

Heyloha Verwerkersovereenkomst

Versie: 1.3

Ingangsdatum: de datum waarop deze overeenkomst als laatste door de Partijen is ondertekend.

Vorm: sjabloon voor klanten. Partijen kunnen de invulvelden aanvullen en dit document als zelfstandige verwerkersovereenkomst sluiten.

Taal: Deze Nederlandse versie is een vertaling van de Engelse versie 1.3 (Heyloha Data Processing Agreement). Bij verschillen tussen beide versies is de Engelse versie leidend.

Partijen

Heyloha by Covalore B.V. — een besloten vennootschap met beperkte aansprakelijkheid naar Nederlands recht, statutair gevestigd te Utrecht en kantoorhoudende aan Regentesselaan 65, 3571 CB Utrecht, Nederland, ingeschreven bij de Nederlandse Kamer van Koophandel onder nummer 99942992 (in deze overeenkomst aangeduid als "**Heyloha**").

Klant — _____ (statutaire naam), _____
(statutaire zetel, adres en inschrijvingsnummer) (in deze overeenkomst aangeduid als "**Klant**").

Ieder afzonderlijk een "**Partij**" en gezamenlijk de "**Partijen**".

Overwegingen

A. Partijen hebben een afzonderlijke overeenkomst gesloten op grond waarvan Heyloha haar AI-agentplatform aan de Klant beschikbaar stelt (de "**Dienstverleningsovereenkomst**"). De Dienstverleningsovereenkomst, tezamen met eventuele orderformulieren, configuratie-instrumenten en dashboardinstellingen, bepaalt de omvang van de diensten die Heyloha aan de Klant levert (de "**Diensten**").

B. Bij de levering van de Diensten verwerkt Heyloha Persoonsgegevens namens de Klant.

C. Deze Verwerkersovereenkomst (de "**Verwerkersovereenkomst**") legt de voorwaarden vast waaronder Heyloha die Persoonsgegevens verwerkt en vormt een aanvulling op de Dienstverleningsovereenkomst. Zij beoogt te voldoen aan artikel 28 van Verordening (EU) 2016/679 ("**AVG**") en aan de toepasselijke overeenkomstige bepalingen van het Britse en het Zwitserse gegevensbeschermingsrecht.

D. Begrippen met een hoofdletter die niet in de tekst van deze Verwerkersovereenkomst zijn gedefinieerd, hebben de betekenis die daaraan wordt gegeven in §11 (Definities) of, bij gebreke daarvan, in de Dienstverleningsovereenkomst en de AVG.

1. Onderwerp, rollen en rangorde

1.1 Rollen. Ten aanzien van Persoonsgegevens van eindgebruikers, werknemers, leveranciers en andere natuurlijke personen van de Klant die Heyloha verwerkt in het kader van de levering van de Diensten, is de Klant de Verwerkingsverantwoordelijke en is Heyloha de Verwerker. Voor zover de Klant zelf Verwerker is die handelt namens een derde Verwerkingsverantwoordelijke, treedt Heyloha op als Subverwerker en gelden dezelfde verplichtingen mutatis mutandis.

1.2 **Onderwerp, aard, doel, duur.** Uiteengezet in Bijlage I.

1.3 **Rangorde.** In geval van tegenstrijdigheid tussen deze Verwerkersovereenkomst, de Dienstverleningsovereenkomst en een orderformulier geldt de volgende rangorde: (i) deze Verwerkersovereenkomst, (ii) het orderformulier, (iii) de Dienstverleningsovereenkomst.

2. Verplichtingen van Heyloha als Verwerker

2.1 Instructies van de Klant. Heyloha verwerkt Persoonsgegevens uitsluitend op basis van de gedocumenteerde instructies van de Klant. De instructies van de Klant worden gevormd door deze Verwerkersovereenkomst, de Dienstverleningsovereenkomst, de configuraties die de Klant in het Heyloha-dashboard toepast en de AI-agents die de Klant beheert. Met uitzondering van de beperkte instructie in §2.12 (geaggregeerde en geanonimiseerde statistieken) verwerkt Heyloha Persoonsgegevens niet voor enig ander doel, waaronder haar eigen marketing, profilering of productontwikkeling, tenzij zij daartoe verplicht is op grond van Unierecht of het recht van een lidstaat waaraan Heyloha is onderworpen; in dat geval stelt Heyloha de Klant vóór de verwerking op de hoogte van dat wettelijke vereiste, tenzij dat recht die kennisgeving verbiedt.

2.2 Melding bij onrechtmatige instructies. Indien een instructie van de Klant naar het redelijk oordeel van Heyloha inbreuk maakt op de AVG of op een andere toepasselijke gegevensbeschermingsbepaling, stelt Heyloha de Klant daarvan zonder onredelijke vertraging in kennis.

2.3 Vertrouwelijkheid van personeel. Heyloha waarborgt dat alle personen die gemachtigd zijn Persoonsgegevens te verwerken, gebonden zijn aan een passende geheimhoudingsplicht, hetzij op grond van een overeenkomst hetzij op grond van de wet, en dat zij een passende training hebben gevolgd over hun verplichtingen inzake gegevensbescherming.

