

# Heyloha Auftragsverarbeitungsvertrag

**Version:** 1.3

**Datum des Inkrafttretens:** das Datum der letzten Unterzeichnung durch die Parteien.

**Form:** Vorlage für Kunden. Die Parteien können die Platzhalterfelder ausfüllen und dieses Dokument als eigenständigen Auftragsverarbeitungsvertrag abschließen.

**Sprache:** Diese deutsche Fassung ist eine Übersetzung der englischen Fassung 1.3 (Heyloha Data Processing Agreement). Bei Abweichungen zwischen beiden Fassungen ist die englische Fassung maßgeblich.

## Parteien

**Heyloha by Covalore B.V.** — eine Gesellschaft mit beschränkter Haftung niederländischen Rechts (besloten vennootschap) mit Sitz in Utrecht, Niederlande, Geschäftsanschrift Regentesselaan 65, 3571 CB Utrecht, eingetragen bei der niederländischen Handelskammer (Kamer van Koophandel) unter der Nummer 99942992 (in diesem Vertrag „**Heyloha**“).

**Kunde** — \_\_\_\_\_ (Firma), \_\_\_\_\_ (Sitz und Registernummer) (in diesem Vertrag „**Kunde**“).

Jeweils eine „**Partei**“ und gemeinsam die „**Parteien**“.

## Präambel

A. Die Parteien haben einen gesonderten Vertrag geschlossen, nach dem Heyloha dem Kunden seine KI-Agenten-Plattform zur Verfügung stellt (der „**Hauptvertrag**“). Der Hauptvertrag legt zusammen mit etwaigen Bestellformularen, Konfigurationswerkzeugen und Dashboard-Einstellungen den Umfang der Leistungen fest, die Heyloha für den Kunden erbringt (die „**Leistungen**“).

B. Bei der Erbringung der Leistungen verarbeitet Heyloha personenbezogene Daten im Auftrag des Kunden.

C. Dieser Auftragsverarbeitungsvertrag (der „**AVV**“) regelt die Bedingungen, unter denen Heyloha diese personenbezogenen Daten verarbeitet, und ergänzt den Hauptvertrag. Er soll die Anforderungen von Artikel 28 der Verordnung (EU) 2016/679 („**DSGVO**“) sowie der entsprechenden Bestimmungen des britischen und des schweizerischen Datenschutzrechts erfüllen.

D. Begriffe, die im Text dieses AVV nicht definiert sind, haben die Bedeutung, die ihnen in §11 (Begriffsbestimmungen) oder, falls dort nicht definiert, im Hauptvertrag und in der DSGVO zukommt.

## 1. Gegenstand, Rollen und Rangfolge

1.1 **Rollen.** In Bezug auf personenbezogene Daten der Endnutzer, Beschäftigten, Lieferanten und anderer natürlicher Personen des Kunden, die Heyloha bei der Erbringung der Leistungen verarbeitet, ist der Kunde Verantwortlicher und Heyloha Auftragsverarbeiter. Ist der Kunde selbst Auftragsverarbeiter im Auftrag eines dritten Verantwortlichen, handelt Heyloha als Unterauftragsverarbeiter; die gleichen Pflichten gelten entsprechend.

1.2 **Gegenstand, Art, Zweck, Dauer.** Siehe Anhang I.

1.3 **Rangfolge.** Bei Widersprüchen zwischen diesem AVV, dem Hauptvertrag und einem Bestellformular gilt folgende Rangfolge: (i) dieser AVV, (ii) das Bestellformular, (iii) der Hauptvertrag.

---

## 2. Pflichten von Heyloha als Auftragsverarbeiter

2.1 **Weisungen des Kunden.** Heyloha verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Kunden. Die Weisungen des Kunden ergeben sich aus diesem AVV, dem Hauptvertrag, den Konfigurationen, die der Kunde im Heyloha-Dashboard vornimmt, und den Agenten, die er betreibt.

Abgesehen von der begrenzten Weisung in §2.12 (aggregierte und anonymisierte Statistiken) verarbeitet Heyloha personenbezogene Daten nicht für andere Zwecke, auch nicht für eigenes Marketing, Profiling oder eigene Produktentwicklung, es sei denn, Heyloha ist nach dem Recht der Union oder der Mitgliedstaaten, dem Heyloha unterliegt, hierzu verpflichtet; in einem solchen Fall teilt Heyloha dem Kunden diese rechtliche Anforderung vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht verbietet.

2.2 **Hinweis auf rechtswidrige Weisungen.** Ist Heyloha der begründeten Auffassung, dass eine Weisung des Kunden gegen die DSGVO oder andere Datenschutzbestimmungen verstößt, informiert Heyloha den Kunden unverzüglich.

2.3 **Vertraulichkeit des Personals.** Heyloha stellt sicher, dass sich alle zur Verarbeitung der personenbezogenen Daten befugten Personen vertraglich zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen und angemessen in ihren Datenschutzpflichten geschult wurden.

2.4 **Sicherheit (Artikel 32).** Heyloha trifft die in Anhang II beschriebenen technischen und organisatorischen Maßnahmen und hält sie aufrecht, unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie des Risikos für die Rechte und Freiheiten natürlicher Personen. Heyloha darf diese Maßnahmen von Zeit zu Zeit anpassen, sofern das Schutzniveau nicht wesentlich verringert wird.

