WhisperTask

Privacy Policy

Last updated 12 November 2026

This policy explains how and why the developer of WhisperTask (“we”, “us”, “our”; full name and postal address in section 17) collects, uses, stores and shares (“processes”) your personal information when you use our services (the “Services”). That includes when you:

- download and use our mobile app, WhisperTask, or any other app of ours that links to this policy;
- visit our website, whispertask.app;
- deal with us in other related ways, including marketing and events.

We decide how your personal information is processed, so we are responsible for it. Reading this policy will help you understand your privacy rights and choices. If you don’t agree with how we handle personal information, please don’t use the Services. Still have questions or concerns? Write to us at support@whispertask.app.

WHO IS RESPONSIBLE	HOW TO REACH US
The developer of WhisperTask, based in the Czech Republic Full name and address: section 17	support@whispertask.app In the app: Account → About → Contact us By post: see section 17

At a glance

The short version. Each point links to the full section, and the contents on the next page list everything.

What personal information do we process?	It depends on how you use the Services, the choices you make and the features you use: for example your account details, your recordings and the thoughts made from them, and technical information about your device. Read more →
Do we process sensitive information?	Some information counts as “special” or “sensitive” in certain places, such as your racial or ethnic origin, sexual orientation or religious beliefs. Because WhisperTask is a personal diary, your recordings can contain such details if you choose to say them. We send your recordings to our speech and AI providers only with your explicit consent, which you give with a separate switch before you can record (when you sign up, or on the next screen if you sign up with Apple or Google). You can withdraw it at any time with the AI processing switch in Account → Manage account. Read more →
Do we get information from third parties?	Only a little: from Apple or Google when you sign in with them, and from the App Store, Google Play or another app store (through Superwall or the store itself) when you buy a subscription.Read more →

How do we use it?	To provide, improve and run the Services, to communicate with you, for security and fraud prevention, and to comply with the law. With your consent we may also use it for other purposes. We process it only when we have a valid legal reason. Read more →
What happens to my recordings?	We turn the audio into text and use the text to create your task or note. The audio is deleted from our servers once its thought is saved, and 30 days after upload at the latest if it never is. Your thoughts stay until you delete them; a deleted one is kept in Recently deleted for 7 days, then erased with its transcript. Read more →
Who do we share it with?	Specific categories of third parties, in specific situations, mainly the providers that run parts of WhisperTask for us. We name them in section 4. Read more →
Are analytics and crash reports on?	Not until you turn them on. The app's usage analytics (through PostHog and Superwall) and crash reports both start off, and you can switch them off again at any time in Account → Privacy. Superwall still runs to show our subscription offers and handle purchases.Read more →
How do we keep it safe?	We have organisational and technical measures in place. Still, no transmission over the internet and no storage technology is 100% secure, so we can't promise that hackers, cybercriminals or other unauthorised third parties will never get past our security and wrongly collect, access, steal or change your information. Read more →
What are your rights?	Depending on where you live, privacy law may give you certain rights over your personal information. Read more →
How do you use your rights?	The easiest way is to email us at support@whispertask.app. In the app, Account → About → Contact us opens your email app with our address filled in. You can also use any of the other ways to contact us. We consider and act on every request in line with applicable data protection law.

Want to know more about what we do with the information we collect? Read the full policy below.

Contents

1	What information we collect	4
	Information you give us	4
	Information collected automatically	5
	Google APIs	6
	Information from other sources	7
2	How we use your information	7
3	The legal bases we rely on	8
4	Who we share your information with	9
5	International transfers	10
6	Cookies and storage on your device	11
7	AI features	11
8	Signing in with Apple or Google	13
9	How long we keep your information	13
10	How we keep your information safe	14
11	Children	15
12	Your privacy rights	15
13	Do-Not-Track signals	16
14	Rights for United States residents	17
15	Rights in other regions	20
16	Changes to this policy	21
17	How to contact us	21
18	Reviewing, correcting or deleting your data	21

1 What information we collect

Information you give us

> **IN BRIEF** We collect the personal information you give us.

We collect personal information you choose to give us when you create an account, when you ask for information about us or our products and Services, when you take part in activities in the Services, and when you contact us.

Personal information you provide. What we collect depends on how you use us and the Services, the choices you make and the features you use. It can include:

- names
- email addresses
- contact or authentication data
- passwords (our sign-in provider stores them only in hashed form)

Recordings, transcripts and thoughts. When you record a thought, we receive the audio, turn it into text (a transcript), and use that text to create the task or note you see in the app, with its folder, dates and reminder. We also store the folders you create, your app settings (such as transcription language and appearance), your recording credits and your subscription status.

How you heard about us. During setup the app may ask how you heard about WhisperTask (for example the App Store, a friend, social media, search or a podcast). Answering is optional, and if you skip the question nothing is sent. If you answer, the app sends your choice while you are signed in, so that each account is counted only once. We then keep only two things: a note on your account that you have answered (not what you chose), and a daily total for each answer. Those totals are not linked to your account, and they stay after you delete it because they contain nothing that identifies you.

Sensitive information. We may process sensitive personal details you choose to include in voice recordings, transcripts, tasks, notes or support messages. This can include health information, religious or political beliefs, sexual orientation or other sensitive details. For your recordings, we do this only with your explicit consent. When you sign up, the app asks for it with its own switch, separate from accepting our terms: “To turn my recordings into tasks and notes, I consent to WhisperTask and its AI providers processing them, including any sensitive information I provide.” If you sign up with Apple or Google, the app asks on the next screen, before you can continue. Without this consent, nothing is sent to our speech or AI providers. Sensitive details you type into tasks or notes yourself, or put in a message to us, are processed only to store them for you or to answer you.

You can withdraw your consent at any time with the AI processing switch in Account → Manage account. Recording then turns off, any recording still waiting on your device stays there unsent, and your saved tasks and notes stay. You can turn it back on at any time. We keep a record of each time you give or withdraw this consent.

