Privacy Notice

1.3 · Customer-facing information

Overview

This Privacy Notice explains how Sefira handles personal data when people use the service, collaborate inside workspaces, upload documents, use AI-assisted features, connect integrations, receive communications, or interact with support, billing, security, and compliance functions.

This notice is intended to describe Sefira’s data-handling posture transparently. It should be read together with the [Data Processing Addendum](/dpa), the [Subprocessor List](/subprocessors), and the [Security White Paper](/compliance/security-white-paper).

Who is responsible for personal data

Sefira acts as controller for personal data processed for:

• account administration;
• authentication and security;
• billing and commercial administration;
• support and service communications;
• product security, abuse prevention, and service reliability;
• legal compliance, auditability, and accountability records.

For Customer Workspace Content, Sefira normally acts as processor where it processes personal data on behalf of a customer under that customer’s instructions.

Some product flows may involve both roles. In those cases, the applicable role is described in the customer agreement, the DPA, product documentation, or the relevant feature path.

For privacy questions, requests, or complaints, contact info@sefira.se.

If Sefira acts only as processor for the relevant data, Sefira may need to refer the request to the relevant customer organization as controller.

Sources of personal data

Sefira may collect personal data:

• directly from the individual;
• from the customer organization that provisions or manages the workspace;
• from other workspace users and collaborators;
• from uploaded documents, files, and workflow content;
• from connected integrations and external service accounts;
• from service providers involved in billing, email delivery, storage, AI processing, or infrastructure;
• from automatically generated service, security, audit, and operational logs.

Categories of personal data

Depending on the feature used, Sefira may process:

• account and identity data such as name, email address, user ID, organization membership, and account state;
• authentication and security data such as password hashes, refresh-token references, verification events, device/session artifacts, and security-related logs;
• authentication and security data such as password hashes, refresh-token references, verification events, device/session artifacts, security-related logs, and abuse-prevention events such as temporary lockouts or rate-limit records;
• collaboration and workspace data such as tasks, comments, assignments, process steps, meeting-related metadata, and related work history;
• document and extracted-content data such as uploaded files, document previews, parsed text, extracted document fields, and derived workflow artifacts;
• AI-related data such as prompts, messages, generated drafts, assistant outputs, selected context, and run metadata;
• integration data such as OAuth connection state, repository metadata, scopes, external account identifiers, and integration event payloads;
• notification and communication data such as invitations, digests, delivery state, and email-dispatch logs;
• billing and subscription data such as provider customer IDs, subscription state, commercial metadata, and payment-related event records;
• support, audit, and compliance data such as governance audit events, portal operations, privacy-handling records, and anonymization-job evidence.

Why Sefira processes personal data

Sefira processes personal data to:

• create and administer accounts and workspace access;
• provide collaboration, planning, process execution, document-backed workflows, and related product functionality;
• secure the service, prevent misuse, investigate incidents, and enforce service integrity;
• provide AI-assisted drafting, analysis, and workflow support where enabled;
• operate requested integrations and connected third-party workflows;
• send transactional and service communications such as invitations, authentication messages, notifications, and digests;
• administer billing, subscriptions, and commercial support;
• respond to support requests and customer inquiries;
• comply with legal, accounting, privacy, security, and accountability obligations.

Legal bases

For EU and EEA-facing processing, Sefira may rely on one or more of the following legal bases depending on the relevant processing activity:

Processing purpose	Typical data categories	Typical legal basis	Notes
Account creation, login, authentication, and workspace access	identity, account,

authentication data | Contract | Required to provide the service |
Workspace collaboration and customer-configured workflows	workspace content, assignments, comments, files, document data	Contract and/or processor role under customer instructions	Customer may be controller for workspace content
Security, abuse prevention, fraud detection, and service reliability	session artifacts, logs, device/security signals, operational records	Legitimate interests	Used to secure accounts, protect the service, and investigate misuse
Billing, subscription administration, and invoicing	billing contact data, provider customer IDs, commercial records	Contract and legal obligation	Accounting and tax retention may apply
Support and service-response handling	support correspondence, account context, troubleshooting data	Contract and legitimate interests	Used to resolve issues and maintain the service
AI-assisted features where enabled	prompts, selected context, outputs, run metadata	Contract, processor role, and/or customer-enabled feature choice	Depends on the relevant feature path and customer configuration
Optional communications where consent is specifically requested	contact data, preference data	Consent	Consent may be withdrawn at any time
Legal compliance, auditability, and accountability records	compliance logs, billing records, audit events, legal response records	Legal obligation and legitimate interests	Used to meet legal duties and defend legal claims

Where Sefira relies on legitimate interests, those interests may include securing accounts, preventing misuse, maintaining audit trails, protecting the service and its users, responding to support requests, improving reliability, enforcing terms, and protecting legal claims.