2.5 **Anträge betroffener Personen.** Heyloha unterstützt den Kunden angesichts der Art der Verarbeitung nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung seiner Pflicht, Anträge betroffener Personen auf Wahrnehmung ihrer Rechte nach Kapitel III der DSGVO (Artikel 15 bis 22) zu beantworten. Erhält Heyloha einen solchen Antrag unmittelbar von einer betroffenen Person in Bezug auf personenbezogene Daten, die im Auftrag des Kunden verarbeitet werden, wird Heyloha (i) den Antrag nicht beantworten, außer um den Eingang zu bestätigen und die betroffene Person an den Kunden zu verweisen, und (ii) den Kunden unverzüglich benachrichtigen, damit dieser den Antrag als Verantwortlicher bearbeiten kann.

2.6 **Unterstützung bei weiteren Pflichten des Kunden.** Unter Berücksichtigung der Art der Verarbeitung und der Heyloha zur Verfügung stehenden Informationen unterstützt Heyloha den Kunden in angemessenem Umfang bei der Einhaltung seiner Pflichten nach den Artikeln 32 bis 36 der DSGVO (Sicherheit, Meldung von Verletzungen, Datenschutz-Folgenabschätzung und vorherige Konsultation).

2.7 **Verletzung des Schutzes personenbezogener Daten.** Heyloha meldet dem Kunden jede Verletzung des Schutzes personenbezogener Daten, die personenbezogene Daten des Kunden betrifft, unverzüglich und in jedem Fall innerhalb von zweiundsiebzig (72) Stunden, nachdem Heyloha von der Verletzung Kenntnis erlangt hat. Die Meldung enthält die in Artikel 33 Absatz 3 DSGVO genannten Informationen, soweit sie Heyloha zu diesem Zeitpunkt bekannt sind, und wird ergänzt, sobald weitere Informationen vorliegen. Meldungen werden an die im Heyloha-Dashboard hinterlegten Kontaktadressen des Kunden gesendet.

**2.8 Überprüfungen.** Heyloha stellt dem Kunden alle Informationen zur Verfügung, die zum Nachweis der Einhaltung der in diesem AVV festgelegten Pflichten vernünftigerweise erforderlich sind. Der Kunde kann nach schriftlicher Ankündigung mit einer Frist von mindestens dreißig (30) Tagen und höchstens einmal innerhalb von zwölf Monaten (oder häufiger, wenn eine zuständige Aufsichtsbehörde dies verlangt oder nach einer erheblichen Verletzung des Schutzes personenbezogener Daten) die Einhaltung dieses AVV durch Heyloha überprüfen. Heyloha kann diese Pflicht, soweit angemessen, durch die Vorlage von Prüfberichten Dritter, Zertifizierungen, ausgefüllten branchenüblichen Fragebögen und der in Anhang II genannten Unterlagen erfüllen. Überprüfungen finden während der Geschäftszeiten, mit möglichst geringer Beeinträchtigung des Betriebs von Heyloha und auf Kosten des Kunden statt; beide Parteien behandeln die Prüfergebnisse vertraulich.

**2.9 Unterauftragsverarbeiter: allgemeine Genehmigung.** Der Kunde erteilt Heyloha hiermit eine allgemeine schriftliche Genehmigung, Unterauftragsverarbeiter zur Unterstützung bei der Erbringung der Leistungen hinzuzuziehen. Die zum Datum des Inkrafttretens eingesetzten Unterauftragsverarbeiter sind in Anhang III aufgeführt. Heyloha informiert den Kunden vorab über jede Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters auf dem in Anhang III beschriebenen Weg und räumt dem Kunden mindestens dreißig (30) Tage ein, um aus berechtigten datenschutzrechtlichen Gründen Einspruch zu erheben. Erhebt der Kunde begründet Einspruch und können sich die Parteien nicht innerhalb von dreißig (30) Tagen nach dem Einspruch auf eine praktikable Lösung einigen, kann der Kunde den betroffenen Teil des Hauptvertrags durch schriftliche Mitteilung kündigen und erhält eine anteilige Erstattung im Voraus gezahlter Entgelte für den betroffenen Zeitraum.

**2.10 Pflichten der Unterauftragsverarbeiter.** Zieht Heyloha einen Unterauftragsverarbeiter hinzu, erlegt Heyloha diesem durch schriftlichen Vertrag Datenschutzpflichten auf, die den Pflichten in diesem AVV im Wesentlichen gleichwertig sind. Heyloha haftet gegenüber dem Kunden für Handlungen und Unterlassungen seiner Unterauftragsverarbeiter wie für eigene.

**2.11 Rückgabe oder Löschung nach Ende der Verarbeitung.** Bei Beendigung oder Ablauf des Hauptvertrags kann der Kunde Heyloha anweisen, (a) seine personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zurückzugeben oder (b) sie zu löschen, jeweils innerhalb von dreißig (30) Tagen nach der Weisung. Erteilt der Kunde keine Weisung, löscht Heyloha die personenbezogenen Daten innerhalb von neunzig (90) Tagen nach Vertragsende. Heyloha darf personenbezogene Daten nach Vertragsende nur aufbewahren, soweit und solange dies nach dem Recht der Union oder der Mitgliedstaaten vorgeschrieben ist (zum Beispiel gesetzliche Aufbewahrungspflichten für Rechnungsdaten); während dieses Zeitraums werden die Daten von der aktiven Verarbeitung getrennt und durch geeignete Maßnahmen geschützt.

