LEGAL

Privacy policy

Last updated 8 November 2026

This policy explains how VoiceHubs collects, stores, and processes personal data when you use voicehubs.io and the VoiceHubs platform at app.voicehubs.io. We've written it to be readable end-to-end. Where a section uses a legal term we define it the first time it appears.

VoiceHubs sits on top of your calendar and makes sure every qualifying meeting is prepared. The meeting's organiser (or whoever they hand it to) sets up a brief by voice or text, attendees read it and react by voice or text before the meeting, and the organiser finalises the brief before it starts. Each of those steps touches some personal data — we explain what, why, where it's stored, and how long for, below.

§1 Who we are

VoiceHubs is a limited liability company under the laws of the Netherlands, with its registered office in Zandvoort, registered with the Dutch Chamber of Commerce under number **83680578**. In this policy, *VoiceHubs*, *we*, *us*, and *our* all refer to the same company.

For privacy questions, requests, or to exercise your rights under the GDPR, email info@voicehubs.io. We read every message and reply within one business day, Monday to Friday.

§2 Your role and ours

The GDPR distinguishes between the party that decides why and how personal data is processed (the controller) and the party that processes data on the controller's behalf (the processor).

WHEN VOICEHUBS IS THE PROCESSOR

When a customer organisation buys VoiceHubs for its team, the organisation decides who to invite, what to discuss, and how long to keep the data — so the organisation is the controller. VoiceHubs processes that data on the organisation's behalf, governed by our Data Processing Agreement (see the Processing agreement page). This covers everything your organisation puts into the platform: calendar events, VoiceHub setups, contributions, transcripts, syntheses.

WHEN VOICEHUBS IS THE CONTROLLER

For a small set of data we collect about you directly — for example, when you create an account, contact us, visit the marketing site, or pay an invoice — we are the controller. Sections 3 and onwards explain those flows.

§3 What we collect and why

ORGANISER ACCOUNT DATA

When you sign up, we store your full name, email address, a hashed password (or the OAuth identifier if you sign in with Google or Microsoft), and the organisation you registered. We use this to authenticate you, associate you with your organisation, and send transactional emails (account confirmations, magic links, password resets, billing).

Legal basis: performance of the contract we have with you (GDPR Art. 6(1)(b)).

CALENDAR DATA (WHEN YOU CONNECT GOOGLE CALENDAR OR OUTLOOK)

When you connect your calendar, we read event titles, times, descriptions, attendee email addresses, and the meeting link. We use this to identify which meetings match the auto-attach rule you've set (default: three or more attendees on meetings you organise), attach a VoiceHub to those meetings, and write the synthesised overview back into the event before the meeting starts. We do not read calendar events on the calendars of contributors who haven't authorised us.

Legal basis: performance of the contract you ask us to provide (GDPR Art. 6(1)(b)). We rely on Google's Limited Use requirements: we use calendar data only to provide the user-facing features you sign up for, and we do not transfer it to third parties for advertising, train AI models on it, or read it for any purpose unrelated to delivering the service.

CONTRIBUTION DATA (VOICE AND TEXT)

When you contribute to a VoiceHub, we store: the audio of your voice notes (if you record audio), the transcribed text, any text contributions you type, and the verified email address you used to authenticate. We use this to deliver the synthesised overview to the meeting's organiser and attendees, and to attribute contributions back to you within the organisation's account (so the organiser knows who contributed and who hasn't).

Unlike anonymous-survey tools, VoiceHubs contributions are attributed by design — your name is visible to the organiser of the VoiceHub you're contributing to. The synthesised overview itself aggregates contributions into themes; whether your individual contribution text or audio is visible to others in the organisation depends on the settings the organiser chose for that VoiceHub.

Legal basis: performance of the contract between us and the organiser's organisation (GDPR Art. 6(1)(b)), and our legitimate interest in delivering accurate, attributable meeting preparation (GDPR Art. 6(1)(f)). Before you contribute, you see a notice explaining how your contribution will be used and who can see it.

BILLING DATA

VoiceHubs currently operates on a free tier only, so no billing data is collected. When paid billing is enabled and you (or your organisation) add a payment method, we will store the billing email, billing address, and the last four digits and brand of the card via our payment processor. We will never see or store full card numbers, expiry dates, or CVV. Invoice records will be stored for as long as Dutch tax law requires (currently seven years). This policy and the sub-processor list will be updated when payment processing goes live.

Legal basis: performance of the contract (Art. 6(1)(b)) and compliance with our legal obligations under Dutch tax law (Art. 6(1)(c)).

USAGE DATA

We collect basic usage data when you use the platform: pages you visit, features you use, timestamps. Marketing-site analytics are handled by Fathom, a cookieless analytics tool that does not identify individual visitors. Application-side error tracking (when something breaks in the app) is handled by Sentry; error reports may include the URL you were on, your user ID, and the technical context of the error.

