Verwerkersovereenkomst voor zakelijke klanten

Status	Geldend leveranciersdocument
Versie / uitgiftedatum	1.2 / 5 november 2026
Documenteigenaar	Summa Labs B.V., handelend onder de naam Summa
Classificatie	Publiek / contractueel

1. Reikwijdte en rangorde

Deze verwerkersovereenkomst geldt wanneer Summa persoonsgegevens verwerkt ten behoeve van een zakelijke klant bij de levering van de Summa-dienst. Zij vormt samen met de zakelijke SaaS-voorwaarden, de dienstbeschrijving en de toepasselijke order/nadere overeenkomst één geheel. Bij strijd over verwerking van persoonsgegevens gaat deze verwerkersovereenkomst voor.

Voor Nederlandse gemeenten wordt deze overeenkomst niet gebruikt ter vervanging van de actuele Standaard Verwerkersovereenkomst Gemeenten (VWO). Wanneer de gemeente de VWO v2.54 of een opvolgende versie voorschrijft, geldt die VWO; de feitelijke leveranciersgegevens, TOM's, subprocessors en verwerkingsbeschrijving uit dit pakket kunnen als leveranciersbijlagen worden gebruikt voor zover zij niet met de officiële VWO botsen.

2. Rollen

De klant is verwerkingsverantwoordelijke voor Klantgegevens die medewerkers, opdrachtnemers of andere bevoegde gebruikers in de werkruimte verwerken. Indien de klant zelf verwerker is, treedt Summa op als subverwerker voor zover de klant daartoe bevoegd is.

Summa is zelfstandig verwerkingsverantwoordelijke voor eigen bedrijfsvoering, waaronder contract- en accountadministratie, facturering, beveiliging en misbruikpreventie, wettelijke administratie, leveranciersbeheer en het behandelen van eigen juridische claims. Die verwerkingen vallen onder de Privacyverklaring en niet onder de instructiebevoegdheid van de klant.

3. Onderwerp, aard en doel

Onderdeel	Verwerking
Onderwerp	Leveren en beveiligen van een organisatiebeheerde AI-werkruimte
Duur	Gedurende de overeenkomst en de overeengekomen verwijder-/exitperiode
Aard	Opslaan, ophalen, structureren, doorzoeken, analyseren, transformeren, genereren, beveiligen, exporteren en verwijderen op instructie van klant
Doelen	AI-assistentie; samenwerking; bestanden/kennis; optionele connectoren/tools; beheer; gebruiksregistratie; security; support; export en verwijdering
Betrokkenen	Medewerkers, opdrachtnemers, beheerders, vertegenwoordigers en personen die in Klantgegevens voorkomen
Categorieën	Identiteit/zakelijke contactgegevens; prompts/antwoorden; bestanden; project- en bedrijfskennis; instructies/geheugen waar toegestaan; meetinggegevens; toolresultaten; gebruiks-, audit- en beveiligingsmetadata
Bijzondere/strafrechtelijke gegevens	Niet noodzakelijk voor de gewone dienst; alleen indien klant daar een rechtmatige grondslag, noodzaak en passende aanvullende maatregelen voor heeft vastgesteld

4. Gedocumenteerde instructies

Summa verwerkt Klantpersoonsgegevens uitsluitend voor de overeengekomen dienst, volgens door bevoegde klantbeheerders ingestelde configuraties, schriftelijke aanvullende instructies en toepasselijk recht. Indien een instructie naar het redelijke oordeel van Summa in strijd is met privacyrecht, meldt Summa dit en schort zij het betreffende deel op totdat de instructie is verduidelijkt of rechtmatig kan worden uitgevoerd.

Wanneer wetgeving Summa verplicht tot verwerking buiten instructie van de klant, informeert Summa de klant vooraf, tenzij dit wettelijk verboden is.