**2.12 Aggregierte und anonymisierte Statistiken.** Der Kunde weist Heyloha an, personenbezogene Daten ausschließlich zu dem zusätzlichen Zweck zu verarbeiten, aggregierte Statistiken über die Nutzung und Leistungsfähigkeit der Leistungen zu erstellen; Heyloha darf die daraus resultierenden aggregierten Daten nutzen, um die Leistungen zu betreiben, abzusichern und zu verbessern sowie um Branchenstatistiken und Benchmarks zu veröffentlichen. Jede der folgenden Bedingungen ist Voraussetzung dieser Weisung:

(a) die Aggregation erfolgt innerhalb der in §4.1 beschriebenen Verarbeitungsumgebung von Heyloha, und das Ergebnis wird so anonymisiert, dass weder Heyloha noch ein Empfänger eine betroffene Person oder einen Kunden unter Berücksichtigung aller Mittel, die nach allgemeinem Ermessen wahrscheinlich genutzt werden, direkt oder indirekt identifizieren kann;

(b) Heyloha wird nicht versuchen, die Anonymisierung rückgängig zu machen, und das aggregierte Ergebnis nicht mit anderen Daten zusammenführen, um eine Person oder einen Kunden erneut zu identifizieren;

(c) kein Ergebnis nennt oder beschreibt einen identifizierbaren Kunden, und kein Ergebnis ermöglicht es, einen Kunden oder eine betroffene Person durch Rückschluss aus einer kleinen Stichprobe auszusondern; Aggregate beruhen auf einer Grundgesamtheit von mindestens fünfundzwanzig (25) Kunden und eintausend (1.000) Interaktionen;

(d) es werden keine Freitextinhalte, Transkripte, Aufzeichnungen, Kontaktdaten oder Inhalte der Wissensdatenbank veröffentlicht, zitiert oder offengelegt, weder wörtlich noch sinngemäß;

(e) die zugrunde liegenden personenbezogenen Daten unterliegen weiterhin allen anderen Pflichten aus diesem AVV, einschließlich §2.4 (Sicherheit), §2.11 (Rückgabe oder Löschung) und der vom Kunden eingestellten Aufbewahrungsfristen; und

(f) der Kunde kann diese Weisung jederzeit mit Wirkung für künftige Verarbeitungen durch schriftliche Mitteilung an Heyloha nach §10 widerrufen. Der Widerruf berührt weder den übrigen AVV noch die Leistungen noch bereits rechtmäßig erstellte aggregierte Ergebnisse.

Zur Klarstellung: Diese Weisung erlaubt Heyloha nicht, personenbezogene Daten für Profiling, für das Training oder Fine-Tuning von Modellen, für Werbung oder für Zwecke zu verarbeiten, die sich an einzelne betroffene Personen richten.

**2.13 Kein Training von Modellen.** Heyloha verwendet Gesprächsinhalte, Transkripte, Inhalte der Wissensdatenbank oder andere nach diesem AVV verarbeitete personenbezogene Daten nicht, um Modelle der künstlichen Intelligenz zu trainieren, feinabzustimmen oder zu verbessern. Der Unterauftragsverarbeiter von Heyloha für Sprachmodelle (OpenAI, Anhang III) verarbeitet solche Inhalte nach Geschäftsbedingungen, die ihre Verwendung zur Entwicklung oder Verbesserung der Dienste von OpenAI, einschließlich des Trainings von Modellen, ausschließen, und Heyloha hat keiner solchen Verwendung zugestimmt. Heyloha wird ohne vorherige schriftliche Zustimmung des Kunden keinen Unterauftragsverarbeiter für Sprachmodelle hinzuziehen, der solche Inhalte für das Training von Modellen verwenden darf.

---

## 3. Pflichten des Kunden als Verantwortlicher

**3.1 Rechtsgrundlage und Informationen.** Der Kunde sichert zu, dass er für die Verarbeitung, die er über die Leistungen durchführt, eine Rechtsgrundlage nach der DSGVO hat und während der gesamten Laufzeit aufrechterhält und dass er den betroffenen Personen alle nach Artikel 13 und 14 DSGVO erforderlichen Informationen bereitgestellt hat.

**3.2 Weisungen durch Konfiguration.** Der Kunde erkennt an, dass die Leistungen weitgehend konfigurierbar sind und dass mehrere Entscheidungen, die einem Verantwortlichen obliegen, vom Kunden im Heyloha-Dashboard getroffen werden, darunter welche Kanäle aktiviert werden, welche Datenfelder erhoben werden, welche Aufbewahrungsfristen gelten, welche Unterauftragsverarbeiter über Integrationen genutzt werden und welche Inhalte in die Wissensdatenbank hochgeladen werden. Der Kunde stellt sicher, dass diese Konfigurationen dem geltenden Datenschutzrecht entsprechen und auf einer gültigen Rechtsgrundlage beruhen.

**3.3 Mitwirkung.** Der Kunde wirkt in angemessenem Umfang mit, damit Heyloha seine Pflichten aus diesem AVV erfüllen kann, insbesondere indem er die zur Beantwortung eines Antrags einer betroffenen Person oder einer Anfrage einer Aufsichtsbehörde erforderlichen Informationen umgehend bereitstellt.

