

Heyloha Data Processing Agreement

Version: 1.3

Effective date: the date last signed by the Parties below.

Form: customer-facing template. The Parties may complete the placeholder fields and execute this document as a stand-alone DPA.

Parties

Heyloha by Covalore B.V. — a private company with limited liability incorporated under the laws of the Netherlands, having its registered office at Regentesselaan 65, 3571 CB Utrecht, the Netherlands, registered with the Dutch Chamber of Commerce under number 99942992 (referred to in this Agreement as "**Heyloha**").

Customer — _____ (legal name) of _____
(registered office and number) (referred to in this Agreement as "**Customer**").

Each a "**Party**" and together the "**Parties**".

Recitals

A. The Parties have entered into a separate agreement under which Heyloha makes its AI-agent platform available to the Customer (the "**Service Agreement**"). The Service Agreement, together with any order forms, configuration tools and dashboard settings, defines the scope of the services Heyloha provides to the Customer (the "**Services**").

B. In delivering the Services, Heyloha processes Personal Data on behalf of the Customer.

C. This Data Processing Agreement (the "**DPA**") sets out the terms on which Heyloha processes that Personal Data and supplements the Service Agreement. It is intended to satisfy Article 28 of Regulation (EU) 2016/679 ("**GDPR**") and applicable equivalent provisions of UK data protection law and Swiss data protection law.

D. Capitalised terms not defined in the body of this DPA have the meanings given in §11 (Definitions) or, failing that, in the Service Agreement and the GDPR.

1. Subject matter, roles and order of precedence

1.1 Roles. With respect to Personal Data of the Customer's end-users, employees, suppliers and other natural persons that Heyloha processes in the course of providing the Services, the Customer is the Controller and Heyloha is the Processor. Where the Customer is itself a Processor acting on behalf of a third-party Controller, Heyloha acts as Sub-processor and the same obligations apply mutatis mutandis.

1.2 Subject matter, nature, purpose, duration. Set out in [Annex I](#).

1.3 Order of precedence. In the event of conflict between this DPA, the Service Agreement and any order form, the order of precedence is: (i) this DPA, (ii) the order form, (iii) the Service Agreement.

2. Heyloha's obligations as Processor

2.1 Customer instructions. Heyloha will process Personal Data only on the documented instructions of the Customer. The Customer's instructions are constituted by this DPA, the Service Agreement, the configurations the Customer applies in the Heyloha dashboard and the agents it operates. Save for the limited instruction in §2.12 (aggregated and anonymised statistics), Heyloha will not process Personal Data for any other purpose, including for its own marketing, profiling or product development, except where required to do so by Union or Member State law to which Heyloha is subject; in that case Heyloha will inform the Customer of that legal requirement before processing, unless that law prohibits the disclosure.

2.2 Notice on unlawful instructions. If, in Heyloha's reasonable opinion, an instruction from the Customer infringes the GDPR or another applicable data protection provision, Heyloha will inform the Customer without undue delay.

2.3 Confidentiality of personnel. Heyloha will ensure that all persons authorised to process Personal Data are bound by an appropriate duty of confidentiality, whether by contract or statute, and have received appropriate training on their data protection obligations.

2.4 Security (Article 32). Heyloha will implement and maintain the technical and organisational measures set out in [Annex II](#), having regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risk to the rights and freedoms of natural persons. Heyloha may update those measures from time to time provided the level of protection is not materially reduced.

2.5 Data-subject requests. Taking into account the nature of the processing, Heyloha will assist the Customer by appropriate technical and organisational measures, in so far as this is possible, to fulfil its obligation to respond to requests from data subjects exercising their rights under Chapter III of the GDPR (Articles 15–22). If Heyloha receives such a request directly from a data subject in respect of Personal Data processed on behalf of the Customer, Heyloha will (i) not respond to the request other than to acknowledge receipt and direct the data subject to the Customer, and (ii) notify the Customer without undue delay so that the Customer may handle the request as Controller.

2.6 Assistance with the Customer's other compliance obligations. Taking into account the nature of the processing and the information available to Heyloha, Heyloha will provide reasonable assistance to the Customer in meeting its obligations under Articles 32 to 36 of the GDPR (security, breach notification, data protection impact assessments and prior consultation).