2.4 Beveiliging (artikel 32). Heyloha treft en handhaaft de technische en organisatorische maatregelen die zijn uiteengezet in Bijlage II, rekening houdend met de stand van de techniek, de uitvoeringskosten en de aard, omvang, context en doeleinden van de verwerking, alsmede met het risico voor de rechten en vrijheden van natuurlijke personen. Heyloha mag die maatregelen van tijd tot tijd bijwerken, mits het beschermingsniveau niet wezenlijk wordt verlaagd.

2.5 Verzoeken van betrokkenen. Rekening houdend met de aard van de verwerking, verleent Heyloha de Klant door middel van passende technische en organisatorische maatregelen, voor zover mogelijk, bijstand bij het nakomen van haar plicht om verzoeken van betrokkenen tot uitoefening van hun rechten uit hoofde van Hoofdstuk III van de AVG (artikelen 15–22) te beantwoorden. Indien Heyloha een dergelijk verzoek rechtstreeks van een betrokkene ontvangt met betrekking tot Persoonsgegevens die namens de Klant worden verwerkt, zal Heyloha (i) niet anders op het verzoek reageren dan door de ontvangst te bevestigen en de betrokkene naar de Klant te verwijzen, en (ii) de Klant zonder onredelijke vertraging op de hoogte stellen, zodat de Klant het verzoek als Verwerkingsverantwoordelijke kan afhandelen.

2.6 Bijstand bij overige nalegingsverplichtingen van de Klant. Rekening houdend met de aard van de verwerking en de aan Heyloha ter beschikking staande informatie, verleent Heyloha de Klant redelijke bijstand bij het nakomen van haar verplichtingen uit hoofde van de artikelen 32 tot en met 36 van de AVG (beveiliging, melding van inbreuken, gegevensbeschermingseffectbeoordelingen en voorafgaande raadpleging).

2.7 Inbreuk in verband met persoonsgegevens. Heyloha stelt de Klant van iedere Inbreuk in verband met persoonsgegevens die de Persoonsgegevens van de Klant betreft in kennis zonder onredelijke vertraging en in ieder geval binnen tweeënzeventig (72) uur nadat Heyloha er kennis van heeft genomen. De kennisgeving

bevat de in artikel 33, lid 3, AVG genoemde informatie voor zover die op dat moment bij Heyloha bekend is, en wordt aangevuld naarmate meer informatie beschikbaar komt. Kennisgevingen worden verzonden naar de voor de Klant in het Heyloha-dashboard vastgelegde contactadressen.

2.8 Audit. Heyloha stelt de Klant alle informatie ter beschikking die redelijkerwijs noodzakelijk is om aan te tonen dat de in deze Verwerkersovereenkomst neergelegde verplichtingen worden nagekomen. De Klant mag, met een voorafgaande schriftelijke kennisgeving van ten minste dertig (30) dagen en niet meer dan eenmaal per twaalf maanden (of vaker indien verzocht door een bevoegde toezichthoudende autoriteit of na een wezenlijke Inbreuk in verband met persoonsgegevens), de naleving door Heyloha van deze Verwerkersovereenkomst controleren. Heyloha mag aan deze verplichting voldoen, waar passend, door het verstrekken van auditrapporten van derden, certificeringen, ingevulde, in de sector gangbare standaardvragenlijsten en de in Bijlage II genoemde documenten. Audits worden uitgevoerd tijdens kantooruren, met minimale verstoring van de bedrijfsvoering van Heyloha, en op kosten van de Klant; beide Partijen behandelen auditbevindingen als vertrouwelijk.

2.9 Subverwerkers: algemene toestemming. De Klant verleent Heyloha hierbij een algemene schriftelijke toestemming om Subverwerkers in te schakelen ter ondersteuning van de levering van de Diensten. De op de Ingangsdatum ingeschakelde Subverwerkers zijn opgenomen in Bijlage III. Heyloha stelt de Klant vooraf in kennis van iedere toevoeging of vervanging van een Subverwerker via het in Bijlage III beschreven kanaal, waarbij de Klant ten minste dertig (30) dagen heeft om op redelijke gronden van gegevensbescherming bezwaar te maken. Indien de Klant redelijkerwijs bezwaar maakt en Partijen binnen dertig (30) dagen na het bezwaar geen werkbare oplossing kunnen overeenkomen, mag de Klant het betreffende onderdeel van de Dienstverleningsovereenkomst schriftelijk opzeggen en een pro-rata terugbetaling verkrijgen van eventuele vooruitbetaalde vergoedingen voor de betreffende periode.

2.10 Verplichtingen van Subverwerkers. Wanneer Heyloha een Subverwerker inschakelt, legt zij die Subverwerker bij schriftelijke overeenkomst verplichtingen inzake gegevensbescherming op die wezenlijk gelijkwaardig zijn aan die in deze Verwerkersovereenkomst. Heyloha blijft jegens de Klant aansprakelijk voor het handelen en nalaten van haar Subverwerkers als ware het haar eigen handelen en nalaten.

