Terms of Use

Version 2.1 · Effective 2026-09-24 · Contract document

In short

Recordstead records, transcribes and summarizes meetings on your Mac. The processing trial lasts 30 days from its first eligible use. A Personal license is a one-time purchase for up to two active Macs and includes updates to version 1.x. Your mandatory consumer rights remain intact.

1. Scope and contact

These terms cover the Recordstead macOS app and this website. Recordstead supplies the app and its license. Paddle sells the license at checkout under its Buyer Terms. Questions about the app go to support@recordstead.app; payment questions can also go through the receipt or Paddle buyer support. Our Privacy Policy explains how service data is handled.

If you use the app for an organization, make sure you have authority to do so. You are responsible for following laws that apply to your use.

2. Trial and Personal license

The free processing trial starts immediately before the first eligible processing operation, after the app completes its online access check. Recording or setting up the app alone does not start the trial. It lasts 30 days. When it ends, you can still record, read, search and export existing meetings; new transcription, speaker analysis and summaries require a license. The trial is limited to one eligible Mac under the trial rules. The Privacy Policy explains the pseudonymous device signal used for this limit.

A Personal purchase grants a non-exclusive, non-transferable license to use Recordstead 1.x on up to two active Macs at once, subject to the replacement limits shown in the app. It is one payment, with no subscription or Recordstead account. Updates to version 1.x are included. A later major version is outside this license unless expressly offered separately; no discount for it is promised. The license key is delivered by email after the purchase is confirmed. Keep it safe. Support can help verify a purchase and resend the same key while the license remains active, but there is no self-service recovery portal.

Initial trial access, key activation and periodic paid access refresh need an internet connection. A paid signed lease can continue offline until its stated cutoff, at most 30 days from issue. A refund or valid revocation prevents a new lease, although an already offline Mac may retain processing access until its existing lease ends. Loss of processing access does not delete meetings stored on your Mac.

3. Refunds and consumer rights

Recordstead offers a full refund if you request it within 14 calendar days of purchase, including after activating or using the app. The date of your request controls this window, even if the refund is completed later. The Refund Policy explains how to ask through Recordstead or Paddle and what happens to access. This guarantee does not limit withdrawal, conformity or other rights that cannot be excluded under applicable law.

4. Your content and lawful use

You retain your rights in recordings, transcripts and other meeting content. Recordstead does not receive it by default. You decide whether you may record, what notice or consent participants need, and whether you may save someone's voice for recognition. The app's acknowledgements do not replace those duties. Exports, backups and external storage you configure are yours to manage. If you choose an external AI service, its own terms and privacy notice govern that destination.

Do not use the app for unlawful covert monitoring, prohibited biometric or emotion inference, infringement, or interference with its licensing service. Do not redistribute or sublicense the app. You may inspect or reverse engineer it to the extent applicable law gives you a right that these terms cannot exclude. Third-party components and models have their own licenses and use policies, listed in the app.

5. Generated output and support

Transcripts, summaries, titles and answers can be inaccurate or incomplete. Check them before relying on or sharing them. Generated output is labelled in the app, and summary exports carry a provenance record. The Support page gives product, privacy and security contacts. We do not promise error-free transcription or uninterrupted online services, but these terms do not reduce any mandatory standard of care or remedy that applies to you.

6. Ending use and updates

You may stop using Recordstead at any time. A completed full refund ends the paid entitlement as described in the Refund Policy. We may restrict access for verified fraud, abuse or a material breach where applicable law permits. Existing local meetings are not erased because access ends.

We may update these terms prospectively. Material changes to rights already purchased require the notice or consent applicable law requires. If a clause is unenforceable, the remaining clauses continue to apply. Mandatory consumer protection rules and remedies remain available wherever they apply.

Refund Policy

Version 1.1 · Effective 2026-09-24 · Contract document

This policy applies to Recordstead Personal purchases.

The 14-day guarantee

Recordstead offers a full refund when you request it within 14 calendar days after purchase, even if you have activated the license key or used the app. The date you send the request determines whether it is within the window; payment processing may finish later. This is an additional commercial guarantee. It does not limit any mandatory withdrawal, nonconformity, payment or other consumer rights you have under applicable law.