5. Geheimhouding en toegang

Personen die onder gezag van Summa toegang kunnen krijgen tot Klantpersoonsgegevens zijn gebonden aan vertrouwelijkheid en krijgen uitsluitend toegang voor aantoonbare operationele noodzaak. Bevoegdheden volgen least privilege, rolgebonden toegang en periodieke beoordeling. Platformbeheer geeft geen algemene functionele bevoegdheid om klantgesprekken te lezen.

6. Beveiliging

Summa handhaaft de maatregelen uit document 09, waaronder tenantisolatie, PostgreSQL row-level security, versleuteld transport, veldversleuteling van geselecteerde gevoelige velden, secretmanagement, private interne services, netwerkpolicies, securityscans, malwarecontrole op uploads, incidentafhandeling en gecontroleerde verwijdering.

De actuele release maakt dagelijks logische PostgreSQL-backups naar Leafcloud-objectopslag in Nederland, maar biedt tijdens de gesloten bèta geen herstelgarantie. Dit is een materiële beperking. Gebruik voor productie met gegevens die niet verloren mogen gaan vereist eerst een succesvolle hersteltest volgens document 15.

7. Subverwerkers en andere ontvangers

De klant verleent algemene toestemming voor de in document 07 als subverwerker aangemerkte partijen. Summa:

- legt relevante artikel 28 AVG-verplichtingen contractueel door;
- blijft verantwoordelijk voor de eigen keuze en aansturing van subverwerkers volgens wet en overeenkomst;
- publiceert het actuele register;
- geeft zakelijke klanten ten minste 30 dagen vooraf kennis van een materiële nieuwe of vervangende subverwerker die Klantpersoonsgegevens verwerkt, tenzij een urgente beveiligingsnoodzaak een kortere invoering vereist; in dat geval volgt kennisgeving zo snel mogelijk.

Een klant kan binnen de kennisgevingstermijn gemotiveerd bezwaar maken op gegevensbeschermingsgronden. Partijen zoeken eerst een redelijke oplossing. Is die niet beschikbaar, dan kan de klant het uitsluitend getroffen onderdeel of, indien dat niet scheidbaar is, de dienst beëindigen zonder beëindigingsboete voor het ongebruikte vooruitbetaalde deel.

Diensten die de klant of gebruiker zelf kiest te koppelen, zoals Google (Inloggen met Google, Google Drive), Microsoft (OneDrive, Microsoft 365/Teams), Salesforce (alleen zakelijke werkruimtes), Dropbox, GitHub of GitLab, zijn geen subverwerkers van Summa: zij handelen onder hun eigen voorwaarden en privacybeleid, gegevens stromen alleen wanneer de functie wordt gebruikt, en zij kunnen persoonsgegevens buiten de EER verwerken. Document 07 maakt dit onderscheid expliciet.

8. Doorgifte buiten de EER

Summa brengt Klantpersoonsgegevens niet buiten de EER via een door Summa geselecteerde subverwerker zonder toepasselijke doorgiftegrondslag en noodzakelijke aanvullende beoordeling/maatregelen. In de actuele architectuur bevinden de kernapplicatie, opslag, back-ups en zelfgehoste modelinference zich op Leafcloud in Nederland; Leafcloud B.V. is de enige infrastructuurprovider. Mailjet verwerkt transactionele e-mail binnen de EU; transactionele e-mails bevatten geen volledige prompts, antwoorden of documenten. Stripe kan voor betalingen gegevens buiten de EER verwerken op basis van adequaatheidsbesluiten en/of standaardcontractbepalingen.

Voor optionele klantgekozen connectoren kan gegevensverkeer naar de door de klant gebruikte externe provider optreden. Dit wordt als expliciete functie en gegevensstroom beschreven in document 07/10.

9. Rechten van betrokkenen

Summa ondersteunt de klant, rekening houdend met de aard van de verwerking, bij verzoeken om inzage, rectificatie, verwijdering, beperking, overdraagbaarheid, bezwaar en relevante rechten rond geautomatiseerde besluitvorming. Summa reageert niet zelfstandig namens de klant op inhoudelijke werkruimtegegevens tenzij daartoe gemachtigd of wettelijk verplicht.