Your agreements. We keep a record of which version of our Terms of Use and this policy you accepted, and when. When you sign up, you also confirm that you are 18 or older, and that confirmation is part of the same record.

Payment data. If you buy a subscription, the payment details needed for it, such as your card number and its security code, are collected and stored by the app store you buy it from, such as Apple (App Store) or Google (Google Play), not by us. You can read their privacy notices here: Apple and Google Payments. Any other app store you buy from has its own privacy notice.

Every subscription is bought inside the app, and we use Superwall to show our subscription offers and manage subscriptions. From each purchase we receive the product, its status and dates, and transaction details such as the price, which we use to give you your plan and recording credits.

Subscription offers and Superwall. Superwall’s software runs in the app whenever it is open, whatever you choose for usage analytics and crash reports, because it shows our subscription offers and handles purchases. To

do that, the app downloads our subscription offers from Superwall's servers, so Superwall always receives your random user ID, device identifiers (such as the identifier Apple gives our app on your iPhone), your IP address, and basic device and app details. The details of each purchase described above also reach Superwall and us from the app store; on iPhone, the purchase record carries your random user ID. Anything more depends on your usage analytics switch (see Usage analytics and crash reports in the app). While it is off, the app tells Superwall to collect no events about what happens on our subscription screens and no user attributes. While it is on, Superwall also receives those events, user attributes, and more details about your device and app. We don't currently use Superwall's install attribution, which works out which link, ad or campaign led to an install by matching IP addresses and device details with recent clicks on links and ads. The app doesn't ask for permission to track you across other companies' apps and websites, so on iPhone your device's advertising identifier is not shared.

Sign-in data from Apple or Google. You can register and sign in with your existing Apple or Google account. If you do, we receive certain profile information about you from that provider, as described in section 8.

App data. If you use our app, we may also collect the following when you give us access or permission:

- **Device access.** We may ask for access to certain features of your device, such as the microphone (to record your thoughts), reminders and notifications, and other features. You can change these permissions at any time in your device's settings.
- **Device data.** We automatically collect device information (such as your device ID, model and manufacturer), operating system and version, system configuration, device and app identification numbers, browser type and version, hardware model, internet service provider or mobile carrier, and IP address (or proxy server). In the app we may also collect information about the phone network your device uses, its operating system or platform, the type of device, its unique device ID, and which features of the app you used.
- **Notifications.** We may ask to send you notifications about your account or certain features of the app. WhisperTask's reminders are scheduled on your device, and Superwall can remind you one day before a free trial ends. You can turn reminders off in Account → Notifications, and every notification from the app, including the trial reminder, in your device's settings.

We need this information mainly to keep the app secure and working, to troubleshoot problems, and for our internal analytics and reporting.

Please make sure the personal information you give us is true, complete and accurate, and let us know if it changes.

Information collected automatically

> **IN BRIEF** Some information, such as your IP address and your browser and device characteristics, is collected automatically when you use the Services.

We automatically collect certain information when you visit, use or move around the Services. On its own this information doesn't reveal your identity (like your name or contact details), and some of it is linked to your account only through a random user ID. It may include device and usage information such as your IP address, browser and device characteristics, operating system, language preferences, referring URLs, device name, country, approximate location (such as your country or city, which a provider may work out from your IP address), how and when you use the Services, and other technical information. The app never asks for or uses your device's location. We need it mainly to keep the Services secure and working, and for our internal analytics and reporting.

Like many businesses, we also collect information through cookies and similar technologies (see section 6).

The information we collect includes:

- **Log and usage data:** service, diagnostic, usage and performance information that our servers record automatically in log files when you access or use the Services. Depending on how you use us, it may include your IP address, device information, browser type and settings, your activity in the Services (such as date and

time stamps, pages and files viewed, searches, and other actions such as which features you use), and device event information (such as system activity, error reports, sometimes called “crash dumps”, and hardware settings).

- **Device data:** information about the computer, phone, tablet or other device you use to access the Services. Depending on the device, it may include your IP address (or proxy server), device and app identification numbers, approximate location worked out from your IP address, browser type, hardware model, internet service provider or mobile carrier, operating system and system configuration.

Usage analytics and crash reports in the app

Account → Privacy has two switches. Both are off until you turn them on, and you can turn them off again at any time. We keep a record of each choice you make about them, including the first one when you start using the app: which switch, whether you turned it on or off, the version of the wording you were shown, and when.

- **Usage analytics (PostHog and Superwall).** Events such as “thought saved”, the screens you open, app starts and updates, and details about your device and app version. Events are linked to your account’s random user ID, never to your name or email address, and never include your recordings or thoughts. PostHog’s session recording is turned off. With this switch on, Superwall also collects events about what happens on our subscription screens, with device and app details and user attributes.
- **Crash reports (Sentry).** Error reports with technical details about your device and the app, the steps that led up to an error, and performance measurements. For some sessions, and when an error happens, Sentry also records a replay of the app’s screens in which all text and images are hidden. Reports carry the random user ID, not your name or email address. If you send a message with Report a problem, it goes through Sentry too, which is why that screen needs crash reports on.

Our servers also report their own errors to Sentry so that we can fix them. While your crash reports are off, these server reports don’t include your user ID.

PostHog and Sentry are both set not to store your IP address. Superwall runs whenever the app is open, because it shows our subscription offers and handles purchases; while usage analytics is off, it collects only what that needs (see Subscription offers and Superwall).

Checking that you are a person at sign-in (Cloudflare Turnstile)

Before you sign up with your email address, sign in with your password, reset your password, ask for a new code, or confirm it’s you with your password, the app opens a page of our website (`whispertask.app/captcha`) in a browser view inside the app. There, Cloudflare Turnstile, a service of Cloudflare, Inc., checks that the request comes from a person and not from an automated program. You don’t need to do anything: the app shows only a short loading indicator while it runs. Signing in with Apple or Google doesn’t use this check.