How to request a refund

Email support@recordstead.app, use the support link in your Paddle receipt, or contact Paddle buyer support. Include the purchase email address and receipt or Paddle transaction reference, if available. Do not send card details, meeting content or your full license key. If you write to Recordstead within the 14-day window, we record when the request arrived and coordinate it with Paddle even if processing finishes later.

Paddle handles the payment refund and sends its payment confirmation. A request is not itself a completed refund. Paddle's Refund Policy and applicable law may provide additional rights or routes.

Access and local data

After a verified full refund, paid processing access ends when the adjustment reaches the licensing service. A Mac that is offline may continue under an earlier signed lease until it reconnects or that lease expires, at most 30 days from issue. A pending or rejected request does not itself end access. Refunds do not delete recordings, transcripts, summaries, exports or files in storage you control.

Privacy Policy

Version 2.10 · Effective 2026-10-06 · Informational notice

In short

- Recordstead records and transcribes meetings on your Mac. The app does not automatically send us recordings, transcripts, summaries, tasks or saved voices. If you choose to send meeting content or a diagnostic archive to support, we receive what you send.
- The app has no analytics, no telemetry, no crash reporting, no account and no sync. The website counts page views without cookies and, only if you allow analytics cookies, uses Google Analytics to understand visits, downloads and purchases. Section 7 explains both. Installer and update download totals are also counted separately, as section 8 explains.
- Audio stays on your Mac unless you send it somewhere yourself. By default a recording never leaves your Mac, and neither does a saved voice. You can turn on offload to a destination you configure, an external disk or your own S3-compatible or SFTP storage, and then a recording is uploaded to your storage, already encrypted, so the destination only ever holds ciphertext. We are never the destination and never hold your credentials. If you connect an AI service yourself, transcript text goes to the service you chose, under your own agreement with them.
- Recognizing people across meetings is off until you turn it on. It stores a numeric voice template; that is biometric data, and it has its own schedule on this page.
- Deleting a meeting removes it from Recordstead permanently. Files you exported and your own backups are not touched.
- Your meetings are encrypted on disk, with a key held in your Mac's keychain. A copy of the folder on another Mac cannot be read without a transfer code you get from this one. Three things are deliberately not encrypted, and section 2 says which and why.
- What we do hold includes website request data, pseudonymous trial and licensing records, billing and delivery records for completed purchases, and messages you send us.
- If you record other people, telling them and having the right to record is your responsibility. The app asks you to confirm that before the first recording.
- Google Calendar is off until you connect it. If you do, the app reads the

coming week of the main calendar of each Google account you connect, straight from Google onto your Mac, to show your next meeting. Your workspace choices can also determine where an automatically recorded call is saved. This connection does not send us your events or Google sign-in.
Section 14 says what is read and kept.

1. Who we are and who is responsible for what

Recordstead provides this software and website. Privacy questions and requests about your data: privacy@recordstead.app. Support: support@recordstead.app.

Two different worlds, kept apart on purpose.

Your meeting data: you decide. For recordings, transcripts, summaries, meeting titles, speaker names and voice data handled on your Mac, Recordstead is neither a controller nor a processor. The app does not send this content to us; you decide why it exists, who is in the room and how long it is kept. We provide a tool and do not determine the purposes or means of that local processing. That stays true when a bundled language model runs on your Mac. If you choose to send content to support, we handle that copy as part of your support correspondence, described in sections 6 and 7.

Our own service data: we are the controller. Recordstead is the controller for the website, licensing and support correspondence.
For purchases, Paddle handles checkout and payment as the seller, while Recordstead handles license delivery and access. Sections 6 to 10 describe these activities.

2. Meeting content on your Mac

The audio of a call, your microphone track, the transcript, the summary, the title, the tasks found in the transcript, the speaker names and the search index live in app-managed files and one database under your user account's Application Support folder. They are readable
only by your macOS user, and they are encrypted: the database is encrypted, and each stored recording is an encrypted file that also detects tampering rather than a playable one. The key is held in your Mac's keychain and is tied to your macOS account, so copying the folder elsewhere is not enough to read it. That copy asks for a transfer code, which you get from the Mac the meetings came from, and which we never see and cannot reproduce.