2.11 Teruggave of verwijdering na afloop van de verwerking. Bij beëindiging of afloop van de Dienstverleningsovereenkomst mag de Klant Heyloha opdragen om (a) haar Persoonsgegevens terug te geven in een gestructureerde, gangbare en machineleesbare vorm, of (b) deze te verwijderen, in beide gevallen binnen dertig (30) dagen na de opdracht. Bij gebreke van een opdracht verwijdt Heyloha de Persoonsgegevens binnen negentig (90) dagen na beëindiging. Heyloha mag Persoonsgegevens na beëindiging uitsluitend bewaren voor zover en gedurende de periode die vereist is op grond van Unierecht of het recht van een lidstaat (bijvoorbeeld verplichte bewaring van factuurgegevens); gedurende die periode worden de gegevens geïsoleerd van actieve verwerking en beschermd door passende maatregelen.

2.12 Geaggregeerde en geanonimiseerde statistieken. De Klant draagt Heyloha op Persoonsgegevens te verwerken uitsluitend voor het aanvullende doel van het opstellen van geaggregeerde statistieken over het gebruik en de prestaties van de Diensten, en Heyloha mag de daaruit voortvloeiende geaggregeerde gegevens gebruiken om de Diensten te exploiteren, te beveiligen en te verbeteren en om branchestatistieken en benchmarks te publiceren. Elk van de volgende punten is een voorwaarde voor die instructie:

(a) de aggregatie vindt plaats binnen de verwerkingsomgeving van Heyloha zoals beschreven in §4.1, en de uitkomst is zodanig geanonimiseerd dat noch Heyloha noch enige ontvanger een betrokkene of een klant van Heyloha, direct of indirect, kan identificeren, rekening houdend met alle middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt;

(b) Heyloha zal niet proberen de anonimisering ongedaan te maken en combineert de geaggregeerde uitkomst niet met andere gegevens om een persoon of klant opnieuw te identificeren;

(c) geen uitkomst noemt of beschrijft een identificeerbare klant van Heyloha, en geen uitkomst maakt het mogelijk een klant of betrokkene door afleiding uit een kleine steekproef te onderscheiden; aggregaten worden gebaseerd op een populatie van ten minste vijftientig (25) klanten van Heyloha en duizend (1.000) interacties;

(d) er worden geen vrije tekst, transcripten, opnamen, contactgegevens of inhoud van een kennisbank gepubliceerd, geciteerd of verstrekt, letterlijk of in parafrase;

(e) de onderliggende Persoonsgegevens blijven onderworpen aan alle overige verplichtingen uit deze Verwerkersovereenkomst, waaronder §2.4 (beveiliging), §2.11 (teruggave of verwijdering) en de door de Klant ingestelde bewaartermijnen; en

(f) de Klant kan deze instructie te allen tijde intrekken, met werking voor toekomstige verwerking, door schriftelijke kennisgeving aan Heyloha op grond van §10. Intrekking laat de rest van deze Verwerkersovereenkomst, de Diensten en reeds rechtmatig tot stand gebrachte geaggregeerde uitkomsten onverlet.

Voor alle duidelijkheid: deze instructie staat Heyloha niet toe Persoonsgegevens te verwerken voor profilering, voor het trainen of fine-tunen van modellen, voor advertenties of voor enig doel dat gericht is op individuele betrokkenen.

2.13 Geen training van modellen. Heyloha gebruikt gespreksinhoud, transcripten, inhoud van de kennisbank of andere op grond van deze Verwerkersovereenkomst verwerkte Persoonsgegevens niet om modellen voor kunstmatige intelligentie te trainen, te fine-tunen of te verbeteren. De Subverwerker van Heyloha voor taalmodellen (OpenAI, Bijlage III) verwerkt zulke inhoud onder zakelijke voorwaarden die het gebruik ervan voor de ontwikkeling of verbetering van de diensten van OpenAI, waaronder het trainen van modellen, uitsluiten, en Heyloha heeft niet ingestemd met een dergelijk gebruik. Heyloha schakelt zonder voorafgaande schriftelijke toestemming van de Klant geen Subverwerker voor taalmodellen in die zulke inhoud mag gebruiken voor het trainen van modellen.

3. Verplichtingen van de Klant als Verwerkingsverantwoordelijke

3.1 Rechtsgrondslag en informatieverstrekking. De Klant verklaart en garandeert dat zij beschikt over, en gedurende de looptijd zal blijven beschikken over, een rechtsgrondslag onder de AVG voor de verwerking die zij via de Diensten uitvoert, en dat zij alle noodzakelijke informatie en kennisgevingen aan betrokkenen heeft verstrekt op grond van de artikelen 13 en 14 AVG.