2.7 Personal data breach. Heyloha will notify the Customer of any Personal Data Breach affecting the Customer's Personal Data without undue delay and in any event within seventy-two (72) hours of Heyloha becoming aware of the breach. The notification will include the information specified in Article 33(3) GDPR to the extent then known to Heyloha and will be supplemented as further information becomes available. Notifications are sent to the contact addresses recorded for the Customer in the Heyloha dashboard.

2.8 Audit. Heyloha will make available to the Customer all information reasonably necessary to demonstrate compliance with the obligations set out in this DPA. The Customer may, on at least thirty (30) days' prior written notice and not more than once in any twelve-month period (or more often if requested by a competent supervisory authority or following a material Personal Data Breach), audit Heyloha's compliance with this DPA. Heyloha may discharge this obligation, where appropriate, by providing third-party audit reports, certifications, completed industry-standard questionnaires and the documents referenced in Annex II. Audits will be conducted during business hours, with minimal disruption to Heyloha's operations, and at the Customer's expense; both Parties will treat audit findings as confidential.

2.9 Sub-processors — general authorisation. The Customer hereby grants Heyloha a general written authorisation to engage Sub-processors to assist in the provision of the Services. The Sub-processors engaged at the Effective Date are listed in [Annex III](#). Heyloha will give the Customer prior notice of any addition or replacement of a Sub-processor through the channel described in Annex III, with at least thirty (30) days for the Customer to object on reasonable data-protection grounds. If the Customer reasonably objects and the Parties cannot agree a workable solution within thirty (30) days of the objection, the Customer may terminate the affected portion of the Service Agreement on written notice and obtain a pro-rata refund of any pre-paid fees for the affected period.

2.10 Sub-processor obligations. Where Heyloha engages a Sub-processor, it will impose data-protection obligations on that Sub-processor by written contract that are materially equivalent to those in this DPA. Heyloha remains liable to the Customer for the acts and omissions of its Sub-processors as if they were its own.

2.11 Return or deletion at end of processing. On termination or expiry of the Service Agreement, the Customer may instruct Heyloha to (a) return its Personal Data in a structured, commonly used and machine-readable format, or (b) delete it, in each case within thirty (30) days of the instruction. In the absence of an instruction, Heyloha will delete the Personal Data within ninety (90) days of termination. Heyloha may retain Personal Data after termination only to the extent and for the period required by Union or Member State law (for example, mandatory retention of invoicing data); during that period the data will be isolated from active processing and protected by appropriate measures.

2.12 Aggregated and anonymised statistics. The Customer instructs Heyloha to process Personal Data for the sole additional purpose of producing aggregated statistics about the use and performance of the Services, and Heyloha may use the resulting aggregated data to operate, secure and improve the Services and to publish industry statistics and benchmarks. Each of the following is a condition of that instruction:

- (a) the aggregation is carried out within Heyloha's processing environment described in §4.1, and the output is anonymised such that neither Heyloha nor any recipient can identify any data subject or any Customer, directly or indirectly, taking account of all means reasonably likely to be used;
- (b) Heyloha will not attempt to reverse the anonymisation and will not combine the aggregated output with other data in order to re-identify any person or Customer;
- (c) no output will name or describe an identifiable Customer, and no output will permit a Customer or a data subject to be singled out by inference from a small sample; aggregates will be drawn from a population of no fewer than twenty-five (25) Customers and one thousand (1,000) interactions;
- (d) no free-text content, transcript, recording, contact detail or knowledge-base content is published, quoted or disclosed, whether verbatim or paraphrased;
- (e) the underlying Personal Data remains subject to every other obligation in this DPA, including §2.4 (security), §2.11 (return or deletion) and the retention periods configured by the Customer; and
- (f) the Customer may withdraw this instruction at any time, with effect for future processing, by written notice to Heyloha under §10. Withdrawal does not affect the remainder of this DPA, the Services or any aggregated output already lawfully produced.

For the avoidance of doubt, this instruction does not permit Heyloha to process Personal Data for profiling, for training or fine-tuning models, for advertising, or for any purpose directed at individual data subjects.

