Gaply

GAPLY B.V. · JURIDISCH

Beveiligingsmaatregelen

Security Measures — bijlage bij de Verwerkersovereenkomst (DPA)

VERSIE	DATUM	CONTACT
1.0	02-09-2026	info@gaply.nl

Beveiligingsmaatregelen (Security Measures) — Gaply B.V.

Versie: 1.0 · **Datum:** 02-09-2026 · Onderdeel van de Verwerkersovereenkomst (DPA), artikel 7.2.

1. Encryptie

Al het externe verkeer loopt via TLS 1.2/1.3 met redirect van HTTP naar HTTPS. Alle opslag — database, bestandsopslag en back-ups — is versleuteld met AES-256. OAuth-tokens van gekoppelde diensten (zoals Google Search Console) worden aanvullend applicatie-niveau versleuteld met AES-256-GCM; API-sleutelgeheimen met een daarvan afgeleide sleutel (HKDF-SHA256).

2. Toegangsbeheer

Rolgebaseerd toegangsmodel met capabilities per organisatie, project en omgeving, per kanaal (UI, REST, MCP) instelbaar. Beheer via persoonlijke accounts; platformbeheer (super-admin) is gescheiden van klanttoegang. Rechten worden toegekend volgens least privilege en zijn per rol granulair te beheren. API-sleutels zijn omgevingsgebonden, met toegestane origins en rate limits.

3. Datascheiding per klant

Alle klantdata — kennisbank, zoekindex/embeddings, logs, instellingen en metingen — is gebonden aan de eigen omgeving van de klant. Er is geen gedeelde index en geen kruislezing tussen organisaties; elke leesroute wordt op omgevings-scope geautoriseerd.

4. Productieomgevingen

Schrijfacties op productieomgevingen via API/MCP zijn per capability beperkt (toegestaan / alleen configuratie / geblokkeerd). Test- en productieomgevingen zijn gescheiden; productie-persoonsgegevens worden niet naar test- of ontwikkelomgevingen gekopieerd.

5. Gegevens van eindgebruikers (bezoekers)

IP-adressen van eindgebruikers worden niet opgeslagen; zij worden bij ontvangst uitsluitend gebruikt voor misbruikdetectie en het herkennen van intern verkeer. Er worden geen cookies of persistente identifiers gezet in de zoek- en chatinterfaces. Contactgegevens (e-mailadressen, telefoonnummers, BSN-achtige nummers) worden vóór opslag uit vraagteksten gefilterd. Zoek- en chatvragen en antwoorden worden standaard maximaal 365 dagen bewaard (per project instelbaar), waarna automatische verwijdering; geaggregeerde maandstatistieken zonder identifiers blijven behouden.

6. AI-verwerking

Taalmodellen worden uitsluitend aangeroepen via zero-data-retention-endpoints: prompts en antwoorden worden door de modelleverancier niet bewaard en niet voor training gebruikt. Gaply traint zelf niet op klantdata. De zoek- en chatinterfaces maken bij elk antwoord kenbaar dat het door AI is gegenereerd, met bronvermelding naar de bronpagina.

7. Logging & monitoring

24/7 monitoring met alerting op infrastructuur- en applicatieniveau. Auditlogging van beheerhandelingen (wie, wat, wanneer). Technische applicatielogs worden 30 dagen bewaard, loadbalancer-logs 90 dagen. Foutregistratie bevat geen IP-adressen van eindgebruikers.

8. Back-ups

Geautomatiseerde, versleutelde database-back-ups met point-in-time-herstel; bewaartermijn 30 dagen. Verwijderde gegevens verdwijnen daarmee uiterlijk 30 dagen na verwijdering ook uit de back-ups.

9. Ontwikkel- en wijzigingsbeheer (SDLC)

Alle wijzigingen lopen via versiebeheer met verplichte review, geautomatiseerde kwaliteits- en beveiligingscontroles (statische analyse, dependency-audit, tests) en beschermde uitrol naar productie. Supply-chain-hardening op dependencies: nieuwe pakketversies zijn pas na een wachttermijn installeerbaar, install-scripts worden expliciet beoordeeld en herkomst-downgrades worden geweigerd. Secrets staan in een beheerde kluis en worden alleen via machine-identiteiten uitgelezen.

10. Incident response

Vastgesteld incident-response-proces. Beveiligingsincidenten worden zonder onredelijke vertraging aan de Klant gemeld conform artikel 10 van de DPA, waar redelijkerwijs mogelijk binnen 48 uur of binnen de kortere termijn die voor het betreffende project is overeengekomen.

11. Subverwerkers

De actuele subverwerkers, hun verwerkingslocatie en de doorgiftegrondslag staan in Bijlage 3 van de DPA. Subverwerkers krijgen ten minste dezelfde gegevensbeschermingsverplichtingen opgelegd; materiële wijzigingen worden vooraf aangekondigd met een bezwaarprocedure.

12. Audits & bewijs

Op verzoek verstrekt Gaply redelijke informatie om naleving aan te tonen (artikel 12 van de DPA), waaronder deze bijlage, de subverwerkerslijst en acceptatie-/auditlogs. Acceptaties van juridische documenten worden vastgelegd met tijdstip, versie en controlegetal (hash) van de aanvaarde tekst.