Personvernærterklæring

Sist oppdatert: 2026-10-26.

Saga er bygget med utgangspunkt i personvern først. Målet er at brukere kan organisere sitt personlige liv uten at dataene deres blir solgt, brukt til annonser eller unødvendig gjennomgått av ansatte eller AI-leverandører.

Denne personvernerklæringen beskriver hvordan Valhalla Systems B.V. behandler personopplysninger for Saga.

1. Hvem er ansvarlig?

Behandlingsansvarlig:

- Valhalla Systems B.V.
- KvK-nummer: 99011786
- MVA-nummer: NL868747865B01
- Korrespondanseadresse: De Nieuwe Erven 3, Unit 15284, 5431 NV Cuijk, Netherlands
- Generelt: info@sagafor.me
- Support: support@sagafor.me
- Personvernspørsmål: privacy@sagafor.me
- Sikkerhet: security@sagafor.me

2. Hvilke data behandler Saga?

Saga behandler bare data som er nødvendige for at appen skal fungere, for å gi brukere kontroll over sine egne data, og for å muliggjøre betalte funksjoner, sikkerhet og support.

Kontodata

- E-postadresse.
- Eventuelt et verifisert telefonnummer.
- Abonnementsstatus.
- Brukerinnstillinger, for eksempel språk, tema, tilgjengelighet og preferanser.
- Innlogging- og verifikasjonsstatus.
- Ved ny selvstendig registrering: den oppgitte fødselsdatoen og den avledede registreringsruten. Under seksten år starter kontoen under tilsyn. En invitasjon som allerede er opprettet av en omsorgsperson for en barnkonto ber ikke om denne fødselsdatoen på nytt. Tilgjengelige Google Play-alderstyper kan bestemme den begrensede ruten uten fødselsdato; Saga ber ikke om foreldreadresse hos Google med dette.
- Ved et barnstartet samtykkesøknad: den oppgitte foreldreadressen, sende- og beslutningsstatus og eventuelle kontrollerte adressekorrigeringer. Barnet kan ikke selv erstatte denne adressen. En rapportert feil blokkerer den gamle invitasjonen. For korrigering registreres en supportforespørsel uten å automatisk sende med chatinnhold eller enhetsinformasjon.

Uten foreldregodkjenning slettes de foreløpige registreringsdataene fjorten dager etter den første samtykkesøknaden fra den aktive registreringsopplagringen. En adressekorrigering eller ny sending forlenger ikke denne fristen. Innlogging- og invitasjonslenker utløper; det er ingen gjenopprettingsperiode på tretti dager for disse. En anonym slettemarkering forhindrer gjenbruk av det gamle kontonummeret. Eksisterende sikkerhetskopier følger sine egne oppbevaringsfrister. - IP-adresser for tilkoblinger og sikkerhet; se Tekniske data.

Saga bruker bevisst ingen passord.

Brukerdata

Brukere kan blant annet lagre:

- Kontakter.
- Kalenderavtaler.
- Oppgaver.
- Notater.
- Kontaktnotater.
- Relasjoner mellom kontakter.
- Objekter.
- Steder.
- Nåværende sted, dersom brukeren har gitt tillatelse til dette.
- Bilder, gjenkjent dokumenttekst og andre vedlegg.
- Import- og eksportfiler.

I delte vaults kan data bli synlige for andre brukere som har tilgang til den aktuelle vaulten. Personlige felt forblir personlige. Dette gjelder i hvert fall for kallenavn, kontaktnotater og stedetiketter. Et delt sted kan derfor ha samme adresse for to brukere, men en annen personlig etikett.

Chat-, tale- og AI-data

Saga kan behandle chattemeldinger, taleopptak, transkripsjoner, vedlegg og begrenset kontekst for å utføre oppgaver. Saga sender ikke standard den fullstendige databasen til en bruker til en AI-modell. Der det er mulig sendes bare minimal kontekst.

Innhold i samtaler deles bare for support eller feilanalyse når brukeren eksplisitt sender tilbakemelding eller en feilrapport der samtalen er nødvendig.

Ved vanlige tekniske feilmeldinger prøver Saga å begrense konteksten til teknisk metadata, for eksempel request-id, tidspunkt, appversjon, skjerm, feilkode og enhetskontekst. Fullstendig chatinnhold, bilder, vedlegg, kontaktlister, notater eller kalenderinnhold sendes bare med når brukeren eksplisitt velger dette i tilbakemelding eller en feilrapport.

