

Akoé Data Protection

TOOLBOX 21 Single Member P.C., Voulgaroktonou 3, 65404 Kavala, Greece. For any questions, complaints, or requests, please contact our privacy contact at dpo@akoe.ai.

Overview

A recording you upload to Akoé is usually a recording that matters. This page says, in plain language, what happens to it. If you require any additional documentation (e.g., for submission to a Research Ethics Committee), please contact us at support@akoe.ai and we'll do our best to help.

What arrives. From video we keep only the audio track. When a large file is handled on our servers rather than in your browser, the raw upload sits in encrypted storage only long enough to extract the audio, then the whole file — video frames included — is deleted. In modern browsers the sound is extracted on your device, so the footage itself never travels. Everything moves encrypted.

Where it lives. On EU-owned, EU-based infrastructure only, encrypted at rest with keys kept per workspace.

Who sees it. Your projects are private to you by default; sharing is explicit. No third-party AI service ever accesses or otherwise processes your files, and nothing you upload is used to train models — ours or anyone else's.

How long it stays. On the schedule you choose: 7, 30 or 90 days, or until you delete it. Audio and transcript are deleted together, immediate deletion is always available, and backups mirror your deletions.

What leaves. Only the exports you download. Search queries are content too: never logged, never stored.

Data Processing

Akoé involves two very different kinds of data, and we wear a different hat for each. This policy is split accordingly.

Part A — Your account and our website (we are the controller)

What data do we process?

- **Account information:** email address, password (stored as a salted hash), workspace name, settings and preferences, billing details (handled by Stripe, our payment provider — see Recipients). We have no name field: an account is an email address.

- **User content:** your audio, video and text data — covered separately in Part B, where we act only on your instructions.
- **Usage data:** usage metadata (such as jobs run, audio-hours consumed, timestamps), minimal technical logs (IP, user agent) for security.
- **Device data:** on our public website only, aggregate statistics include coarse device information (browser, operating system, device type) — see Analytics. The application records no device data beyond the user agent in the security logs.
- **Communications data:** support correspondence (messages you send us through the in-app contact form are stored encrypted on our EU servers and read only to provide you with a suitable answer).

We do not use advertising trackers anywhere in the application. We also do not use cookies beyond those strictly necessary for login and security.

How do we receive these data?

- **You provide them:** account details, uploads, vocabulary terms, support messages, your billing country at checkout, and your marketing-consent choice.
- **Collected automatically:** the usage metadata, the security logs, and the cookieless website statistics described under Analytics.
- **From external sources:** our merchant of record sends us confirmation of each payment (transaction identifiers, amount, billing country — never your card details); our email providers report delivery status of what we send you; and for invoiced business plans we may validate your VAT number against the EU VIES register. We gather nothing else from anyone.

Analytics

Our public marketing pages (akoe.ai) use self-hosted, cookieless first-party analytics: aggregate visit counts only — no cookies, no cross-site tracking, and no profile of you. The data never leaves our servers and is never shared. The application itself (app.akoe.ai) contains no analytics at all; product usage is measured only by our own content-free counts and durations, never your content.

Marketing and commercial communications

Product news (new features, plans, offers) is sent only with your prior consent (Art. 6(1)(a)): the signup checkbox is unticked by default, consent counts only after you confirm it from your inbox (double opt-in), and you can withdraw it any time in Account settings or via the unsubscribe link in every such email. These emails are sent through Brevo (Sendinblue SAS, France, EU), which receives your email address and consent state — never your content — and records standard delivery, open, and click statistics for the news emails you receive; we use them only to judge whether the news is worth sending. The contact and its statistics are removed the moment you withdraw or delete your account. None of this applies unless you opted in. Operational notices workspace owners must receive (subprocessor changes, terms changes, deletion warnings) are not marketing and are sent to everyone.

Purposes and legal bases

We process data only for the purposes of: providing the service and account (contract, Art. 6(1)(b)); invoicing and tax (legal obligation, 6(1)(c)); security, abuse prevention, and service improvement based on aggregate usage (legitimate interests, 6(1)(f)); operational notices workspace owners must receive (subprocessor changes, terms changes, deletion warnings — contract and legal obligation); and product news (new features, plans, offers) only with your prior consent (Art. 6(1)(a)). In the latter case, withdrawal of consent does not affect provision of the service. We do not process your data for any purpose other than those explicitly stated here.

Retention

- **Account data:** for the life of the account; you can delete the account at any time, and deletion is immediate.
- **Invoicing data:** per Greek tax law (currently up to 10 years) — content-free billing records only.
- **Security logs:** at most 12 months, then deleted automatically.
- **Support threads:** 12 months, then deleted automatically.

Recipients

- **Hetzner Online GmbH (Germany, EU)** — hosting.
- **Stripe, acting as our merchant of record through its entity Link, LLC (South San Francisco, California, USA)** — Link/Stripe is the seller of record for your purchase, issues your invoice, and collects and remits EU VAT. It receives your billing details (email, billing country, and transaction amount; your card details go straight to Stripe's hosted checkout and never reach us) and never processes your recordings or transcripts. Because this entity is US-based, that billing data is transferred to the USA under Standard Contractual Clauses; the underlying card processing runs through Stripe Payments Europe, Ltd. (Ireland, EU).
- **Scaleway SAS (France, EU)** — delivery of our transactional email (sign-in links, job notifications — recipient address and message only).
- **Brevo (Sendinblue SAS, France, EU)** — product-news emails, only to users who opted in (see Marketing and commercial communications).
- **Our accounting provider** — as required by law.