If you turn on *offload*, a finished recording is moved off your Mac to a destination you configure, an external volume or your own S3-compatible or SFTP storage, to keep the internal disk from filling. It is the same encrypted file that is uploaded, so the destination holds only ciphertext; the key stays on your Mac. The transcript, summary and everything else stay on your Mac, so search and reading a meeting still work with the audio away. Offload is off by default, you choose the destination and supply its credentials (kept in your Mac's keychain), and switching the active destination never moves recordings already stored elsewhere. We are never a destination.

External recordings remain in your storage until you remove them yourself. Deleting a meeting or disconnecting a destination does not delete those files. Downloaded local copies expire six hours after their last use; playback, export and processing protect a copy until the operation finishes. Expired copies are cleaned while the app runs or when it next opens. Reconnecting an archive restores access only to verified files for meetings still in the app, not deleted meetings.

Three things are deliberately not encrypted:

- A recording while it is still being made. It is written to a staging area in the clear and encrypted when the finished recording is filed. A stream that is still being written cannot be both encrypted and recoverable if the Mac loses power, and we chose recoverable.
- The app's operational log, which holds the processing queue, timings and a record of what the app did. It contains no meeting content: meetings appear in it under an opaque handle, never by title. It stays readable so the app can tell you why it cannot open your meetings when something is wrong with the key.
- A technical log of what the app did, kept in your Mac's own logs folder at ~/Library/Logs/Recordstead/ for 7 days and then deleted. It is the app writing down its own steps: timings, errors, which processing stage ran, the names and formats of the audio devices in use, and a loudness reading every few seconds while recording, so that a fault can be explained afterwards. It holds no meeting content. Titles and people's names are withheld by macOS itself, which is why they appear in it as <private>.

The app sends none of this to us automatically. There is no automatic server-side copy, diagnostic upload or "help us improve" channel. The app contains no analytics or crash-reporting library. The technical log reaches us only if you decide to send it: the *Diagnostic log* row in *Settings > Advanced* has an *Export* button that writes the last seven days of it into a zip file in your export folder, and what happens to that file is then yours to choose.

3. AI services you connect yourself

Summaries, suggested titles, tasks found in your transcripts and Ask answers are produced by a language model.
Four paths exist, and all of them are your choice:

Path	What is sent	Where
Built-in (default)	Transcript text, speaker names, meeting date	Nowhere. A model that ships with the app, running on your Mac
OpenAI-compatible endpoint	The same text, plus each transcript chunk if you enable Ask over your archive	The address you type. We do not choose it, host it or see the traffic
Claude Code	The same prompt text	Your own Claude Code installation, under your own account and Anthropic's terms
Codex	The same prompt text	Your own Codex installation, under your own account and OpenAI's terms

If you use one of the two assistant tools, the app runs the copy already on your Mac and sends the text to its standard input. It signs you in to nothing, holds no account of yours, and each tool is confirmed separately: confirming Claude Code does not turn on Codex. It also narrows what that tool may do while it writes your summary, so your own configured extensions do not receive the text and the tool keeps no copy of the conversation in its own history.

Finding your tasks. After writing a summary, the same provider can read the full transcript again to find tasks assigned to the name you set as *Your name*. That request includes the speaker names or labels, your *Your name* label, the meeting date and the summary language. Choosing *Find Tasks* runs that search again. With a remote provider, the transcript is sent to that provider for each search, under the same confirmation that covers summaries and tasks. The tasks found for you, their source quotes and any due dates are stored with the meeting in the encrypted database on your Mac.

Calendar data obtained through Google APIs is not included in these requests. Section 14 describes that separate connection.

Never sent on any path: audio, voice templates, or the numbers derived from a voice. Each remote path is off until you confirm it for a specific destination, and the app tells you what will be sent before you do. If you point the app at a remote endpoint, that endpoint's operator decides what happens to the text and their policy governs, not this one. A remote address must use HTTPS; the app refuses a non-local address over plain HTTP.

4. Saved voices and the retention schedule

If you turn on recognizing people across meetings, the app stores a numeric voice template per named person so it can label them in later meetings. This is biometric data (special-category data under the GDPR, a voiceprint under Illinois law and similar statutes). Consequences:

- The feature is off in every fresh installation and stays off until you explicitly enable it and confirm a description of what it does.
- Even then, nothing is saved for a new person until you confirm, for that person and by name, that you told them and may keep a record of their voice. Decline, and they are still named in that meeting's notes; nothing about their voice is kept.
- Templates never leave your Mac and are never sent to any AI service.
- They are deleted when you use Forget Person, when you delete the meetings that produced them, and automatically after 90 days without a confirmation.

