VERWERKERSOVEREENKOMST (DPA) – RAGENTLY

Laatst bijgewerkt: 20-08-2026

Deze verwerkersovereenkomst ("DPA") vormt een juridisch bindende aanvulling op de overeenkomst tussen:

• de Klant ("Verwerkingsverantwoordelijke" / "Controller") – de partij die persoonsgegevens van haar klanten verwerkt via haar webshop of andere kanalen;
• Ragently VOF ("Verwerker" / "Processor"), gevestigd in Nederland – aanbieder van AI-klantenservice- en automatiseringssoftware.

Deze DPA is opgesteld in overeenstemming met de Algemene Verordening Gegevensbescherming (AVG / GDPR).

ARTIKEL 1 – ONDERWERP VAN DE VERWERKING

1. Ragently verwerkt persoonsgegevens uitsluitend namens en in opdracht van de Controller, en niet voor eigen doeleinden.
2. De verwerking omvat onder andere: opslag, structurering, analyse, doorgifte, raadpleging en verwijdering.
3. De categorieën van persoonsgegevens omvatten: naam, e-mailadres, adres, telefoonnummer, ordergegevens, chatgesprekken (inclusief bijlagen) en door de Controller geüploade documenten.
4. Categorieën van betrokkenen: klanten en websitebezoekers van de Controller, en medewerkers van de Controller die het platform gebruiken.
5. De Controller behoudt te allen tijde volledige zeggenschap over de verwerking.

ARTIKEL 2 – DUUR VAN DE VERWERKING

Deze DPA blijft van kracht zolang Ragently persoonsgegevens verwerkt namens de Controller en eindigt bij beëindiging van de hoofdovereenkomst, tenzij anders overeengekomen.

ARTIKEL 3 – VERPLICHTINGEN VAN RAGENTLY (PROCESSOR)

Ragently verplicht zich tot:
a) Verwerking uitsluitend volgens schriftelijke of gedocumenteerde instructies van de Controller.
b) Minimalisatie van dataverwerking en doelbinding.
c) Geheimhouding: toegang tot persoonsgegevens is beperkt tot een klein aantal geautoriseerde personen dat aan geheimhouding is gebonden.
d) Implementatie van passende technische en organisatorische beveiligingsmaatregelen, waaronder:
  – versleutelde verbindingen (TLS) voor alle gegevensoverdracht,
  – versleutelde opslag van gevoelige gegevens zoals toegangstokens,
  – toegangscontrole op basis van rollen en strikte scheiding per klantomgeving (tenant-isolatie),
  – logging van fouten en beveiligingsrelevante gebeurtenissen,
  – dagelijkse versleutelde back-ups met een kopie op een gescheiden locatie,
  – gescheiden productie- en ontwikkelomgevingen.
e) Het melden van beveiligingsincidenten met betrekking tot persoonsgegevens aan de Controller zonder onredelijke vertraging, en uiterlijk binnen 72 uur nadat het incident bij Ragently bekend is geworden.
f) Assistentie bieden aan de Controller bij verzoeken van betrokkenen (inzage, correctie, verwijdering, dataportabiliteit) en, waar relevant, bij gegevensbeschermingseffect- beoordelingen.
g) Het niet inschakelen van subverwerkers zonder passend toezicht en contractuele garanties (zie artikel 5).
h) Authenticatie en autorisatie via OAuth 2.0 en beveiligde, kortlopende tokens.

ARTIKEL 4 – VERPLICHTINGEN VAN DE CONTROLLER

De Controller is verantwoordelijk voor:
a) Een geldige juridische grondslag voor het verzamelen van persoonsgegevens.
b) Het juist en transparant informeren van betrokkenen, waaronder het informeren van websitebezoekers

over het gebruik van de AI-chatfunctie.
c) Het rechtmatig gebruik van de functies van het platform, waaronder ingestelde bewaartermijnen.
d) Aanlevering van correcte, rechtmatige, veilige en niet-inbreukmakende informatie en inhoud.
e) Tijdige communicatie van wijzigingen in bedrijfsvoering of privacybeleid die de verwerking raken.

ARTIKEL 5 – SUBVERWERKERS

1. Ragently mag subverwerkers inschakelen mits deze voldoen aan gelijkwaardige beveiligingsnormen en contractuele verplichtingen.
2. Een actuele lijst met subverwerkers is gepubliceerd op https://ragently.nl/subverwerkers. Bij wijzigingen wordt deze pagina bijgewerkt; de Controller kan tegen een nieuwe subverwerker schriftelijk bezwaar maken binnen 30 dagen na publicatie.
3. Ragently blijft volledig verantwoordelijk en aansprakelijk voor de subverwerkers die zij inschakelt.
4. Koppelingen die de Controller zelf activeert (zoals CRM-, agenda-, of notificatie-integraties) gelden als een instructie van de Controller om gegevens met de betreffende dienst te delen; de Controller is verantwoordelijk voor haar eigen relatie met die dienst.