**3.4 Keine besonderen Kategorien personenbezogener Daten ohne Anzeige.** Der Kunde leitet besondere Kategorien personenbezogener Daten im Sinne von Artikel 9 DSGVO oder Daten über strafrechtliche Verurteilungen und Straftaten im Sinne von Artikel 10 DSGVO nicht bewusst über die Leistungen, ohne Heyloha vorab zu informieren und sicherzustellen, dass eine zusätzliche Rechtsgrundlage besteht. Der

Kunde erkennt an, dass besondere Kategorien personenbezogener Daten beiläufig in Freitexteingaben von Endnutzern vorkommen können; Heyloha wendet auf schriftliche Chat-Eingaben die in Anhang II beschriebene Pseudonymisierung an.

---

## 4. Internationale Datenübermittlungen

**4.1 Verarbeitungsort von Heyloha.** Heyloha verarbeitet personenbezogene Daten in erster Linie in den Niederlanden. Datenbank und Anwendungsinfrastruktur werden innerhalb der Europäischen Union gehostet.

**4.2 Weiterübermittlung an Unterauftragsverarbeiter außerhalb der EU.** Werden personenbezogene Daten an einen Unterauftragsverarbeiter oder von einem Unterauftragsverarbeiter weiter in ein Land außerhalb des Europäischen Wirtschaftsraums, des Vereinigten Königreichs oder der Schweiz übermittelt, für das kein Angemessenheitsbeschluss besteht, stellt Heyloha sicher, dass ein geeigneter Übermittlungsmechanismus besteht. Die aktuellen Übermittlungsmechanismen sind in Anhang III aufgeführt und in Anhang IV beschrieben. Auf Anfrage des Kunden stellt Heyloha, soweit zumutbar, eine Kopie der maßgeblichen Übermittlungsbedingungen zur Verfügung, sofern der Vertrag mit dem Unterauftragsverarbeiter dies zulässt.

**4.3 Daten aus dem Vereinigten Königreich und der Schweiz.** Fallen personenbezogene Daten in den Anwendungsbereich der UK GDPR oder des schweizerischen Bundesgesetzes über den Datenschutz, gelten die entsprechenden Übermittlungsmechanismen (UK International Data Transfer Addendum beziehungsweise vom Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) anerkannte Standardvertragsklauseln) durch Verweis.

**4.4 Transfer-Folgenabschätzungen.** Heyloha führt Transfer-Folgenabschätzungen für die wesentlichen Unterauftragsverarbeiter außerhalb des EWR und stellt dem Kunden auf Anfrage, soweit zumutbar, eine Zusammenfassung zur Verfügung.

---

## 5. Haftung

Die Haftung jeder Partei aus diesem AVV, gleich ob vertraglich, deliktisch oder aus anderem Rechtsgrund, unterliegt der Haftungsbegrenzung und den Haftungsausschlüssen des Hauptvertrags. Dieser AVV beschränkt oder schließt keine Haftung aus, die nach geltendem Recht nicht beschränkt oder ausgeschlossen werden kann, einschließlich der Haftung einer Partei gegenüber einer betroffenen Person nach Artikel 82 DSGVO.

---

## 6. Laufzeit und Beendigung

Dieser AVV wird am Datum des Inkrafttretens wirksam und gilt, solange Heyloha personenbezogene Daten im Auftrag des Kunden verarbeitet. Bestimmungen, die ihrer Natur nach über die Beendigung hinaus fortgelten sollen, insbesondere §2.11 (Rückgabe oder Löschung), §5 (Haftung), §7 (anwendbares Recht) und §10 (Mitteilungen), bleiben auch nach Beendigung dieses AVV und des Hauptvertrags wirksam.

---

---

## 7. Anwendbares Recht und Gerichtsstand

Dieser AVV unterliegt niederländischem Recht. Ausschließlicher Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit diesem AVV ist Utrecht, Niederlande, unbeschadet der Rechte betroffener Personen nach Artikel 79 DSGVO und zwingender Verbraucherschutzrechtlicher Bestimmungen.

---

## 8. Änderungen

Heyloha kann diesen AVV von Zeit zu Zeit anpassen, um (i) Änderungen des geltenden Datenschutzrechts, (ii) Entscheidungen von Aufsichtsbehörden oder zuständigen Gerichten oder (iii) Änderungen der Leistungen oder der Liste der Unterauftragsverarbeiter Rechnung zu tragen. Wesentliche Änderungen werden dem Kunden mindestens dreißig (30) Tage vor ihrem Inkrafttreten mitgeteilt.

---

## 9. Salvatorische Klausel

Sollte eine Bestimmung dieses AVV unwirksam oder undurchführbar sein, bleiben die übrigen Bestimmungen in vollem Umfang wirksam; die Parteien werden nach Treu und Glauben verhandeln, um die unwirksame Bestimmung durch eine wirksame zu ersetzen, die ein wirtschaftlich und rechtlich gleichwertiges Ergebnis erzielt.

---

## 10. Mitteilungen

Mitteilungen an Heyloha nach diesem AVV werden an **Stefan Hoogers** unter [support@heyloha.ai](mailto:support@heyloha.ai) gesendet, mit Kopie an **Heyloha by Covalore B.V., Regentesselaan 65, 3571 CB Utrecht, Niederlande**. Mitteilungen an den Kunden werden an die im Heyloha-Dashboard hinterlegten Kontaktadressen gesendet.