To tell people from bots, Cloudflare processes technical signals from your device and browser, such as your IP address, browser and device characteristics, and signals about interaction and behaviour on the page, and it may store information such as cookies or local storage in that browser view. The app passes the page only your light or dark theme and your language; your email address, name, recordings and thoughts are never sent to Cloudflare. The check produces a one-time token, which goes to our sign-in provider, Supabase, and Supabase verifies it with Cloudflare. We use this check to protect your account, our sign-in and our email system against automated abuse, such as bots, spam and attempts to use up the emails we can send, and we rely on our legitimate interests in security and preventing abuse (see section 3). Cloudflare also uses these signals, under its own responsibility, to improve its bot detection. How Cloudflare handles them is explained in its Turnstile Privacy Addendum.

Google APIs

Our use of information received from Google APIs follows the Google API Services User Data Policy, including its Limited Use requirements.

Information from other sources

> **IN BRIEF** We receive limited information from services you use together with WhisperTask, such as Apple or Google sign-in and app store purchases.

Besides what you give us and what we collect automatically, we receive information about you from:

- **Apple or Google sign-in,** if you use it: the profile information described in section 8.
- **The App Store, Google Play or another app store, through Superwall or the store itself,** if you buy a subscription: the product, its status and dates, and transaction details such as the price (see Payment data).

If you contact us through a social media platform, we receive what you share with us there, such as your name and your message. What we receive depends on the privacy settings of your account on that platform, and the platform's own use of your information is not covered by this policy. You may have the right to withdraw your consent to this processing (see Withdrawing your consent).

2 How we use your information

> **IN BRIEF** We use your information to provide, improve and run the Services, to communicate with you, for security and fraud prevention, and to comply with the law. We may also use it for other purposes, but only with your prior explicit consent.

Depending on how you use the Services, we use your personal information to:

- **Create and manage your account,** so you can sign up, sign in and keep your account working. How long: account profile information is kept while your account exists, and removed from our live database when you delete your account.
- **Provide the Services you ask for,** such as turning a recording into a task or note. How long: tasks, notes and folders are kept until you delete them or your account. A deleted task or note stays in Recently deleted for 7 days, then is erased with its transcript. The transcript of a recording that never becomes a thought is erased when you discard it in Review, or 30 days after the recording at the latest. The audio you upload is deleted by a scheduled clean-up once its thought is saved, normally within about 15 minutes, or 30 days after upload if it is never saved. A recording that hasn't been sent yet stays on your device until it has been sent and processed, until you discard it, or until you sign out. If your session simply expires, it stays so it can be sent after you sign in again.
- **Answer your questions and give you support,** and solve any problems you have with the Services.
- **Send you administrative information,** such as details about our products and services, changes to our terms and policies, and similar information.
- **Fulfil and manage your orders,** payments, returns and exchanges made through the Services.
- **Ask for feedback** and contact you about your use of the Services. How long: the counters and settings for the rating prompt are stored on your device with no automatic expiry, until the app's local data is cleared. Reviews you submit are handled by the app store.
- **Protect the Services,** including monitoring for and preventing fraud.
- **Identify usage trends,** so we understand how the Services are used and can improve them.
- **Plan, measure and improve our marketing and promotional campaigns,** for example by looking at the daily totals of how people heard about WhisperTask, app store statistics, and the results of the channels and campaigns we use to promote WhisperTask.
- **Protect someone's vital interests,** for example to prevent harm.

3 The legal bases we rely on

> **IN BRIEF** We process personal information only when we believe it is necessary and we have a valid legal reason (a "legal basis") under applicable law: your consent, compliance with the law, providing services to you or entering into or fulfilling a contract with you, protecting your rights, or our legitimate business interests.

If you are in the EU or UK

The General Data Protection Regulation (GDPR) and the UK GDPR require us to explain the legal bases we rely on to process your personal information. We may rely on the following:

- **Consent.** We may process your information if you have given us permission (consent) to use it for a specific purpose. You can withdraw your consent at any time (see Withdrawing your consent).
- **Performance of a contract.** We may process your information when we believe it is necessary to meet our contractual obligations to you, including providing the Services, or at your request before entering into a contract with you.
- **Legitimate interests.** We may process your information when we believe it is reasonably necessary for our legitimate business interests and those interests are not outweighed by your interests and fundamental rights and freedoms. For example, to:
  - analyse how the Services are used so we can improve them to engage and keep users;
  - support our marketing;
  - diagnose problems and/or prevent fraud;
  - protect accounts, sign-in and our email system against automated abuse, such as bots and spam (through Cloudflare Turnstile, see Checking that you are a person at sign-in);
  - understand how our users use our products and services so we can improve their experience;
  - show our subscription offers and handle purchases (through Superwall).
- **Legal obligations.** We may process your information when we believe it is necessary to comply with our legal obligations, for example to cooperate with a law enforcement body or regulator, to exercise or defend our legal rights, or to disclose your information as evidence in litigation we are involved in.
- **Vital interests.** We may process your information when we believe it is necessary to protect your vital interests or someone else's, such as when a person's safety may be at risk.

For example, we rely on the contract with you to run your account; on your explicit consent to send your recordings and transcripts to our speech and AI providers and turn them into thoughts, including any sensitive information they contain (see Sensitive information); on your consent for the app's optional usage analytics (including Superwall's subscription screen events) and crash reports; and on our legitimate interests to keep the Services secure, prevent fraud, keep our servers working, and show our subscription offers and handle purchases through Superwall.

If you are in Canada

We may process your information if you have given us specific permission (express consent) to use it for a specific purpose, or where your permission can be inferred (implied consent). You can withdraw your consent at any time.

