

Privacy Policy

This Policy explains how Cohearo handles personal data and the choices and rights available to you.

Version 0.1.7

Effective 9 September 2026

1. Scope and roles

This Policy explains how Cohearo collects, uses, shares, retains and protects personal data through its applications, websites, APIs and integrations.

Cohearo is operated by **RECHIA & MILOCO DESENVOLVIMENTO DE SOFTWARES LTDA**, CNPJ 65.175.527/0001-00, Rua Visconde do Rio Branco, 1488, Conj. 909, Andar 09 — Condomínio Universe Life Square, Bloco Comercial, Centro, Curitiba — PR, Brazil. Contact: contact@cohearo.com.

Cohearo is controller for account, billing, security, support and product-operation data whose purposes it determines. For customer content supplied to our cloud services, the customer may determine the purposes and act as controller, while Cohearo processes that content on the customer's instructions as processor or operator where applicable. The roles depend on the processing activity.

Customers must have a lawful basis and give any required notice before recording people or processing their content. A transcript is not automatically sensitive personal data, but it may contain health, biometric, religious, political or other sensitive information. The customer must satisfy the applicable requirements, including Article 11 of Brazil's LGPD where relevant. Cohearo's own processing must also meet the requirements that apply to it.

2. Audio, transcripts and cloud storage

Audio recording and transcription occur locally on the user's device. Audio is not sent to Cohearo's servers or AI enhancement providers. Device operating systems, backups or other software may handle local files under their own settings.

Data	Handling and retention
Audio recording	Local to the device, with a 72-hour automatic-cleanup policy. Cleanup depends on the app being able to run.
Local transcript and edits	Local until the user deletes them, removes app data or uninstalls, subject to device backups.
Free-plan cloud transcript	Stored for up to 7 days, then deleted from active cloud storage, unless the user deletes it sooner.

Data	Handling and retention
Synced transcripts created while on a paid plan	Retained indefinitely under the Terms until the user deletes them or closes the account. Later moving to Free does not shorten this retention.

Where a local-only choice is offered, synchronization is optional. Synced data may include transcript text, titles, notes, edits, enhancement results, preset or custom instructions, speaker labels, timestamps, language, device and application metadata, content identifiers and sharing or workspace metadata needed for the selected feature.

Voice embeddings used to distinguish speakers stay on your device. Speaker-profile identifiers and names may sync, but the voice embeddings do not.

3. Information we process

Depending on the features used, we process:

- **Account and identity:** email, account identifiers, optional profile information, locale, authentication events and information returned by supported sign-in providers.
- **Customer content:** synced content and metadata described above, enhancement prompts and results, and content submitted through the API or Model Context Protocol (MCP).
- **Billing:** plan, trial and entitlement status, currency, billing country, invoice and transaction references and limited payment metadata. Stripe processes card details; Cohearo does not store full card numbers.
- **Support:** messages, attachments and information supplied when seeking help.
- **Optional analytics:** after opt-in, events about feature use, navigation, device and application characteristics and coarse technical context. Session replay is disabled.
- **Diagnostics:** no reports are sent in on-device mode. In cloud mode, crash and error reports are on by default and can be disabled in Settings. Before a report leaves the device, known personal-content fields such as recording, preset and speaker names, email addresses and file paths are filtered automatically. Filtering is not perfect, so a user-entered value could unexpectedly appear in error context.
- **Security and network data:** IP address, request time, user agent, device and app identifiers, authentication and authorization results, rejected-key and rate-limit events, and limited logs needed to prevent abuse and investigate incidents. We filter known secret and content fields from logs.

We do not sell personal data or share it with advertisers or data brokers. We do not use transcripts to train Cohearo or third-party AI models.

4. Purposes and legal bases

Purpose	Typical legal basis
Accounts, sync, enhancements, API and MCP	Contract or requested pre-contract steps
Subscriptions, invoices and payments	Contract and legal obligation
Authentication, abuse prevention, limits and security	Legitimate interests in service integrity; legal obligation where applicable
Support and service messages	Contract and legitimate interests
Optional product analytics	Consent
Diagnostics and reliability	Legitimate interests, with available opt-out controls
Legal compliance, disputes and claims	Legal obligation and regular exercise of rights

Where legitimate interests apply, we consider necessity, proportionality and affected rights. Consent may be withdrawn without affecting earlier lawful processing.

5. Providers and integrations

We disclose information reasonably needed for a provider or integration to perform its function:

- **AWS** hosts our core services. Production account and transcript storage is in São Paulo, Brazil. Global services, such as content delivery, may process request data elsewhere.
- **Stripe** processes subscriptions, payments, fraud and billing information in the United States.
- **OpenRouter**, in the United States, and downstream model providers process enhancement requests as described below. Their processing locations are separate from our cloud-storage location.
- **PostHog**, hosted in the United States, receives analytics only after opt-in. Analytics events are retained for one year on our current plan. The consent cookie lasts 180 days, after which we ask again. We honor Global Privacy Control, provide in-product opt-out and keep session replay disabled.
- **Sentry** handles diagnostics under the current EU-region configuration, subject to filtering and opt-out controls.
- **Cloudflare** hosts the public website and provides DNS. Its global network receives website request data such as IP address, browser details and visit time.
- **Google** processes sign-in information when Google sign-in is chosen.

Providers may use subprocessors. You can request further information about recipients and safeguards from contact@cohearo.com. Material changes follow the notice process below.

AI enhancement

When requested, Cohearo sends through OpenRouter the text needed for enhancement. A request may include transcript text, preset or custom instructions and limited technical framing. Audio is not sent.