---

## 11. Begriffsbestimmungen

Für die Zwecke dieses AVV gilt:

- „**Verantwortlicher**“, „**Auftragsverarbeiter**“, „**Unterauftragsverarbeiter**“, „**personenbezogene Daten**“, „**Verletzung des Schutzes personenbezogener Daten**“, „**Verarbeitung**“, „**betroffene Person**“ und „**Aufsichtsbehörde**“ haben die Bedeutung, die ihnen in der DSGVO zukommt.
- „**DSGVO**“ bezeichnet die Verordnung (EU) 2016/679 in der jeweils geltenden Fassung einschließlich etwaiger Nachfolgeregelungen und umfasst, soweit der Zusammenhang es erfordert, die entsprechenden Bestimmungen der UK GDPR und des schweizerischen Bundesgesetzes über den Datenschutz.
- „**Standardvertragsklauseln**“ bezeichnet die von der Europäischen Kommission am 4. Juni 2021 erlassenen Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer (Durchführungsbeschluss (EU) 2021/914) in der jeweils geltenden Fassung einschließlich etwaiger Nachfolgeregelungen und umfasst gegebenenfalls das UK International Data Transfer Addendum.
- „**Leistungen**“ hat die im Hauptvertrag festgelegte Bedeutung und wird in Anhang I beschrieben.

- „**Unterauftragsverarbeiter**“ bezeichnet einen Dritten, den Heyloha hinzuzieht, um personenbezogene Daten im Auftrag des Kunden im Zusammenhang mit den Leistungen zu verarbeiten. Die aktuelle Liste befindet sich in Anhang III.

## Unterschriften

| Für Heyloha by Covalore B.V.           | Für den Kunden      |
|----------------------------------------|---------------------|
| Name: Stefan Hoogers                   | Name: _____         |
| Funktion: Geschäftsführer (bestuurder) | Funktion: _____     |
| Datum: _____                           | Datum: _____        |
| Unterschrift: _____                    | Unterschrift: _____ |

# Anhang I — Einzelheiten der Verarbeitung

## A. Liste der Parteien

| Rolle                                   | Identität                                                                                                                                                                 |
|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Datenexporteur<br>(Verantwortlicher)    | Der zu Beginn dieses AVV genannte Kunde                                                                                                                                   |
| Datenimporteur<br>(Auftragsverarbeiter) | Heyloha by Covalore B.V., Regentesselaan 65, 3571 CB Utrecht, Niederlande. Datenschutzkontakt: Stefan Hoogers, <a href="mailto:support@heyloha.ai">support@heyloha.ai</a> |

## B. Beschreibung der Verarbeitung

- **Gegenstand.** Erbringung der Leistungen, nämlich der KI-Agenten-Plattform von Heyloha über Web-Chat, Telefon, WhatsApp, Instagram, LinkedIn und E-Mail, einschließlich des zugehörigen Dashboards, der Wissensdatenbank, der Integrationen und der Auswertungsfunktionen.
- **Art und Zweck.** Betrieb von KI-Agenten im Auftrag des Kunden, um mit den Endnutzern des Kunden zu kommunizieren, Antworten zu erstellen, Kontaktdaten zu erfassen, sofern der Agent des Kunden dafür konfiguriert ist, Termine zu vereinbaren, Informationen über vom Kunden konfigurierte Tool-Integrationen abzurufen und ein Gesprächstranskript zu erstellen, das der Kunde im Heyloha-Dashboard einsehen kann. Pflege der Wissensdatenbank des Kunden aus Inhalten, die der Kunde hochlädt oder verbindet (Dateien, Webseiten), und, sofern der Kunde dies aktiviert, aus wiederverwendbarem Wissen, das aus den vom Kunden selbst gesendeten E-Mails gewonnen wird, nachdem personenbezogene Daten entfernt wurden und das Ergebnis vor der Verwendung geprüft wurde. Überwachung der Qualität der Antworten der Agenten.
- **Kategorien personenbezogener Daten.**
  - Freitextinhalte von Nachrichten der Endnutzer und Antworten der Agenten.
  - Vom Agenten erfasste Kontaktdaten, sofern der Kunde die Erfassung konfiguriert hat: Name, E-Mail-Adresse, Telefonnummer, Postleitzahl, Hausnummer.
  - Sitzungsmerkmale im Web-Chat: User-Agent, Browser, Bildschirmauflösung, Sprache, Zeitzone, aktuelle URL, Referrer, Gerätetyp, UTM-Parameter, Traffic-Quelle.
  - Telefonnummer des Anrufers und Live-Audio des Anrufs (nur im Datenstrom) bei Telefonaten; das daraus erstellte Texttranskript.
  - Absender, Empfänger, Betreff, Inhalt, Header und Anhänge bei der Verarbeitung im E-Mail-Kanal.
  - Vom Kunden bereitgestellte Zugangsdaten für die Integration der Messaging-Kanäle (von Heyloha verschlüsselt gespeichert).
  - Vom Kunden bereitgestellte oder verbundene Inhalte der Wissensdatenbank (Dateien, Webseiten und aus den gesendeten E-Mails des Kunden gewonnenes Wissen), die beiläufig personenbezogene Daten enthalten können.
  - Termin- und Kalenderdaten, sofern der Kunde einen Kalender verbindet: Datum und Uhrzeit, Betreff sowie Name und Kontaktdaten des Teilnehmers.
  - Daten, die von vom Kunden konfigurierten Tool-Integrationen zurückgegeben werden, etwa Abfragen in CRM-, Webshop- oder Buchungssystemen.