In some exceptional cases, applicable law may allow us to process your information without your consent, for example:

- if collecting it is clearly in a person's interests and consent can't be obtained in time;
- for investigations, and for detecting and preventing fraud;
- for business transactions, if certain conditions are met;
- if it is contained in a witness statement and collecting it is necessary to assess, process or settle an insurance claim;

- to identify injured, ill or deceased people and to communicate with their next of kin;
- if we have reasonable grounds to believe a person has been, is, or may be the victim of financial abuse;
- if it is reasonable to expect that collecting and using it with consent would compromise its availability or accuracy, and collecting it is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province;
- if disclosure is required to comply with a subpoena, warrant, court order or court rules on the production of records;
- if it was produced by a person in the course of their employment, business or profession, and collecting it is consistent with the purposes for which it was produced;
- if collecting it is solely for journalistic, artistic or literary purposes;
- if the information is publicly available and is specified by the regulations.

We may also disclose de-identified information for approved research or statistics projects, subject to ethics oversight and confidentiality commitments.

4 Who we share your information with

> **IN BRIEF** We may share information in the specific situations described in this section and with the categories of third parties listed below.

Vendors, consultants and other service providers. We may share your data with third-party vendors, service providers, contractors or agents ("third parties") who work for us or on our behalf and need access to the data to do that work. We have contracts with them that are designed to help protect your personal information. This means they may do nothing with it unless we have instructed them to, they commit to protect the data they hold for us, and they keep it only for the period we instruct. They will not share it with any organisation apart from us, except their own sub-processors, who work under similar obligations. For example, OpenRouter passes each request on to one of the AI providers named in section 7, which does the processing.

The categories of third parties we may share personal information with are:

- AI platforms
- Cloud computing services
- Communication and collaboration tools
- Data analytics services
- Data storage providers
- Payment processors
- Performance monitoring tools
- User account registration and authentication services
- Subscription and paywall management services

The providers we use today

PROVIDER	WHAT THEY DO FOR US	WHAT THEY RECEIVE	WHERE
Supabase	Hosts our database, file storage, sign-in and server functions	Your account details, recordings, transcripts, thoughts, folders, settings (including your time zone), credits and subscription records, including the purchase events Superwall sends us; the IP address and device or browser details of your sign-ins; your new email address while you are changing it; and the record of which version of our terms and this policy you accepted, and when	Database: EU (Ireland). Server functions may run in the region closest to you (see section 5)
Deepgram	Turns your recordings into text	The audio of each recording; it sends back the transcript	United States

PROVIDER	WHAT THEY DO FOR US	WHAT THEY RECEIVE	WHERE
OpenRouter and the AI providers it routes to	Turns transcripts into tasks and notes; backup transcription if Deepgram is unavailable	The transcript, the names of your folders, and the local date, time and time zone of the recording; during a Deepgram outage, the audio (see section 7)	United States, and each AI provider's own locations
Superwall	Shows our subscription offers and manages subscriptions; usage analytics for our subscription screens, only if you turn it on	Your random user ID, device identifiers, your IP address, basic device and app details, and purchase events. Only if you turn on usage analytics: subscription screen events, user attributes, and more device and app details. Superwall runs whenever the app is open (see Subscription offers and Superwall).	United States
Apple and **Google**, and any other app store you get WhisperTask from	App stores, payments, and optional sign-in (Apple and Google only)	Payment details and purchase records, which they collect directly; sign-in requests if you use Apple or Google sign-in; and, when you delete your account, where possible a request to remove WhisperTask's access to your Apple or Google account	Their own locations
PostHog	Usage analytics, only if you turn it on	Usage events and device details, linked to your random user ID. PostHog is set not to store your IP address.	EU
Sentry	Crash reports and performance monitoring, only if you turn them on in the app; errors on our servers	Error reports, device and app details, masked screen replays, your random user ID, and messages you send with Report a problem. Sentry is set not to store your IP address.	EU
Resend	Sends account emails, such as sign-in codes and security notices	Your email address and the content of the email. Open and click tracking is turned off.	EU sending region; company in the US
Cloudflare	Hosts our website, forwards emails sent to our support address, and checks that email and password sign-ins come from a person (Turnstile)	Website requests (including your IP address), the emails you send us, and the device and browser signals of the check at sign-in (see Checking that you are a person at sign-in)	Global network

We may also need to share your personal information in these situations:

- **Business transfers.** We may share or transfer your information in connection with, or during negotiations of, any merger, sale of company assets, financing, or acquisition of all or part of our business by another company.
- **Business partners.** We may share your information with business partners we work with, for example to offer you certain products, services or promotions, or to build and provide features together. Where the law requires it, we will ask for your consent first.

5 International transfers

> **IN BRIEF** WhisperTask is available worldwide. Our main database is in the EU, but some processing happens in other countries, mainly the United States, and some may happen close to where you are.

WhisperTask is available to people around the world. We are based in the Czech Republic, and our main database is hosted in the EU (Ireland). Your information can still be processed outside the EU, and outside the country where you live:

- Some of the providers in section 4, including Deepgram, OpenRouter and the AI providers it routes to, Superwall and Cloudflare, process information in the United States or other countries whose data protection laws may differ from those where you live.
- Our server functions, which receive your recordings and pass them to our speech and AI providers, run on our database host's global network. Each request may be handled in the region closest to you, which can be outside the EU. The results are then stored in our main database in Ireland.

Wherever you live, we protect your information as this policy describes. When personal information is transferred outside the EEA, the UK or Switzerland, we rely on safeguards recognised by data protection law, such as the European Commission's adequacy decision for the EU-U.S. Data Privacy Framework where a provider is certified under it, or the Standard Contractual Clauses in our providers' data processing terms. Contact us if you would like more detail about these safeguards.

6 Cookies and storage on your device

> **IN BRIEF** We store information on your device to keep the Services working, and for the analytics and crash reports you can choose to turn on.

Like most apps and websites, the Services store some information on your device using cookies or similar technologies. We use them to keep the Services and your account secure, prevent crashes, fix bugs, save your preferences and support basic functions, and, if you turn them on, for usage analytics and crash reports.