3.2 Instructies van de Klant via configuratie. De Klant erkent dat de Dienst in hoge mate configureerbaar is en dat verschillende beslissingen die naar hun aard aan een Verwerkingsverantwoordelijke toekomen, waaronder welke kanalen worden ingeschakeld, welke gegevensvelden worden verzameld, welke bewaartermijn wordt ingesteld, van welke Subverwerkers via integraties gebruik wordt gemaakt en welke inhoud naar de kennisbank wordt geüpload, door de Klant worden genomen via het Heyloha-dashboard. De Klant waarborgt dat die configuraties in overeenstemming zijn met het toepasselijke gegevensbeschermingsrecht en berusten op een geldige rechtsgrondslag.

3.3 Medewerking. De Klant werkt redelijkerwijs met Heyloha samen om Heyloha in staat te stellen haar verplichtingen uit hoofde van deze Verwerkersovereenkomst na te komen, onder meer door onverwijld de informatie te verstrekken die nodig is om te reageren op een verzoek van een betrokkene of een vraag van een toezichthoudende autoriteit.

3.4 Geen bijzondere categorieën van persoonsgegevens tenzij aangemeld. De Klant zal geen bijzondere categorieën van persoonsgegevens in de zin van artikel 9 AVG, noch persoonsgegevens betreffende

strafrechtelijke veroordelingen en strafbare feiten in de zin van artikel 10 AVG, doelbewust via de Dienst laten verwerken zonder Heyloha daarvan vooraf in kennis te stellen en zonder ervoor te zorgen dat een aanvullende rechtsgrondslag bestaat. De Klant erkent dat incidentele bijzondere categorieën van persoonsgegevens kunnen voorkomen in vrije-tekstinvoer van eindgebruikers; Heyloha past een pseudonimiseringslaag toe op geschreven chatinvoer zoals beschreven in Bijlage II.

4. Internationale doorgiften

4.1 Verwerkingslocatie van Heyloha. De primaire verwerking van Persoonsgegevens door Heyloha vindt plaats in Nederland. De database- en applicatie-infrastructuur wordt gehost binnen de Europese Unie.

4.2 Verdere doorgiften aan Subverwerkers buiten de EU. Wanneer Persoonsgegevens aan een Subverwerker, of door een Subverwerker verder, worden doorgegeven naar een land buiten de Europese Economische Ruimte, het Verenigd Koninkrijk of Zwitserland waarvoor geen adequaatheidsbesluit geldt, waarborgt Heyloha dat een passend doorgiftemechanisme aanwezig is. De actuele doorgiftemechanismen zijn opgenomen in Bijlage III en beschreven in Bijlage IV. Op redelijk verzoek van de Klant verstrekt Heyloha een afschrift van de relevante doorgiftevoorwaarden, voor zover het contract met de Subverwerker dat toestaat.

4.3 Gegevens uit het Verenigd Koninkrijk en Zwitserland. Wanneer Persoonsgegevens onder de reikwijdte van de UK GDPR of de Zwitserse federale wet inzake gegevensbescherming vallen, zijn de overeenkomstige doorgiftemechanismen (het UK International Data Transfer Addendum, respectievelijk de door de Zwitserse Federale Toezichthouder voor gegevensbescherming en openbaarheid erkende Standaardcontractbepalingen) door verwijzing van toepassing.

4.4 Doorgifte-effectbeoordelingen. Heyloha onderhoudt doorgifte-effectbeoordelingen (Transfer Impact Assessments) voor de wezenlijke Subverwerkers die zich buiten de EER bevinden en stelt op redelijk verzoek een samenvatting daarvan ter beschikking aan de Klant.

5. Aansprakelijkheid

De aansprakelijkheid van iedere Partij uit hoofde van deze Verwerkersovereenkomst, hetzij uit overeenkomst, onrechtmatige daad of anderszins, is onderworpen aan de aansprakelijkheidsbeperking en de uitsluitingen van aansprakelijkheid die zijn opgenomen in de Dienstverleningsovereenkomst. Niets in deze Verwerkersovereenkomst beperkt of sluit aansprakelijkheid uit die op grond van toepasselijk recht niet kan worden beperkt of uitgesloten, waaronder de aansprakelijkheid van een Partij jegens een betrokkene uit hoofde van artikel 82 AVG.

6. Looptijd en beëindiging

Deze Verwerkersovereenkomst treedt in werking op de Ingangsdatum en blijft van kracht zolang Heyloha Persoonsgegevens namens de Klant verwerkt. De bepalingen die naar hun aard de beëindiging behoren te overleven, waaronder §2.11 (teruggave of verwijdering), §5 (aansprakelijkheid), §7 (toepasselijk recht) en §10 (kennisgevingen), blijven van kracht na beëindiging van deze Verwerkersovereenkomst en de Dienstverleningsovereenkomst.

7. Toepasselijk recht en bevoegde rechter

Op deze Verwerkersovereenkomst is Nederlands recht van toepassing. De bevoegde rechter te Utrecht, Nederland, heeft bij uitsluiting bevoegdheid ten aanzien van ieder geschil dat voortvloeit uit of verband houdt met deze Verwerkersovereenkomst, onverminderd de rechten van een betrokkene uit hoofde van artikel 79 AVG of enige dwingendrechtelijke bepaling van consumentenbeschermingsrecht.

