HAL

A Cloud Frontier ApS · CVR 37174181 · Aalborg, Denmark

Data Processing Agreement

Version 1.1 · Effective date: 29 October 2026

This Data Processing Agreement ("DPA") is entered into between:

(1) the Customer identified in the Terms of Service or order form (the "Controller"); and
(2) A Cloud Frontier ApS, CVR no. 37174181, with registered address at Ivigtutvej 2, 9210 Aalborg SØ, Denmark (the "Processor", "Hal", "we").

Each a "Party" and together the "Parties". This DPA forms an integral part of the Terms of Service available at gethal.ai/legal (the "Agreement"). In the event of conflict between this DPA and the Agreement, this DPA prevails in relation to the processing of personal data.

This DPA is concluded electronically when the Controller accepts it in the Service. Hal keeps a record of each acceptance (version, time, user, and company) and provides it to the Controller on request. The current version is available as a PDF at gethal.ai/dpa.pdf, and each version at a versioned address (for example gethal.ai/dpa-v1.1.pdf), so the Controller can keep the exact version it accepted.

Version 1.1 applies to new acceptances from 29 October 2026, and to Controllers who accepted an earlier version from 28 November 2026, or from their acceptance of this version in the Service if earlier.

1. Definitions

Capitalised terms not defined here have the meaning given in the Agreement or in Regulation (EU) 2016/679 ("GDPR").

- **"Personal Data"** means any information relating to an identified or identifiable natural person, as defined in the GDPR, that is processed by Hal on behalf of the Controller under the Agreement.
- **"Processing", "Controller", "Processor", "Data Subject", "Supervisory Authority", and "Personal Data Breach"** have the meanings given in the GDPR.
- **"Sub-processor"** means any third party engaged by Hal to process Personal Data on behalf of the Controller.
- **"SCCs"** means the Standard Contractual Clauses approved by the European Commission in Decision 2021/914 of 4 June 2021.
- **"Hal"** means A Cloud Frontier ApS, the Processor. **"HAL"** means the software agent through which Hal provides the Service.

2. Subject Matter and Scope

2.1 Hal processes Personal Data solely as a Processor on behalf of the Controller, for the purpose of providing the Service as described in the Agreement.

2.2 The subject matter, duration, nature, and purpose of the processing, as well as the types of Personal Data and categories of Data Subjects, are set out in Annex 1.

2.3 The Controller remains the Controller of the Personal Data and is responsible for the lawfulness of the processing, including having a valid legal basis under the GDPR for instructing Hal to process the Personal Data.

3. Controller's Instructions

3.1 Hal processes Personal Data only on the documented instructions of the Controller. The Agreement, this DPA, and the Controller's configuration and use of the Service constitute the Controller's documented instructions.

3.2 Hal will immediately inform the Controller if, in Hal's opinion, an instruction infringes the GDPR or other Union or Member State data protection law. Hal does not monitor the content of Customer instructions or usage and is not obliged to assess their lawfulness proactively. The Controller remains solely responsible for ensuring that all instructions to Hal have a valid legal basis under the GDPR.

3.3 If Hal is required to process Personal Data to comply with Union or Member State law, Hal will inform the Controller of that legal requirement before processing, unless that law prohibits such disclosure on important grounds of public interest.

4. Confidentiality

4.1 Hal ensures that persons authorised to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

4.2 Access to Personal Data is restricted to personnel who need it to perform their duties.

5. Security of Processing

5.1 Hal implements appropriate technical and organisational measures ("TOMs") to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of processing.

5.2 The TOMs in force as at the Effective Date are described in Annex 2. Hal may update the TOMs from time to time, provided the overall level of security is not materially reduced.

6. Sub-processors

6.1 **General authorisation.** The Controller grants Hal general written authorisation to engage Sub-processors for the processing of Personal Data. The current list of Sub-processors is maintained at gethal.ai/subprocessors, including those listed in Annex 3.

6.2 **Changes.** Hal will notify the Controller of any intended addition or replacement of a Sub-processor at least 14 days in advance by updating the list at gethal.ai/subprocessors. Controllers who wish to be

notified by email may register their preference by writing to jan.verdier@acloudfrontier.com.