A template is not stored for a meeting you merely transcribe. When recognition is off, nothing voice-derived survives the run at all.

Who holds the voice data

Nobody but you. Recordstead never receives a saved voice, never transmits one, and has no means of obtaining one. No voice template is sent to any AI service on any processing path, and none is sold, licensed or otherwise profited from, because we do not have it. Where a law requires the person holding voiceprints to publish a retention and destruction schedule, that person is the user of the app, and the schedule their installation enforces is the one below.

The schedule the software enforces

Data	Where it is	Destroyed
Saved voice (template, samples, usage counters)	Your Mac, in the app's database, scoped to one workspace	On Forget Person; when the meetings that produced it are permanently deleted; automatically after 90 days with no confirmation
A speaker question you have not answered yet, which keeps that run's voice numbers so the question can be reopened	Same database, one row per open question	On answering, skipping or cancelling it; automatically after 7 days
Per-meeting voice numbers computed while separating speakers	Not stored anywhere	At the end of the operation that computed them

Two properties of the 90-day rule, and the first is easy to get backwards. "Without a confirmation" means nobody has vouched for the voice, not that the app has stopped using it: recognizing somebody is a read and changes nothing, so a person the app labels automatically for three months, without you ever confirming their name again, *is* deleted at 90 days. And 90 days is a hard ceiling in the code, not a setting; nothing can widen any window in this table.

What "destroyed" means, exactly

The record is removed from the app's database and the app cannot recover it. That is the whole of the promise, and it is deliberately narrower than it could sound:

- We do not claim the underlying disk blocks are overwritten. The database is an ordinary local file and deletion is a database delete, not a secure erase.
- The record was encrypted while it existed, and that is not a secure erase either: we do not claim the underlying ciphertext is overwritten, and the key that could read it is still on your Mac.
- Copies you made yourself, such as exports, Time Machine, iCloud or a duplicated folder, are outside the app entirely and are not touched.

One thing is kept: a record that a voice was destroyed, when, and on what basis it had been saved. It holds an identifier and dates, no name and no voice data, so it cannot say whose voice it described.

Changing this schedule

A material change here is also a change to what you agreed to in the app, so it bumps the version of the in-app description (currently version 4) and every installation is asked again before the feature keeps running.

5. If you record other people

Recordstead does not tell anyone that a recording started, and it cannot. Before your first recording the app asks you to confirm that recording lawfully and informing participants is your responsibility; before automatic call detection starts, it asks again, separately. Settings › General offers a plain-language notice you can paste into an invitation. Where you record, and where the participants are, may require their consent, and where you enable saved voices you may also need their written consent and your own retention policy.

6. Data we hold, at a glance

App operations do not send us meeting content. Support correspondence may include content or diagnostics you choose to send.

Activity	Data	Purpose	Legal basis	Recipients	Kept
Trial licensing	Installation public key, pseudonymous device signal, request identifiers, trial dates, IP address in requests	Grant and check the 30-day trial and prevent repeat use	Trial terms and legitimate interest in preventing abuse	Cloudflare (hosting and database)	Trial device link until its recorded retention date, 24 months after trial expiry or registration without a start; installation and trial records have no general automatic expiry
Paid licensing	License reference and status, public installation keys, up to two activations, optional label sent by the app, replacement history	Activate and check the purchased right	Purchase contract and fraud prevention	Cloudflare (hosting and database)	Active entitlement and activation records have no general automatic expiry; completed replacement records are swept after 90 days

Activity	Data	Purpose	Legal basis	Recipients	Kept
Purchase and delivery	Buyer email and transaction facts supplied by Paddle; a key generated by Recordstead; encrypted stored copies of the email and key; delivery status	Fulfil orders, send or resend the key, process refunds and disputes	Purchase contract and applicable legal obligations	Paddle (independent seller and source of buyer data, not a recipient of the key), Cloudflare (billing database and work queue), Resend (mail delivery)	Encrypted key and email have no automatic expiry, including after refund or revocation. Financial, event and delivery metadata also have no general automatic deletion schedule. Temporary encrypted mail envelopes are wiped after delivery or swept after 23 hours
Private download links	Browser IP address and request time	Serve a build through a signed link we send you	Legitimate interest in delivery	Cloudflare	Signed link expires after 24 hours; the download Worker stores nothing

