Privacy Statement

Last updated: 2026-10-26.

Saga is built with a privacy-first approach. The goal is for users to organize their personal lives without their data being sold, used for advertisements, or unnecessarily viewed by employees or AI suppliers.

This Privacy Statement describes how Valhalla Systems B.V. processes personal data for Saga.

1. Who is responsible?

Data controller:

- Valhalla Systems B.V.
- KvK number: 99011786
- VAT number: NL868747865B01
- Correspondence address: De Nieuwe Erven 3, Unit 15284, 5431 NV Cuijk, Netherlands
- General: info@sagafor.me
- Support: support@sagafor.me
- Privacy questions: privacy@sagafor.me
- Security: security@sagafor.me

2. What data does Saga process?

Saga only processes data that is necessary for the app to function, for users to have control over their data, and to enable paid features, security and support.

Account data

- Email address.
- Optionally a verified phone number.
- Subscription status.
- User settings, such as language, theme, accessibility and preferred settings.
- Login and verification status.
- For new independent registration: the provided date of birth and the registration route derived from it. Under sixteen, the account starts under supervision. An invitation already created by a caregiver for a child account does not ask for this date of birth again. Available Google Play age bands can determine the restricted route without a date of birth; Saga does not request a parent's address from Google for this.
- For a child-initiated consent request: the provided parent address, the sending and decision status, and any verified address corrections. The child cannot replace this address themselves. A reported error blocks the old invitation. For correction, a support request is registered without automatically sending chat content or device information.

Without parental approval, the provisional registration data is removed from active registration storage fourteen days after the first consent request. An address correction or new sending does not extend this period. Login and invitation links expire; there is no thirty-day recovery period for these. An anonymous deletion mark prevents reuse of the old account number. Existing backups follow their separate retention periods. - IP addresses for connections and security; see Technical data.

Saga deliberately does not use passwords.

User data

Users can store, among other things:

- Contacts.
- Calendar appointments.
- Tasks.
- Notes.
- Contact notes.
- Relationships between contacts.
- Objects.
- Locations.
- Current location, if the user gives permission for this.
- Images, recognized document text, and other attachments.
- Import and export files.

In shared vaults, data may be visible to other users who have access to that vault. Personal fields remain personal. This applies at least to nicknames, contact notes and location labels. A shared location can therefore have the same address for two users, but a different personal label.

Chat, voice and AI data

Saga can process chat messages, voice recordings, transcriptions, attachments and limited context to execute commands. Saga does not by default send the full database of a user to an AI model. Where possible, only the minimal context is sent.

Conversation content is only shared for support or bug analysis when the user explicitly sends feedback or a bug report in which the conversation is necessary.

For regular technical error reports, Saga tries to keep the context limited to technical metadata, such as request ID, time, app version, screen, error code and device context. Full chat content, photos, attachments, contact lists, notes or calendar content are only sent when the user explicitly chooses to do so in feedback or a bug report.

Payment and invoice data

For paid subscriptions, payment and invoice data are processed for subscriptions, billing, fraud prevention, and legal administration. Payments are processed via Stripe or Google Play, depending on the payment route. Card details are processed directly by the payment provider and not stored by Saga.

Technical data

Saga processes technical data to keep the app reliable and secure, to investigate errors, and to prevent abuse. This includes, for example, timestamps, app versions, error codes, login and management actions, response times, and usage of paid services. Regular technical logs are not intended to store full conversations, contact lists, notes, images, or audio. Context that you deliberately include with a bug report is processed separately.

Your IP address is needed for the connection and can be used to limit abuse. Saga omits IP addresses from regular technical and audit logs. Where full IP addresses are needed in separate security logs, a retention period of a maximum of seven days applies. For investigating a specific security incident, necessary data may be stored separately for a longer period; the purpose and necessity are documented and periodically reviewed. The other retention periods are listed under Retention periods.

3. Why does Saga process this data?

Saga processes personal data for:

- Delivering the app and the browser environment.
- Creating, displaying, sharing, importing and exporting user data.
- Login, verification and account recovery.
- Executing chat, voice, OCR and AI features.
- Managing subscriptions and invoices.
- Security, abuse prevention and error detection.
- Complying with legal obligations.
- Support, only when the user requests it or provides feedback.

4. Legal bases

Depending on the purpose and the person involved, Saga uses the following legal bases:

- **Performance of the contract:** processing that is necessary to provide your account and the requested features, such as storing, organizing, and controlled sharing of data, import/export, and paid features.
- **Consent:** for processing for which we ask for your separate consent, such as using your current location and enabling discoverability. You can withdraw consent; this does not affect the lawfulness of prior processing. A device permission or enabling an optional feature is not in itself the legal basis for all associated processing.
- **Legal obligation:** for, among other things, tax administration and handling legal privacy requests.
- **Legitimate interest:** for necessary, proportionate security, abuse prevention, error analysis, and limited operational logging. We balance our interests against your privacy and rights, with special attention to children.

For new registrations under sixteen years of age, Saga uses the parental supervision route. When the processing of a child's data is based on consent and the law requires it, that consent must be given or approved by the person holding parental responsibility. Enabling features in Saga does not replace these legal requirements. A confirmed email proves access to a mailbox, not in itself legal authority.

Data about other persons, for example in your contacts, does not automatically fall under your contract with Saga. The permissibility of this also depends on the purpose and context of use. For organizational use, the responsible organization must have an appropriate legal basis and inform those involved.

5. Vaults and sharing

A vault is a shielded collection of data. You can use it for yourself or share it with other users.

- **Read-only:** view data.
- **Edit:** add and modify data within the assigned rights.
- **Owner/administration:** manage access, participants, and roles within the available administrative rights.

