Security-, trust- en complianceverklaring

Status	Geldend leveranciersdocument
Versie / uitgiftedatum	1.0 / 28 augustus 2026
Documenteigenaar	Schmeitzke, handelend onder de namen Summa en Summa Labs
Classificatie	Publiek

1. Doel

Deze verklaring geeft klanten één leesbare samenvatting van wat Summa aantoonbaar heeft ingericht en wat nog niet als externe assurance of certificering mag worden voorgesteld.

2. Aantoonbaar ingericht

- Nederlandse kernapplicatie, database, objectstorage en self-hosted identity op Leafcloud.
- Actieve zelfgehoste AI-inference op Leafcloud in Nederland, op NVIDIA RTX 6000-serie GPU's via een private, geauthenticeerde interne route.
- Tenantautorisatie met backendpolicy en PostgreSQL RLS.
- Encryptie in transit en tenant-scoped veldversleuteling voor relevante gevoelige velden.
- Private interne model-/data-/toolservices en Kubernetes network policies.
- Malwarecontrole en begrensde documentextractie.
- Geïsoleerde Python sandbox zonder netwerk/secrets/persistent volume/Kubernetes token.
- CI: tests, lint/typecheck, migration checks, Gitleaks, dependency audits, Trivy, CycloneDX SBOM backend/frontend, OSV second-source CVE gate.
- Durable account erasure met componentretries.
- Gescheiden privacy/securitycontactpunten.
- AI-interactiedisclosure in de productervaring en AI-generated metadata in dataexports.

3. Geen geclaimde certificeringen

Summa is op uitgiftedatum niet door dit document gecertificeerd als ISO 27001-, SOC 2-, BIO2-, NEN-, ENSIA- of GIBIT-compliant. Leverancierscertificaten, bijvoorbeeld van infrastructuurproviders, zijn bewijs over die provider en niet automatisch over Summa.

4. Huidige beperkingen

De live deployment heeft geen off-cluster backup en geen gevalideerde productie-RPO/RTO. Platformbrede MFA-enforcement staat uit; alleen het eigenaaroppervlak vereist MFA. Audit-digest signing staat uit. Een volledige onafhankelijke penetratietest/TPM/ISO-assurance is niet als Summa-bewijs beschikbaar in dit pakket.

Daarom wordt gemeentelijke productie met kritieke of niet-vervangbare informatie pas vrijgegeven nadat de releasegate in document 00 is gesloten.

5. Privacy- en datasoevereiniteit

Summa verkoopt klantgesprekken niet en gebruikt zakelijke Klantgegevens niet voor algemene modeltraining zonder afzonderlijke schriftelijke afspraak. Kernopslag en kerninference bevinden zich in Nederland op Leafcloud. Resend/Stripe en klantgekozen connectoren kunnen andere jurisdicties creëren zoals in document 07 beschreven. "Sovereign" betekent daarom controleerbare keuzes, Nederlandse kernverwerking en transparante uitzonderingen, niet een onbeperkte absolute claim.

6. Responsible disclosure

Kwetsbaarheden kunnen vertrouwelijk worden gemeld via security@summalabs.ai. Verstrek voldoende reproduceerbare informatie en vermijd onnodige inzage/wijziging van echte klantdata, social engineering, denial-of-service of publicatie

voordat een redelijke hersteltermijn is geboden. Summa bevestigt ontvangst zo snel mogelijk, triageert op ernst en coördineert waar passend herstel/publicatie.

7. Beschikbaar bewijs voor due diligence

Onder redelijke vertrouwelijkheid kan Summa relevante delen beschikbaar stellen van TOM's, architectuur/dataflows, privacydossier, AI-dossier, GIBIT/BIO2-mappings, CI/securityscanbeleid, SBOM, incident-/continuïteitsbeleid, subprocessorregister en herstel-/exitprocedures. Secrets, exploiteerbare details, persoonsgegevens van andere klanten en onevenredig gevoelige infrastructuurinformatie worden niet verstrekt.

8. Onafhankelijke assurance-roadmap

Voor reguliere gemeentelijke SaaS-productie is de doelroute een jaarlijks vernieuwde onafhankelijke assurance die voldoet aan GIBIT 2025 artikel 38, bijvoorbeeld een passend ISO-certificaat, TPM of toegelaten equivalent van een onafhankelijke deskundige. Dit document is nadrukkelijk geen vervanging van die externe verklaring.