Privacyverklaring

Status	Geldend leveranciersdocument
Versie / uitgiftedatum	1.3 / 5 november 2026
Documenteigenaar	Summa Labs B.V., handelend onder de naam Summa
Classificatie	Publiek

1. Wie is verantwoordelijk?

Summa is een dienst van Summa Labs B.V., een in Nederland ingeschreven besloten vennootschap die handelt onder de naam Summa. Voor verwerkingen waarvoor Summa zelf het doel en de essentiële middelen bepaalt, is Summa Labs B.V. verwerkingsverantwoordelijke.

Gegeven	Waarde
Adres	Sint Annadal 12-D, 6214 PA Maastricht, Nederland
KVK	42164183
BTW-id	NL869994797B01
Contact	info@summalabs.ai (algemene vragen, privacy- en AVG-verzoeken, security- en kwetsbaarheidsmeldingen)

Bij zakelijke werkruimten bepaalt de klant in beginsel waarom medewerkers en andere betrokkenen hun werkgegevens in Summa verwerken. Voor die klantdata treedt Summa doorgaans op als verwerker. Summa blijft zelfstandig verwerkingsverantwoordelijke voor eigen account-, contract-, facturatie-, beveiligings-, fraudepreventie- en wettelijke administratieve verwerkingen.

2. Welke persoonsgegevens verwerken wij?

Afhankelijk van het gebruik kunnen de volgende categorieën worden verwerkt:

- account- en identiteitsgegevens, zoals naam, e-mailadres, organisatie, rol, externe identity-id, aanmeld- en authenticatiegebeurtenissen en voorkeuren;
- wachtlijst- en onboardinggegevens;
- prompts, chatberichten, modelantwoorden, titels, instructies, geheugenfeiten, bestanden, gegenereerde artefacten en bronverwijzingen;
- bedrijfskennis en gegevens die via toegestane integraties door een gebruiker of beheerder beschikbaar worden gemaakt;
- Microsoft 365-mail en -agenda wanneer de gebruiker Summa Work koppelt: een kopie van de mail in de mappen die de gebruiker aan laat staan (onderwerp, tekst, afzender, ontvangers en metadata; bijlagen alleen als naam, type en grootte) en van agenda-items, plus concepten en verzonden berichten die de gebruiker via Summa maakt;
- Teams-vergadermetadata en, na expliciete verwerking van een vergadering, transcript, aanwezigheid en chat voor zover Microsoft deze aan de bevoegde gebruiker beschikbaar stelt;
- usage- en tokengegevens, model- en toolmetadata en auditgebeurtenissen;
- IP-adressen en request-/securitymetadata voor beveiliging en misbruikpreventie; de interne webanalyticsfunctie is ontworpen zonder IP-opslag of een identificator die een dag overleeft;
- factuur- en abonnementsgegevens; volledige betaalkaartgegevens worden door Stripe verwerkt en niet in de Summa-applicatiedatabase opgeslagen;
- support-, privacy-, klacht- en incidentcorrespondentie.

Gebruikers kunnen bijzondere persoonsgegevens of gegevens over derden in vrije tekst invoeren. Summa heeft deze gegevens niet standaard nodig. Klanten en gebruikers moeten dataminimalisatie toepassen en mogen geen wachtwoorden, volledige betaalkaartgegevens of andere authenticatiegeheimen in chats plaatsen.

3. Doeleinden en rechtsgrondslagen

Doel	Grondslag bij Summa als verantwoordelijke
Account aanmaken en dienst leveren	Uitvoering overeenkomst / stappen voorafgaand aan overeenkomst
Persoonlijke AI-chat en functies leveren	Uitvoering overeenkomst
Zakelijke werkruimte op instructie van klant	Verwerkersrol; grondslag wordt door klant bepaald
Facturatie en administratie	Overeenkomst en wettelijke verplichting
Beveiliging, misbruikpreventie en audit	Gerechtvaardigd belang en waar nodig wettelijke verplichting