Other participants can view or modify shared data within their rights. Personal fields such as nicknames, contact notes, and personal location labels are not shared with them.

Discoverability is separate from access to a vault. Through your discoverability settings, you determine whether others can find you using a verified contact method. An alias is the business card with which you share data. A contact link does not provide general access to your vaults; the shared data depends on the chosen link and the contact level.

Families, associations, and teams can use the same shared vaults. There too, the assigned roles determine who may view, modify, or manage data. Anyone processing personal data on behalf of an organization must take into account the privacy obligations of that organization.

When linking with a partner website, Saga displays which data is requested. You decide whether you transfer this data. After transfer, the recipient processes its copy according to its own privacy policy.

6. AI, voice and external suppliers

How Saga uses AI, image recognition, and voice, what content is processed in doing so, and what limitations apply, is stated in AI in Saga.

The external services used, their functions, and the data involved are listed in Suppliers and data processing.

7. Location data

Saga processes addresses and locations that you enter or store, for example for contacts or appointments. For address searches and suggestions, Saga uses Geoapify. The search text and used country or location preferences may be sent along to improve results.

For features with nearby places, Saga can, with your consent, use the estimated device location. You can refuse this consent or withdraw it via your device settings. Manually searching for an address remains separate from this.

For map display, your browser or app retrieves map images from OpenStreetMap. The map service receives technical request data, including your IP address. Therefore, not giving location permission does not prevent all map requests. See Suppliers and data processing.

8. Retention periods

Saga applies the following retention periods:

- Deleting your account: 30 days recovery period.
- After the recovery period: definitive deletion of user data from active systems.
- Invoices and tax administration: retention period according to legal obligations.
- Money-back guarantee: to monitor the one-time guarantee per email address, we store an identifier derived from the email address using a secret key for as long as we offer this guarantee. This identifier is retained even after account deletion. The value is not a readable email address and is used solely to prevent repeated use of the guarantee. Requests and refunds are part of the payment administration. Statutory refund rights are not limited by this.
- Security and audit logs without IP addresses: maximum 12 months; for necessary IP security logs, the separate limit of seven days and the described incident exception apply.
- Technical debug logs: 90 days.
- AI/STT/TTS, SMS and email cost logs: 12 months, as much as possible without content.
- Feedback and bug reports: six months from submission; deletion at the next daily cleanup, including any accompanying context and internal notes.
- Backups: daily restore points within 14 days and weekly restore points within 70 days; shared data blocks are reused by restic.

9. Backups

Saga creates encrypted backups daily using Restic. The production environment is located in Paris; the backup storage is located with Scaleway in Amsterdam. Access is restricted to technical administration. Each restore point contains a fully restorable dataset; unchanged data is reused between restore points.

The configured rotation retains daily restore points for fourteen days and weekly restore points for ten weeks. Saga monitors the backups and performs periodic restore tests.

A deletion in the active app is not individually removed from each existing restore point. The data disappears through rotation and cleanup of the backup storage. If the backup task fails, the most recent restore points may persist longer; storage versions may also extend physical retention. Therefore, the rotation windows are not a guarantee that every copy is erased within that timeframe.

When restoring after an outage, deletions and revoked permissions since the restore point must be reprocessed before the restored environment is released.

10. Security

Saga uses secure connections (TLS), access control on accounts and vaults, restricted administrative access, and encrypted backups. Security measures are maintained and adapted to the risks of the processing.

If you suspect a security issue or data breach, report it via security@sagafor.me. Saga investigates incidents and takes measures to limit the consequences. Where required by law, we report a data breach to the supervisory authority and inform the affected individuals. The internal data breach procedure is a work instruction for handling, not an additional obligation for users.

11. User rights

Users can, to the extent legally applicable, request:

- Access.
- Correction.
- Deletion.
- Export/data portability.
- Restriction of processing.
- Objection to certain processing.
- Withdrawal of consent.

Contact: privacy@sagafor.me.

You can view, modify, delete, and export data within your permissions in the app. Saga supports the export of vault data and settings. This does not grant a right to data of other users to whom you do not have access.

For a privacy request, you can email privacy@sagafor.me. We may request additional information to verify your identity. You will in principle receive a response within one month; if a legally permitted extension is needed, we will inform you within that month with the reason.

You can also file a complaint with the Dutch Data Protection Authority or another competent privacy supervisory authority. Withdrawing consent does not make previous lawful processing unlawful.

12. Cookies and local storage

See Cookie Statement.

13. Feedback and bug reports

See Feedback and Bug Reporting Flow.

14. Deleting your account

See Account Deletion Flow.

15. Changes

Saga may adjust this Privacy Statement when the app, legislation, or suppliers change. We will inform you of significant changes by email to the address of your Saga account.

Accounts under parental supervision

For an account under parental supervision, Saga processes the data necessary to link the child to their caregivers and to manage consent and access. This includes account and contact details, invitations, supervision settings, and decisions on requests.

Linked caregivers can view the supervision settings, involved caregivers, access rights, and relevant requests. They can also see the web addresses listed on the child's own contact card, such as a website or profile page. These are not the invitation links used by Saga to share contact details. Parental supervision does not automatically give caregivers access to the content of the child's personal storage space. For shared data, the access rights of the relevant vault apply.

Where parental consent is legally required, the conditions under Legal grounds apply. A user can delete their own supervised account without the consent of caregivers, after confirmation via their own email. For recovery via parental supervision, the consent of all linked caregivers remains necessary. This does not limit the child's legal privacy rights. The child or a legal representative can contact us for this via privacy@sagafor.me. Saga assesses who may make the request and what verification is required.

The retention periods and information on sharing, local storage, and account deletion elsewhere in this statement also apply to supervised accounts.