8. Wijziging

Heyloha mag deze Verwerkersovereenkomst van tijd tot tijd bijwerken om rekening te houden met (i) wijzigingen in het toepasselijke gegevensbeschermingsrecht, (ii) beslissingen van toezichthoudende autoriteiten of bevoegde rechters, of (iii) wijzigingen in de Diensten of in de lijst van Subverwerkers. Wezenlijke wijzigingen worden ten minste dertig (30) dagen voordat zij van kracht worden aan de Klant meegedeeld.

9. Nietigheid van afzonderlijke bepalingen

Indien enige bepaling van deze Verwerkersovereenkomst nietig of niet-afdwingbaar wordt geacht, blijven de overige bepalingen onverkort van kracht, en zullen Partijen te goeder trouw onderhandelen om de nietige bepaling te vervangen door een geldige bepaling die een economisch en juridisch gelijkwaardig resultaat bereikt.

10. Kennisgevingen

Kennisgevingen aan Heyloha uit hoofde van deze Verwerkersovereenkomst worden verzonden naar **Stefan Hoogers** via support@heyloha.ai, met een afschrift aan **Heyloha by Covalore B.V., Regentesselaan 65, 3571 CB Utrecht, Nederland**. Kennisgevingen aan de Klant worden verzonden naar de in het Heyloha-dashboard vastgelegde contactadressen.

11. Definities

Voor de toepassing van deze Verwerkersovereenkomst:

- **"Verwerkingsverantwoordelijke", "Verwerker", "Subverwerker", "Persoonsgegevens", "Inbreuk in verband met persoonsgegevens", "Verwerking", "Betrokkene"** en **"Toezichthoudende autoriteit"** hebben de betekenis die daaraan wordt gegeven in de AVG.
- **"AVG"** betekent Verordening (EU) 2016/679, zoals van tijd tot tijd gewijzigd of vervangen, en omvat, waar de context dat vereist, de overeenkomstige bepalingen van de UK GDPR en de Zwitserse federale wet inzake gegevensbescherming.
- **"Standaardcontractbepalingen"** of **"SCC's"** betekent de standaardcontractbepalingen voor de doorgifte van persoonsgegevens naar derde landen die op 4 juni 2021 door de Europese Commissie zijn

vastgesteld (Uitvoeringsbesluit (EU) 2021/914), zoals van tijd tot tijd gewijzigd of vervangen, en omvat waar van toepassing het UK International Data Transfer Addendum.

- "**Diensten**" heeft de betekenis die daaraan wordt gegeven in de Dienstverleningsovereenkomst en is beschreven in Bijlage I.
- "**Subverwerker**" betekent een derde die door Heyloha wordt ingeschakeld om Persoonsgegevens namens de Klant te verwerken in verband met de Diensten. De actuele lijst is opgenomen in Bijlage III.

Ondertekening

Voor Heyloha by Covalore B.V.	Voor de Klant
Naam: Stefan Hoogers	Naam: _____
Functie: Bestuurder	Functie: _____
Datum: _____	Datum: _____
Handtekening: _____	Handtekening: _____

Bijlage I — Details van de verwerking

A. Lijst van partijen

Rol	Identiteit
Gegevensexporteur (Verwerkingsverantwoordelijke)	De Klant zoals aangeduid aan het hoofd van deze Verwerkersovereenkomst
Gegevensimporteur (Verwerker)	Heyloha by Covalore B.V., Regentesselaan 65, 3571 CB Utrecht, Nederland. Privacycontact: Stefan Hoogers, support@heyloha.ai

B. Beschrijving van de verwerking

- **Onderwerp.** Levering van de Diensten, te weten het AI-agentplatform van Heyloha over de kanalen webchat, telefoon, WhatsApp, Instagram, LinkedIn en e-mail, tezamen met de bijbehorende dashboard-, kennisbank-, integratie- en rapportagefuncties.
- **Aard en doel.** Het exploiteren van AI-agents namens de Klant om te communiceren met de eindgebruikers van de Klant, antwoorden te genereren, contactgegevens vast te leggen waar de agent van de Klant daartoe is geconfigureerd, afspraken in te plannen, informatie op te zoeken via door de Klant geconfigureerde toolintegraties, en een gesprekstranscript te produceren dat voor de Klant zichtbaar is in het Heyloha-dashboard. Het bijhouden van de kennisbank van de Klant op basis van inhoud die de Klant uploadt of koppelt (bestanden, webpagina's) en, waar de Klant dit inschakelt, op basis van herbruikbare kennis die wordt afgeleid uit de door de Klant zelf verzonden e-mails, nadat persoonsgegevens zijn verwijderd en het resultaat vóór gebruik is beoordeeld. Het bewaken van de kwaliteit van de antwoorden van de agents.
- **Categorieën van Persoonsgegevens.**
 - Vrije-tekstinhoud van berichten van eindgebruikers en antwoorden van de agent.
 - Contactgegevens die door de agent worden verzameld waar de Klant verzameling heeft geconfigureerd: naam, e-mailadres, telefoonnummer, postcode, huisnummer.
 - Sessiekenmerken voor webchat: user agent, browser, schermresolutie, taal, tijdzone, huidige URL, referrer, apparaattype, UTM-parameters, verkeersbron.
 - Telefoonnummer van de beller en live gespreksaudio (uitsluitend in de stream) voor telefoongesprekken; het daaruit voortvloeiende teksttranscript.
 - Afzender, ontvangers, onderwerp, tekst, headers en bijlagen voor de verwerking op het e-mailkanaal.
 - Inloggegevens die door de Klant worden verstrekt voor de integratie van het berichtenkanaal (door Heyloha versleuteld opgeslagen).
 - Inhoud van de kennisbank die door de Klant wordt aangeleverd of gekoppeld (bestanden, webpagina's en kennis die is afgeleid uit de verzonden e-mails van de Klant), die incidenteel Persoonsgegevens kan bevatten.
 - Afspraak- en agendagegegevens wanneer de Klant een agenda koppelt: datum en tijd, onderwerp, en de naam en contactgegevens van de deelnemer.
 - Gegevens die door de Klant geconfigureerde toolintegraties teruggeven, zoals opvragingen in een CRM-, webshop- of boekingssysteem.