What we use today

- **Our website** sets no cookies and loads no third-party scripts, except on the page for the check at sign-in described below. If you choose a light or dark theme, your browser remembers it (under the name `wt-theme`) until you change it or clear your browser data. Our hosting provider, Cloudflare, also asks browsers to report network errors when the site can't be reached (Network Error Logging), which helps keep the site available.
- **The check at sign-in.** The page the app opens to check that you are a person loads Cloudflare Turnstile's script, and Cloudflare may store information in that browser view, such as cookies or local storage, to run the check (see Checking that you are a person at sign-in).
- **The app** stores on your device what it needs to work: your sign-in session (in the iOS Keychain, or encrypted storage on Android); your settings and small preferences, such as your display name, transcription language, theme, haptics and the folder you used last; your progress through setup; the rating-prompt counters; recordings waiting to be sent; and the IDs of thoughts waiting for your review. Reminders you set are scheduled with your device's notification system, which keeps the task's text and folder name until the reminder goes off, you change it, you turn Notifications off, or you sign out. The app also remembers your AI processing choice on the device. If you turn on usage analytics or crash reports, PostHog or Sentry store identifiers and reports waiting to be sent on your device. Superwall also stores data on your device to show subscription offers and handle purchases.

How you can refuse cookies is explained under Cookies and similar technologies in section 12.

7 AI features

> **IN BRIEF** We offer products, features and tools powered by artificial intelligence, machine learning or similar technologies.

As part of the Services we offer products, features and tools powered by artificial intelligence, machine learning or similar technologies (together, "AI Products"). They are designed to improve your experience and give you useful new ways to work. This policy governs your use of the AI Products in our Services.

Who provides them

We provide the AI Products through third-party providers ("AI Service Providers").

- **Main providers.** Deepgram turns your recordings into text, and Google Vertex AI (Google Cloud), which we reach through OpenRouter, turns the text into your tasks and notes.
- **Backup providers.** If a main provider is unavailable or fails, the request goes through OpenRouter to a backup provider instead, so that your recording can still be processed. Backups can include Microsoft Azure AI, DeepInfra, Groq, Google AI Studio, OpenAI, Anthropic, Amazon Bedrock, Amazon Web Services (AWS) AI and DigitalOcean. Which one is used depends on which are available at the time.

As this policy explains, your input, output and personal information are shared with and processed by these AI Service Providers so you can use our AI Products, for the purposes described in section 3. You must not use the AI Products in any way that breaks the terms or policies of an AI Service Provider.

What they are for

Our AI Products are designed for:

- AI applications
- AI automation
- Natural language processing
- Text analysis

What happens to a recording

1. **Transcription.** The audio goes to Deepgram, which sends back the text. If Deepgram is unavailable, the audio goes through OpenRouter to a backup speech model (today, a Whisper model run by DeepInfra or Groq) instead. Only this step receives your audio.
2. **Organising.** The transcript, the names of your folders, and the local date, time and time zone of the recording go through OpenRouter to a language model: Google Gemini on Google Vertex AI, or a backup model if Gemini is unavailable. It sends back the task or note with its folder, priority, dates and reminder, which you can review and edit. The language model receives the transcript, not the audio.
3. **What the providers keep.** Every request to Deepgram opts out of its model improvement programme, so under Deepgram's terms it keeps the audio and transcript only as long as it needs to process the request. It does keep request details and usage logs, which contain no audio or text. Every request through OpenRouter asks for zero data retention, so OpenRouter sends it only to AI providers that have committed not to keep or train on your data.

How we process your data with AI

All personal information processed by our AI Products is handled in line with this policy and our agreements with the third parties involved, to keep it secure and protected throughout.

What is outside our control. We don't run our own data centres or AI models. Each AI Service Provider runs its own systems under its own terms and privacy policy, and we can't see inside those systems or control what happens there. The settings above are what we ask for and what the providers commit to, but a provider may still store some of your data, for example for security, to prevent abuse, because the law requires it, or if it doesn't keep to its commitments. How long a provider keeps data, and what it does with it, depends on that provider, not on us. We choose providers that offer these protections, and we will update this policy if the providers we use change.

8 Signing in with Apple or Google

> **IN BRIEF** If you register or sign in with Apple or Google, we may receive certain information about you from them.

You can register and sign in with your Apple account (on iPhone) or your Google account. If you do, we receive certain profile information about you from the provider. It varies by provider, but usually includes your name, your email address and an account identifier. Apple shares your name only the first time you sign in, and if you choose Hide My Email we receive an Apple relay address instead of your own. Google may also share your profile picture.

We use this information only for the purposes described in this policy, or that we otherwise make clear to you in the Services. Please note that we don't control, and aren't responsible for, how Apple or Google otherwise use your personal information. We recommend reading their privacy notices (Apple, Google) to understand how they collect, use and share it, and how to set your privacy preferences with them.

When you delete your WhisperTask account, we also ask Apple and Google to remove WhisperTask's access to your account where your device allows it.

9 How long we keep your information

> **IN BRIEF** We keep your information for as long as we need it for the purposes in this policy, unless the law requires otherwise.

We keep your personal information only as long as we need it for the purposes in this policy, unless a longer period is required or allowed by law (for example for tax, accounting or other legal requirements). If you are in the EU or UK, section 2 gives the retention period for each purpose, and the table below gives more detail.

