form.

B6. Purpose limitation and separation

- The Client's personal data is not used to train or fine-tune AI models (section 7.1).
- Production, test and development environments are separate; the Client's production data is not used in test or development environments.
- Model services are configured so that inputs and outputs are not used for training and are not stored longer than required to provide the service.
- Different clients' data is processed separately; access across installation boundaries is precluded.

B7. Review, assessment and evaluation

B7.1 **Data protection management. Documented procedures, a record of processing activities under Article 30(2) GDPR, a designated data protection contact (security@mimirio.com) and regular training.**

B7.2 **Vulnerability management.** Continuous updating of dependencies and systems, automated vulnerability and dependency scanning, and remediation prioritised by severity. Penetration tests are carried out where there is specific cause and on material changes.

B7.3 **Incident response.** A defined process for detecting, assessing, containing, remedying and documenting security incidents, including the notification paths under section 9.

B7.4 **Defaults.** Privacy-friendly defaults; new functions requiring additional permissions are not activated without the Client's authorisation.

B7.5 **Supplier management.** Selection and review of sub-processors under section 11, formalised engagement management and prior assessment before appointment.

Annex C — Sub-processors

C1.1 The table below names every sub-processor Mimirio may engage for services under this Agreement. Not all of them are used in every deployment: which ones are actually engaged depends on the deployment model, hosting provider and model provider agreed in the Order Form. The "Used" column states the condition for each. For an installation operated by the Client, Mimirio engages no sub-processors for hosting, storage and model operation in so far as the Client provides those components itself.

Sub-processor	Service	Used	Place of processing	Certifications and audit reports
Microsoft Ireland Operations Ltd. (Microsoft Azure)	Hosting and storage of the platform; operation of the model services via Azure AI Foundry	Where agreed in the Order Form as hosting or model provider (the default for the cloud service)	EU (region per Order Form)	ISO/IEC 27001, ISO/IEC 27017; SOC 1/2/3 (Microsoft Service Trust Portal)
Amazon Web Services EMEA SARL (AWS)	Hosting and storage of the platform; operation of the model services via Amazon Bedrock	Only where agreed in the Order Form as hosting or model provider	EU (region per Order Form)	ISO/IEC 27001, ISO/IEC 27017; SOC 1/2/3 (AWS Artifact)
SNS – Saturn Networking Solutions GmbH	Hosting and storage of the platform in an Austrian data centre	Only where agreed in the Order Form as hosting provider	Austria	ISO/IEC 27001 certification in progress; further evidence on request
Schwarz Digits GmbH & Co. KG (STACKIT)	Hosting and storage of the platform	Only where agreed in the Order Form as hosting provider	Germany	ISO/IEC 27001 (on the basis of IT-Grundschutz), ISO/IEC 27017; BSI C5 Type 2; ISAE 3000 (SOC 2), ISAE 3402
Microsoft Ireland Operations Ltd. (Microsoft 365)	Support and ticket correspondence in Mimirio's own environment	In every deployment model, as soon as support correspondence contains personal data	EU	ISO/IEC 27001, ISO/IEC 27017; SOC 1/2/3 (Microsoft Service Trust Portal)

C1.2 An agreement under Article 28(4) GDPR is in place with every sub-processor engaged — with Microsoft and AWS on the basis of their respective Data Processing Addendum. Mimirio provides the evidence held by the providers engaged (B1.3) on request. Model services are used exclusively in a configuration that does not train on Client data (section 7).

C1.3 Changes to this list are governed by section 11. No other service providers with access to the Client's personal data are used.

C1.4 Services with no access to the Client's personal data do not constitute processing on the Client's behalf (section 11.5).