- **Kategorien betroffener Personen.** Die Endnutzer des Kunden (Website-Besucher, Anrufer, Nutzer von Messaging-Apps, E-Mail-Korrespondenten); Dritte, die von Endnutzern in ihren Interaktionen genannt werden; die Beschäftigten des Kunden, die das Heyloha-Dashboard nutzen.
  - **Besondere Kategorien personenbezogener Daten.** Werden nicht bewusst erhoben. Beiläufige Inhalte besonderer Kategorien können in Freitexteingaben vorkommen. Heyloha wendet die in Anhang II beschriebene Pseudonymisierung an.
  - **Häufigkeit.** Fortlaufend während der Laufzeit des Hauptvertrags.
  - **Dauer.** Für die Laufzeit des Hauptvertrags zuzüglich der in §2.11 festgelegten Frist für Rückgabe oder Löschung nach Vertragsende.
- 

## C. Zuständige Aufsichtsbehörde

Autoriteit Persoonsgegevens (niederländische Datenschutzbehörde), Postbus 93374, 2509 AJ Den Haag, Niederlande.

---

# Anhang II — Technische und organisatorische Maßnahmen

Dieser Anhang fasst die Maßnahmen zusammen, mit denen Heyloha personenbezogene Daten schützt. Eine ausführlichere Compliance-Übersicht, die dieselben Maßnahmen beschreibt, ist auf Anfrage unter [support@heyloha.ai](mailto:support@heyloha.ai) erhältlich.

---

## 1. Verschlüsselung

- **Bei der Übertragung.** Alle für Kunden erreichbaren Endpunkte verwenden ausschließlich HTTPS mit aktuellen TLS-Versionen. Zertifikate werden je Host von Let's Encrypt ausgestellt und automatisch erneuert.
  - **Im Ruhezustand auf Anwendungsebene.** Sensible Zugangsdaten (Geheimnisse ausgehender Webhooks, Zugangsdaten für Tool-Integrationen Dritter wie Shopify-Zugriffstoken) werden mit authentifizierter symmetrischer Verschlüsselung (auf Basis von libsodium) in einem versionierten Umschlag verschlüsselt, der Schlüsselrotation unterstützt.
  - **Infrastrukturstandort.** Datenbank und Dateispeicher werden auf niederländischer Infrastruktur gehostet (siehe TransIP in Anhang III).
  - **Netzwerkisolierung.** Die Datenbank befindet sich in einem privaten Netzwerk und ist nicht aus dem öffentlichen Internet erreichbar.
- 

## 2. Pseudonymisierung von Freitexteingaben

Freitexteingaben, die für die OpenAI Responses API bestimmt sind, durchlaufen eine Pseudonymisierungsschicht, die reguläre Ausdrücke mit Named-Entity-Recognition kombiniert. Die Schicht erkennt die Entitäten NAME, EMAIL, PHONE, POSTAL, HOUSENR, ADDRESS, BSN (niederländische Identifikationsnummer), IBAN, IP, PLATE und LOCATION und ersetzt sie durch stabile Token je Chat, bevor die Anfrage Heyloha verlässt. Die Rückzuordnung wird im Chat-Datensatz gespeichert und verwendet, um in der Antwort des Modells an den Endnutzer die ursprünglichen Werte wiederherzustellen. Die zugrunde liegenden personenbezogenen Daten erscheinen nicht im Klartext im Anfragetext an OpenAI.

---

## 3. Authentifizierung und Zugriffskontrolle

- Kundenkonten verwenden eine E-Mail-Adresse und ein mit bcrypt gehashtes Passwort.
  - Der API-Zugriff erfolgt über kurzlebige JWT-Bearer-Token mit Refresh-Token.
  - Die Autorisierung ist rollenbasiert; die am höchsten privilegierten Vorgänge erfordern `ROLE_SUPER_ADMIN`.
  - Der Produktionszugriff durch Personal von Heyloha ist auf namentlich benannte Personen nach dem Need-to-know-Prinzip beschränkt.
- 

## 4. Webhook-Authentifizierung, Ratenbegrenzung und Missbrauchsschutz

- Eingehende Webhooks werden per Signatur oder gemeinsamem Geheimnis authentifiziert.
- Ausgehende Webhooks werden mit einer HMAC-SHA256-Signatur signiert, die der Kunde prüfen kann, sofern der Kunde für den Webhook ein Signaturgeheimnis konfiguriert hat.

- Für sensible Schnittstellen gelten Ratenbegrenzungen, unter anderem für den Versand ausgehender Webhooks (60 pro Minute) und die Annahme eingehender E-Mail-Webhooks (100 pro Minute je Quelle).
- 

## 5. Datenminimierung und Aufbewahrung

- Nutzdaten eingehender Webhooks werden nach dreißig (30) Tagen automatisch gelöscht.
  - Auf Seiten von OpenAI werden Conversations-Objekte, Traces und Logs, die von der Heyloha-Organisation erstellt wurden, nach sieben (7) Tagen automatisch gelöscht.
  - Auf Seiten von Heyloha gelten für Chat-Transkripte, Kontaktdatensätze und Besucherdatensätze die vom Kunden festgelegten Aufbewahrungsfristen.
  - Anrufe werden nicht aufgezeichnet; gespeichert wird nur das Texttranskript.
- 

## 6. Protokollierung und Fehlerüberwachung

- Anwendungsprotokolle werden im JSON-Format auf die Standardfehlerausgabe geschrieben.
  - Fehlerereignisse, die an den Fehlerüberwachungsdienst von Heyloha übermittelt werden, durchlaufen einen Filter, der Nachrichteninhalte, Betreffzeilen, Empfängerlisten, rohe Webhook-Nutzdaten, Authorization-Header, API-Schlüssel, Zugriffs- und Refresh-Token, Cookies, das Webhook-Geheimnis der Messaging-Integration und jede Freitext-Zeichenfolge entfernt, die einer E-Mail-Adresse entspricht.
- 