Voor eigen controllerverwerkingen behandelt Summa verzoeken rechtstreeks via info@summalabs.ai.

10. Datalekken en beveiligingsincidenten

Bij een bevestigde inbreuk op Klantpersoonsgegevens meldt Summa dit zonder onredelijke vertraging aan de klant. De interne doelstelling is een eerste melding binnen 24 uur na bevestiging. De eerste melding bevat voor zover beschikbaar: aard en tijdlijn; betrokken systemen en gegevenscategorieën; bekende/geschatte omvang; waarschijnlijke gevolgen; getroffen beheersmaatregelen; actuele status; contactpunt en vervolgafspraken.

De klant blijft verantwoordelijk voor zijn eigen meldplicht aan toezichthouders/betrokkenen, tenzij anders uit wet volgt. Summa verleent redelijke medewerking.

11. DPIA, toezicht en informatie

Summa levert op redelijk verzoek informatie die nodig is om de klant te helpen met AVG-verplichtingen, waaronder DPIA, beveiligingsbeoordeling en voorafgaande raadpleging. Voor gemeenten is hiervoor document 21 bedoeld.

12. Audit en bewijs

Summa stelt eerst bestaande, proportionele bewijsmiddelen beschikbaar: TOM's, architectuur, relevante beleidstukken, subprocessorregister, test-/scanresultaten en beschikbare onafhankelijke assurance. Indien dat onvoldoende is, mag de klant maximaal eenmaal per twaalf maanden een proportionele audit laten uitvoeren en daarnaast na een ernstig incident of concrete aanwijzing van wezenlijke tekortkoming.

Audits beschermen andere klanten en securitygevoelige informatie, worden in beginsel tijdens werkuren uitgevoerd door een deskundige onafhankelijke partij en beperken verstoring. Gewone auditkosten zijn voor de klant; indien de audit een materiële tekortkoming van Summa aantoont, draagt Summa haar redelijke eigen herstel- en verificatiekosten volgens de overeenkomst.

13. Teruggave en verwijdering

Tijdens de overeenkomst kan de klant beschikbare gegevens exporteren. Na beëindiging krijgt de klant in beginsel minimaal 30 dagen voor een laatste export, tenzij de klant onmiddellijke verwijdering opdraagt of recht dit vereist. Daarna verwijdert Summa actieve Klantgegevens volgens document 08 en levert op verzoek een verwijderingsverklaring.

Voor gedeelde ruimten kan verwijdering van een individuele auteur ertoe leiden dat diens bijdrage wordt geredigeerd terwijl het gezamenlijke record voor overige rechthebbenden blijft bestaan. Dat voorkomt dat één individuele verwijdering gegevens van andere betrokken gebruikers vernietigt.

Backups vervallen via de backupcyclus en worden niet teruggezet voor gewone verwerking nadat een verwijdering is voltooid, behalve indien herstel van de gehele dienst noodzakelijk is; dan wordt de verwijderingslogica opnieuw toegepast.

14. Overheidsverzoeken

Summa beoordeelt een verzoek om toegang op bevoegde instantie, rechtsgrond, reikwijdte en proportionaliteit; verstrekt niet meer dan wettelijk noodzakelijk; maakt waar rechtmatig bezwaar tegen ongeldige of disproportionele verzoeken; en informeert de klant tenzij dit wettelijk verboden is. Zie document 10.

15. Einde en wijziging

Deze verwerkersovereenkomst geldt zolang Summa voor de klant Klantpersoonsgegevens verwerkt. Een wijziging die categorieën verwerking, materiële securitymaatregelen, internationale routes of subprocessors wezenlijk verandert, wordt versieerbaar vastgelegd en waar nodig opnieuw overeengekomen.