Activity	Data	Purpose	Legal basis	Recipients	Kept
Updates and public downloads	Request data; on an update download, installation public key, timestamp and request signature	Offer and serve updates and the public installer, and count downloads as totals	Legitimate interest in delivering working software and in knowing how often it is downloaded	Cloudflare	The download Worker stores nothing; Cloudflare operational logs may remain, and the download totals we read reach back 31 days. The public installer download does not require an installation key or a token
Website visits	Request data including IP address, browser and page; cookieless page-view measurements	Serve and protect the site and measure pages read	Legitimate interest in running and measuring the site	Cloudflare	Provider operational logs; analytics in full for seven days, then as aggregates

Activity	Data	Purpose	Legal basis	Recipients	Kept
Optional website analytics	Cookie identifier, browser and device information, approximate location, sanitized pages, referring origin, campaign labels and website events; random session purchase identifier	Understand acquisition, download clicks and purchases	Consent	Google (Google Analytics and Tag Manager)	Analytics cookies: up to 180 days; GA4 user and event data: two-month retention without activity reset, deletion in monthly processing; standard aggregated reports are outside that limit
Website privacy choice	Acceptance or rejection, time of choice and notice version in browser storage	Remember and apply your choice	Legitimate interest in respecting your privacy choice; storage needed to remember it	Stored in your browser; not sent as a separate consent record to us	Used for 180 days; an expired entry is ignored and replaced when you choose again

Activity	Data	Purpose	Legal basis	Recipients	Kept
Support and privacy mail	Your address, message, attachments you choose and the exchange	Answer and document the matter	Legitimate interest in answering and legal rights; a contract where applicable	Cloudflare Email Routing and our mailbox provider	No configured automatic deletion schedule; retained for the matter and applicable dispute or legal obligations, with deletion requests assessed individually

The Google Calendar integration does not send calendar events to these service providers: it reads them directly from Google on your Mac. Section 14 explains that connection and distinguishes information you choose to send to support.

We do not sell personal information or use it for cross-context advertising, and we make no automated decisions about you.

7. Website and support mail

Hosting. The website is served by Cloudflare. Cloudflare processes request data, including IP addresses, as our processor to serve and protect the site (Cloudflare privacy policy, Cloudflare customer DPA).
Fonts are served from our own domain. Optional analytics cookies and the locally saved consent choice are described below.

Counting page views. The site counts page views with Cloudflare Web Analytics. It stores nothing on your device and reads nothing from it: no cookie, no local storage, no device fingerprint, and no identifier that could tie one visit to another or to you. A page view reports the page you opened, the address of the site that linked you, your country, your browser, operating system and device type, how the page was loaded, and how long it took. Cloudflare processes this for us and states that it does not track individual visitors across the sites it serves. Measurements are kept in full for seven days and as aggregates after that. Because nothing is stored on or read from your device, we rely on our legitimate interest in knowing whether the site works and which pages are read. Any content blocker that stops Cloudflare's script stops the measurement, and the site works the same without it.

Optional Google Analytics. If you choose *Accept analytics*, we load Google Tag Manager and Google Analytics to understand how people find and use the website, including clicks to download or buy, opened checkouts and confirmed purchases. A download click does not tell us whether you finished downloading or installed the app. We rely on your consent for analytics cookies and the associated personal data processing. Until you accept, including if you reject or leave the banner unanswered, we do not load these Google services or send them analytics measurements. You can still read the site, download the app and buy a license.

The measurements include a cookie identifier, pages visited, the referring site, campaign labels, browser and device information, approximate location and website activity. Cookie identifiers can link visits from the same browser; these measurements are pseudonymous, not anonymous. Google receives network requests including your IP address; Google states that GA4 does not log or store individual IP addresses. We send page addresses without their query parameters or fragments and only the referring site's origin. We do not send your email, license key, Paddle transaction identifier, payment details or meeting content. To avoid counting a consented purchase twice, we send a random identifier created for that browser session. These counts are incomplete when cookies are refused or blocked; they do not replace Paddle's purchase records.