Legal basis: our legitimate interest in operating and improving the service (Art. 6(1)(f)).

CONTACT FORM AND SUPPORT MESSAGES

When you contact us — through the website, by email, or by reply to a transactional email — we store your message and the email address you used, so we can reply and (if needed) follow up. Support conversations are stored for as long as needed to resolve the issue plus a reasonable archive period.

Legal basis: our legitimate interest in responding to people who contact us (Art. 6(1)(f)).

§4 Where we store it

We store and process personal data primarily inside the European Economic Area. The primary application database and file storage are in Germany (AWS eu-central-1, operated by Supabase). Email delivery and any AWS-hosted file storage we use directly are in Ireland (eu-west-1). The large-language model that processes contribution content for synthesis is operated by Mistral AI in France.

Two sub-processors involve limited processing outside the EEA, in each case adequate or transient: **Speechmatics** in the United Kingdom (covered by the UK adequacy decision) processes audio for speech-to-text transcription on a transient basis and returns the transcript before deleting the audio; **Sentry** in the United States receives application error logs that may include user identifiers in the error context.

Where data is transferred outside the EEA to a non-adequacy country, we rely on the European Commission's Standard Contractual Clauses (2021/914) and the supplementary measures required by them.

§5 Who we share it with (sub-processors)

We use a small set of trusted sub-processors to deliver the service. Each one is bound by a data processing agreement that limits what they can do with your data, requires them to apply appropriate security measures, and restricts onward transfers.

CURRENT SUB-PROCESSORS

SUB-PROCESSOR	PURPOSE	REGION	STORAGE
Supabase Inc. (database)	Primary application database (user profiles, VoiceHubs, contributions, organisation data, authentication)	Germany (AWS eu-central-1)	Persistent

SUB-PROCESSOR	PURPOSE	REGION	STORAGE
Supabase Inc. (storage)	File storage (audio recordings, attachments, organisation logos)	Germany (AWS eu-central-1)	Persistent
Amazon Web Services Inc.	Additional file storage and transcoded audio	Ireland (eu-west-1)	Persistent
Mistral AI	Large-language model for question generation, theme extraction, and synthesis of contributions; speech-to-text and note-taking for our own research interviews	France	Transient (processed in-memory, not persisted)
Speechmatics	Speech-to-text transcription of voice contributions	United Kingdom (UK adequacy decision)	Transient (audio deleted after transcript is returned)
Upstash Inc.	Statistics on personal demo links (when opened, how far viewed, next step chosen) and notes from our research interviews	Cloud-hosted database; region available on request	Up to 13 months
Resend Inc.	Transactional email delivery (account, billing, notifications)	Ireland (AWS eu-west-1)	Email delivery logs and bounce data
Functional Software Inc. (Sentry)	Application error logs and performance monitoring	European Union (EU region)	Persistent
Fathom Analytics	Cookieless website analytics (aggregate visitor data only, no individual identification)	Canada	Aggregated, no personal identifiers

CALENDAR DATA FLOW

When you connect Google Calendar or Outlook, event data (event titles, times, descriptions, attendee information) may be processed by Supabase, Mistral AI, and Resend as described above. We do not sell or share Google user data with any third party other than the sub-processors listed in this policy, and we do not use Google user data for advertising or to train AI models.

DEMO LINKS AND RESEARCH INTERVIEWS

When you ask for a demo, your name, company and email go into your own demo link, and we keep the statistics described above for up to 13 months. At events we sometimes ask people about their meetings. We only record such an interview if you agree first. The recording is made on the interviewer's phone.

Mistral AI types it out and sorts it into notes, and the transcript and notes are kept for up to 13 months. Ask us at any time and we delete your recording, transcript and notes.

CHANGES TO THIS LIST

If we add a new sub-processor with access to customer data, we update this list and post a notice on this page at least 30 days before the change takes effect, so controllers can object. If we cannot resolve an objection, the affected controller may terminate the relevant service with a pro-rated refund of any unused prepaid fees.

§6 How we secure it

We apply technical and organisational security measures appropriate to the risk, including: encryption in transit (TLS 1.2 or higher) and at rest, role-based access control with least-privilege principles, multi-factor authentication for all internal access to production systems, regular dependency and vulnerability scanning, separation of staging and production environments, and audit logging of administrative actions on customer data.

Personnel with access to customer data are subject to confidentiality obligations and are trained on data protection and security practices. Access is granted only on a need-to-know basis and revoked when no longer required.

§7 How long we keep it, and when we delete it

Different categories of data have different retention periods. The table below summarises the defaults. Your organisation's admin can adjust some of these through the platform settings (where the data is theirs to govern as controller).