6.3 **Right to object.** The Controller may object on reasonable data protection grounds within the 14-day notice period by writing to jan.verdier@acloudfrontier.com. If the Parties cannot agree on a resolution, the Controller may terminate the Agreement without penalty with respect to the processing affected by the new Sub-processor; any unused credits associated with that processing will be refunded pro rata.

6.4 **Sub-processor obligations.** Hal will impose on each Sub-processor, by written contract, data protection obligations substantially the same as those in this DPA. Hal remains fully liable to the Controller for the performance of each Sub-processor's obligations.

6.5 **Customer-provided integrations.** Where the Controller provides credentials or access tokens enabling the Service to interact with the Controller's own third-party accounts (for example, the Controller's Microsoft 365 mailbox via Microsoft Graph to send outreach emails on the Controller's behalf), the providers of those accounts are selected and contracted with by the Controller, not by Hal, and are not Sub-processors of Hal under this DPA. The Controller remains responsible for its direct relationship with such providers.

7. Assistance to the Controller

7.1 **Data subject requests.** Taking into account the nature of the processing, Hal will assist the Controller by appropriate technical and organisational measures, insofar as this is possible, to respond to requests from Data Subjects to exercise their rights under the GDPR. Where a Data Subject contacts Hal directly, Hal will forward the request to the Controller without undue delay.

7.2 **Compliance assistance.** Taking into account the nature of the processing and the information available to Hal, Hal will on a reasonable efforts basis assist the Controller in ensuring compliance with the obligations under Articles 32 to 36 of the GDPR, including security, breach notification, data protection impact assessments, and prior consultation with Supervisory Authorities.

7.3 Hal may charge reasonable costs for assistance that falls outside what is strictly required of a Processor under the GDPR, subject to prior written agreement.

8. Personal Data Breach

8.1 Hal will notify the Controller of any Personal Data Breach affecting the Controller's Personal Data without undue delay, and in any event within 72 hours of becoming aware of it.

8.2 The notification will include, to the extent known and available at the time:

- (a) the nature of the Personal Data Breach, including where possible the categories and approximate number of Data Subjects and records concerned;
- (b) the likely consequences of the Personal Data Breach;
- (c) the measures taken or proposed to address the Personal Data Breach and mitigate its adverse effects; and
- (d) a point of contact for further information.

8.3 Hal will provide further information as it becomes available. The Controller remains responsible for notifying the competent Supervisory Authority and, where required, affected Data Subjects.

9. International Transfers

9.1 Hal may transfer Personal Data to a country outside the European Economic Area ("EEA") only where at least one of the following applies:

- (a) the European Commission has decided that the country ensures an adequate level of protection;
- (b) the SCCs have been put in place with the recipient, together with any supplementary measures required; or
- (c) another transfer mechanism recognised under the GDPR applies.

9.2 **No transfer between the Parties.** Hal processes Personal Data in the EEA (Annex 2). Transfers outside the EEA occur only at Sub-processor level (clause 9.3), where Hal acts as data exporter. Should Hal itself process Personal Data outside the EEA in future, it will first conclude Module Two (Controller to Processor) of the SCCs with the Controller, with Datatilsynet as competent Supervisory Authority and Annexes 1 to 3 of this DPA as the SCC annexes, and give notice under clause 14.1.

9.3 **Onward transfers.** Where a Sub-processor processes Personal Data outside the EEA without an adequacy decision, Hal relies on Module Three (Processor to Processor) of the SCCs, with Hal as data exporter. For Anthropic: Anthropic Ireland, Limited is Hal's contracting entity, and processing takes place at its affiliate Anthropic, PBC in the USA. The transfer to the USA is covered by Module Three of the SCCs incorporated in Anthropic's Data Processing Addendum, which forms part of Anthropic's Commercial Terms of Service under which Hal uses the Anthropic API. Hal has carried out a transfer impact assessment for this transfer and will provide a copy to the Controller on request, under confidentiality.

9.4 Hal does not rely on the EU-US Data Privacy Framework for transfers to Anthropic.

10. Audits

10.1 Hal will make available to the Controller all information necessary to demonstrate compliance with Article 28 of the GDPR and this DPA, and will allow for and contribute to audits, including inspections, conducted by the Controller or an auditor mandated by the Controller.