Google processes these measurements for us under its data processing terms. Read how Google uses information from sites that use its services and Google's Privacy Policy. Section 10 explains international processing. We disable Google Signals, user-provided data collection, detailed location and device collection, advertising personalization and optional account data sharing. We do not use this consent for advertising cookies or remarketing.

Cookies and browser storage. These are separate from the cookie-free Cloudflare measurements above:

Item	Purpose	Lifetime
_ga cookie	Distinguish browsers and link their visits for Google Analytics	Configured to expire after 180 days, without extending expiry on each visit
_ga_<identifier> cookie	Keep Google Analytics session state	Up to 180 days; expiry may be refreshed when Analytics updates session state
recordstead.analytics-consent.v1 in local storage	Remember acceptance or rejection, the time and the notice version	We honour the choice for 180 days, then ask again; the old entry may remain until replaced or browser storage is cleared
recordstead.analytics-purchase.v1 in session storage	Remember a random purchase marker and whether its event was sent, after analytics consent	For the browser tab's session, or until removed when analytics is stopped

Refreshing a session cookie does not extend our 180-day consent period. Your browser may clear cookies or storage sooner. We save either privacy choice so that we can respect it without asking on each page; this record is not used to track you. If the browser cannot save a new consent, analytics stays off. A temporary session-storage flag may remember a rejection when local storage is unavailable. Clearing site storage can make the banner appear again. The choice applies to this browser, not all your devices.

User-level and event-level retention in GA4 is set to two months with reset on new activity disabled; deletion follows Google's monthly process. Standard aggregated reports are outside that retention limit and can remain longer.

You can change your choice at any time in *Cookie settings* in the website footer. Rejecting after accepting stops future Google measurement and removes the Analytics cookies accessible to this website. Withdrawal does not undo processing that took place while consent was valid or automatically erase reports already collected. For a privacy or deletion request, contact privacy@recordstead.app.

Former access requests. The waitlist and its request database have been removed. The website no longer accepts access requests. Earlier messages may remain with their recipients or in the mail provider's delivery records under that provider's retention practices (Resend privacy policy, Resend DPA).

Writing to us. Mail to any recordstead.app or recordstead.com address is received by Cloudflare Email Routing and forwarded to the mailbox we read. There is no automatic deletion schedule for this mailbox. We keep the exchange while handling the matter and any applicable claim or legal obligation. Ask privacy@recordstead.app for access or deletion.

8. Licensing and purchases

The app checks trial and paid access with the Recordstead service at license.recordstead.com, hosted on Cloudflare. It sends a per-installation public key and signature, a request identifier and, for public trial deduplication, a SHA-256 derivative of the Mac's platform identifier. The raw identifier stays on your Mac; the service HMACs the derivative for lookup. This is pseudonymous personal data, not anonymous data. The service also sees your IP address for ordinary network delivery and rate limiting. It does not receive meeting content.

The trial-device link has a recorded expiry 24 months after the trial ends or registration without a start; its cleanup occurs during later licensing requests. Installation, trial and activation records do not have a general automatic expiry today. You may contact privacy@recordstead.app about these records.

For a purchase, Paddle collects and handles checkout and payment information as the seller under its own Privacy Policy. Paddle supplies Recordstead with the buyer email and transaction information needed to issue and manage the license. Recordstead generates the license key and encrypts both the key and buyer email before storing them in its billing database. The app supplies any optional activation label you type; Paddle does not supply that label or the license key. We use Resend to deliver the key.

The encrypted key and email have no automatic expiry, including after a refund or revocation ends processing access. They support manual resend while a license is active, but that purpose is not an implemented deletion trigger. Financial, event and delivery metadata also have no general automatic deletion schedule. Temporary encrypted mail envelopes are removed when delivery is resolved or swept after 23 hours; that cleanup does not remove the stored key or email. You can request deletion through privacy@recordstead.app. We assess a request against any active license, purchase or refund dispute and applicable legal obligation, and explain what can be removed. We do not promise a deletion date that has not been implemented.

