Data Processing Addendum (DPA)

1.2 · Customer-facing information

Scope

This Data Processing Addendum ("DPA") forms part of the agreement between Sefira and the customer for the provision of the Sefira service (the "Agreement").

This DPA applies where Sefira processes Customer Personal Data on behalf of Customer as processor.

Definitions

For purposes of this DPA:

• "Customer Personal Data" means personal data contained in Customer Content that Sefira processes on behalf of Customer as processor in connection with the Agreement.
• "Customer Content" means data, documents, messages, workflow inputs, configuration, prompts, outputs, attachments, and other content submitted to or generated within the service for Customer’s use.
• "Sefira Controller Data" means account, billing, support, security, operational, compliance, and service-administration data that Sefira processes as independent controller for its own legitimate service-operation purposes.
• "Subprocessor" means a third party engaged by Sefira to process Customer Personal Data on behalf of Customer in connection with the service.
• "Personal Data Breach" has the meaning given in applicable data protection law.

Roles of the parties

For Customer Personal Data, Customer acts as controller and Sefira acts as processor.

Sefira shall process Customer Personal Data only on documented instructions from Customer, unless otherwise required by applicable Union or Member State law. Where Sefira is required by law to process Customer Personal Data other than on Customer’s instructions, Sefira shall inform Customer of that legal requirement before processing, unless the law prohibits such notice on important grounds of public interest.

Sefira Controller Data is outside the processor scope of this DPA and is described in the privacy notice and related service terms.

Subject matter, duration, nature, and purpose of processing

The subject matter of the processing is the provision, operation, support, security, and improvement of the Sefira service under the Agreement.

The nature and purpose of the processing may include:

• account and workspace administration

• collaboration, planning, and process-execution functionality
• document upload, preview, extraction, and derivative workflow support
• AI-assisted drafting, analysis, and process-building where enabled by Customer
• notifications, integrations, support, security, and related service operation

The processing shall continue for the term of the Agreement and for any limited post-termination period required to return, delete, anonymize, retain, or evidence data in accordance with the Agreement, this DPA, and applicable law.

Categories of data subjects

Depending on Customer's use of the service, Customer Personal Data may relate to:

• Customer users, administrators, members, and invited collaborators
• employees, contractors, stakeholders, or contacts referenced in workspace content
• external participants referenced in tasks, documents, meetings, or workflows
• third parties whose information appears in uploaded, extracted, or workflow-derived records

Categories of personal data

Depending on Customer's use of the service, Customer Personal Data may include:

• identity and account data
• membership and collaboration data
• workspace content and comments
• uploaded documents and extracted document content
• AI prompts, messages, outputs, and run metadata
• integration metadata and connection state
• notification and communication records
• support, audit, security, and compliance records to the extent they contain Customer Personal Data

Documented instructions

Customer instructs Sefira to process Customer Personal Data as necessary to:

1. provide the service under the Agreement;
2. maintain the agreed service operation, security, and support posture;
3. perform Customer-enabled configurations, workflows, integrations, and AI-assisted features; and
4. comply with other documented lawful instructions agreed by the parties.

Customer is responsible for:

• ensuring it has an appropriate legal basis for Customer Personal Data submitted to the

service;
• determining which users, documents, integrations, workflows, and AI-assisted features are permitted in its environment;
• ensuring its instructions to Sefira are lawful; and
• notifying Sefira where Customer requires customer-specific retention, deletion, transfer, or localization restrictions beyond the platform default.

If Sefira considers that an instruction from Customer infringes applicable data protection law, Sefira shall inform Customer without undue delay.

Confidentiality

Sefira shall ensure that persons authorized to process Customer Personal Data:

• are subject to confidentiality obligations or statutory duties of confidentiality;
• are granted access only to the extent necessary for their role; and
• are instructed to process Customer Personal Data only in accordance with this DPA and Customer's documented instructions.

Security of processing

Sefira shall implement appropriate technical and organizational measures designed to protect Customer Personal Data in accordance with Article 32 GDPR, taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of processing, as well as the risks to natural persons.

Those measures shall include, as appropriate to the relevant service path:

• access-controlled administrative and compliance surfaces
• least-privilege access management
• authentication abuse protections such as request throttling, failed-attempt tracking, and temporary lockouts on sensitive access paths
• protected handling of tokens and integration secrets
• encryption in transit and other transport protections
• environment and operational controls for sensitive systems
• signed external callback and webhook verification patterns where relevant
• logging, auditability, and security event review
• backup and recovery controls
• vulnerability and change-management practices
• data-class-specific anonymization, deletion, and retained-history handling

The parties agree that the more detailed technical and organizational measures may be described in an annex, security schedule, or equivalent customer package materials, including the Security White Paper and customer-specific diligence responses where applicable.

Subprocessors

Customer grants Sefira a general authorization to engage Subprocessors in connection with the service.