2.13 No model training. Heyloha does not use conversation content, transcripts, knowledge-base content or other Personal Data processed under this DPA to train, fine-tune or improve artificial-intelligence models. Heyloha's language-model Sub-processor (OpenAI, Annex III) processes such content under business terms that exclude its use to develop or improve OpenAI's services, including model training, and Heyloha has not

agreed to any such use. Heyloha will not engage a language-model Sub-processor that may use such content for model training without the Customer's prior written consent.

3. Customer's obligations as Controller

3.1 Lawful basis and notices. The Customer represents and warrants that it has, and will maintain throughout the term, a lawful basis under the GDPR for the processing it performs through the Services and that it has provided all necessary information and notices to data subjects under Articles 13 and 14 GDPR.

3.2 Customer instructions through configuration. The Customer acknowledges that the Service is highly configurable and that several decisions of a Controller nature — including which channels to enable, which data fields to collect, what retention to set, which Sub-processors to make use of via integrations, and which content to upload to the knowledge base — are taken by the Customer through the Heyloha dashboard. The Customer will ensure that those configurations comply with applicable data protection law and reflect a valid lawful basis.

3.3 Cooperation. The Customer will reasonably cooperate with Heyloha to enable Heyloha to fulfil its obligations under this DPA, including by promptly providing the information needed to respond to a data-subject request or supervisory authority enquiry.

3.4 No special-category data unless declared. The Customer will not deliberately route special-category data within the meaning of Article 9 GDPR, or data relating to criminal convictions and offences within the meaning of Article 10 GDPR, through the Service without notifying Heyloha in advance and ensuring that an additional lawful basis exists. The Customer acknowledges that incidental special-category data may appear in free-text input from end-users; Heyloha applies a pseudonymisation layer to written-chat input as described in Annex II.

4. International transfers

4.1 Heyloha's processing location. Heyloha's primary processing of Personal Data takes place in the Netherlands. The database and application infrastructure are hosted within the European Union.

4.2 Onward transfers to non-EU Sub-processors. Where Personal Data is transferred to a Sub-processor, or onward by a Sub-processor, to a country outside the European Economic Area, the United Kingdom or Switzerland that is not covered by an adequacy decision, Heyloha ensures that an appropriate transfer mechanism is in place. The current transfer mechanisms are listed in [Annex III](#) and described in [Annex IV](#). Heyloha will, on the Customer's reasonable request, provide a copy of the relevant transfer terms to the extent permitted under the Sub-processor's contract.

4.3 UK and Swiss data. Where Personal Data falls within the scope of the UK GDPR or the Swiss Federal Act on Data Protection, the equivalent transfer mechanisms (UK International Data Transfer Addendum / Swiss FDPIC-recognised SCCs) apply by reference.

4.4 Transfer Impact Assessments. Heyloha maintains Transfer Impact Assessments for the substantive Sub-processors located outside the EEA and will make a summary available to the Customer on reasonable request.

5. Liability

Each Party's liability under this DPA, whether in contract, tort or otherwise, is subject to the liability cap and exclusions of liability set out in the Service Agreement. Nothing in this DPA limits or excludes liability that cannot be limited or excluded under applicable law, including a Party's liability towards a data subject under Article 82 GDPR.

6. Term and termination

This DPA takes effect on the Effective Date and continues for as long as Heyloha processes Personal Data on behalf of the Customer. The provisions that by their nature should survive termination — including §2.11 (return or deletion), §5 (liability), §7 (governing law) and §10 (notices) — survive termination of this DPA and the Service Agreement.

7. Governing law and jurisdiction

This DPA is governed by the laws of the Netherlands. The competent courts of Utrecht, the Netherlands have exclusive jurisdiction over any dispute arising out of or in connection with this DPA, without prejudice to the rights of a data subject under Article 79 GDPR or to any mandatory provision of consumer-protection law.

8. Variation

Heyloha may update this DPA from time to time to reflect (i) changes to applicable data protection law, (ii) decisions of supervisory authorities or competent courts, or (iii) changes to the Services or to the Sub-processor list. Material changes will be notified to the Customer at least thirty (30) days before they take effect.

9. Severability

If any provision of this DPA is held to be invalid or unenforceable, the remaining provisions remain in full force and effect, and the Parties will negotiate in good faith to replace the invalid provision with a valid provision that achieves an economically and legally equivalent result.