No one else, and never for advertising. The subprocessors that touch content on our instructions are a separate, deliberately short public list: [Subprocessors](#).

Your rights

Every user is entitled to the following:

- **The right to access** – You have the right to request copies of your personal data.
- **The right to rectification** – You have the right to request that we correct information that is inaccurate.

- **The right to erasure** – You have the right to request that we erase your personal data, under certain conditions.
- **The right to restrict processing** – You have the right to request that we restrict the processing of your personal data, under certain conditions.
- **The right to object to processing** – You have the right to object to the processing of your personal data, under certain conditions.
- **The right to data portability** – You have the right to request that we transfer the data that we have collected to another organization, or directly to you, under certain conditions.

Exercising these rights is free of charge. If you would like to exercise any of them, please send an email to dpo@akoe.ai.

Part B — Recordings and transcripts (we are the processor)

The audio, video, and transcripts you process through Akoé are your data, under your control. For this content, the controller is you — your organisation where you use Akoé on its behalf, or you personally where you upload your own recordings — and we act strictly on your instructions under our Data Processing Agreement (available on request: info@akoe.ai).

What that means in practice:

- Everything is processed and stored only in the EU, on infrastructure we control.
- Your audio and transcripts are deleted together, automatically, on the retention schedule you set (7, 30, or 90 days — or kept until you delete them). The audio stays available in-between so you can play it back while correcting the transcript. Unpaid uploads delete themselves after 24 hours.
- We keep only the audio track — video frames never survive ingest. In modern browsers the video never leaves your computer; when a large file is uploaded whole, the raw upload is held briefly in encrypted storage only until we extract the audio, then deleted right away. The audio track follows the same retention schedule as your transcript.
- Everything derived from your content — the search index and the mentions index — is built from your transcript and deleted together with it.
- Your deletions are kept in a private Deletion history in your workspace, which you can erase whenever you like.
- We never use your content to train models, never sell it, never review it proactively, and exclude it from all system logs.
- Speaker separation tells voices apart within one recording (Speaker 1, Speaker 2). It does not identify who a voice belongs to, keeps no voiceprints, and never matches voices across recordings.
- If a recorded person contacts us about a recording, we will refer them to you (the controller) — we don't even have the context to answer, and usually no longer have the data.

How this content is protected: [Security](#) · [Subprocessors](#) (full Art. 32 detail on request).

Security

We're built to hold as little as possible, for as short as possible — we can't leak, lose, or be compelled to produce what we no longer have.

- **EU-only.** Everything — upload, processing, storage — happens on servers we control in **ISO 27001-certified data centres in the European Union**, run by EU-owned, EU-based companies. No content ever leaves the EU.
- **Encrypted in transit and at rest, with per-workspace isolation.** Your workspace's keys are independent of your password, so a password reset never loses your work.
- **Access is restricted and logged, and we never look at your content** — we process it with machines, on your instructions, and nothing more.
- **No third-party AI, ever.** Transcription, translation and entity recognition run only on machines we operate in the EU. We never use your content to train models — ours or anyone else's — and never sell it or analyse it for advertising.
- **Deleted on your schedule.** Audio and transcript are deleted together (7, 30, 90 days, or until you delete them); immediate deletion is always available; and our EU backups mirror your deletions.
- **Your email is your account.** If you lose access to it, we will not move the account, disable two-factor authentication, or release recordings on the strength of an emailed request — we have no way to verify who is asking, and that same rule is what stops someone else claiming your account. Keep your recovery codes safe.

For your paperwork — the full technical and organisational measures (Art. 32: encryption and key management, access logging, backup and deletion mechanics, breach handling), an Art. 28 **Data Processing Agreement**, and the full **process concept** written to attach to a DPIA or ethics application — are available on request: info@akoe.ai. Transcripts are AI-generated and may contain errors; the editor exists for human review.

When our architecture changes, this page changes in the same release.

Subprocessors

The complete list of companies that may process customer content on our behalf:

Subprocessor	Country	What they do for us	Safeguards
Hetzner Online GmbH	Germany (EU)	Hosting and infrastructure for the entire service	Art. 28 DPA · ISO/IEC 27001-certified data centres · EU-only
Scaleway SAS	France (EU)	GPU computing for speech transcription and speaker separation	Art. 28 DPA · ISO/IEC 27001-certified data centres · EU-only

That's the whole list. We add a row only when a provider actually enters production — and we tell you first (see below).

Notification of changes: workspace owners receive email notice **14 days** before any addition or replacement, per our Data Processing Agreement. You may object on reasonable data-protection grounds.

What you won't find here: no US cloud provider ever processes your recordings or transcripts, no third-party AI touches your content, and no analytics or advertising services anywhere. One deliberate exception, named plainly: **payments** run through our merchant of record, **Stripe via Link, LLC (South San Francisco, USA)** — they handle billing data only, never your recordings or transcripts, with the US transfer covered by Standard Contractual Clauses. Full detail is in Part A above. And if you opt in to product-news emails (off by default, double-confirmed), those are sent via **Brevo (Sendinblue SAS, France, EU)** — your email address and consent state only, never your content, removed the moment you unsubscribe.

How to contact the appropriate authority

Should you wish to report a complaint or if you feel that we have not addressed your concern in a satisfactory manner, you may contact the Hellenic Data Protection Authority.

Email: contact@dpa.gr · Phone: +30 210 6475600 · Address: Hellenic Data Protection Authority, Kifissias 1-3, PC 115 23, Athens, Greece.

Changes

Last updated: 17 July 2026. We may occasionally update this notice. If we make significant changes, we will notify you in advance of the changes, but we encourage you to periodically review this notice for the latest information on our privacy practices.