Support en klachten	Overeenkomst, gerechtvaardigd belang of wettelijke verplichting
Privacyverzoeken en bewijs van afhandeling	Wettelijke verplichting en rechtsvorderingen
Wachtlijst / optionele marketing	Toestemming; altijd intrekbaar
Wettig verzoek van bevoegde autoriteit	Wettelijke verplichting, met toetsing van bevoegdheid en proportionaliteit

Summa gebruikt geen toestemming voor verwerking die objectief noodzakelijk is om de gevraagde contractuele dienst te leveren. Marketingtoestemming staat los van algemene voorwaarden en kan afzonderlijk worden ingetrokken.

4. Hoe werkt AI-verwerking?

De browser communiceert met de Summa-frontend en -backend. De backend is de beleidsgrens: daar worden identiteit, tenant, rechten, quota en tooltoegang gecontroleerd voordat informatie naar een model of tool gaat.

De kernapplicatie, databases, objectopslag, back-ups, zelf gehoste identiteit en AI-inference draaien op Leafcloud-infrastructuur in Nederland; Leafcloud B.V. is de enige infrastructuurprovider. Het model wordt door Summa zelf gehost op GPU-servers van Leafcloud in Nederland (NVIDIA A30); inference draait nergens anders. Prompts en noodzakelijke modelcontext blijven voor de kerninference binnen deze Nederlandse omgeving. Summa gebruikt geen stilzwijgende externe commerciële model-API als fallback.

Klantcontent wordt niet gebruikt om het algemene Summa-model te trainen of fine-tunen, tenzij daarover afzonderlijk, uitdrukkelijk en schriftelijk met de betreffende klant afspraken zijn gemaakt.

AI-output kan feitelijk onjuist, onvolledig, bevooroordeeld of ongeschikt zijn. Belangrijke informatie moet door een mens worden gecontroleerd. De standaarddienst is niet bedoeld om zonder betekenisvolle menselijke beoordeling besluiten met juridische of vergelijkbaar ingrijpende gevolgen over personen te nemen.

5. Tools, bronnen en integraties

Wanneer een gebruiker een tool activeert, worden alleen de gegevens verzonden die redelijkerwijs nodig zijn voor die tool. Webresearch stuurt zoektermen naar Linkup; rechtstreeks openen van publieke webpagina's gebeurt via een eigen, SSRF-afgeschermde retrievalservice en kan bij bepaalde blokkades via Linkup Fetch verlopen.

Sommige functies koppelen Summa aan een dienst die de gebruiker zelf kiest: Google (Inloggen met Google en bestanden importeren uit Google Drive), Microsoft (importeren uit OneDrive/SharePoint en Microsoft 365- of Teams-werkfuncties) en Salesforce (CRM-koppeling, alleen voor zakelijke werkruimtes); daarnaast zijn Dropbox, GitHub en GitLab optionele gegevensbronnen. Deze aanbieders zijn geen subverwerkers van Summa: zij handelen onder hun eigen voorwaarden en privacybeleid, gegevens gaan alleen naar of komen alleen van hen wanneer de functie wordt gebruikt, en zij kunnen persoonsgegevens buiten de EER verwerken. De concrete toegang volgt de OAuth-/appmachtigingen en het tenantbeleid. Dropbox wijkt af doordat de technische OAuth-grant, ondanks alleen-lezen scopes, Full Dropbox-toegang kan hebben; Summa beperkt feitelijke reads applicatief tot door de gebruiker via de Dropbox Chooser geselecteerde objecten. GitLab `read_api` kan technisch breder zijn dan één repository; Summa beperkt gebruik aanvullend via configuratie en gebruikersactie.