10. Notices

Notices to Heyloha under this DPA are sent to **Stefan Hoogers** at support@heyloha.ai, with a copy to **Heyloha by Covalore B.V., Regentesselaan 65, 3571 CB Utrecht, Netherlands**. Notices to the Customer are sent to the contact addresses recorded in the Heyloha dashboard.

11. Definitions

For the purposes of this DPA:

- **"Controller", "Processor", "Sub-processor", "Personal Data", "Personal Data Breach", "Processing", "Data Subject" and "Supervisory Authority"** have the meanings given in the GDPR.
 - **"GDPR"** means Regulation (EU) 2016/679, as amended or replaced from time to time, and includes the equivalent provisions of the UK GDPR and the Swiss Federal Act on Data Protection where the context requires.
 - **"Standard Contractual Clauses" or "SCCs"** means the standard contractual clauses for the transfer of personal data to third countries adopted by the European Commission on 4 June 2021 (Decision (EU) 2021/914), as amended or replaced from time to time, and includes the UK International Data Transfer Addendum where applicable.
 - **"Services"** has the meaning given in the Service Agreement and is described in [Annex I](#).
 - **"Sub-processor"** means a third party engaged by Heyloha to process Personal Data on behalf of the Customer in connection with the Services. The current list is in [Annex III](#).
-

Signatures

For Heyloha by Covalore B.V.	For the Customer
Name: Stefan Hoogers	Name: _____
Title: Director	Title: _____
Date: _____	Date: _____
Signature: _____	Signature: _____

Annex I — Details of the processing

A. List of parties

Role	Identity
Data exporter (Controller)	The Customer identified at the head of this DPA
Data importer (Processor)	Heyloha by Covalore B.V., Regentesselaan 65, 3571 CB Utrecht, Netherlands. Privacy contact: Stefan Hoogers, support@heyloha.ai

B. Description of the processing

- **Subject matter.** Provision of the Services, namely Heyloha's AI-agent platform across web chat, phone, WhatsApp, Instagram, LinkedIn and email channels, together with associated dashboard, knowledge-base, integrations and reporting features.
- **Nature and purpose.** Operating AI agents on behalf of the Customer to interact with the Customer's end-users, generate replies, capture contact details where the Customer's agent is configured to do so, schedule appointments, look up information through Customer-configured tool integrations, and produce a conversation transcript visible to the Customer in the Heyloha dashboard. Maintaining the Customer's knowledge base from content the Customer uploads or connects (files, web pages) and, where the Customer enables it, from reusable knowledge distilled from the Customer's own sent emails, after personal data has been removed and the result has been reviewed before use. Monitoring the quality of agent replies.
- **Categories of Personal Data.**
 - Free-text content of end-user messages and agent replies.
 - Contact details collected by the agent where the Customer has configured collection: name, email, phone number, postal code, house number.
 - Session attributes for web-chat: user agent, browser, screen resolution, language, time zone, current URL, referrer, device type, UTM parameters, traffic source.
 - Caller phone number and live call audio (in stream only) for phone calls; the resulting text transcript.
 - Sender, recipients, subject, body, headers and attachments for email-channel processing.
 - Account credentials supplied by the Customer for the messaging-channel integration (encrypted at rest by Heyloha).
 - Knowledge-base content supplied or connected by the Customer (files, web pages and knowledge distilled from the Customer's sent emails), which may incidentally contain Personal Data.
 - Appointment and calendar data where the Customer connects a calendar: date and time, subject, and the attendee's name and contact details.
 - Data returned by Customer-configured tool integrations, such as CRM, webshop or booking-system lookups.
- **Categories of Data Subjects.** The Customer's end-users (website visitors, callers, messaging-app users, email correspondents); third parties referenced by end-users in their interactions; the Customer's employees who use the Heyloha dashboard.

- **Special-category data.** Not deliberately collected. Incidental special-category content can appear in free-text input. Heyloha applies the pseudonymisation measure described in Annex II.
- **Frequency.** Continuous, throughout the term of the Service Agreement.
- **Duration.** For the term of the Service Agreement plus the post-termination return-or-deletion period set out in §2.11.

C. Competent supervisory authority

Autoriteit Persoonsgegevens (Dutch Data Protection Authority), Postbus 93374, 2509 AJ Den Haag, Netherlands.