INFORMATION	HOW LONG WE KEEP IT
Account details, settings, credits and subscription records	Until you delete your account
Tasks, notes and folders	Until you delete them, or your account. A task or note you delete goes to Account → Recently deleted, where you can restore it for 7 days. After 7 days, or straight away if you choose Delete now, it is erased from our database with its transcript.
Transcripts	Kept once, with the thought made from them, and erased with it. The transcript of a recording that never becomes a thought is erased as soon as you discard it in Review, and 30 days after the recording at the latest.
Audio of your recordings on our servers	Deleted once its thought is saved, normally within about 15 minutes. If it is never saved, deleted 30 days after upload at the latest.
Recordings not yet sent, on your device	Until they have been sent and processed, until you discard them, or until you sign out. If your session simply expires, they stay so they can be sent after you sign in again.
Reminders scheduled on your device	Until the reminder goes off, you change or remove it, you delete its task, you turn Notifications off, or you sign out
Records of accepting our terms and this policy, and of giving or withdrawing consent to AI processing, usage analytics and crash reports	Until you delete your account

INFORMATION	HOW LONG WE KEEP IT
A scrambled (hashed) form of your email address, used to limit how many sign-in and confirmation emails can be sent to one address	Usually about 24 hours; deleted with the next such email we send to anyone after that
Usage analytics (PostHog)	Until you delete your account. PostHog then removes your events, usually within a week.
Crash reports and replays (Sentry)	Until Sentry deletes them automatically under our plan's retention period (at most 90 days for error reports and replays). They can't be deleted per person, but they carry only a random user ID, and once your account is deleted nothing links that ID to you.
Subscription data held by Superwall	Under Superwall's own retention. Ask us and we will request that Superwall deletes it.
Signals from the check at sign-in (Cloudflare Turnstile)	We don't receive them. Cloudflare keeps them under its own retention. The one-time token that reaches Supabase expires after 5 minutes.
Daily totals of "How did you hear about us?"	Kept, because they contain nothing that identifies you

When we no longer have a legitimate business need to process your personal information, we delete or anonymise it. If that isn't possible (for example, because it is stored in backup archives), we store it securely and keep it from any further processing until it can be deleted. Our database host keeps no backups of our database on our current plan; if we move to a plan with backups, they are kept for up to 7 days, so something erased can remain in a backup for at most 7 more days.

10 How we keep your information safe

> **IN BRIEF** We aim to protect your personal information through organisational and technical security measures.

We have put in place appropriate and reasonable technical and organisational security measures designed to protect the personal information we process. For example:

- connections between the app, our servers and our providers are encrypted;
- each account can reach only its own data in our database;
- your sign-in session is kept in your device's secure storage (the iOS Keychain, or encrypted storage on Android);
- the keys to our speech and AI providers stay on our servers and are never in the app.

However, despite our safeguards and efforts, no electronic transmission over the internet and no information storage technology can be guaranteed to be 100% secure, so we cannot promise or guarantee that hackers, cybercriminals or other unauthorised third parties will not be able to defeat our security and improperly collect, access, steal or change your information. We will do our best to protect your personal information, but sending it to and from the Services is at your own risk. You should only access the Services in a secure environment.

11 Children

> **IN BRIEF** We do not knowingly collect data from, or market to, children under 18, or under the equivalent age set by law where you live.

We do not knowingly collect or ask for data from, or market to, children under 18 or the equivalent age set by law in your jurisdiction, and we do not knowingly sell such personal information. WhisperTask is only for adults: when you sign up, the app asks you to confirm that you are 18 or older, and you can't use the app without confirming it. If we learn that we have collected personal information from a user under 18 (or the equivalent age in your jurisdiction), we will deactivate the account and take reasonable steps to promptly delete the data from our records. If you become aware of any data we may have collected from a child under 18 (or the equivalent age in your jurisdiction), please contact us at support@whispertask.app.

12 Your privacy rights

> **IN BRIEF** Depending on where you live (for example a US state, the European Economic Area (EEA), the United Kingdom (UK), Switzerland or Canada), you have rights that give you more access to and control over your personal information. Depending on your country, province or state, you can review, change or close your account at any time.

In some regions (such as the EEA, the UK, Switzerland and Canada), data protection law gives you certain rights. These may include the right:

i. to ask for access to, and a copy of, your personal information;

ii. to ask us to correct or erase it;

iii. to restrict how we process it;

iv. where applicable, to data portability; and

v. not to be subject to automated decision-making.

If a decision that has legal or similarly significant effects on you is made solely by automated means, we will tell you, explain the main factors, and offer you a simple way to ask for a human review. In certain circumstances you may also have the right to object to the processing of your personal information. You can make any of these requests using the contact details in section 17.

We will consider and act on any request in line with applicable data protection law.

Controls in the app.

- Account → Privacy has the usage analytics and crash report switches, and Recently deleted, where you can restore a deleted task or note, or erase it straight away with Delete now.
- Account → Notifications turns reminders on or off.
- Account → Manage account has the AI processing switch (see Sensitive information), and lets you change your name and delete your account (see section 18). If you sign in with an email address and password, you can also change them there. If you sign in with Apple or Google, your email address and password are managed by that provider.
- You can edit or delete any of your tasks, notes and folders at any time.

Complaints if you are in the UK

If you are in the UK and unhappy with how we have handled your personal information, you can complain to us directly. This is in addition to your rights under the UK General Data Protection Regulation and the Data Protection Act 2018.

How to reach us

- Email: support@whispertask.app (in the app, Account → About → Contact us opens your email app with this address filled in)
- Post: see section 17

What happens after you complain

- We will acknowledge your complaint within 30 days of receiving it.
- We will investigate it without unjustifiable or excessive delay.
- We will keep you informed of our progress and explain the outcome.

If you are not happy with our final response, you can refer your complaint to the Information Commissioner's Office (ICO), the UK supervisory authority:

> Website: ico.org.uk/make-a-complaint
> Helpline: 0303 123 1113
> Post: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Complaints in the EEA and Switzerland

If you are in the EEA or UK and believe we are processing your personal information unlawfully, you also have the right to complain to your national data protection authority or the UK data protection authority. Because we are based in the Czech Republic, our lead authority is the Office for Personal Data Protection (Úřad pro ochranu osobních údajů, uoou.gov.cz).

If you are in Switzerland, you can contact the Federal Data Protection and Information Commissioner.