ARTIKEL 6 – BEVEILIGING

Ragently implementeert passende beveiligingsmaatregelen overeenkomstig art. 32 AVG, zoals beschreven in artikel 3 onder d. Ragently evalueert deze maatregelen periodiek en past ze aan wanneer de stand van de techniek of het risico daartoe aanleiding geeft.

ARTIKEL 7 – INTERNATIONALE DATADOORGIFTE

Indien doorgifte buiten de EU/EER plaatsvindt (bijvoorbeeld naar AI-aanbieders in de Verenigde Staten), gebeurt dit op basis van een geldig doorgiftemechanisme conform hoofdstuk V AVG, zoals Standard Contractual Clauses (SCC's) of een adequaatheidsbesluit (waaronder het EU-U.S. Data Privacy Framework). Zie de subverwerkerspagina voor de locatie per subverwerker.

ARTIKEL 8 – AUDITRECHTEN

1. De Controller heeft het recht jaarlijks een audit uit te voeren.
2. Audits moeten vooraf worden aangekondigd, proportioneel zijn en de bedrijfsvoering van Ragently niet onnodig verstoren.
3. Ragently zal redelijke medewerking verlenen en kan in eerste instantie volstaan met het aanleveren van relevante documentatie.

ARTIKEL 9 – BEËINDIGING EN VERWIJDERING

Na beëindiging van het contract:
• worden persoonsgegevens binnen 30 dagen verwijderd of onomkeerbaar geanonimiseerd, tenzij een wettelijke bewaarplicht anders vereist;
• wordt alle toegang tot de gegevens beëindigd;
• verdwijnen verwijderde gegevens door de automatische back-uprotatie binnen maximaal 14 dagen ook uit de back-ups.

ARTIKEL 10 – AANSPRAKELIJKHEID

Partijen zijn aansprakelijk zoals vastgelegd in de onderliggende hoofdovereenkomst (de algemene voorwaarden van Ragently, tenzij schriftelijk anders overeengekomen). Indien strijdig, prevaleert de hoofdovereenkomst boven deze DPA, met uitzondering van bepalingen die dwingend uit de AVG voortvloeien.

ARTIKEL 11 – VERZOEKEN VAN OVERHEDEN EN OPSPORINGSINSTANTIES

1. Ragently verstrekt geen persoonsgegevens die zij namens de Controller verwerkt aan overheidsinstanties, tenzij zij daartoe wettelijk verplicht is op grond van een bindend en geldig bevel. Informele of vrijwillige verzoeken worden geweigerd.

2. Ragently beoordeelt elk verzoek op rechtsgeldigheid: de bevoegdheid van de instantie, de wettelijke grondslag, de vorm van het bevel en de reikwijdte ervan.
3. Ragently stelt de Controller onverwijld op de hoogte van elk verzoek dat gegevens betreft die Ragently namens de Controller verwerkt, tenzij dat wettelijk verboden is; in dat geval spant Ragently zich in om die beperking te laten opheffen of beperken. Waar dat mogelijk is verwijst Ragently de instantie door naar de Controller als verwerkingsverantwoordelijke.
4. Ragently maakt bezwaar tegen verzoeken die zij onrechtmatig, te ruim geformuleerd of buitenproportioneel acht, en schakelt daarbij zo nodig juridische bijstand in.
5. Indien verstrekking uiteindelijk verplicht is, blijft deze beperkt tot het strikt noodzakelijke minimum dat het bevel vereist.
6. Ragently legt elk verzoek vast in een intern register, met daarin ten minste: datum, instantie, opgegeven wettelijke grondslag, gevraagde gegevens, de juridische afweging, de betrokken personen en de gegeven reactie.

ARTIKEL 12 – SLOTBEPALINGEN

1. Wijzigingen in deze DPA dienen schriftelijk te worden overeengekomen; bij een nieuwe gepubliceerde versie geldt de versie die van kracht was bij het aangaan van de hoofdovereenkomst, tenzij de Controller met de nieuwe versie instemt.
2. Indien enige bepaling ongeldig blijkt, blijven de overige bepalingen volledig van kracht.
3. Deze DPA wordt beheerst door Nederlands recht.