- **Categorieën van Betrokkenen.** De eindgebruikers van de Klant (websitebezoekers, bellers, gebruikers van berichten-apps, e-mailcorrespondenten); derden waarnaar door eindgebruikers in hun interacties wordt verwezen; de werknemers van de Klant die het Heyloha-dashboard gebruiken.
 - **Bijzondere categorieën van persoonsgegevens.** Niet doelbewust verzameld. Incidenteel kunnen bijzondere categorieën van persoonsgegevens voorkomen in vrije-tekstinvoer. Heyloha past de in Bijlage II beschreven pseudonimiseringsmaatregel toe.
 - **Frequentie.** Doorlopend, gedurende de looptijd van de Dienstverleningsovereenkomst.
 - **Duur.** Voor de looptijd van de Dienstverleningsovereenkomst plus de in §2.11 vastgelegde periode voor teruggave of verwijdering na beëindiging.
-

C. Bevoegde toezichhoudende autoriteit

Autoriteit Persoonsgegevens, Postbus 93374, 2509 AJ Den Haag, Nederland.

Bijlage II — Technische en organisatorische maatregelen

Deze Bijlage vat de maatregelen samen die Heyloha toepast om Persoonsgegevens te beschermen. Een uitgebreider extern compliance-overzicht waarin dezelfde maatregelen worden beschreven, is op verzoek verkrijgbaar via support@heyloha.ai.

1. Versleuteling

- **Tijdens transport.** Alle naar buiten gerichte endpoints gebruiken uitsluitend HTTPS met actuele TLS-versies. Certificaten worden per host uitgegeven door Let's Encrypt en automatisch vernieuwd.
- **Op applicatieniveau in rust.** Gevoelige toegangsgegevens (geheime sleutels van uitgaande webhooks, toegangsgegevens voor toolintegraties van derden zoals Shopify-toegangstokens) worden versleuteld met geauthenticeerde symmetrische versleuteling (op basis van libsodium) met een geversioneerde envelop die sleutelrotatie ondersteunt.
- **Locatie van de infrastructuur.** Database- en bestandsopslag worden gehost op Nederlandse infrastructuur (zie TransIP in Bijlage III).
- **Netwerkisolatie.** De database bevindt zich op een privénetwerk en is niet toegankelijk vanaf het openbare internet.

2. Pseudonimisering van vrije-tekstinvoer

Vrije-tekstinvoer die bestemd is voor de OpenAI Responses API wordt door een pseudonimiseringslaag geleid die matching op basis van reguliere expressies combineert met named-entity recognition. De laag detecteert de entiteiten NAME (naam), EMAIL (e-mailadres), PHONE (telefoonnummer), POSTAL (postcode), HOUSENR (huisnummer), ADDRESS (adres), BSN (Nederlands nationaal identificatienummer), IBAN, IP, PLATE (kenteken) en LOCATION (locatie) en vervangt deze door stabiele tokens per chat voordat het verzoek Heyloha verlaat. De omgekeerde toewijzing wordt bewaard in het chatrecord en gebruikt om de oorspronkelijke waarden in het antwoord van het model voor de eindgebruiker te herstellen. De onderliggende persoonsgegevens verschijnen niet in leesbare vorm in de tekst van het OpenAI-verzoek.

3. Authenticatie en toegangsbeheer

- Klantaccounts gebruiken een e-mailadres en een met bcrypt gehasht wachtwoord.
- API-toegang maakt gebruik van kortlevende JWT-bearertokens met refreshtokens.
- Autorisatie is rolgebaseerd; de meest bevoorrechte bewerkingen vereisen `ROLE_SUPER_ADMIN`.
- Productietoegang door personeel van Heyloha is beperkt tot met name genoemde personen op need-to-know-basis.