Withdrawing your consent

If we rely on your consent to process your personal information (which may be express and/or implied consent, depending on the applicable law), you have the right to withdraw it at any time. You can do this by contacting us using the details in section 17, or by changing your settings. For usage analytics and crash reports, turn off the switches in Account → Privacy. For processing your recordings with AI, turn off AI processing in Account → Manage account.

Please note that withdrawing consent does not affect the lawfulness of processing before you withdrew it. Nor, where applicable law allows, does it affect processing based on legal grounds other than consent.

Account information

If at any time you would like to review or change the information in your account, or close your account, you can sign in and update it in your account settings.

When you ask us to close your account, we will deactivate or delete your account and information from our active databases. However, we may keep some information in our files to prevent fraud, troubleshoot problems, help with any investigations, enforce our legal terms and/or comply with legal requirements.

Cookies and similar technologies

Most web browsers accept cookies by default. If you prefer, you can usually set your browser to remove or reject cookies. If you do, some features or services of the Services may be affected.

If you have questions or comments about your privacy rights, email us at support@whispertask.app.

13 Do-Not-Track signals

Most web browsers, and some mobile operating systems and apps, include a Do-Not-Track ("DNT") feature or setting you can turn on to signal that you don't want data about your online browsing activities monitored and

collected. No uniform technology standard for recognising and implementing DNT signals has been finalised yet, so we do not currently respond to DNT browser signals or any other mechanism that automatically communicates your choice not to be tracked online. If a standard for online tracking is adopted that we must follow in the future, we will tell you about it in a revised version of this policy.

California law requires us to tell you how we respond to web browser DNT signals. Because there is currently no industry or legal standard for recognising or honouring them, we do not respond to them at this time.

14 Rights for United States residents

> **IN BRIEF** If you live in California, Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Rhode Island, Tennessee, Texas, Utah or Virginia, you may have the right to ask for access to, and details about, the personal information we hold about you and how we have processed it, to correct inaccuracies, and to get a copy of or delete your personal information. You may also have the right to withdraw your consent to our processing of your personal information. Applicable law may limit these rights in some circumstances. More details follow below.

Categories of personal information we collect

The table below shows the categories of personal information we have collected in the past twelve (12) months. It gives illustrative examples of each category and does not reflect the specific personal information we collect from you. For a complete list of everything we process, see section 1.

CATEGORY	EXAMPLES	COLLECTED
A. Identifiers	Contact details such as real name, alias, postal address, telephone or mobile number, unique personal identifier, online identifier, IP address, email address and account name	**Yes**
B. Personal information as defined in the California Customer Records statute	Name, contact information, education, employment, employment history and financial information	**Yes**
C. Protected classification characteristics under state or federal law	Gender, age, date of birth, race and ethnicity, national origin, marital status and other demographic data	**No**
D. Commercial information	Transaction information, purchase history, financial details and payment information	**Yes** subscription purchase records only
E. Biometric information	Fingerprints and voiceprints	**No**
F. Internet or other similar network activity	Browsing history, search history, online behaviour, interest data, and interactions with our and other websites, applications, systems and advertisements	**Yes** in-app usage, only if analytics is on; signals for the check at sign-in
G. Geolocation data	Device location	**No**
H. Audio, electronic, sensory or similar information	Images and audio, video or call recordings created in connection with our business activities	**Yes**

CATEGORY	EXAMPLES	COLLECTED
I. Professional or employment-related information	Business contact details in order to provide you our Services at a business level, or job title, work history and professional qualifications if you apply for a job with us	**No**
J. Education information	Student records and directory information	**No**
K. Inferences drawn from collected personal information	Inferences drawn from any of the personal information listed above to create a profile or summary about, for example, a person's preferences and characteristics	**No**
L. Sensitive personal information	Account login information, and sensitive details you choose to include in your recordings	**Yes**

We collect sensitive personal information only as defined by applicable privacy laws, for the purposes the law allows, or with your consent. Sensitive personal information may be used, or disclosed to a service provider or contractor, for additional, specified purposes. You may have the right to limit the use or disclosure of your sensitive personal information. We do not collect or process sensitive personal information to infer characteristics about you.

We may also collect other personal information outside these categories when you interact with us in person, online, or by phone or mail in the context of:

- getting help through our customer support channels;
- taking part in customer surveys or contests; and
- delivering our Services and responding to your enquiries.

We will use and keep the personal information we collect as needed to provide the Services, or for:

- Category B: as long as you have an account with us.

Sources of personal information

Read more about where the personal information we collect comes from in section 1.

How we use and share personal information

Read more about how we use your personal information in section 2.

We collect and share your personal information through native mobile analytics, diagnostics and paywall SDKs that use account or device identifiers and storage on your device (PostHog, Sentry and Superwall).

Will your information be shared with anyone else?

We may disclose your personal information to our service providers under a written contract between us and each service provider. Read more about who we disclose personal information to in section 4.

We may use your personal information for our own business purposes, such as internal research for technological development and demonstration. This is not considered "selling" your personal information.

We have not sold or shared any personal information to third parties for a business or commercial purpose in the preceding twelve (12) months. In the preceding twelve (12) months we have disclosed the following categories of personal information to third parties for a business or commercial purpose:

- Category A. Identifiers
- Category B. Personal information as defined in the California Customer Records law
- Category D. Commercial information
- Category F. Internet or other similar network activity

- Category H. Audio, electronic, visual and similar information
- Category L. Sensitive personal information

The categories of third parties we disclosed personal information to for a business or commercial purpose are listed in section 4.

Your rights

Certain US state data protection laws give you rights. These rights are not absolute, and in some cases we may decline your request as the law allows. They include the right to:

- know whether or not we are processing your personal data;
- access your personal data;
- correct inaccuracies in your personal data;
- ask us to delete your personal data;
- get a copy of the personal data you previously shared with us;
- not be discriminated against for exercising your rights;
- opt out of the processing of your personal data if it is used for targeted advertising (or "sharing" as defined in California's privacy law), the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects ("profiling").