DATA	DEFAULT RETENTION	ON ACCOUNT CLOSURE
Organiser account data	Active for the life of the account	Deleted within 30 days of cancellation
Calendar event data	Only as long as the calendar connection is active	Deleted when the calendar connection is revoked or the account is cancelled
Contribution audio	Audio is deleted immediately after transcription completes (no persistent audio storage by default; organisations can opt in to retention via account settings)	Any retained audio is deleted within 30 days of cancellation
Contribution transcripts and text	Retained for as long as the parent VoiceHub or organisation account is active, subject to controller-configured retention	Deleted within 30 days of cancellation
Syntheses	Retained as long as the parent VoiceHub is active	Deleted within 30 days of cancellation

DATA	DEFAULT RETENTION	ON ACCOUNT CLOSURE
Billing and invoice records	Seven years (Dutch tax law)	Retained for seven years from invoice date regardless of account status
Support messages	Two years after resolution	Retained two years after the conversation ends
Application error logs (Sentry)	90 days	Rolling 90-day window, oldest events expire automatically

After the cancellation window closes, we permanently delete personal data from our active systems. Backups containing the data are overwritten on the regular backup-rotation schedule (currently 35 days). For data your organisation is the controller of, you can export it from the admin dashboard at any time and during the 30-day cancellation window.

§8 Data breaches

If we become aware of a personal data breach affecting your data, we will notify the affected customer organisations without undue delay, and in any case within 48 hours of becoming aware. The notification will include, to the extent known, a description of the breach, the categories and approximate number of data subjects and records concerned, likely consequences, and the measures we are taking to address it.

Where required by GDPR Art. 33 and Art. 34, we will notify the relevant supervisory authority (in the Netherlands, the Autoriteit Persoonsgegevens) and, where the breach is likely to result in a high risk to the rights and freedoms of natural persons, the affected data subjects directly.

§9 Children's data

VoiceHubs is built for workplace use. We do not knowingly collect personal data from anyone under the age of 16. If you believe a child has provided personal data to us, please contact us at info@voicehubs.io and we will delete it.

§10 Your rights under the GDPR

If we hold personal data about you, you have the rights set out below. To exercise any of them, email info@voicehubs.io from the address we have on file (or include enough information for us to verify your identity). We respond within one month, free of charge in the first instance.

- **Access (Art. 15)**: ask for a copy of the personal data we hold about you.
- **Rectification (Art. 16)**: ask us to correct inaccurate or incomplete data.
- **Erasure (Art. 17)**: ask us to delete your data, subject to lawful retention requirements (for example, invoice records under Dutch tax law).
- **Restriction (Art. 18)**: ask us to limit how we process your data while a question is being resolved.
-

Portability (Art. 20): ask for a machine-readable copy of data you provided to us, where processing is based on contract or consent.

- **Object (Art. 21)**: object to processing based on our legitimate interests, including profiling.
- **Withdraw consent (Art. 7(3))**: where processing relies on consent, withdraw it at any time without affecting the lawfulness of prior processing.
- **Lodge a complaint**: you can complain to the Dutch supervisory authority (Autoriteit Persoonsgegevens, autoriteitpersoonsgegevens.nl) or the authority in your EU country of residence.

Where you contributed to a VoiceHub created by an organisation that uses VoiceHubs, that organisation is the controller for your contribution and the questions above are usually best addressed to them. We will assist them in responding to you within the legal time frame.

§11 Cookies and local storage

We use only strictly-necessary cookies and local storage: to keep you signed in, to remember language and UI preferences, and to maintain CSRF protection on form submissions. We do not use advertising cookies, third-party tracking cookies, or analytics cookies that identify you.

Marketing-site analytics are handled by Fathom, which operates without cookies and without collecting personal identifiers. Because we do not use non-essential cookies, we do not display a cookie consent banner.

§12 Automated decision-making

VoiceHubs uses AI (large-language models operated by Mistral AI in France) to generate questions, transcribe audio, extract themes, and write synthesised overviews. The output is presented to organisers as aggregated themes and a summary, not as a decision or recommendation about any individual contributor.

We do not use automated decision-making within the meaning of GDPR Art. 22 — no decision producing legal effects or similarly significant effects on a data subject is taken solely by automated means. Interpretation and any follow-up actions are left to the human organiser.

Customer audio, transcripts, and contribution text are not used to train third-party machine-learning models. We have confirmed this with Mistral AI and Speechmatics as part of their respective data processing agreements with us.

§13 Changes to this policy

We may update this policy from time to time — for example, when we add a new feature that changes what we process, when we add or remove a sub-processor, or when the law changes. Material changes will be communicated by email to account holders at least 30 days before they take effect. The last-updated date at the top of this page always reflects the date the current version took effect.

Previous versions are available on request by emailing info@voicehubs.io.

§14 Contact