4. Webhook-authenticatie, rate limiting en misbruikbescherming

- Inkomende webhooks worden geauthenticeerd door middel van een handtekening of een gedeeld geheim.

- Uitgaande webhooks worden ondertekend met een HMAC-SHA256-handtekening die de Klant kan verifiëren, wanneer de Klant een ondertekeningsgeheim op de webhook heeft geconfigureerd.
- Er worden rate limits afgedwongen voor gevoelige onderdelen, waaronder het verzenden van uitgaande webhooks (60 per minuut) en het verwerken van inkomende e-mailwebhooks (100 per minuut per bron).

5. Gegevensminimalisatie en bewaring

- Payloads van inkomende webhooks worden automatisch verwijderd na dertig (30) dagen.
- Conversations-objecten, traces en logs aan de OpenAI-zijde die door de Heyloha-organisatie zijn aangemaakt, worden automatisch verwijderd na zeven (7) dagen.
- Door de Klant beheerde bewaring geldt aan de Heyloha-zijde voor gesprekstrascripten, contactrecords en bezoekersrecords.
- Telefoongesprekken worden niet opgenomen; uitsluitend het teksttranscript wordt bewaard.

6. Logging en foutmonitoring

- Applicatielogs worden in JSON weggeschreven naar standard error.
- Foutgebeurtenissen die naar de foutmonitoringprovider van Heyloha worden verzonden, passeren een scrubber die berichtinhoud, onderwerpregels, ontvangerslijsten, ruwe webhook-payloads, autorisatie-headers, API-sleutels, toegangs- en refreshtokens, cookies, het webhook-geheim van de berichtenintegratie en iedere vrije tekststring die overeenkomt met een e-mailadres verwijdert.

7. Bedrijfsvoering en personeel

- Stack: PHP 8.4 LTS met Symfony 7.4 LTS, gehouden op ondersteunde releases.
- Zware webhook-verkeersstromen worden asynchroon verwerkt met retry- en dead-letter-queues.
- Vastgelopen inbox-rijen worden elke vijf minuten automatisch heropgepakt.
- Alle personeelsleden met productietoegang zijn gebonden aan geheimhoudingsverplichtingen en volgen een privacy- en beveiligingsbriefing.

8. Gegevensbeschermingseffectbeoordelingen (DPIA's)

Heyloha onderhoudt een intern DPIA-register dat de verwerkingsactiviteiten met een hoog risico op platformniveau bestrijkt (conversationele AI van OpenAI; telefoongesprekken met de telefoonagent; verwerking op het e-mailkanaal). DPIA's worden ten minste elke zes maanden herzien, bij iedere wezenlijke wijziging, en na ieder meldingsplichtig incident. Samenvattingen van de DPIA's op platformniveau zijn op redelijk verzoek beschikbaar voor de Klant.

9. Incidentrespons

Heyloha hanteert een incidentresponsprocedure die is afgestemd op de artikelen 33–34 AVG, met inbegrip van triage, indamming, sleutelrotatie, een intern inbreukregister, kennisgeving aan de toezichthoudende autoriteit binnen tweeënzeventig (72) uur waar de drempel wordt bereikt, en kennisgeving aan de Klant overeenkomstig §2.7 van deze Verwerkersovereenkomst.

Bijlage III — Subverwerkers

A. Lijst van Subverwerkers op de Ingangsdatum

Subverwerker	Functie	Gedeelde Persoonsgegevens	Hosting-regio	Doorgiftemechanisme
OpenAI Ireland Ltd. (met OpenAI OpCo, LLC als verdere importeur)	LLM-inferentie, bestands- en vectorzoeken, realtime spraak	Gespreksinhoud (na pseudonimisering), geüploade bestanden, gespreks-ID's	Ierland (EU); verder naar de Verenigde Staten	OpenAI Data Processing Addendum. Verdere doorgifte naar de Verenigde Staten op grond van het EU-VS Data Privacy Framework en de in dat addendum opgenomen SCC's (2021/914); UK Addendum waar van toepassing
Stripe Inc. / Stripe Technology Europe Ltd.	Betalingsverwerking	Factuurgegevens van de Klant, Stripe-identificatoren	Ierland (EU) en VS	SCC's onder de Stripe-DPA
Twilio Inc.	Telefonietransport (geen gespreksopname geconfigureerd) en compliance-bundels	Telefoonnummers, live gespreksaudio (in de stream), gespreksmetadata, identiteits-compliance documenten	Verenigde Staten, met EU-regionale opslag waar gekozen	SCC's onder de Twilio-DPA
Unipile	Integratie van WhatsApp, Instagram, LinkedIn en e-mail	Inloggegevens van gekoppelde accounts, berichten en e-mailinhoud, bijlagen	Europese Unie	DPA met SCC's
Mailgun (Sinch)	Bezorging van transactionele e-mail (aanmelding, wachtwoordherstel, AI-gebeurtenissen)	E-mailadres van ontvanger, berichtinhoud	EU-regio	SCC's onder de Mailgun-DPA
Sentry (Functional Software, Inc.)	Foutmonitoring	Stack traces en verzoekmetadata na de in Bijlage II beschreven scrubbing aan de Heyloha-zijde	Verenigde Staten	SCC's onder de Sentry-DPA