Depending on the state where you live, you may also have the right to:

- access the categories of personal data being processed (as allowed by applicable law, including Minnesota's privacy law);
- get a list of the categories of third parties we have disclosed personal data to (as allowed by applicable law, including the privacy laws of California, Delaware and Maryland);
- get a list of the specific third parties we have disclosed personal data to (as allowed by applicable law, including the privacy laws of Minnesota and Oregon);
- get a list of the third parties we have sold personal data to (as allowed by applicable law, including Connecticut's privacy law);
- review, understand, question and, depending on where you live, correct how personal data has been profiled (as allowed by applicable law, including the privacy laws of Connecticut and Minnesota);
- limit the use and disclosure of sensitive personal data (as allowed by applicable law, including California's privacy law);
- opt out of the collection of sensitive data and personal data collected through a voice or facial recognition feature (as allowed by applicable law, including Florida's privacy law).

How to use your rights

To use these rights, email us at support@whispertask.app, or use the other contact details in section 17.

Under certain US state data protection laws, you can appoint an authorised agent to make a request for you. We may refuse a request from an authorised agent who does not provide proof that they have been validly authorised to act for you under applicable law.

Verifying your request

When we receive your request, we need to verify your identity to confirm you are the person our records are about. We use the personal information in your request only to verify your identity or your authority to make the request. If we can't verify your identity from the information we already hold, we may ask you for more information to verify your identity, and for security or fraud prevention.

If you make the request through an authorised agent, we may need to collect more information to verify your identity before processing it, and the agent will need to provide your written and signed permission to make the request for you.

Appeals

Under certain US state data protection laws, if we decline to act on your request, you may appeal our decision by emailing support@whispertask.app. We will tell you in writing what action we took or did not take in response, including a written explanation of the reasons for our decision. If your appeal is denied, you may complain to your state attorney general.

California “Shine the Light” law

California Civil Code Section 1798.83, known as the “Shine the Light” law, lets our users who are California residents ask us, once a year and free of charge, for information about the categories of personal information (if any) we disclosed to third parties for direct marketing purposes, and the names and addresses of all third parties we shared personal information with in the immediately preceding calendar year. If you are a California resident and would like to make such a request, please send it to us in writing using the details in section 17.

15 Rights in other regions

> **IN BRIEF** You may have additional rights depending on the country you live in.

Australia and New Zealand

We collect and process your personal information under the obligations and conditions set by Australia’s Privacy Act 1988 and New Zealand’s Privacy Act 2020 (Privacy Act).

This policy meets the notice requirements of both Privacy Acts, in particular: what personal information we collect from you, from which sources, for which purposes, and who else receives it.

If you do not want to provide the personal information needed for a particular purpose, it may affect our ability to provide our services, in particular to:

- offer you the products or services you want;
- respond to or help with your requests;
- manage your account with us;
- confirm your identity and protect your account.

At any time, you have the right to ask for access to, or correction of, your personal information. You can make such a request using the details in section 18.

If you believe we are processing your personal information unlawfully, you have the right to complain about a breach of the Australian Privacy Principles to the Office of the Australian Information Commissioner, and about a breach of New Zealand’s Privacy Principles to the Office of the New Zealand Privacy Commissioner.

Republic of South Africa

At any time, you have the right to ask for access to, or correction of, your personal information. You can make such a request using the details in section 18.

If you are not satisfied with how we deal with a complaint about our processing of your personal information, you can contact the regulator:

> The Information Regulator (South Africa)
> General enquiries: enquiries@inforegulator.org.za

> Complaints (complete POPIA/PAIA form 5): PAIAComplaints@inforegulator.org.za and POPIAComplaints@inforegulator.org.za

16 Changes to this policy

> **IN BRIEF** Yes, we will update this policy when needed to stay compliant with the relevant laws.

We may update this policy from time to time. The new version will show a new “Last updated” date at the top. If we make material changes, we may tell you by posting a prominent notice of the changes or by sending you a notification directly. We encourage you to review this policy regularly to stay informed about how we protect your information.

17 How to contact us

If you have questions or comments about this policy, email us at support@whispertask.app. The same address is in the app, where Account → About → Contact us opens your email app with it filled in, and on our website at whispertask.app/#contact. You can also write to us at:

> Antonín Vondrouš
> Vsetinska 292/11
> 15500 Prague
> Czech Republic

18 Reviewing, correcting or deleting your data

Depending on the laws of your country, or of your state if you live in the US, you may have the right to ask for access to the personal information we collect from you and details of how we have processed it, to correct inaccuracies, or to delete your personal information. You may also have the right to withdraw your consent to our processing of your personal information. Applicable law may limit these rights in some circumstances. To ask to review, update or delete your personal information, email us at support@whispertask.app. You can also make many of these changes yourself in the app, as described below and in section 12.

Deleting your account in the app

Go to Account → Manage account → Delete account. You will be asked to confirm it is you (with your password, or with Apple or Google), and then to type DELETE. This permanently deletes:

- your account and profile;
- your recordings, transcripts, tasks, notes and folders, including any still in Recently deleted;
- your credits, subscription records, the record of your agreement to our terms and this policy, and your consent records for AI processing, usage analytics and crash reports;
- our copies of the purchase events Superwall sent us about you;
- your usage analytics at PostHog.

If you signed in with Apple and confirm the deletion with Apple, we also ask Apple to revoke WhisperTask’s access to your Apple account. If you signed in with Google, the app also tries to disconnect WhisperTask from your Google account. If either doesn’t happen, you can remove WhisperTask in your Apple or Google account settings.

Crash reports at Sentry expire on their own (see section 9). Deleting your account does not cancel a subscription bought through the App Store, Google Play or another app store; cancel it in that store's subscription settings to stop being charged.