Annex II — Technical and organisational measures

This Annex summarises the measures Heyloha applies to protect Personal Data. A more detailed external compliance overview describing the same measures is available on request from support@heyloha.ai.

1. Encryption

- **In transit.** All customer-facing endpoints use HTTPS only with current TLS versions. Certificates are issued per host by Let's Encrypt and renewed automatically.
 - **Application-layer at rest.** Sensitive credentials (outbound webhook secrets, third-party tool-integration credentials such as Shopify access tokens) are encrypted using authenticated symmetric encryption (libsodium-based) with a versioned envelope that supports key rotation.
 - **Infrastructure location.** Database and file storage are hosted on Dutch infrastructure (see TransIP in Annex III).
 - **Network isolation.** The database is on a private network and is not exposed to the public internet.
-

2. Pseudonymisation of free-text input

Free-text input destined for the OpenAI Responses API is run through a pseudonymisation layer that combines regular-expression matching with named-entity recognition. The layer detects NAME, EMAIL, PHONE, POSTAL, HOUSENR, ADDRESS, BSN (Dutch national identifier), IBAN, IP, PLATE and LOCATION entities and replaces them with stable per-chat tokens before the request leaves Heyloha. The reverse mapping is held in the chat record and used to restore the original values in the model's reply for the end-user. The underlying personal data does not appear in plaintext in the OpenAI request body.

3. Authentication and access control

- Customer accounts use email and a password hashed with bcrypt.
 - API access uses short-lived JWT bearer tokens with refresh tokens.
 - Authorisation is role-based; the most privileged operations require `ROLE_SUPER_ADMIN`.
 - Production access by Heyloha personnel is restricted to named individuals on a need-to-know basis.
-

4. Webhook authentication, rate limiting and abuse protection

- Inbound webhooks are authenticated by signature or shared secret.
- Outbound webhooks are signed with an HMAC-SHA256 signature the Customer can verify, when the Customer has configured a signing secret on the webhook.
- Rate limits are enforced for sensitive surfaces, including outbound webhook dispatch (60 / minute) and inbound email-webhook ingestion (100 / minute per source).

5. Data minimisation and retention

- Inbound webhook payloads are automatically purged after thirty (30) days.
- OpenAI-side Conversations objects, traces and logs created by the Heyloha organisation are deleted automatically after seven (7) days.
- Customer-controlled retention applies on the Heyloha side to chat transcripts, contact records and visitor records.
- Voice calls are not recorded; only the text transcript is retained.

6. Logging and error monitoring

- Application logs are written in JSON to standard error.
- Error events shipped to Heyloha's error-monitoring provider pass through a scrubber that removes message bodies, subject lines, recipient lists, raw webhook payloads, authorisation headers, API keys, access and refresh tokens, cookies, the messaging-integration webhook secret, and any free-form string matching an email address.

7. Operations and personnel

- Stack: PHP 8.4 LTS with Symfony 7.4 LTS, kept on supported releases.
- Heavy webhook traffic is processed asynchronously with retry and dead-letter queues.
- Stuck inbox rows are reclaimed automatically every five minutes.
- All personnel with production access are bound by confidentiality obligations and complete a privacy and security briefing.

8. Data Protection Impact Assessments

Heyloha maintains an internal DPIA register covering the high-risk processing activities at the platform layer (OpenAI conversational AI; phone-agent calls; email-channel processing). DPIAs are reviewed at least every six months, on any material change, and after every notifiable incident. Summaries of the platform-layer DPIAs are available to the Customer on reasonable request.

9. Incident response

Heyloha operates an incident-response procedure aligned with Articles 33–34 GDPR, including triage, containment, key rotation, an internal breach register, supervisory-authority notification within seventy-two (72) hours where the threshold is met, and customer notification per §2.7 of this DPA.