Sefira shall:

• maintain a current Subprocessor List at `/subprocessors`;
• impose data protection obligations on each Subprocessor that are no less protective than those set out in this DPA, to the extent applicable to the services performed by that Subprocessor;
• remain responsible for the performance of its Subprocessors' data protection obligations to the extent required by applicable law; and
• provide notice of material new Subprocessors before their use, unless urgency, security, or legal constraints require a shorter period.

Customer may object to a new Subprocessor on reasonable data protection grounds. Where Customer raises a reasonable objection, the parties shall work in good faith to address the concern through a commercially reasonable alternative, a restriction of the affected feature path, or another reasonable solution. If no reasonable solution is available, either party may address the affected processing path under the Agreement.

International transfers

Where Customer Personal Data is transferred outside the EEA or another restricted-transfer jurisdiction, Sefira shall ensure that such transfer is subject to an applicable lawful transfer mechanism, including adequacy decisions, the EU Standard Contractual Clauses, or another valid mechanism under applicable data protection law.

Where relevant to the transfer path, Sefira shall apply supplementary safeguards appropriate to the circumstances and shall make transfer-path information available through the Subprocessor List or customer diligence materials where the processing path depends on enabled features or configured providers.

Assistance with data subject requests

Taking into account the nature of the processing and the information available to Sefira, Sefira shall provide reasonable assistance to Customer to enable Customer to respond to requests from data subjects exercising their rights under applicable data protection law.

Assistance with compliance obligations

Taking into account the nature of the processing and the information available to Sefira, Sefira shall provide reasonable assistance to Customer with:

• security of processing obligations;
• Personal Data Breach notification and remediation support;
• data protection impact assessments where required by Customer's use of the service; and
• consultations with supervisory authorities where such assistance is required in relation to processor-scope Customer Personal Data.

Personal Data Breaches

If Sefira becomes aware of a Personal Data Breach affecting Customer Personal Data, Sefira shall:

• assess, contain, investigate, document, and remediate the incident;
• notify Customer without undue delay after confirming that Customer Personal Data is affected; and
• provide available information reasonably necessary for Customer to understand the incident and meet its own notification obligations.

Unless otherwise agreed in writing, Sefira will aim to provide initial notice within 72 hours after confirming that Customer Personal Data is affected.

The notice may include, as available at the relevant time:

• the nature of the incident;
• the categories of Customer Personal Data concerned;
• the categories of affected data subjects;
• the likely consequences of the incident;
• the measures taken or proposed to address the incident; and
• a contact point for follow-up.

Return, deletion, anonymization, and retained history

Upon termination or expiry of the Agreement, Sefira shall, at Customer’s choice and subject to the Agreement and applicable law, delete or return Customer Personal Data, unless applicable law requires storage of some or all Customer Personal Data.

The parties acknowledge that the service includes retained-history, audit, and integrity-sensitive records. Accordingly:

• some data classes may be deleted directly;
• some records may be anonymized or de-identified instead of purged;
• some records may be retained for legal, accounting, fraud-prevention, security, or audit purposes; and
• backups may persist temporarily until overwritten in the ordinary course.

The parties may supplement this DPA with a more detailed retention and deletion schedule describing default retention by data class, deletion path, backup handling, and justified exceptions.

AI-assisted processing

Where Customer enables AI-assisted features, Sefira may process Customer Personal Data through AI-related service paths strictly as part of providing the enabled feature.

Sefira shall identify AI-related providers through the Subprocessor List and related customer-facing materials where those providers process Customer Personal Data on behalf of Customer.

Unless expressly agreed otherwise in writing, Sefira shall not use Customer Personal Data to train general-purpose AI models for its own independent purposes.

Customer remains responsible for deciding whether AI-assisted features are enabled for its environment and whether Customer Personal Data may be submitted into those feature paths.

Audits and information rights

Sefira shall make available to Customer information reasonably necessary to demonstrate compliance with this DPA.

For most customers, this may be satisfied in the first instance through:

• this DPA;
• the privacy notice;
• the Security White Paper;
• the Subprocessor List;
• AI and transfer-path disclosures; and
• responses to reasonable customer diligence requests under appropriate confidentiality controls.

Where required by applicable law or reasonably necessary to demonstrate compliance, Sefira shall allow for audits or inspections, subject to reasonable notice, confidentiality obligations, security restrictions, proportionality, and measures designed to avoid disruption to Sefira’s operations or exposure of other customers’ data.

Sefira may satisfy overlapping audit requests through shared audit artifacts, questionnaires, certifications, or summaries where appropriate. Customer shall bear its own audit costs except where otherwise required by applicable law or agreed in writing.

Annex structure

The DPA package may include, at minimum:

1. the main DPA body;
2. processing instructions;
3. categories of data subjects and personal data;
4. technical and organizational measures;
5. Subprocessors and transfer map;
6. retention and deletion schedule; and
7. any customer-specific annexes required by the Agreement or applicable law.