6. Ontvangers en locaties

Ontvanger / categorie	Functie	Hoofdlocatie / relevante uitzondering
Leafcloud B.V.	Enige infrastructuurprovider: Kubernetes, compute, opslag, netwerk, back-ups (objectopslag) en zelfgehoste AI-inference op NVIDIA A30 GPU-servers	Nederland
Linkup Technologies SAS	Webzoekfunctie: zoekopdrachten en URL's uit een gesprek wanneer webzoeken wordt gebruikt, en optionele fetch	Frankrijk (EU)
Mailjet SAS (onderdeel van Sinch)	Transactionele e-mail	Europese Unie
Stripe Payments Europe, Ltd. (Ierland) en Stripe-groep	Betalingen, abonnementen, facturen en fraudepreventie	EER, Verenigde Staten en andere Stripe-locaties onder adequaatheidsbesluiten en/of standaardcontractbepalingen; voor sommige activiteiten zelfstandig verwerkingsverantwoordelijke
Door de gebruiker gekozen diensten: Google, Microsoft, Salesforce en andere connectoren	Inloggen, bestandsimport, meetings, repositories of CRM; geen subverwerkers van Summa	Volgens de eigen voorwaarden van de provider; mogelijk buiten de EER
X (Twitter International Unlimited Company, Ierland, en X Corp., Verenigde Staten)	Optionele X-pixel voor advertentiemeting; laadt alleen na toestemming; geen naam, e-	Ierland en Verenigde Staten; eigen privacybeleid van X

	mailadres of gespreksinhoud	

Een actuele, uitgebreidere lijst staat in het register Subverwerkers, integraties en datalocaties. Summa verkoopt persoonsgegevens niet en gebruikt chatinhoud niet voor advertentietargeting.

7. Doorgifte buiten de EER

Wanneer persoonsgegevens buiten de EER worden verwerkt, wordt per relatie een geldige doorgiftegrondslag vereist, bijvoorbeeld een adequaatheidsbesluit, het EU-US Data Privacy Framework waar van toepassing, of de door de Europese Commissie vastgestelde standaardcontractbepalingen met benodigde aanvullende maatregelen. Derde-landverwerking wordt niet verborgen achter de term 'EU-region'.

Mailjet verwerkt transactionele e-mail binnen de Europese Unie; transactionele mails bevatten geen volledige chats, prompts of documenten. Stripe kan persoonsgegevens verwerken in of vanuit landen buiten de EER, waaronder de Verenigde Staten, op basis van adequaatheidsbesluiten en/of standaardcontractbepalingen. Door de gebruiker gekozen diensten en de optionele X-pixel kunnen gegevens buiten de EER verwerken onder hun eigen voorwaarden.

8. Bewaartermijnen

Gegevenscategorie	Standaardtermijn
Lopende wachtlijst	Tot 365 dagen na laatste relevante interactie
Geweigerde/verlopen wachtlijst	90 dagen
Omgezette wachtlijst	Binnen 30 dagen verwijderen/minimaliseren
Gewone chatinhoud	Tot je deze verwijdert of je account wordt beëindigd, tenzij een zakelijk bewaarbeleid een termijn instelt; een verwijderde chat wordt binnen 24 uur definitief uit actieve systemen verwijderd
Tijdelijke chat	Tot sluiting en uiterlijk 24 uur na start; daarna snelle actieve verwijdering
Projecten / bedrijfskennis	Tot verwijdering, tenantbeëindiging of toepasselijk organisatiebeleid; niet louter op leeftijd weggeveegd
OAuth-/connectorcredentials	Tot ontkoppeling, accountwissing of intrekking
Summa Work-kopie van mail en agenda	Zolang het bericht in de mailbox bestaat: verwijderd wanneer het in Outlook wordt verwijderd, de map in Summa Work wordt uitgezet, de koppeling wordt verbroken of het account wordt beëindigd
Teams transcript/attendance/chat	90 dagen voor ruwe vergaderdata; afgeleide notities volgen tenantretentie
Webanalytics ruwe events	90 dagen
Gewone securitylogs	Doeltermijn 90 dagen, tenzij incident/legal hold
Zakelijke auditrecords	Doeltermijn 12 maanden, tenzij overeengekomen of wettelijk langer nodig
Contract-, DPA- en acceptatiebewijs	Relatie plus maximaal 7 jaar waar bewijsbelang dit rechtvaardigt
Facturen/fiscale administratie	7 jaar of wettelijk vereiste termijn
Supportdossiers	2 jaar na afsluiting, tenzij langer nodig voor geschil
Incidentdossiers	5 jaar na afsluiting of langer bij wettelijke noodzaak