## 7. Betrieb und Personal

- Technologie: PHP 8.4 LTS mit Symfony 7.4 LTS, auf unterstützten Versionen gehalten.
  - Hohes Webhook-Aufkommen wird asynchron mit Wiederholungsversuchen und Dead-Letter-Queues verarbeitet.
  - Hängengebliebene Einträge in der Eingangswarteschlange werden alle fünf Minuten automatisch wieder aufgenommen.
  - Alle Mitarbeitenden mit Produktionszugriff sind zur Vertraulichkeit verpflichtet und absolvieren eine Einweisung in Datenschutz und Sicherheit.
- 

## 8. Datenschutz-Folgenabschätzungen

Heyloha führt ein internes Verzeichnis von Datenschutz-Folgenabschätzungen für die Verarbeitungstätigkeiten mit hohem Risiko auf Plattformebene (konversationelle KI mit OpenAI; Telefonagenten; Verarbeitung im E-Mail-Kanal). Die Datenschutz-Folgenabschätzungen werden mindestens alle sechs Monate, bei jeder wesentlichen Änderung und nach jedem meldepflichtigen Vorfall überprüft. Zusammenfassungen der Datenschutz-Folgenabschätzungen auf Plattformebene stellt Heyloha dem Kunden auf Anfrage, soweit zumutbar, zur Verfügung.

---

## 9. Reaktion auf Sicherheitsvorfälle

Heyloha betreibt ein an den Artikeln 33 und 34 DSGVO ausgerichtetes Verfahren zur Reaktion auf Sicherheitsvorfälle, einschließlich Triage, Eindämmung, Schlüsselrotation, eines internen Verzeichnisses von

Datenschutzverletzungen, der Meldung an die Aufsichtsbehörde innerhalb von zweiundsiebzig (72) Stunden, sofern die Meldeschwelle erreicht ist, und der Benachrichtigung des Kunden nach §2.7 dieses AVV.

---

# Anhang III — Unterauftragsverarbeiter

## A. Liste der Unterauftragsverarbeiter zum Datum des Inkrafttretens

| Unterauftragsverarbeiter                                                | Funktion                                                                                            | Übermittelte personenbezogene Daten                                                                     | Hosting-Region                                                | Übermittlungsmechanismus                                                                                                                                                                                                                |
|-------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| OpenAI Ireland Ltd. (mit OpenAI OpCo, LLC als nachgelagerter Importeur) | LLM-Inferenz, Datei- und Vektorsuche, Echtzeit-Sprache                                              | Gesprächsinhalte (nach Pseudonymisierung), hochgeladene Dateien, Gesprächs-IDs                          | Irland (EU); Weiterübermittlung in die Vereinigten Staaten    | OpenAI Data Processing Addendum. Weiterübermittlung in die Vereinigten Staaten auf Grundlage des EU-US Data Privacy Framework und der in diesem Addendum enthaltenen Standardvertragsklauseln (2021/914); UK Addendum, soweit anwendbar |
| Stripe Inc. / Stripe Technology Europe Ltd.                             | Zahlungsabwicklung                                                                                  | Rechnungsdaten des Kunden, Stripe-Kennungen                                                             | Irland (EU) und USA                                           | Standardvertragsklauseln gemäß Stripe DPA                                                                                                                                                                                               |
| Twilio Inc.                                                             | Telefonie-Transport (keine Anrufaufzeichnung konfiguriert) und regulatorische Compliance-Unterlagen | Telefonnummern, Live-Audio des Anrufs (im Datenstrom), Anrufmetadaten, Unterlagen zur Identitätsprüfung | Vereinigte Staaten, mit Speicherung in der EU, sofern gewählt | Standardvertragsklauseln gemäß Twilio DPA                                                                                                                                                                                               |
| Unipile                                                                 | Integration von WhatsApp, Instagram, LinkedIn und E-Mail                                            | Zugangsdaten verbundener Konten, Nachrichten- und E-Mail-Inhalte, Anhänge                               | Europäische Union                                             | DPA mit Standardvertragsklauseln                                                                                                                                                                                                        |
| Mailgun (Sinch)                                                         | Versand transaktionaler E-Mails (Registrierung, Zurücksetzen des Passworts, KI-Ereignisse)          | E-Mail-Adresse des Empfängers, Nachrichteninhalt                                                        | EU-Region                                                     | Standardvertragsklauseln gemäß Mailgun DPA                                                                                                                                                                                              |
| Sentry (Functional Software, Inc.)                                      | Fehlerüberwachung                                                                                   | Stacktraces und Anfrage-Metadaten nach der in Anhang II beschriebenen Bereinigung durch Heyloha         | Vereinigte Staaten                                            | Standardvertragsklauseln gemäß Sentry DPA                                                                                                                                                                                               |

