Data processing agreement

These are our standard terms. They bind both parties once they are signed together with the main agreement. Version 2026-11-24.

When your company uses Saga, you are the controller of the personal data in your workspace and Saga Compliance AB is the processor. This agreement sets out how we handle that data, as GDPR Article 28 requires.

1. Parties and precedence

This agreement is between Saga Compliance AB, organisation number 559608-6214, Stockholm, Sweden ("Saga", the processor) and the customer named in the main agreement for the Saga service ("the customer", the controller).

It is part of the main agreement. Where the two conflict on the processing of personal data, this agreement applies.

2. What Saga processes

Purpose: Saga processes personal data only to provide the Saga service under the main agreement. Duration: for as long as the main agreement runs, and until the data is returned or deleted under section 10.

Nature: hosting and storage, organising and searching records, AI-assisted analysis and drafting, and sending the emails the customer starts in Saga, such as policy acknowledgement requests and training invitations.

Data subjects: the customer's staff and board members, contacts at the customer's suppliers and partners, and people named in records the customer keeps in Saga, such as incidents and privacy requests.

Personal data: names, work email addresses, job titles and roles, sign-in and activity records, training and policy acknowledgement records, and the content the customer uploads or writes. The customer decides what it puts in Saga. Saga is not built for special categories of personal data (GDPR Article 9); the customer adds them only when a compliance record needs them.

3. Instructions

Saga processes personal data only on the customer's documented instructions. The instructions are this agreement, the main agreement and the way the customer uses and configures Saga.

Saga tells the customer at once if it believes an instruction breaks the GDPR or other data protection law. If EU or Swedish law requires Saga to process the data in another way, Saga tells the customer first, unless that law forbids it.

4. Confidentiality

Everyone at Saga who can access customer personal data is bound by confidentiality. Access is given only to people who need it to run or support the service.

5. Security

Saga takes the technical and organisational measures GDPR Article 32 requires and keeps them at least at the level described on our security page for as long as this agreement applies.

In short: traffic is encrypted with TLS 1.2 or 1.3. Each customer's records are kept apart by row-level security in the database. The database is backed up every night, and a backup counts only after it has been restored and checked. Changes in a workspace are written to an audit trail that the database refuses

to edit or delete.

Security page: https://saga-compliance.com/#security

6. Sub-processors

The customer gives Saga general authorisation to use the sub-processors on our sub-processor list.

Before a new sub-processor starts handling customer personal data, Saga updates the list and emails the contact named in the main agreement, so the customer can object. If an objection cannot be resolved, the customer may end the affected part of the service.

Saga puts the same data protection obligations as in this agreement on each sub-processor in a written contract, and remains responsible to the customer for their work.

Ask for the sub-processor list: https://saga-compliance.com/contact

7. Transfers outside the EU/EEA

Customer data is stored in a data centre in Frankfurt, Germany. Some sub-processors process data outside the EU/EEA or have a parent company in the United States. Today the AI model provider, xAI, processes data in the United States, with zero data retention switched on.

Saga transfers personal data outside the EU/EEA only to sub-processors on the list, and tells the customer the transfer basis for each one on request. Customer data is never used to train AI models.

8. Helping the customer

Saga helps the customer answer requests from data subjects. A request Saga receives about data in a customer's workspace is passed to that customer; Saga does not answer it itself.

Saga also helps the customer meet its duties under GDPR Articles 32 to 36: security, breach notification, data protection impact assessments and prior consultation, based on the nature of the processing and the information Saga has.

9. Personal data breaches

Saga tells the customer without undue delay after it becomes aware of a personal data breach that affects customer data, so the customer can report it to the supervisory authority within 72 hours.

Saga gives what is known at the time: what happened, which data and people are affected, the likely consequences and the measures taken. The rest follows as soon as it is known.

10. Return and deletion

When the main agreement ends, the customer chooses whether Saga returns or deletes the customer personal data, unless law requires Saga to keep it. Before the end, the customer can download its documents and reports from Saga, and Saga provides a copy of the rest on request.

Archiving a company in Saga keeps its data. Deletion happens on the customer's written instruction, and Saga confirms in writing when it is done. Saga keeps only the latest verified nightly backup, so deleted data leaves the backups once the next backup has replaced it.

11. Information and audits

Saga makes available the information the customer needs to show that this agreement and GDPR Article 28 are met. Saga allows audits, including inspections, by the customer or an auditor it appoints who is bound by confidentiality, after reasonable notice.

Saga does not hold an ISO 27001 or SOC 2 certification today.

12. Term, liability and law

This agreement applies for as long as Saga processes personal data for the customer. Liability follows the main agreement.

This agreement is governed by Swedish law. Disputes are resolved as set out in the main agreement.

How to get it signed

1 Ask for it through the contact form, or tell your contact at Saga. Name the person who signs for your company.

2 We attach this agreement to your main agreement and email that person a link to sign. The password comes in a separate email.

3 Your signer reads the PDF and signs online with a simple electronic signature. Saga Compliance AB then countersigns.

4 The signed copy and a signing certificate are then available from the signing link.

https://saga-compliance.com/contact