Zero data retention is enabled on our OpenRouter account, restricting routing to endpoints OpenRouter identifies as meeting that policy for inference content. Cohearo does not use your transcripts to train AI models. This routing setting does not govern content stored in your Cohearo account or an external assistant you connect separately. See our Security and data handling page and OpenRouter's policy for the scope of this setting.

API and MCP

An enabled API or MCP client may access content and features within its granted scopes and permissions. Cohearo processes request content, authentication data, operation metadata, usage and quota data and security logs needed to provide and protect access. Customers control which external client they connect and should review its privacy and security practices.

Analytics and diagnostics choices

Third-party analytics stays off unless the user opts in. The choice can be changed in settings, and Global Privacy Control is honored. Separately, Cohearo counts public website page views and download clicks on its own infrastructure in Brazil without cookies or cross-visit identifiers, including when analytics is declined. Diagnostics are never sent in on-device mode; in cloud mode they are on by default and may be disabled in Settings. These choices do not prevent strictly necessary security, billing or operational logging.

After consent, PostHog may receive page addresses, referring sites, IP address and approximate location, browser/device details, navigation, interaction and performance events, and account events such as sign-up or subscription changes. It uses a cookie and local-storage identifier. When you sign up or sign in, that identifier may be linked to your account and earlier consented page activity. We may use in-page surveys. Session replay requires a policy update and fresh consent before activation.

In the dashboard, Data and Privacy in Settings controls account analytics: opting out stops server account events and dashboard collection across signed-in devices. The public website's choice is browser-specific; use Cookie settings in each browser where you accepted. Withdrawing consent stops collection and removes the PostHog cookie from that browser. Necessary sign-in and security cookies are separate.

6. Retention, deletion and anonymization

We retain data for the periods stated here or while needed to provide the service, comply with law, resolve disputes and protect the service.

Deleted cloud content is removed or scheduled for deletion from active systems. Account deletion is completed within 30 days after a valid request unless an earlier legal deadline applies. Limited tax, accounting, fraud-prevention, security or claims records may be retained where

necessary.

Copies may remain temporarily in backups until they expire under the backup lifecycle. Limited billing, usage or security records may also remain where retention is necessary and lawful. Removing direct identifiers does not always make a record anonymous; we continue to protect retained personal data and restrict its use. Local content and device backups remain under your control and your backup provider's settings.

Analytics events are currently retained up to one year. The browser consent cookie lasts 180 days; records of consent decisions are retained as needed to demonstrate the choice. Cohearo's cookieless website counts are aggregate and not tied to an account. Security, diagnostic and operational log periods vary by system and are limited to operational, security and legal needs.

7. Security and incidents

We use safeguards appropriate to the processing, including access controls, least privilege, encryption in transit, encrypted database and object storage at rest, secret management, monitoring, rate limits and incident procedures. No service can guarantee absolute security. Users must protect devices, accounts, API keys and connected clients.

We investigate, contain, remediate and document suspected incidents. For a confirmed personal-data incident that may cause relevant risk or damage, Cohearo will notify Brazil's ANPD and affected people as required—generally within three business days under the current ANPD rule, subject to its scope and permitted exceptions. The notification period is counted from our knowledge that personal data were affected. A shorter applicable legal or contractual deadline controls. An initial notice may be supplemented as facts develop. As processor or operator, Cohearo will notify and assist the responsible customer as required.

8. International transfers

Some providers and subprocessors may process personal data outside Brazil. We use appropriate contractual, organizational and technical safeguards and seek to apply a transfer mechanism permitted by Article 33 of the LGPD when required. European contractual clauses or general provider terms do not by themselves establish compliance with Brazilian transfer requirements.

We are reviewing the safeguards and LGPD transfer mechanism for each international data flow. We will update this section as that review is completed; this Policy does not certify a particular provider's transfer mechanism.

9. Your rights

Subject to applicable law, a person may request confirmation of processing; access; correction; anonymization, blocking or deletion of unnecessary, excessive or unlawful data; portability where regulated; sharing information; information about withholding consent; consent withdrawal; deletion of consent-based data subject to exceptions; review of solely automated deci-

sions where applicable; objection; and petition to the ANPD.

For confirmation and access under Article 19 of the LGPD, we provide an immediate simplified response or a clear, complete declaration within 15 days of the request. Other requests follow the period required for that right and jurisdiction; there is no blanket 30-day deadline where a shorter rule controls.

Export is available through your account and includes account information, transcripts, folders, presets, organization membership, subscription and usage history, and API-key metadata. Passwords and secret key values are not included. You may also contact us to exercise your access and portability rights, including for personal data not available through that export. Send other requests, including account deletion, to contact@cohearo.com. We may verify identity and authority. When Cohearo handles customer content only for a customer, we may direct the request to that controller and assist as required. Account deletion is completed within 30 days after a valid request unless an earlier deadline applies.

10. Children, changes and contact

Cohearo is for people aged 18 or older. We do not knowingly collect personal data from children or adolescents and the service is not set up to provide the protections their data requires. If you believe a person under 18 created an account, write to contact@cohearo.com.

We publish policy updates with a version and effective date and keep previous versions available. We notify account holders by email before material changes take effect. A changed policy does not replace consent where fresh consent is required.

RECHIA & MILOCO DESENVOLVIMENTO DE SOFTWARES LTDA CNPJ 65.175.527/0001-00 Rua Visconde do Rio Branco, 1488, Conj. 909, Andar 09 Condomínio Universe Life Square, Bloco Comercial, Centro, Curitiba — PR, Brazil contact@cohearo.com