10.2 The Parties agree that audits under clause 10.1 will be satisfied by Hal providing, on reasonable request and no more than once per calendar year:

- (a) a copy of Hal's then-current TOMs and security documentation;
- (b) any relevant third-party audit reports or certifications (e.g. SOC 2, ISO 27001) where available; and
- (c) written responses to the Controller's reasonable data protection questionnaires.

10.3 On-site audits may be requested only where (a) clause 10.2 does not satisfy a reasonable audit requirement of the Controller or a Supervisory Authority, (b) the Controller gives at least 30 days' prior written notice, (c) the audit is conducted during normal business hours, (d) the Controller and any mandated auditor are bound by appropriate confidentiality obligations, and (e) the audit does not unreasonably interfere with Hal's business operations. The Controller bears its own costs; Hal may charge reasonable costs for on-site audits.

11. Return and Deletion

11.1 On termination or expiry of the Agreement, and at the Controller's choice, Hal will delete or return all Personal Data processed on behalf of the Controller.

11.2 Where the Controller does not express a choice before termination, Hal will delete the Personal Data without undue delay after termination.

11.3 Hal may retain Personal Data to the extent required by Union or Member State law, in which case Hal will continue to protect the confidentiality and security of the Personal Data and will not further process it except as required by that law.

12. Liability

12.1 Liability under this DPA is subject to the limitations of liability set out in the Agreement.

12.2 Nothing in this DPA limits liability that cannot be limited under mandatory law, including liability towards Data Subjects under Article 82 of the GDPR.

13. Term

13.1 This DPA takes effect on the Effective Date and remains in force for as long as Hal processes Personal Data on behalf of the Controller.

13.2 The provisions of clauses 11, 12, and any provisions that by their nature are intended to survive termination will survive.

14. Miscellaneous

14.1 **Changes.** Hal may amend this DPA to reflect changes in law, regulatory guidance, or the Service, with 30 days' prior notice by email or in-app notice. Amendments will not reduce the level of protection provided to Personal Data.

14.2 **Governing law and jurisdiction.** This DPA is governed by the laws of Denmark and subject to the same exclusive jurisdiction as the Agreement, without prejudice to the rights of Data Subjects and Supervisory Authorities under the GDPR.

14.3 **Severability.** If any provision of this DPA is held invalid or unenforceable, the remainder remains in force.

14.4 **Notices.** Notices to Hal under this DPA must be sent to jan.verdier@acloudfrontier.com, marked "Data Protection".

Annex 1: Details of the Processing

Item	Details
Subject matter	Provision of the HAL sales-pipeline Service, including discovery, research, qualification, enrichment, and drafting of outreach to potential business contacts on behalf of the Controller.
Duration	For the term of the Agreement, and until deletion or return of Personal Data under clause 11.

Item	Details
Nature and purpose	Collection, storage, organisation, enrichment, analysis, display, transmission, and drafting of communications, for the Controller's sales and business-development purposes.
Types of Personal Data	Business contact details (name, work email address, work phone number, job title), employer, professional profile information, publicly available professional information, and communications drafted or exchanged in relation to such Data Subjects. The Controller must not submit special categories of Personal Data (Art. 9 GDPR) or data relating to criminal convictions (Art. 10 GDPR).
Categories of Data Subjects	Prospects, leads, business contacts, and other individuals identified by the Controller as potential customers, partners, or decision-makers.
Frequency	Continuous, for the term of the Agreement.
Retention	• *Customer Data in HAL (leads, prospects, accounts, drafted and exchanged communications):* retained until deleted by the Controller in the Service, or until termination of the Agreement (clause 11). On deletion, Personal Data is erased or irreversibly anonymised so that no Data Subject can be re-identified. • *Prompts and model outputs stored by HAL:* same rule as Customer Data above (kept until deleted by the Controller or termination, then erased or irreversibly anonymised). • *Application and access logs:* 30 days, kept for security and diagnostics only. Google Cloud audit logs of administrative actions (no Customer Data) are kept 400 days as mandated by Google. • *Anthropic:* API inputs and outputs are deleted by Anthropic within 30 days of receipt or generation. Anthropic may keep inputs and outputs flagged for Usage Policy violations for up to 2 years, and classification scores for up to 7 years, or longer where required by law.
Competent Supervisory Authority	Datatilsynet (Danish Data Protection Agency).

