HAL

A Cloud Frontier ApS · CVR 37174181 · Aalborg, Denmark

Privacy Policy

Effective date: 8 November 2026

This Privacy Policy explains how A Cloud Frontier ApS, CVR no. 37174181, with registered address at Ivigtutvej 2, 9210 Aalborg SØ, Denmark ("Hal", "we", "us") processes personal data in connection with the HAL software-as-a-service platform at gethal.ai (the "Service").

This policy covers the processing of personal data about our business customers and their users. A separate Data Processing Agreement (DPA) governs the processing of personal data that our customers instruct us to handle on their behalf (e.g. data about their prospects and leads); see section 3 below.

1. Controller

The data controller for the processing described in this policy is:

A Cloud Frontier ApS
CVR no. 37174181
Ivigtutvej 2, 9210 Aalborg SØ
Denmark
Email: jan.verdier@acloudfrontier.com

2. Who This Policy Applies To

This policy applies to:

- representatives, administrators, and end users of our business customers who access the Service; and
- visitors who contact us via email or sign up for an account.

The Service is intended only for business use. We do not knowingly offer it to consumers or to children under 16.

3. Two Roles: Controller vs. Processor

We process personal data in two distinct capacities. It matters which applies, because your rights differ in each case.

(a) As controller: for personal data about our customers and their users: account registration data, billing information, support correspondence, and usage telemetry. This policy describes that processing.

(b) As processor: for personal data that our customers upload to, or instruct the Service to collect about, third parties (for example, names, work email addresses, job titles, and company affiliations of prospects the customer wants to contact). Here, our customer is the controller and decides the purposes. We process such data only on the customer's documented instructions, under the terms of our DPA. If you are a prospect or lead and want to exercise your rights in relation to that data, please contact the customer who initiated contact with you. We will assist that customer in responding to your request.

4. What Personal Data We Collect (as Controller)

Category	Examples	Source
Account data	Name, business email, phone, job title, employer, password hash	You, when creating an account
Billing data	Company name, VAT number, billing address, billing email, top-up records, credit balance	You; payment provider
Usage data	Log-in timestamps, IP address, browser/device, pages viewed, features used, API calls, error logs	Automatically, via the Service
Communications	Emails, support tickets, chat messages	You; our support tools
Demo requests	Name, work email, company, how you heard about us and an optional note; the campaign tags (UTM), referring site and first page of the visit in which you sent the request	You, on the demo request form on gethal.ai

5. Why We Process It, and on What Legal Basis

Under the GDPR we rely on the following legal bases:

- **Performance of a contract (Art. 6(1)(b))**: to create and manage your account, deliver the Service, process top-ups, and provide support, and to answer a demo request you send us. Without this data we cannot provide the Service.
- **Legitimate interests (Art. 6(1)(f))**: to secure the Service against abuse and fraud, maintain server and application logs, learn which posts, searches and campaigns lead to demo requests, and (for existing business customers) send direct B2B marketing about similar services. You can object at any time by contacting us.
- **Legal obligation (Art. 6(1)(c))**: to comply with accounting, tax, and bookkeeping obligations under Danish law (notably the Bookkeeping Act, "Bogføringsloven"), to respond to lawful requests from authorities, and to comply with the GDPR itself.
- **Consent (Art. 6(1)(a))**: for analytics and tracking cookies placed on our website. You can withdraw consent at any time via "Cookie settings" at the bottom of every page.

We do not use your personal data, or any Customer Data, to train artificial-intelligence models. We do not sell personal data.

6. Who We Share Personal Data With

We share personal data only with the following categories of recipients, under appropriate contractual safeguards:

