Datenschutzerklärung

Zuletzt aktualisiert: 2026-10-26.

Saga wurde ausgehend von einem Privacy-First-Ansatz entwickelt. Ziel ist es, dass Nutzer ihr persönliches Leben organisieren können, ohne dass ihre Daten verkauft, für Werbung genutzt oder unnötig von Mitarbeitern oder KI-Anbietern eingesehen werden.

Diese Datenschutzerklärung beschreibt, wie Valhalla Systems B.V. personenbezogene Daten für Saga verarbeitet.

1. Wer ist verantwortlich?

Verantwortlicher für die Datenverarbeitung:

- Valhalla Systems B.V.
- Handelsregisternummer: 99011786
- USt-IdNr.: NL868747865B01
- Korrespondenzadresse: De Nieuwe Erven 3, Unit 15284, 5431 NV Cuijk, Netherlands
- Allgemein: info@sagafor.me
- Support: support@sagafor.me
- Datenschutzfragen: privacy@sagafor.me
- Sicherheit: security@sagafor.me

2. Welche Daten verarbeitet Saga?

Saga verarbeitet nur Daten, die erforderlich sind, damit die App funktioniert, Nutzern die Kontrolle über ihre Daten zu geben und kostenpflichtige Funktionen, Sicherheit sowie Support zu ermöglichen.

Kontodaten

- E-Mail-Adresse.
- Optional eine verifizierte Telefonnummer.
- Abonnementstatus.
- Nutzereinstellungen wie Sprache, Design, Barrierefreiheit und bevorzugte Einstellungen.
- Login- und Verifizierungsstatus.
- Bei einer neuen eigenständigen Registrierung: das angegebene Geburtsdatum und der daraus abgeleitete Registrierungsweg. Unter sechzehn Jahren beginnt das Konto unter Aufsicht. Eine Einladung, die bereits von einem Betreuer für ein Kinderkonto erstellt wurde, fragt dieses Geburtsdatum nicht erneut ab. Verfügbare Google-Play-Altersstufen können den eingeschränkten Weg ohne Geburtsdatum bestimmen; Saga fragt hiermit keine Elternadresse bei Google ab.
- Bei einem kindgestarteten Zustimmungsantrag: die angegebene Elternadresse, der Versand- und Entscheidungsstatus sowie ggf. geprüfte Adresskorrekturen. Das Kind kann diese Adresse nicht selbst ersetzen. Ein gemeldeter Fehler blockiert die alte Einladung. Für eine Korrektur wird ein Supportantrag registriert, ohne automatisch Chatinhalte oder Geräteinformationen zu übermitteln.

Ohne elterliche Zustimmung werden die vorläufigen Registrierungsdaten vierzehn Tage nach dem ersten Zustimmungsantrag aus dem aktiven Registrierungsspeicher gelöscht. Eine Adresskorrektur oder ein neuer Versand verlängert diese Frist nicht. Anmelde- und Einladungslinks verfallen; es gibt hierfür keine Wiederherstellungsfrist von dreißig Tagen. Eine namenlose Löschmarkierung verhindert die Wiederverwendung der alten Kontonummer. Vorhandene Backups folgen ihren jeweiligen Aufbewahrungsfristen. - IP-Adressen für Verbindungen und Sicherheit; siehe Technische Daten.

Saga verwendet bewusst keine Passwörter.

Nutzerdaten

Nutzer können unter anderem speichern:

- Kontakte.
- Kalendereinträge.
- Aufgaben.
- Notizen.
- Kontaktnotizen.
- Beziehungen zwischen Kontakten.
- Objekte.
- Standorte.
- Aktueller Standort, sofern der Nutzer dafür die Erlaubnis erteilt.
- Bilder, erkannte Dokumenttexte und andere Anhänge.
- Import- und Exportdateien.

Bei geteilten Vaults können Daten für andere Nutzer sichtbar sein, die Zugriff auf diesen Vault haben. Persönliche Felder bleiben persönlich. Dies gilt zumindest für Spitznamen, Kontaktnotizen und Standortbezeichnungen. Ein geteilter Standort kann also für zwei Nutzer dieselbe Adresse haben, aber eine andere persönliche Bezeichnung.