Betalings- og fakturadata

For betalte abonnementer behandles betalings- og fakturadata for abonnementer, fakturering, svindelforebygging og lovlig administrasjon. Betalinger går via Stripe eller Google Play, avhengig av betalingsruten. Kortdata behandles direkte av betalingsleverandøren og lagres ikke av Saga.

Tekniske data

Saga behandler tekniske data for å la appen fungere pålitelig og sikkert, for å undersøke feil og for å forhindre misbruk. Dette gjelder for eksempel tidspunkter, appversjoner, feilkoder, innlogging- og administrasjonsoperasjoner, svartider og forbruk av betalte tjenester. Vanlige tekniske logger er ikke ment å lagre komplette samtaler, kontaktlister, notater, bilder eller lyd. Kontekst du bevisst sender med en feilrapport, behandles separat.

Din IP-adresse er nødvendig for tilkoblingen og kan brukes for å begrense misbruk. Saga utelater IP-adresser fra vanlige tekniske og revisjonslogger. Der komplette IP-adresser er nødvendig i separate sikkerhetslogger, gjelder en oppbevaringsfrist på maksimalt syv dager. For undersøkelse av et konkret sikkerhetsincident kan nødvendige data lagres lenger separat; formålet og nødvendigheten dokumenteres og vurderes periodisk. De øvrige oppbevaringsfristene står under Oppbevaringsfrister.

3. Hvorfor behandler Saga disse dataene?

Saga behandler personopplysninger for:

- Å levere appen og nettlesermiljøet.
- Å opprette, vise, dele, importere og eksportere brukerdata.
- Innlogging, verifisering og kontohenting.
- Å utføre chat-, tale-, OCR- og AI-funksjoner.
- Å administrere abonnementer og fakturaer.
- Sikkerhet, misbrukforebygging og feilretting.
- Å oppfylle lovpålagte forpliktelser.
- Support, utelukkende når brukeren ber om det eller gir tilbakemelding.

4. Juridiske grunnlag

Avhengig av formålet og den involverte personen bruker Saga følgende rettsgrunnlag:

- **Utførelse av avtalen:** behandling som er nødvendig for å levere kontoen din og de forespurte funksjonene, som lagring, organisering og kontrollert deling av data, import/eksport og betalte funksjoner.
- **Samtykke:** for behandlinger der vi ber deg om separat samtykke, som bruk av din nåværende posisjon og aktivering av synlighet. Du kan trekke tilbake samtykket; dette endrer ikke lovligheten av tidligere behandling. En enhetsautorisering eller åpning av en valgfri funksjon er ikke i seg selv rettsgrunnlaget for all tilknyttet behandling.
- **Lovlig forpliktelse:** for blant annet skattemelding og behandling av lovlige personvernforespørsler.
- **Berettiget interesse:** for nødvendig, proporsjonal sikkerhet, misbruksforebygging, feilanalyse og begrenset operativ logging. Vi veier da våre interesser mot din personvern og rettigheter, med særlig hensyn til barn.

Ved nye registreringer under seksten år bruker Saga ruten for foreldrekontroll. Når behandlingen av data om et barn bygger på samtykke og loven krever dette, må samtykket gis eller godkjennes av den som bærer foreldresorgen. Å frigjøre funksjoner i Saga erstatter ikke disse lovlige vilkårene. En bekreftet e-post beviser tilgang til en e-postboks, ikke i seg selv juridisk myndighet.

Data om andre personer, for eksempel i kontaktene dine, faller ikke automatisk under din avtale med Saga. Lovligheten av dette avhenger også av formålet og konteksten for bruken. For organisasjonsbruk må den ansvarlige organisasjon ha et passende rettsgrunnlag og informere de involverte.

5. Vaults og deling

En vault er en skjermet samling av data. Du kan bruke den for deg selv eller dele den med andre brukere.

- **Kun lesing:** vise data.
- **Redigering:** legge til og endre data innenfor de tildelte rettighetene.
- **Eier/administrasjon:** administrere tilgang, deltakere og roller innenfor de tilgjengelige administrasjonsrettighetene.

Andre deltakere ser eller endrer delte data innenfor sine rettigheter. Personlige felter som kallenavn, kontaktnotater og personlige posisjonsetiketter deles ikke med dem.