- **Infrastructure provider**: Google Cloud (including Cloud Run) for hosting and storage, in EU regions only.
- **Analytics**: Google Analytics (Google Ireland Limited / Google LLC), only if you accept analytics cookies; see the cookie banner. Google may process analytics data in the United States under the Standard Contractual Clauses in Google's data processing terms.
- **Demo request mail**: AgentMail, Inc. (San Francisco, USA) sends the confirmation and notification emails for the demo request form on gethal.ai, so what you enter there (name, email, company, how you heard about us and an optional note) and the campaign tags and first page of your visit are processed by AgentMail in the United States. AgentMail's privacy notice provides for the EU Standard Contractual Clauses for data from the EEA.
- **AI model provider**: Anthropic Ireland, Limited (Claude), with processing by Anthropic, PBC in the United States, to operate HAL's reasoning capabilities. Prompts and outputs are sent to Anthropic to produce results. We use API configurations under which Anthropic does not use our data to train its models. Anthropic processes this data in the United States under the Standard Contractual Clauses incorporated in Anthropic's Data Processing Addendum (Module Two where we act as controller, Module Three where we act as processor), and deletes API inputs and outputs within 30 days, subject to its Usage Policy and legal obligations.
- **Website host**: Cloudflare, Inc. serves gethal.ai and handles the demo request form, so website visitor data passes through Cloudflare's global network under Standard Contractual Clauses in Cloudflare's Data Processing Addendum.
- **Email provider**: Microsoft Ireland Operations Limited (Microsoft 365) for sending account and transactional email. Billing receipts are sent automatically by Stripe.
- **Payment provider**: Stripe Payments Europe Limited (Ireland) for processing credit top-ups. Card data is handled directly by Stripe under its own privacy policy (stripe.com/privacy); we do not store full card numbers.
- **Professional advisors**: auditors, accountants, and lawyers, under confidentiality.
- **Authorities**: where required by law, a court order, or to protect our rights.

A current list of our sub-processors (relevant to our processor role under the DPA) is maintained at gethal.ai/subprocessors.

7. International Transfers

Some of our service providers are established outside the European Economic Area, notably in the United States. Where personal data is transferred outside the EEA, we rely on:

- the European Commission's adequacy decisions, where they apply (including the EU-US Data Privacy Framework for certified recipients); or
- Standard Contractual Clauses approved by the European Commission, combined with supplementary technical and organisational measures as appropriate.

For Anthropic, which is not certified under the EU-US Data Privacy Framework, we rely on Standard Contractual Clauses together with the supplementary measures described in our DPA.

You can request a copy of the relevant safeguards by contacting us at jan.verdier@acloudfrontier.com.

8. Retention

We keep personal data only for as long as necessary:

- **Account data**: deleted without undue delay after your account is closed, except where law requires longer retention.
- **Billing and transaction records**: retained at least 5 years from the end of the financial year, as required by the Danish Bookkeeping Act.
- **Usage logs**: 30 days.
- **Support correspondence**: up to 3 years after the matter is closed.

After the retention period, data is deleted or anonymised. Deletion is irreversible; backups containing deleted data expire within 7 days.

9. Your Rights

Subject to the conditions in the GDPR, you have the right to:

- access your personal data and receive a copy of it;
- rectify inaccurate or incomplete data;
- erase your data ("right to be forgotten");
- restrict processing in certain circumstances;
- data portability: receive your data in a structured, commonly used, machine-readable format;
- object to processing based on legitimate interests, including for direct marketing; and
- withdraw consent at any time, where processing is based on consent.

To exercise your rights, email jan.verdier@acloudfrontier.com. We will respond within one month (extendable by two further months for complex requests). There is no fee unless the request is manifestly unfounded or excessive.

If you are unsatisfied with how we handle your personal data, you have the right to lodge a complaint with the Danish Data Protection Agency:

> Datatilsynet
> Carl Jacobsens Vej 35 · 2500 Valby · Denmark
> dt@datatilsynet.dk · www.datatilsynet.dk

10. Security

We implement appropriate technical and organisational measures to protect personal data, including encryption in transit, access controls, least-privilege permissions, logging and monitoring, secure software development practices, vendor due diligence, and staff confidentiality obligations. No system is perfectly secure; we continue to review and improve our measures.

11. Automated Decisions

We do not make decisions based solely on automated processing that produce legal or similarly significant effects on the individuals described in this policy.

The Service itself uses AI to assist our customers in their sales workflows; decisions about whether to contact or engage with a prospect are made by the customer, not by the Service in isolation.

12. Changes to This Policy

We may update this policy from time to time. Material changes will be notified by email or in-app notice at least 30 days in advance where feasible. The "Effective date" at the top reflects the latest version.

13. Contact

Questions about this policy or our data practices:

A Cloud Frontier ApS
Ivigtutvej 2, 9210 Aalborg SØ
Denmark
Email: jan.verdier@acloudfrontier.com