Chat-, Sprach- und KI-Daten

Saga kann Chat-Nachrichten, Sprachnachrichten, Transkriptionen, Anhänge und begrenzte Kontextinformationen verarbeiten, um Befehle auszuführen. Saga sendet standardmäßig nicht die gesamte Datenbank eines Nutzers an ein KI-Modell. Wo möglich wird nur der minimale Kontext übermittelt.

Gesprächsinhalte werden nur für Support oder Fehleranalysen geteilt, wenn der Nutzer explizit Feedback oder einen Fehlerbericht sendet, bei dem das Gespräch erforderlich ist.

Bei normalen technischen Fehlermeldungen versucht Saga, den Kontext auf technische Metadaten zu beschränken, wie z. B. Request-ID, Zeitpunkt, App-Version, Bildschirm, Fehlercode und Gerätekontext. Der vollständige Chat-Inhalt, Fotos, Anhänge, Kontaktlisten, Notizen oder Kalenderinhalte werden nur übermittelt, wenn der Nutzer dies explizit in Feedback oder einem Fehlerbericht auswählt.

Zahlungs- und Rechnungsdaten

Bei bezahlten Abonnements werden Zahlungs- und Rechnungsdaten für Abonnements, Abrechnung, Betrugsprävention und gesetzliche Buchhaltung verarbeitet. Zahlungen laufen über Stripe oder Google Play, je nach Zahlungsroute. Kartendaten werden direkt vom Zahlungsanbieter verarbeitet und nicht von Saga gespeichert.

Technische Daten

Saga verarbeitet technische Daten, um die App zuverlässig und sicher zu betreiben, Fehler zu untersuchen und Missbrauch zu verhindern. Es handelt sich beispielsweise um Zeitstempel, App-Versionen, Fehlercodes, Anmelde- und Verwaltungsvorgänge, Antwortzeiten und den Verbrauch bezahlter Dienste. Regelmäßige technische Logs sind nicht dazu bestimmt, vollständige Gespräche, Kontaktlisten, Notizen, Bilder oder Audio aufzubewahren. Kontext, den du bewusst mit einem Fehlerbericht mitsendest, wird separat verarbeitet.

Deine IP-Adresse wird für die Verbindung benötigt und kann verwendet werden, um Missbrauch einzuschränken. Saga lässt IP-Adressen aus regulären technischen und Audit-Logs weg. Wo vollständige IP-Adressen in separaten Sicherheitslogs erforderlich sind, gilt eine Aufbewahrungsfrist von maximal sieben Tagen. Für die Untersuchung eines konkreten Sicherheitsvorfalls können notwendige Daten separat länger aufbewahrt werden; der Zweck und die Notwendigkeit werden dokumentiert und regelmäßig überprüft. Die übrigen Aufbewahrungsfristen findest du unter Aufbewahrungsfristen.

3. Warum verarbeitet Saga diese Daten?

Saga verarbeitet personenbezogene Daten für:

- Die Bereitstellung der App und der Browserumgebung.
- Das Erstellen, Anzeigen, Teilen, Importieren und Exportieren von Nutzerdaten.
- Login, Verifizierung und Kontowiederherstellung.
- Die Ausführung von Chat-, Sprach-, OCR- und KI-Funktionen.
- Die Verwaltung von Abonnements und Rechnungen.
- Sicherheit, Missbrauchsprävention und Fehlererkennung.
- Die Erfüllung gesetzlicher Verpflichtungen.
- Support, ausschließlich wenn der Nutzer danach fragt oder Feedback gibt.

4. Rechtliche Grundlagen

Je nach Zweck und betroffener Person verwendet Saga die folgenden Rechtsgrundlagen:

- **Vertragserfüllung:** Verarbeitung, die erforderlich ist, um dein Konto und die angeforderten Funktionen bereitzustellen, wie das Speichern, Organisieren und kontrollierte Teilen von Daten, Import/Export und bezahlte Funktionen.
- **Einwilligung:** für Verarbeitungen, für die wir dich gesondert um Einwilligung bitten, wie die Nutzung deines aktuellen Standorts und das Aktivieren der Auffindbarkeit. Du kannst deine Einwilligung jederzeit widerrufen; dies ändert nichts an der Rechtmäßigkeit der vorherigen Verarbeitung. Eine Geräteberechtigung oder das Öffnen einer optionalen Funktion ist nicht an sich die Rechtsgrundlage für alle damit verbundenen Verarbeitungen.
- **Gesetzliche Verpflichtung:** für unter anderem die steuerliche Buchführung und die Bearbeitung gesetzlicher Datenschutzanfragen.
- **Berechtigtes Interesse:** für notwendige, verhältnismäßige Sicherheit, Missbrauchsprävention, Fehleranalyse und begrenzte operative Protokollierung. Dabei wiegen wir unsere Interessen gegen deine Privatsphäre und Rechte ab, mit besonderer Aufmerksamkeit für Kinder.