Annex III — Sub-processors

A. List of Sub-processors at the Effective Date

Sub-processor	Function	Personal Data shared	Hosting region	Transfer mechanism
OpenAI Ireland Ltd. (with OpenAI OpCo, LLC as onward importer)	LLM inference, file and vector search, real-time voice	Conversation content (after pseudonymisation), uploaded files, conversation IDs	Ireland (EU); onward to United States	OpenAI Data Processing Addendum. Onward transfer to the United States under the EU-US Data Privacy Framework and the SCCs (2021/914) incorporated in that addendum; UK Addendum where applicable
Stripe Inc. / Stripe Technology Europe Ltd.	Payment processing	Customer billing data, Stripe identifiers	Ireland (EU) and US	SCCs under the Stripe DPA
Twilio Inc.	Telephony transport (no call recording configured) and regulatory compliance bundles	Phone numbers, live call audio (in stream), call metadata, identity-compliance documents	United States, with EU regional storage where elected	SCCs under the Twilio DPA
Unipile	WhatsApp, Instagram, LinkedIn and email integration	Connected-account credentials, message and email content, attachments	European Union	DPA with SCCs
Mailgun (Sinch)	Transactional email delivery (sign-up, password reset, AI events)	Recipient email, message content	EU region	SCCs under the Mailgun DPA
Sentry (Functional Software, Inc.)	Error monitoring	Stack traces and request metadata after the Heyloha-side scrubbing described in Annex II	United States	SCCs under the Sentry DPA
Langfuse GmbH	Quality monitoring of agent replies (LLM observability)	Conversation text after one-way removal of personal data, chat, session and brand identifiers, quality scores	EU (Ireland, with backups in Germany)	Langfuse Data Processing Agreement; EU hosting

Sub-processor	Function	Personal Data shared	Hosting region	Transfer mechanism
PostcodeApi	Dutch address validation	Postcode and house number	Netherlands	EU
Altum	Dutch real-estate data (home valuation, energy labels, WOZ values, historical sale and rental transactions); used only when the Customer's agent is configured to call the real-estate tools	End-user-supplied Dutch addresses	Netherlands	EU
WebBridge	Dutch mortgage calculations; used only when the Customer's agent is configured to call the mortgage tools	End-user-supplied mortgage inputs (loan amount, income, term)	Netherlands	EU
Google Ireland Ltd. (with Google LLC as onward importer)	Street View imagery and distance calculations; used only when the Customer's agent is configured to call the real-estate tools	End-user-supplied addresses or coordinates	Ireland (EU); onward to United States	EU-US Data Privacy Framework and SCCs under the Google Maps Platform terms
Mercure (Heyloha self-hosted at push.heyloha.ai)	Real-time push to widgets	Live chat messages in transit	Netherlands	Heyloha infrastructure, not a third-party transfer
TransIP (hosting)	Application and database hosting	All Personal Data Heyloha holds	Netherlands	EU

B. Notification of new or replacement Sub-processors

Heyloha publishes its current Sub-processor list at heyloha.ai/en/sub-processors, with the date of the last change. Heyloha notifies the Customer of any addition or replacement by email to the contact addresses recorded in the Heyloha dashboard, at least thirty (30) days before the new Sub-processor starts processing the Customer's Personal Data. The Customer's right to object is set out in §2.9 of this DPA.

C. Marketing-site processors (out of scope)

The processors used on the heyloha.ai marketing website (Google, LinkedIn, Meta, Cloudflare, ActiveCampaign) are not Sub-processors under this DPA. They operate solely on the heyloha.ai marketing site, are gated by consent, and do not have access to Customer Personal Data. They are listed in Heyloha's public privacy notice for completeness.

Annex IV — Transfer mechanisms

Heyloha processes Personal Data in the Netherlands, and most Sub-processors process it within the EU. Where Personal Data leaves the EEA, the transfer relies on the mechanism stated for the relevant Sub-processor in Annex III:

- **EU-US Data Privacy Framework.** Where the receiving entity is certified under the EU-US Data Privacy Framework, the transfer relies on the European Commission's adequacy decision of 10 July 2023.
- **Standard Contractual Clauses.** Where the SCCs are relied upon, alone or alongside the Data Privacy Framework, they are the SCCs incorporated in the Sub-processor's own data processing agreement, with the module and options chosen there. Where Heyloha acts as Processor on behalf of the Customer, that is Module Three (Processor-to-Processor).
- **Copies.** Heyloha provides a copy of the relevant transfer terms on the Customer's reasonable request, under §4.2.

For UK transfers, the UK International Data Transfer Addendum applies as incorporated in the relevant Sub-processor's data processing agreement. For Swiss transfers, the SCCs apply with the adjustments confirmed by the Swiss Federal Data Protection and Information Commissioner.

End of Heyloha Data Processing Agreement, version 1.3.