Dagelijks worden logische PostgreSQL-backups gemaakt naar Leafcloud-objectopslag in Nederland. Tijdens de gesloten bèta geldt geen herstelgarantie. Na voltooide verwijdering uit actieve systemen kan een kopie in een backup achterblijven totdat die backup volgens de backupcyclus vervalt; zo'n kopie wordt niet teruggezet voor gewone verwerking.

9. Verwijdering en gedeelde ruimten

Een accountwisverzoek wordt door een duurzame workflow verwerkt over PostgreSQL, Redis, de identity-service en gekoppelde observabilitygegevens, met retry en een wisbewijs. In gedeelde ruimten kunnen bijdragen van een vertrekkende gebruiker niet altijd volledig worden verwijderd zonder de rechten en werkcontext van andere deelnemers te beschadigen. In dat geval wordt identiteit/attributie waar passend verwijderd of geredigeerd en blijft gedeelde inhoud onder verantwoordelijkheid van de eigenaar van de gedeelde ruimte bestaan.

10. Rechten van betrokkenen

Afhankelijk van de situatie bestaan rechten op inzage, rectificatie, verwijdering, beperking, overdraagbaarheid, bezwaar en rechten rond uitsluitend geautomatiseerde besluitvorming. Verzoeken kunnen naar info@summalabs.ai. Summa kan noodzakelijke identiteitsverificatie vragen en reageert binnen de wettelijke termijn.

Voor persoonsgegevens waarvoor een zakelijke klant verwerkingsverantwoordelijke is, stuurt Summa het verzoek in beginsel door naar of ondersteunt het de klant. Voor eigen verwerkingen behandelt Summa het verzoek zelf.

11. Beveiliging

Summa gebruikt onder meer tenantafscherming, row-level security, TLS, versleuteling van aangewezen gevoelige velden, private databases/modelendpoints, Kubernetes-netwerkbeleid, malwarecontrole van uploads, secrets-management, CI-tests, dependency- en containerkwetsbaarheidsscans, Gitleaks en gecontroleerde verwijdering. Geen enkel beveiligingssysteem is absoluut; actuele beperkingen en assurance-status staan in de publieke security- en complianceverklaring.

12. Cookies, lokale opslag en analytics

Functionele opslag die nodig is voor authenticatie, beveiliging of gebruikersvoorkeuren kan worden gebruikt. Niet-noodzakelijke tracking of marketingtechnologie wordt alleen ingezet met een passende grondslag/toestemming; dat geldt voor de optionele X-pixel, die alleen laadt nadat de bezoeker daarmee instemt. De huidige interne webanalyticsfunctie is ontworpen als first-party, cookieless analytics zonder IP-opslag of identifier die een dag overleeft. Een afzonderlijke cookie-/local-storage inventaris wordt technisch bijgehouden en bij materiële wijziging in deze privacy-informatie verwerkt.

13. Klachten en toezichthouder

Neem bij privacyvragen eerst contact op via info@summalabs.ai. Een betrokkene kan daarnaast een klacht indienen bij de Autoriteit Persoonsgegevens of, waar van toepassing, een andere bevoegde Europese toezichthouder.

14. Wijzigingen

Materiële wijzigingen in doelen, categorieën, belangrijke ontvangers, locaties of rechten worden transparant gecommuniceerd. Voor zakelijke verwerkingen die een nieuwe verwerkersinstructie vereisen, wordt zo nodig nieuwe contractuele aanvaarding gevraagd.

15. Normenkader

AVG (EU 2016/679), UAVG, relevante Nederlandse telecommunicatie-/cookievoorschriften, EU AI Act voor transparantie, EU Data Act voor data-processing services en toepasselijke consumentenwetgeving.