Bei neuen Registrierungen unter sechzehn Jahren verwendet Saga den Weg der elterlichen Aufsicht. Wenn die Verarbeitung von Kinderdaten auf Einwilligung beruht und das Gesetz dies verlangt, muss diese Einwilligung von der Person erteilt oder genehmigt werden, die die elterliche Verantwortung trägt. Das Freischalten von Funktionen in Saga ersetzt diese gesetzlichen Voraussetzungen nicht. Eine bestätigte E-Mail beweist den Zugang zu einem Postfach, nicht an sich die rechtliche Vertretungsbefugnis.

Daten über andere Personen, beispielsweise in deinen Kontakten, fallen nicht automatisch unter deinen Vertrag mit Saga. Die Zulässigkeit hängt unter anderem vom Zweck und dem Kontext der Nutzung ab. Für die Nutzung durch Organisationen muss die verantwortliche Organisation eine geeignete Rechtsgrundlage haben und die Betroffenen informieren.

5. Vaults und Teilen

Ein Vault ist eine abgeschirmte Datensammlung. Du kannst ihn für dich selbst nutzen oder mit anderen Benutzern teilen.

- **Nur lesen:** Daten anzeigen.
- **Bearbeiten:** Daten hinzufügen und ändern innerhalb der zugewiesenen Berechtigungen.
- **Eigentümer/Verwaltung:** Zugriff, Teilnehmer und Rollen innerhalb der verfügbaren Verwaltungsberechtigungen verwalten.

Andere Teilnehmer sehen oder ändern geteilte Daten innerhalb ihrer Berechtigungen. Persönliche Felder wie Spitznamen, Kontaktnotizen und persönliche Standortbeschriftungen werden nicht mit ihnen geteilt.

Die Auffindbarkeit ist unabhängig vom Zugriff auf einen Vault. Über deine Auffindbarkeitseinstellungen bestimmst du, ob andere dich mit einer verifizierten Kontaktmethode finden können. Ein Alias ist die Visitenkarte, mit der du Daten teilst. Eine Kontaktverknüpfung gewährt keinen allgemeinen Zugriff auf deine Vaults; die geteilten Daten hängen von der gewählten Verknüpfung und der Kontakstufe ab.

Familien, Vereine und Teams können dieselben geteilten Vaults nutzen. Auch dort bestimmen die zugewiesenen Rollen, wer Daten anzeigen, ändern oder verwalten darf. Wer im Namen einer Organisation personenbezogene Daten verarbeitet, muss die Datenschutzpflichten dieser Organisation berücksichtigen.

Bei einer Verknüpfung mit einer Partnerwebsite zeigt Saga an, welche Daten angefordert werden. Du entscheidest, ob du diese übermittelst. Nach der Übermittlung verarbeitet der Empfänger seine Kopie gemäß seiner eigenen Datenschutzerklärung.

6. KI, Sprache und externe Anbieter

Wie Saga KI, Bilderkennung und Sprache verwendet, welche Inhalte dabei verarbeitet werden und welche Einschränkungen gelten, steht in KI in Saga.

Die verwendeten externen Dienste, ihre Funktionen und die betroffenen Daten stehen in Lieferanten und Datenverarbeitung.

7. Standortdaten

Saga verarbeitet Adressen und Standorte, die du eingibst oder speicherst, beispielsweise bei Kontakten oder Terminen. Für Adresssuchen und Vorschläge verwendet Saga Geoapify. Der Suchtext und die verwendeten Länder- oder Standortpräferenzen können dabei zur Verbesserung der Ergebnisse mitgesendet werden.

Für Funktionen mit Orten in der Nähe kann Saga nach deiner Einwilligung den geschätzten Gerätestandort verwenden. Du kannst diese Einwilligung verweigern oder über deine Geräteeinstellungen widerrufen. Das manuelle Suchen einer Adresse bleibt davon unabhängig.