Synlighet er uavhengig av tilgang til en vault. Via synlighetsinnstillingene dine bestemmer du om andre kan finne deg med en verifisert kontaktmåte. En alias er visitkortet du bruker til å dele data. En kontaktkobling gir ikke generell tilgang til vaultene dine; de delte dataene avhenger av den valgte koblingen og kontaktnivået.

Familier, foreninger og lag kan bruke de samme delte vaultene. Også der bestemmer de tildelte rollene hvem som kan se, endre eller administrere data. Den som behandler persondata på vegne av en organisasjon, må ta hensyn til personvernforpliktelsene til den organisasjonen.

Ved en kobling til et partners nettsted viser Saga hvilke data som blir bedt om. Du bestemmer om du vil overføre disse. Etter overføring behandler mottakeren sin kopi i henhold til sitt eget personvernreglement.

6. AI, tale og eksterne leverandører

Hvordan Saga bruker AI, bildegjenkjenning og tale, hvilken innhold som behandles i den forbindelse og hvilke begrensninger som gjelder, står i AI i Saga.

De eksterne tjenestene som brukes, deres funksjoner og de involverte dataene står i Leverandører og databehandling.

7. Steddata

Saga behandler adresser og posisjoner som du oppgir eller lagrer, for eksempel ved kontakter eller avtaler. For adresseøk og forslag bruker Saga Geoapify. Søketeksten og brukte land- eller posisjonsinnstillinger kan sendes med for å forbedre resultatene.

For funksjoner med steder i nærheten kan Saga, etter ditt samtykke, bruke den estimerte enhetsposisjonen. Du kan avvise dette samtykket eller trekke det tilbake via enhetsinnstillingene dine. Manuell adresseøk er uavhengig av dette.

Ved kartvisning henter nettleseren eller appen din kartbilder fra OpenStreetMap. Karttjenesten mottar da tekniske forespørselsdata, inkludert IP-adressen din. Å ikke gi posisjonssamtykke hindrer derfor ikke alle kartforespørsler. Se Leverandører og databehandling.

8. Oppbevaringstider

Saga anvender følgende oppbevaringsfrister:

- Slett konto: 30 dagers gjenopprettingsperiode.
- Etter gjenopprettingsperioden: endelig sletting av brukerdata fra aktive systemer.
- Fakturaer og skattemessig administrasjon: oppbevaringstid i henhold til lovpålagte forpliktelser.
- Penger-tilbake-garanti: For å overvåke den engangsgarantien per e-postadresse, lagrer vi en identifikasjonsverdi avledet fra e-postadressen med en hemmelig nøkkel så lenge vi tilbyr denne garantien. Denne verdien beholdes også etter at kontoen er slettet. Verdien er ikke en lesbar e-postadresse og brukes kun for å forhindre gjentatt bruk av garantien. Søknader og tilbakebetalinger inngår i betalingsadministrasjonen. Lovbestemte rettigheter til tilbakebetaling begrenses ikke av dette.
- Sikkerhets- og revisjonslogger uten IP-adresser: maksimalt 12 måneder; for nødvendige IP-sikkerhetslogger gjelder den separate grensen på syv dager og den beskrevne unntaket for hendelser.
- Tekniske feillogger: 90 dager.
- AI/STT/TTS-, SMS- og e-postkostnadslogger: 12 måneder, så mye som mulig uten innhold.
- Tilbakmeldinger og feilrapporter: seks måneder fra innsending; sletting ved neste daglige rydding, inkludert medsendt kontekst og interne notater.
- Sikkerhetskopier: daglige gjenopprettingspunkter innenfor 14 dager og ukentlige gjenopprettingspunkter innenfor 70 dager; delte datablokker gjenbrukes av restic.

9. Sikkerhetskopier

Saga lager krypterte sikkerhetskopier daglig med Restic. Produksjonsmiljøet ligger i Paris; lagringen av sikkerhetskopier ligger hos Scaleway i Amsterdam. Tilgang er begrenset til teknisk drift. Hvert gjenopprettingspunkt inneholder et fullstendig gjenopprettbart datasett; uendrede data gjenbrukes mellom gjenopprettingspunkter.

Den innstilte rotasjonen beholder daglige gjenopprettingspunkter i fjorten dager og ukentlige gjenopprettingspunkter i ti uker. Saga kontrollerer sikkerhetskopiene og utfører periodiske gjenopprettingstester.