Individuals may have the right to object where Sefira relies on legitimate interests.

Whether data is required

Some personal data is required to create an account, authenticate users, provide the service, maintain security, administer billing, or comply with legal obligations.

If required data is not provided, Sefira may not be able to provide the relevant account, feature, support, billing, or compliance function.

Optional features, integrations, and AI-assisted workflows may be disabled or not used if the relevant data is not provided.

Recipients and service providers

Personal data may be processed with or through service providers involved in:

• hosting and infrastructure;
• storage;

• email delivery;
• billing;
• AI processing;
• requested integrations.

Sefira maintains a public Subprocessor List at /subprocessors. The exact provider path can vary depending on enabled features, configured providers, active integrations, and deployment environment.

International transfers

Some provider paths may involve processing outside Sweden or the EEA.

Where personal data is transferred outside the EEA to a country without an adequacy decision, Sefira uses appropriate safeguards such as the EU Standard Contractual Clauses or another valid transfer mechanism under applicable data protection law.

More detailed provider-path information is available through the Subprocessor List and, where needed, customer-specific diligence materials.

Retention, deletion, and retained history

Sefira does not treat every deletion event as immediate erasure of all historical service records.

The retention model distinguishes between:

• data that should be purged, such as active secrets, credentials, and certain operational links;
• data that may be anonymized or tombstoned to break direct identity;
• customer or organization work product that may remain retained during the relevant service relationship;
• audit, billing, compliance, security, or legally required records that may need to remain for accountability, legal retention, or historical integrity.

Typical retention criteria include:

• account data: while the account is active and for a limited period after closure where needed for security, support, or legal follow-up;
• workspace content: for the term of the customer relationship unless deleted, exported, anonymized, or otherwise handled under customer-controlled retention rules;
• security and abuse-prevention logs: for a limited operational period and longer where needed for investigation or legal defense;
• billing and tax records: for the period required by applicable accounting or legal obligations;
• support records: for a reasonable period after case closure;
• AI prompts, outputs, and run metadata: according to the relevant feature path, workspace setting, provider path, and operational retention requirement;
• backups: for a rolling backup period until overwritten in the ordinary course.

This means deletion and access requests are handled against the specific data class, legal context, and applicable role, not against a blanket "delete everything instantly" promise.

Security and safeguards

Sefira applies layered access control, protected token and secret handling, signed external callback patterns where relevant, authentication abuse protections such as throttling and temporary lockouts, logging and auditability measures, and service-security controls appropriate to the product environment.

Further detail is available in the Security White Paper.

AI-assisted features

Some Sefira features use AI to assist with drafting, analysis, process-building, and document-related tasks.

Public handling principles:

• AI output is assistive and reviewable, not autonomous legal or operational truth by itself;
• AI-assisted features may process prompts, selected workspace context, uploaded document excerpts, generated outputs, and related run metadata through configured AI providers listed in the Subprocessor List;
• provider choice, retention, and transfer implications can differ by feature and environment;
• customers remain responsible for deciding which data classes and workflows may be used with AI-assisted functionality.

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

Sefira does not use personal data for solely automated decisions that produce legal or similarly significant effects on individuals, unless expressly stated in feature-specific terms.

Cookies and similar technologies

Sefira may use strictly necessary cookies, authentication/session technologies, and similar service-operation mechanisms required to provide secure access and maintain product functionality.

If analytics, telemetry, or other optional tracking mechanisms are used, they are disclosed through the relevant product or customer-facing notice for that implementation path.

Marketing and service communications

Sefira may send:

• transactional or security communications required to operate the service;
• product notifications and operational digests related to the service;

• support and account-response communications;
• optional communications where consent or another lawful basis is used.

Where marketing or optional communications rely on consent, consent may be withdrawn at any time. Individuals may also have opt-out rights where applicable.

Children and special category data

The service is intended for business and organizational use and is not directed to children.

Customers remain responsible for determining whether they may lawfully submit special category personal data or data relating to children into the service. Unless otherwise expressly agreed, the service is not described as a general-purpose repository for sensitive personal data without customer-side legal assessment and appropriate controls.

Data subject rights

Depending on applicable law, individuals may have rights including:

• access;
• rectification;
• erasure;
• restriction;
• objection;
• portability;
• withdrawal of consent where consent is used; and
• the right to complain to a supervisory authority.

Requests can be sent to info@sefira.se.

Sefira may need to verify identity before acting on a request. Where Sefira acts only as processor for the relevant data, Sefira may need to refer the request to the relevant customer controller.

Complaints

Individuals who believe their personal data has been handled unlawfully may have the right to complain to a supervisory authority.

In Sweden, this is normally IMY.