Bei der Kartendarstellung ruft dein Browser oder deine App Kartenbilder von OpenStreetMap ab. Dabei erhält der Kartendienst technische Anfrageinformationen, darunter deine IP-Adresse. Das Verweigern der Standorterlaubnis verhindert daher nicht alle Kartenanfragen. Siehe Lieferanten und Datenverarbeitung.

8. Aufbewahrungsfristen

Saga wendet die folgenden Aufbewahrungsfristen an:

- Konto löschen: 30 Tage Wiederherstellungsfrist.
- Nach der Wiederherstellungsfrist: endgültige Löschung der Nutzerdaten aus aktiven Systemen.
- Rechnungen und steuerliche Verwaltung: Aufbewahrungsfrist gemäß gesetzlichen Verpflichtungen.
- Geld-zurück-Garantie: Um die einmalige Garantie pro E-Mail-Adresse zu überwachen, speichern wir einen mit einem geheimen Schlüssel abgeleiteten Kennwert der E-Mail-Adresse, solange wir diese Garantie anbieten. Dieser wird auch nach der Kontolöschung beibehalten. Der Wert ist keine lesbare E-Mail-Adresse und wird ausschließlich verwendet, um die wiederholte Inanspruchnahme der Garantie zu verhindern. Anträge und Erstattungen sind Teil der Zahlungsabwicklung. Gesetzliche Erstattungsrechte werden dadurch nicht eingeschränkt.
- Sicherheits- und Audit-Protokolle ohne IP-Adressen: maximal 12 Monate; für notwendige IP-Sicherheitsprotokolle gilt die separate Grenze von sieben Tagen und die beschriebene Ausnahme für Vorfälle.
- Technische Debug-Protokolle: 90 Tage.
- KI/STT/TTS-, SMS- und E-Mail-Kostenprotokolle: 12 Monate, soweit möglich ohne Inhalt.
- Feedback und Bugmeldungen: sechs Monate ab Einreichung; Löschung bei der nächsten täglichen Bereinigung, einschließlich mitgesendeter Kontextinformationen und interner Notizen.
- Backups: tägliche Wiederherstellungspunkte innerhalb von 14 Tagen und wöchentliche Wiederherstellungspunkte innerhalb von 70 Tagen; geteilte Datenblöcke werden von restic wiederverwendet.

9. Backups

Saga erstellt täglich verschlüsselte Backups mit Restic. Die Produktionsumgebung befindet sich in Paris; die Backup-Speicherung befindet sich bei Scaleway in Amsterdam. Der Zugriff ist auf das technische Management beschränkt. Jeder Wiederherstellungspunkt enthält einen vollständig wiederherstellbaren Datensatz; unveränderte Daten werden zwischen den Wiederherstellungspunkten wiederverwendet.

Die eingestellte Rotation bewahrt tägliche Wiederherstellungspunkte über vierzehn Tage und wöchentliche Wiederherstellungspunkte über zehn Wochen. Saga prüft die Backups und führt regelmäßig Wiederherstellungstests durch.

Eine Löschung in der aktiven App wird nicht separat aus jedem bestehenden Wiederherstellungspunkt entfernt. Die Daten verschwinden durch Rotation und Aufräumung des Backup-Speichers. Bei einem Ausfall der Backup-Aufgabe können die letzten Wiederherstellungspunkte länger bestehen bleiben; auch Speicher-Versionen können die physische Aufbewahrung verlängern. Die Rotationsfenster sind daher keine Garantie dafür, dass jede Kopie innerhalb dieser Frist gelöscht wurde.

Bei einer Wiederherstellung nach einer Störung müssen Löschungen und zurückgezogene Berechtigungen seit dem Wiederherstellungspunkt erneut verarbeitet werden, bevor die wiederhergestellte Umgebung freigegeben wird.

10. Sicherheit

Saga verwendet gesicherte Verbindungen (TLS), Zugriffskontrolle auf Konten und Vaults, eingeschränkten Administratorzugriff und verschlüsselte Backups. Sicherheitsmaßnahmen werden gepflegt und an die Risiken der Verarbeitung angepasst.