En sletting i den aktive appen fjernes ikke separat fra hvert eksisterende gjenopprettingspunkt. Dataene forsvinner gjennom rotasjon og rydding av sikkerhetskopilagringen. Ved feil i sikkerhetskopijobbene kan de siste gjenopretttingspunktene eksistere lenger; også lagringsversjoner kan forlenge den fysiske oppbevaringen. Rotasjonsvinduene er derfor ingen garanti for at hver kopi er slettet innen denne fristen.

Ved gjenoppretting etter en feil må slettinger og inndrevne rettigheter siden gjenopprettingspunktet behandles på nytt før det gjenopprettede miljøet frigis.

10. Sikkerhet

Saga bruker sikrede tilkoblinger (TLS), tilgangskontroll på kontoer og vaults, begrenset administratortilgang og krypterte sikkerhetskopier. Sikkerhetstiltak vedlikeholdes og tilpasses risikoen ved behandlingen.

Mistanker du et sikkerhetsproblem eller et datalekkasje, meld dette via security@sagafor.me. Saga etterforsker hendelser og iverksetter tiltak for å begrense konsekvensene. Der loven krever det, melder vi en datalekkasje til tilsynsmyndigheten og informerer de berørte personene. Den interne prosedyren for datalekkasjer er en arbeidsinstruks for håndtering, ikke en ekstra forpliktelse for brukere.

11. Brukerrettigheter

Brukere kan, i den grad loven tillater det, be om:

- Innsyn.
- Korrigering.
- Sletting.
- Eksport/dataportabilitet.
- Begrensning av behandling.
- Innvending mot bestemt behandling.
- Tilbakekalling av samtykke.

Kontakt: privacy@sagafor.me.

Du kan se, endre, slette og eksportere data innenfor dine rettigheter i appen. Saga støtter eksport av vaultdata og innstillinger. Dette gir ikke rett til data fra andre brukere som du ikke har tilgang til.

For en personvernforespørsel kan du sende e-post til privacy@sagafor.me. Vi kan be om ytterligere informasjon for å verifisere din identitet. Du mottar som regel svar innen en måned; hvis en lovlig forlengelse er nødvendig, lar vi deg vite dette innen denne måneden med grunnen.

Du kan også klage til Datatilsynet eller en annen kompetent personvernmyndighet. Tilbaketrekking av samtykke gjør ikke tidligere lovlig behandling ulovlig.

12. Cookier og lokal lagring

Se Cookie-erklæring.

13. Tilbakemeldinger og feilrapporter

Se Flyt for tilbakemeldinger og feilrapportering.

14. Slett konto

Se Flyt for sletting av konto.

15. Endringer

Saga kan endre denne personvernerklæringen når appen, lovgivningen eller leverandørene endres. Vi informerer deg om viktige endringer per e-post på adressen til din Saga-konto.

Kontoer under foreldrekontroll

For en konto under foreldrekontroll behandler Saga de dataene som er nødvendige for å koble barnet til omsorgspersonene og administrere samtykke og tilgang. Dette omfatter konto- og kontaktopplysninger, invitasjoner, kontrollinnstillinger og beslutninger om forespørsler.

Koblede omsorgspersoner kan se kontrollinnstillingene, involverte omsorgspersoner, tilgangsrettigheter og relevante forespørsler. De kan også se nettsidene som står på barnets egen kontaktkort, for eksempel en nettside eller profilside. Dette er ikke invitasjonslenkene som Saga bruker til å dele kontaktopplysninger. Foreldrekontroll gir omsorgspersoner ikke automatisk tilgang til innholdet i barnets personlige lagringsplass. For delte data gjelder tilgangsrettighetene til den aktuelle vaulten.

Der foreldresamtykke er lovlig påkrevd, gjelder vilkårene under Juridiske grunnlag. En bruker kan slette sin egen konto under kontroll uten samtykke fra omsorgspersoner, etter bekreftelse via sin egen e-post. For gjenoppretting via foreldrekontroll kreves fortsatt samtykke fra alle koblede omsorgspersoner. Dette begrenser ikke barnets lovlige personvernrettigheter. Barnet eller en berettiget representant kan kontakte oss via privacy@sagafor.me for dette. Saga vurderer hvem som kan gjøre forespørselen og hvilken kontroll som er nødvendig for dette.

Oppbevaringsfrister og informasjon om deling, lokal lagring og sletting av kontoer andre steder i denne erklæringen gjelder også for kontoer under kontroll.