Subverwerker	Functie	Gedeelde Persoonsgegevens	Hosting-regio	Doorgiftemechanisme
Langfuse GmbH	Kwaliteitsbewaking van de antwoorden van de agents (LLM-observability)	Gesprekstekst na onomkeerbare verwijdering van persoonsgegevens, chat-, sessie- en merk-ID's, kwaliteitsscores	EU (Ierland, met back-ups in Duitsland)	Langfuse Data Processing Agreement; hosting in de EU
Postcode-API	Nederlandse adresvalidatie	Postcode en huisnummer	Nederland	EU
Altum	Nederlandse woningdata (waardebepaling, energielabels, WOZ-waarden, historische verkoop- en huurtransacties); alleen gebruikt wanneer de agent van de Klant is ingesteld om de vastgoedtools aan te roepen	Door eindgebruikers opgegeven Nederlandse adressen	Nederland	EU
WebBridge	Nederlandse hypotheekberekeningen; alleen gebruikt wanneer de agent van de Klant is ingesteld om de hypotheektools aan te roepen	Door eindgebruikers opgegeven hypotheekgegevens (leenbedrag, inkomen, looptijd)	Nederland	EU
Google Ireland Ltd. (met Google LLC als verdere importeur)	Street View-beelden en afstandsberekeningen; alleen gebruikt wanneer de agent van de Klant is ingesteld om de vastgoedtools aan te roepen	Door eindgebruikers opgegeven adressen of coördinaten	Ierland (EU); verder naar de Verenigde Staten	EU-VS Data Privacy Framework en SCC's onder de Google Maps Platform-voorwaarden
Mercure (door Heyloha zelf gehost op push.heyloha.ai)	Realtime push naar widgets	Live chatberichten tijdens transport	Nederland	Heyloha-infrastructuur, geen doorgifte aan een derde
TransIP (hosting)	Applicatie- en databasehosting	Alle Persoonsgegevens die Heyloha bewaart	Nederland	EU

B. Kennisgeving van nieuwe of vervangende Subverwerkers

Heyloha publiceert haar actuele lijst van Subverwerkers op heyloha.ai/nl/subverwerkers, met de datum van de laatste wijziging. Heyloha stelt de Klant per e-mail aan de in het Heyloha-dashboard vastgelegde contactadressen in kennis van iedere toevoeging of vervanging, ten minste dertig (30) dagen voordat de

nieuwe Subverwerker Persoonsgegevens van de Klant gaat verwerken. Het recht van de Klant om bezwaar te maken is uiteengezet in §2.9 van deze Verwerkersovereenkomst.

C. Verwerkers van de marketingwebsite (buiten reikwijdte)

De verwerkers die worden gebruikt op de marketingwebsite heyloha.ai (Google, LinkedIn, Meta, Cloudflare, ActiveCampaign) zijn geen Subverwerkers onder deze Verwerkersovereenkomst. Zij opereren uitsluitend op de marketingwebsite heyloha.ai, worden alleen met toestemming ingezet en hebben geen toegang tot Persoonsgegevens van de Klant. Zij zijn volledigheidshalve opgenomen in de openbare privacyverklaring van Heyloha.

Bijlage IV — Doorgiftemechanismen

Heyloha verwerkt Persoonsgegevens in Nederland, en de meeste Subverwerkers verwerken ze binnen de EU. Wanneer Persoonsgegevens de EER verlaten, berust de doorgifte op het mechanisme dat in Bijlage III voor de betreffende Subverwerker is vermeld:

- **EU-VS Data Privacy Framework.** Wanneer de ontvangende entiteit is gecertificeerd onder het EU-VS Data Privacy Framework, berust de doorgifte op het adequaatheidsbesluit van de Europese Commissie van 10 juli 2023.
- **Standaardcontractbepalingen.** Wanneer op de SCC's wordt vertrouwd, al dan niet naast het Data Privacy Framework, gaat het om de SCC's die zijn opgenomen in de eigen verwerkersovereenkomst van de Subverwerker, met de daarin gekozen module en opties. Wanneer Heyloha als Verwerker optreedt namens de Klant, is dat Module Drie (verwerker aan verwerker).
- **Afschriften.** Op redelijk verzoek van de Klant verstrekt Heyloha op grond van §4.2 een afschrift van de relevante doorgiftevoorwaarden.

Voor doorgiften uit het Verenigd Koninkrijk geldt het UK International Data Transfer Addendum zoals opgenomen in de verwerkersovereenkomst van de betreffende Subverwerker. Voor doorgiften uit Zwitserland gelden de SCC's met de aanpassingen die zijn bevestigd door de Zwitserse Federale Toezichthouder voor gegevensbescherming en openbaarheid.

Einde van de Heyloha Verwerkersovereenkomst, versie 1.3 (Nederlandse versie).