Annex 2: Technical and Organisational Measures

Hal maintains, at minimum, the following TOMs. The specific controls may evolve over time; the overall level of protection will not be materially reduced. Hal holds no ISO 27001 or SOC 2 certification of its own; its hosting provider (Google Cloud) and model provider (Anthropic) do, and Hal reviews their reports as part of vendor due diligence.

Access control

- Role-based access control with least-privilege permissions.
- Multi-factor authentication for administrative access.
- Unique user accounts; no shared credentials for access to Personal Data.

- Access reviews performed periodically.

Encryption

- TLS 1.2 or higher for Personal Data in transit.
- Encryption at rest for databases and object storage using industry-standard algorithms (AES-256 or equivalent).
- Secrets and credentials stored in a dedicated secrets manager.

Network and infrastructure

- Hosting on Google Cloud in EU regions only (currently europe-west1 and europe-north1), including databases, storage, backups, and logs.
- Network segregation between production and non-production environments.
- Vulnerability scanning and patch management on hosted components.
- Web application firewall and rate-limiting on public endpoints.

Application security

- Secure software development lifecycle, including code review and dependency scanning.
- Protection against common web application vulnerabilities (OWASP Top 10).
- Separate production credentials; production access limited to authorised personnel.

Logging and monitoring

- Application and access logs retained for security and diagnostic purposes for the period stated in Annex 1 (30 days).
- Monitoring and alerting on anomalous events.
- Incident response procedures for suspected security incidents.

Personnel

- Background-appropriate onboarding for personnel with access to Personal Data.
- Written confidentiality undertakings.
- Security awareness and data protection training on hire and periodically thereafter.

Resilience and recovery

- Automated daily backups of production data, stored in the EU and retained for 7 days.
- Documented incident response and business continuity procedures.
- Periodic restore testing.

Deletion

- On deletion by the Controller or on termination, Personal Data is erased or irreversibly anonymised. Anonymisation removes or generalises all direct and indirect identifiers (name, email, phone, job title combined with employer, free-text content); no mapping table or key allowing re-identification is kept.

- Backups containing deleted Personal Data expire within 7 days.

International transfers (Anthropic)

- Only business contact data and business communications are sent to Anthropic; no special-category or criminal-offence data (Annex 1).
- Data minimisation: only the fields needed for the task are included in prompts.
- TLS 1.2 or higher in transit; Anthropic encrypts data at rest (AES-256).
- Anthropic does not use Customer Data sent via the API under its Commercial Terms to train its models.
- Retention at Anthropic is limited as set out in Annex 1.
- Anthropic holds ISO 27001:2022, ISO/IEC 42001:2023, and SOC 2 Type I and Type II; Hal reviews these as part of vendor due diligence.

Sub-processor management

- Written data processing terms with each Sub-processor.
- Vendor due diligence before engagement and on material changes.

Annex 3: Authorised Sub-processors (as of Effective Date)

Sub-processor	Role	Location of processing	Transfer mechanism
Google Ireland Limited / Google LLC (Google Cloud)	Hosting, storage, managed infrastructure	EU only: data is stored and processed in Google Cloud regions europe-west1 and europe-north1, including backups and logs	Not needed for storage or processing. Any remote support access by Google staff outside the EU is covered by the SCCs in Google's Cloud Data Processing Addendum
Anthropic, PBC (USA), contracted through Anthropic Ireland, Limited	Large-language-model inference (Claude) for HAL's reasoning	USA	SCC Module Three, incorporated in Anthropic's Data Processing Addendum (clause 9.3)

Service providers for Hal's own account and billing data, where Hal is the controller (see the Privacy Policy, section 6), are not Sub-processors under this DPA: Stripe Payments Europe Limited (payments, EEA) and Microsoft Ireland Operations Limited (Microsoft 365, account and transactional email, EEA).

The current list is published at gethal.ai/subprocessors.

Change log

- **Version 1.0** (24 April 2026): first version. PDF
- **Version 1.1** (29 October 2026): electronic acceptance and acceptance records (preamble); transfer basis for Anthropic stated as SCC Module Three with a transfer impact assessment, no reliance on the Data Privacy Framework (9.3, 9.4); retention periods per data category and at Anthropic (Annex 1); EU-

only hosting, log and backup retention, anonymisation on deletion, and transfer safeguards for Anthropic (Annex 2); sub-processor entity and transfer mechanism (Annex 3). PDF