

SONTARA DATA PROCESSING ADDENDUM

Version 1.0 — August 15, 2026 · Human Frontier Labs Inc. · sontara.ai/dpa

This Data Processing Addendum (“DPA”) forms part of the agreement between Human Frontier Labs Inc. (“Sontara,” “we”) and the customer identified in the applicable subscription (“Customer”) governing Customer’s use of the Sontara service (the “Agreement”). It applies whenever we process Customer Data on Customer’s behalf.

1. Definitions, plainly

“Customer Data”— the content and personal information Customer (and its users) submits to the Service: conversations, files, agent memory, channel content, and account information.

“Process”— anything we do with Customer Data to run the Service: store, transmit, analyze at Customer’s direction, delete.

“Subprocessor”— a vendor we use to help operate the Service that touches Customer Data.

Terms like “controller,” “processor,” “business,” and “service provider” carry their meanings under applicable privacy laws (including the California Consumer Privacy Act as amended). Between the parties, **Customer is the controller/business and Sontara is the processor/service provider** for Customer Data.

2. What we do — and don’t do — with Customer Data

We process Customer Data **only** to provide, maintain, secure, and support the Service, at Customer’s documented instructions (the Agreement, this DPA, and Customer’s configuration of the Service are those instructions).

We do **not**: sell Customer Data; share it for advertising; use it to train AI or machine-learning models; or combine it with other customers’ data. Our AI infrastructure

provider (Google Cloud Vertex AI) is contractually prohibited from using Customer Data to train its models under Google Cloud's enterprise terms.

If a law requires us to process Customer Data otherwise, we will tell Customer before we do, unless the law forbids that notice.

3. If Customer is a service provider itself (MSPs, agencies, firms)

If Customer uses the Service to process data belonging to its own clients, Customer represents that it has the rights and notices needed to submit that data, and Sontara acts as Customer's subprocessor. The commitments in this DPA are designed to flow down: Customer may share this DPA and the Security Annex with its clients to document Sontara's role.

4. Confidentiality

Everyone we authorize to process Customer Data is bound by confidentiality obligations. Human access to Customer Data is restricted to what is necessary for security, support Customer requests, or legal compliance — our systems are built so that operating the Service does not require humans to read Customer content.

5. Security

We maintain the technical and organizational measures described in the **Security Annex** below. The headline, because it is architectural rather than aspirational: **every customer agent runs in its own isolated runtime with its own dedicated storage and its own service identity**. We will not materially weaken the Annex during a subscription term.

6. Subprocessors

Customer authorizes the subprocessors listed in the **Subprocessor Annex**. We bind each to data-protection obligations no less protective than this DPA. We will give notice (email or in-product) at least 15 days before adding a subprocessor that will touch Customer Data; if Customer reasonably objects on data-protection grounds and we cannot resolve it, Customer may terminate the affected subscription and receive a prorated refund of prepaid fees — our only obligation for such an objection.

7. Helping Customer meet its own obligations

Taking into account the nature of the Service, we will reasonably assist Customer with: (a) responding to data-subject/consumer requests (access, correction, deletion, portability) concerning Customer Data — much of this Customer can do directly in-product; (b) security-incident notifications; and (c) reasonable information requests needed for Customer's privacy assessments (see Section 9).

8. Security incidents

If we confirm a breach of security leading to accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of or access to Customer Data, we will notify Customer **without undue delay and no later than 72 hours after confirmation**, with what we know: nature of the incident, data categories affected, measures taken. We will keep Customer informed as remediation proceeds. Our notice is not an admission of fault.

9. Verification (how audit works here)

Once per year on request, we will provide: this DPA's current annexes, a written summary of our security measures, and written responses to a reasonable security questionnaire. This documentation route is the audit mechanism under this DPA. (We are a small company with a genuinely isolated architecture; we put our effort into the isolation, and we document it honestly. We do not offer on-site audits at this tier.)

10. Deletion and return

Customer can export Customer Data during the term. Upon account deletion or termination, we delete Customer Data — including agent memory, files, and the dedicated storage bucket — with deletion beginning immediately and completing within **30 days**, except records we must retain for legal, tax, or fraud-prevention purposes (which stay protected under this DPA until deleted), and encrypted system backups, which are overwritten on their own rotation and are never used to restore a deleted account. Details: sontara.ai/data-deletion.

11. International processing

The Service is operated from the United States; Customer Data is processed in the United States on Google Cloud infrastructure. Customer instructs this processing location.

12. The legal spine

This DPA is part of the Agreement. Liability under this DPA is subject to the Agreement's limitations of liability (they apply once, across the Agreement and this DPA together). If this DPA conflicts with the Agreement on data protection, this DPA controls. This DPA terminates with the Agreement, surviving as long as we hold Customer Data.

Security Annex (current as of August 18, 2026)

Architecture (the important part):

Per-customer isolation is structural, not logical. Each customer agent runs as its own dedicated runtime service (Google Cloud Run), with its **own dedicated storage bucket** (Google Cloud Storage) and its **own dedicated service identity** (per-instance service account). Agent memory, uploaded files, and conversation history are stored in that customer's dedicated storage — there is no shared memory store and no cross-customer vector database. Two categories are held centrally, and we name them

rather than imply otherwise: operational traces used for debugging and reliability are exported to our own self-hosted observability system — for customer accounts, as structure only: timings, tool and span names, token counts, and error levels, never prompt or response content. Trace data is retained a maximum of 30 days. Message bodies for organization relay and support threads are stored in our control-plane database. Both categories are subject to the confidentiality and access-control commitments in Sections 4 and 5.

Encryption: in transit (TLS) and at rest (Google-managed keys; customer-managed keys supported on request for higher-compliance deployments).

AI processing: Google Cloud Vertex AI exclusively, under enterprise terms prohibiting the use of customer content to train Google models. No other model provider receives Customer Data.

Access control: least-privilege engineering access; secrets in a managed secret store (Google Secret Manager), deleted with the account.

Deletion:destroying an account destroys its runtime service, its bucket (including agent memory), and its secrets — immediately, with a 30-day completion ceiling.

Billing/tax data: card data is handled by PCI-compliant payment processors; we never store card numbers. Partner tax data is held by Stripe, not by us.

Organizational: confidentiality obligations for all personnel; security-incident response with the 72-hour customer notice above; subprocessors bound in writing; no advertising or analytics SDKs in mobile apps; privacy-preserving, cookieless web analytics.

Subprocessor Annex (current as of August 18, 2026)

Subprocessor	Role	Location
Google Cloud (Cloud Run, GCS, Vertex AI, Secret Manager)	Infrastructure, storage, AI inference	US
Clerk	Authentication & identity	US
Stripe	Payments (and partner payouts/KYC)	US
Neon	Database (Postgres)	US (AWS us-east-2)
Vercel	Web hosting; cookieless analytics	US
Resend	Transactional email	US

Subprocessor	Role	Location
RevenueCat	Mobile app-store billing (not used for Teams/org subscriptions)	US
ImprovMX	Inbound email forwarding for sontara.ai mailboxes	EU/US
E2B	Sandboxed code execution for agent tools (Python REPL)	US-based vendor; processing region not contractually restricted
ElevenLabs	Voice synthesis (accounts with voice features enabled)	US-based vendor; processing region not contractually restricted
Current list also available on request via privacy@sontara.ai .		

Execution

Human Frontier Labs Inc.

By: _____
 Name: _____
 Title: _____
 Date: _____

Customer

By: _____
 Name: _____
 Title: _____
 Organization: _____
 Date: _____