haaify

HAAIFY TALKS

Data Processing Agreement (DPA)

Haaify Talks · Version 1.1 · October 30, 2026 · Annex to the Terms of Use

HAAIFY SOLUCOES E TECNOLOGIA LTDA · CNPJ 45.890.870/0001-11

HAAIFY TALKS

Data Processing Agreement (DPA)

Version 1.1 · October 30, 2026 · Annex to the Terms of Use

This Agreement is part of the Haaify Talks Terms of Use and applies between the contracting company ("**Controller**" or "Customer Company") and **HAAIFY SOLUCOES E TECNOLOGIA LTDA**, CNPJ 45.890.870/0001-11, headquartered in Belo Horizonte/MG, Brazil ("**Processor**" or "Haaify"). It is accepted when the service is installed or purchased and governs the processing of personal data by Haaify on behalf of the Customer Company, under Law 13,709/2018 (LGPD).

1. Subject and roles

- The Customer Company is the **controller** of the personal data entered or accessed in Haaify Talks, including end-customer data obtained from Blip.
- Haaify is the **processor** and processes that data only to provide the service described in the Terms of Use, following the Controller's documented instructions.
- For the Customer Company's own registration and billing data, for feedback sent to Haaify and for the access records required by the Internet Civil Framework, Haaify acts as controller, under the Privacy Policy.

2. Processing details

Item	Description
Data subjects	Customer Company users (employees and authorized third parties) and end customers served by the Customer Company on Blip
Data	User profile (including profile photo); message and file content; usage and security records; calendar, when the user connects it; customer-service data from Blip (name, phone, contact fields, tickets, tags, comments, conversation summary, campaigns)
Purposes	Internal communication, Blip customer-service support, calendar and meetings, notifications, usage reports, security and support
Operations	Collection via the app and the Blip API, storage, querying, display, sending notifications and e-mails, backup and deletion
Duration	For the term of the agreement, plus the return and deletion period in clause 9

3. Haaify's obligations

- Process data only according to the Controller's instructions and for the purposes above; notify the Controller if it believes an instruction breaches the law.
- Ensure that people with access to the data are bound by confidentiality. The Haaify team does not read conversation content; exceptional access for support only happens at the Controller's request or with its authorization, and is logged.
- Maintain the security measures in Annex II.
- Help the Controller respond to data-subject requests (access, correction, portability, deletion, etc.) within 15 days.
- Support the Controller in impact assessments and ANPD inquiries, as far as the service is concerned.
- Not sell, rent or use the data for its own purposes, advertising or training artificial intelligence models.

4. Customer Company's obligations

- Have a legal basis for the data it enters or accesses in Haaify Talks, including Blip end-customer data.
- Give lawful instructions, configure its team's access profiles and keep the Blip keys it provides secure.
- Inform data subjects about the processing, according to its own policies.
- Keep administrators' e-mail addresses up to date, as they receive incident notices.

5. Sub-processors

The Controller authorizes the sub-processors listed in Annex I. Haaify will require from them data protection obligations equivalent to those in this Agreement and is liable for their acts towards the Controller. New sub-processors will be announced **30 days** in advance; if the Controller has a reasoned objection and there is no alternative, it may cancel without penalty.

6. International transfer

Some sub-processors are located outside Brazil (mainly in the United States). Haaify ensures these transfers follow article 33 of the LGPD and Resolution CD/ANPD No. 19/2024, adopting the standard contractual clauses approved by the ANPD or another valid safeguard.

7. Incidents

- **Downtime:** if Haaify Talks is down or unstable for the Controller, Haaify notifies the administrators by e-mail **within 30 minutes** of identifying the problem, with updates until it is resolved and a final notice when everything is back to normal.
- **Security incident involving personal data:** Haaify notifies the Controller **within 24 hours** of confirming the incident, with what is known so far: nature, data and data subjects affected, risks, measures taken and a contact for follow-up, supplementing the information as soon as possible.
- Haaify will help the Controller meet the deadline to notify the ANPD and data subjects (Resolution CD/ANPD No. 15/2024) and will keep a record of the incident for at least 5 years.

8. Audit

Upon written request, with 15 days' notice and at most once a year (except in case of an incident or a requirement from an authority), Haaify will provide the information needed to demonstrate compliance with this Agreement, such as security questionnaires, a description of the controls and the history of backup checks.

9. Return and deletion

After the agreement ends, the Controller's Master user can download the data in Administration › Export conversations, or ask support for the export, for up to **30 days**. Haaify will delete the data within **90 days** after termination, including from backups at the end of the rotation cycle, except for legal retention obligations (such as access records, kept for 6 months), and will confirm the deletion in writing upon request.

10. General provisions

In case of conflict, this Agreement prevails over the Terms of Use regarding data protection. The limitations of liability in the Terms apply, unless the law provides otherwise. Jurisdiction: courts of Belo Horizonte/MG, Brazil. The Portuguese version prevails in case of discrepancy.

ANNEX I

Authorized sub-processors

Sub-processor	Service	Location
DigitalOcean, LLC	Hosting of the app, database, files and backups	United States
Resend, Inc.	Sending e-mails: access codes, free-trial and account notices, alerts and incident notices	United States
Google LLC	Sign-in, profile photo, Google Calendar and Google Meet (when the user uses them)	Global
Microsoft Corporation	Outlook / Microsoft 365 calendar and Teams (when the user connects them; not used for sign-in)	Global
Take Blip (Blip)	Customer-service integration, conversation summary (Copilot), Blip Store subscription and WhatsApp code (when enabled)	Brazil
Browser notification services (Apple, Google, Mozilla, Microsoft)	Notification delivery, with encrypted content	Global
GIPHY, Inc.	GIF search (receives only the search term)	United States

ANNEX II

Security measures

- Encryption in transit (HTTPS/TLS) on all connections.
- Logical separation of data by company: each Customer Company can only access its own users, conversations, files and reports.
- Signed and temporary file links; 25 MB limit per file.
- Integration keys (Blip, e-mail, Google, Microsoft) stored only on the server.
- Session in a protected cookie (httpOnly, secure connections only) and protection against forged requests (CSRF).
- Access profiles (administrator, supervisor and user) and logging of customer-service actions.
- 24-hour monitoring (server health, database, disk and errors) with automatic e-mail alarms to the Haaify team.
- Technical logs without message content, e-mails, phone numbers or keys, kept for 30 days; access records (date, time and IP) for 6 months.
- Daily database backups, kept for 30 days, with an automatic restore check of every copy and an alarm if it fails.
- Security updates to the server and the app dependencies.
- Incident response plan with an owner, deadlines (downtime notice within 30 minutes; security incident within 24 hours) and a tool to notify all administrators by e-mail.
- Data Protection Officer (DPO): Daniel Batista Ferreira, daniel.ferreira@haaify.com.