| Unterauftragsverarbeiter                                          | Funktion                                                                                                                                                                                             | Übermittelte personenbezogene Daten                                                                                              | Hosting-Region                                             | Übermittlungsmechanismus                                                                       |
|-------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| Langfuse GmbH                                                     | Qualitätsüberwachung der Antworten der Agenten (LLM-Observability)                                                                                                                                   | Gesprächstext nach unumkehrbarer Entfernung personenbezogener Daten, Chat-, Sitzungs- und Marken-Kennungen, Qualitätsbewertungen | EU (Irland, mit Sicherungskopien in Deutschland)           | Langfuse Data Processing Agreement; Hosting in der EU                                          |
| PostcodeApi                                                       | Prüfung niederländischer Adressen                                                                                                                                                                    | Postleitzahl und Hausnummer                                                                                                      | Niederlande                                                | EU                                                                                             |
| Altum                                                             | Niederländische Immobilien-daten (Wertermittlung, Energieausweise, WOZ-Werte, historische Verkaufs- und Mietdaten); nur genutzt, wenn der Agent des Kunden für die Immobilien-Tools konfiguriert ist | Von Endnutzern angegebene niederländische Adressen                                                                               | Niederlande                                                | EU                                                                                             |
| WebBridge                                                         | Niederländische Hypothekenberechnungen; nur genutzt, wenn der Agent des Kunden für die Hypotheken-Tools konfiguriert ist                                                                             | Von Endnutzern angegebene Hypothekendaten (Darlehensbetrag, Einkommen, Laufzeit)                                                 | Niederlande                                                | EU                                                                                             |
| Google Ireland Ltd. (mit Google LLC als nachgelagertem Importeur) | Street-View-Bilder und Entfernungsberechnungen; nur genutzt, wenn der Agent des Kunden für die Immobilien-Tools konfiguriert ist                                                                     | Von Endnutzern angegebene Adressen oder Koordinaten                                                                              | Irland (EU); Weiterübermittlung in die Vereinigten Staaten | EU-US Data Privacy Framework und Standardvertragsklauseln gemäß den Google Maps Platform Terms |
| Mercure (von Heyloha selbst betrieben unter push.heyloha.ai)      | Echtzeit-Push an Widgets                                                                                                                                                                             | Live-Chat-Nachrichten während der Übertragung                                                                                    | Niederlande                                                | Infrastruktur von Heyloha, keine Übermittlung an Dritte                                        |
| TransIP (Hosting)                                                 | Hosting von Anwendung und Datenbank                                                                                                                                                                  | Alle personenbezogenen Daten, die Heyloha speichert                                                                              | Niederlande                                                | EU                                                                                             |

---

## **B. Mitteilung neuer oder ersetzter Unterauftragsverarbeiter**

Heyloha veröffentlicht die aktuelle Liste der Unterauftragsverarbeiter unter [heyloha.ai/de/unterauftragsverarbeiter](https://heyloha.ai/de/unterauftragsverarbeiter), mit dem Datum der letzten Änderung. Heyloha informiert den Kunden über jede Hinzuziehung oder Ersetzung per E-Mail an die im Heyloha-Dashboard hinterlegten Kontaktadressen, mindestens dreißig (30) Tage bevor der neue Unterauftragsverarbeiter mit der Verarbeitung personenbezogener Daten des Kunden beginnt. Das Einspruchsrecht des Kunden ist in §2.9 dieses AVV geregelt.

---

## **C. Dienste der Marketing-Website (nicht Gegenstand dieses AVV)**

Die auf der Marketing-Website [heyloha.ai](https://heyloha.ai) eingesetzten Dienste (Google, LinkedIn, Meta, Cloudflare, ActiveCampaign) sind keine Unterauftragsverarbeiter im Sinne dieses AVV. Sie werden ausschließlich auf der Marketing-Website [heyloha.ai](https://heyloha.ai) eingesetzt, nur nach Einwilligung aktiviert und haben keinen Zugriff auf personenbezogene Daten des Kunden. Sie sind der Vollständigkeit halber in der öffentlichen Datenschutzerklärung von Heyloha aufgeführt.

---

# Anhang IV — Übermittlungsmechanismen

Heyloha verarbeitet personenbezogene Daten in den Niederlanden, und die meisten Unterauftragsverarbeiter verarbeiten sie innerhalb der EU. Verlassen personenbezogene Daten den EWR, stützt sich die Übermittlung auf den in Anhang III für den jeweiligen Unterauftragsverarbeiter angegebenen Mechanismus:

- **EU-US Data Privacy Framework.** Ist die empfangende Stelle nach dem EU-US Data Privacy Framework zertifiziert, stützt sich die Übermittlung auf den Angemessenheitsbeschluss der Europäischen Kommission vom 10. Juli 2023.
- **Standardvertragsklauseln.** Werden Standardvertragsklauseln allein oder neben dem Data Privacy Framework herangezogen, handelt es sich um die im Auftragsverarbeitungsvertrag des jeweiligen Unterauftragsverarbeiters enthaltenen Standardvertragsklauseln mit dem dort gewählten Modul und den dort gewählten Optionen. Handelt Heyloha als Auftragsverarbeiter im Auftrag des Kunden, ist dies Modul drei (Übermittlung von Auftragsverarbeitern an Auftragsverarbeiter).
- **Kopien.** Auf Anfrage des Kunden stellt Heyloha, soweit zumutbar, nach §4.2 eine Kopie der maßgeblichen Übermittlungsbedingungen zur Verfügung.

Für Übermittlungen aus dem Vereinigten Königreich gilt das UK International Data Transfer Addendum, wie es im Auftragsverarbeitungsvertrag des jeweiligen Unterauftragsverarbeiters enthalten ist. Für Übermittlungen aus der Schweiz gelten die Standardvertragsklauseln mit den vom Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) bestätigten Anpassungen.

---

*Ende des Heyloha Auftragsverarbeitungsvertrags, Version 1.3 (deutsche Fassung).*