Verdächtigst du ein Sicherheitsproblem oder einen Datenverlust, melde dies über security@sagafor.me. Saga untersucht Vorfälle und ergreift Maßnahmen, um die Folgen zu begrenzen. Wo das Gesetz es verlangt, melden wir einen Datenverlust an die Aufsichtsbehörde und informieren die betroffenen Personen. Die interne Datenverlust-Verfahrensanweisung ist eine Arbeitsanweisung für die Bearbeitung, keine zusätzliche Verpflichtung für Benutzer.

11. Rechte der Nutzer

Nutzer können, soweit gesetzlich anwendbar, folgende Rechte geltend machen:

- Auskunft.
- Berichtigung.
- Löschung.
- Datenübertragbarkeit/Export.
- Einschränkung der Verarbeitung.
- Widerspruch gegen bestimmte Verarbeitungen.
- Widerruf der Einwilligung.

Kontakt: privacy@sagafor.me.

Du kannst Daten innerhalb deiner Berechtigungen in der App anzeigen, ändern, löschen und exportieren. Saga unterstützt den Export von Vault-Daten und Einstellungen. Dies gewährt kein Recht auf Daten anderer Benutzer, auf die du keinen Zugriff hast.

Für eine Datenschutzanfrage kannst du eine E-Mail an privacy@sagafor.me senden. Wir können zusätzliche Informationen anfordern, um deine Identität zu überprüfen. Du erhältst grundsätzlich innerhalb eines Monats eine Antwort; wenn eine gesetzlich zulässige Verlängerung erforderlich ist, teilen wir dies innerhalb dieses Monats mit Begründung mit.

Du kannst auch eine Beschwerde bei der Autoriteit Persoonsgegevens oder einer anderen zuständigen Datenschutz-Aufsichtsbehörde einreichen. Der Widerruf der Einwilligung macht eine frühere rechtmäßige Verarbeitung nicht unrechtmäßig.

12. Cookies und lokale Speicherung

Siehe Cookie-Erklärung.

13. Feedback und Fehlerberichte

Siehe Feedback- und Fehlerberichtsprozess.

14. Konto löschen

Siehe Konto-Löschprozess.

15. Änderungen

Saga kann diese Datenschutzerklärung anpassen, wenn sich die App, die Gesetzgebung oder die Lieferanten ändern. Über wichtige Änderungen informieren wir dich per E-Mail an die Adresse deines Saga-Kontos.

Konten unter elterlicher Aufsicht

Bei einem Konto unter elterlicher Aufsicht verarbeitet Saga die Daten, die erforderlich sind, um das Kind mit seinen Betreuern zu verknüpfen und Einwilligung und Zugriff zu verwalten. Dies umfasst Konto- und Kontaktdaten, Einladungen, Aufsichtseinstellungen und Entscheidungen über Anfragen.

Verknüpfte Betreuer können die Aufsichtseinstellungen, die beteiligten Betreuer, die Zugriffsrechte und die relevanten Anfragen anzeigen. Sie können auch die Webadressen sehen, die auf der eigenen Kontaktkarte des Kindes stehen, beispielsweise eine Website oder Profilseite. Dies sind nicht die Einladungslinks, mit denen Saga Kontaktdaten teilt. Elterliche Aufsicht gewährt Betreuern nicht automatisch Zugriff auf den Inhalt eines persönlichen Speicherbereichs des Kindes. Für geteilte Daten gelten die Zugriffsrechte des betreffenden Vaults.

Wo eine elterliche Einwilligung gesetzlich erforderlich ist, gelten die Bedingungen unter Rechtliche Grundlagen. Ein Benutzer kann sein eigenes Konto unter Aufsicht ohne Zustimmung der Betreuer löschen, nach Bestätigung über die eigene E-Mail. Für die Wiederherstellung über elterliche Aufsicht bleibt die Zustimmung aller verknüpften Betreuer erforderlich. Dies schränkt die gesetzlichen Datenschutzrechte des Kindes nicht ein. Das Kind oder ein bevollmächtigter Vertreter kann sich dazu über privacy@sagafor.me in Verbindung setzen. Saga bewertet, wer die Anfrage stellen darf und welche Überprüfung dafür erforderlich ist.

Die Aufbewahrungsfristen und Informationen zu Teilen, lokaler Speicherung und Kontolöschung an anderer Stelle in dieser Erklärung gelten auch für Konten unter Aufsicht.