Updates and downloads. A build can keep itself up to date. When it starts, and every few hours while it runs, it asks dl.recordstead.app, also on Cloudflare, whether a newer build exists. You can also ask it to look, and you can switch automatic checks off. The feed request carries no app-specific identifier; Cloudflare sees your IP address, as it does for any web request. The public installer from the download page needs no installation key or token. A private download link we send you is signed and expires after 24 hours. For an update download, the app sends its installation public key, the request time and a signature proving that installation made the request. The service verifies that installation before serving the update. None of them sends meeting content, file names, a list of apps on your Mac or a report of how you use Recordstead. Nothing is checked or downloaded while you are recording.

Cloudflare download totals. Separately from optional Google Analytics, we use Cloudflare's request analytics to count downloads as totals: how often the download link on the website was used, and how many installer and update downloads there were, per day, per version and per country. The country is the one Cloudflare derives from the request's IP address. The totals come from Cloudflare's own request analytics; we read nothing else there, no IP address and no installation key, and we store none of it. They reach back 31 days. If you accept website analytics, Google Analytics also measures download-link clicks associated with a cookie identifier, as described in section 7. It does not measure downloads performed by the app's updater or report app usage.

A build compiled locally from source carries no endpoint, no update feed and contacts nothing.

9. Model downloads

Speech and language models come from Hugging Face and its content delivery network when the app needs a model that is not already on your Mac. The active transcription model may download during launch preload; a processing hold may defer that preload. Other models download when their features need them. The request is anonymous,
with no token, no account and no identifier; Hugging Face sees your IP address, the time and which model was requested, under its own
privacy policy. This connection carries no
meeting content, and the download is verified against a pinned checksum before the model is used.

10. International transfers

Cloudflare and Resend are United States companies operating global networks. Both are certified under the EU-U.S. Data Privacy Framework, including its UK Extension, and both incorporate the EU Standard Contractual Clauses in their data processing agreements linked above.

Optional website analytics. Google may process website measurements outside the EEA, including in the United States. Google's
data processing terms
provide for European Commission Standard Contractual Clauses where required for restricted transfers. Google also describes reliance on adequacy decisions, including the EU-U.S. Data Privacy Framework for covered transfers to Google LLC, in its transfer framework information.
These safeguards do not mean that all processing takes place in the EEA.
The linked terms and framework information explain the safeguards; you can also ask us about them at privacy@recordstead.app.

Services your Mac connects to. Hugging Face, any AI provider you configure yourself and Google, if you connect your calendar, are connections your Mac makes directly; their handling of your IP address, text or account is governed by their terms.

11. Your rights

For anything we hold, write to privacy@recordstead.app. You may ask for access, rectification, erasure, restriction, objection, portability, or withdraw a consent you gave us. We answer within one month; if a request is complex we may take up to two further months and will tell you why within the first month. We ask only for what is needed to be sure it is you, normally that you write from the address the record is associated with, and we do not collect more documents to try. Requests are free unless manifestly unfounded or repetitive. You may complain to the data protection authority of the country where you live.

If you asked us to forget you, we may keep a minimal entry saying that this address must not be written to again, so that the request itself is honoured.

For meeting data kept only on someone's Mac, we cannot act on that archive: we have no access to it or a way to find out who recorded you. If someone voluntarily sent us a copy for support, you can ask us about that copy through the privacy address above. The person who made the recording answers requests about their own archive, and the app gives them the tools:

- Export Person Data in People writes a document listing every meeting you appear in, what you were recorded saying, where you are named, and whether a voice template is stored for you. It works whether or not a voice is saved.
- Forget Person removes the voice template and the app's record of recognizing you. Deleting the whole meeting removes the recording, transcript and summary permanently.
- Renaming a speaker corrects a wrong name across their library.

If you write to us about a recording we do not hold, we will explain this and point you to the recorder; we cannot forward the request because we do not know who they are. If the recorder refuses or does not answer, you can contact a data protection authority about their handling of the recording.

If you run Recordstead and receive such a request: check that it really comes from the person, export what you hold from People, answer, then act. Deletion is *Forget Person* for a voice, or permanently deleting the meetings. The export covers one name as your library spells it and one installation; copies you have already exported, sent or backed up are yours to handle. The app keeps no request log; if you need one, keep it yourself.

12. How long things are kept on your Mac

Data	Kept until
Your transcripts, summaries and saved tasks	You delete the meeting. There is no automatic expiry and no cap we impose
Your recordings	Under Settings > Storage, choose an age of 1, 3, 7, 30 or 90 days (7 by default), or keep the newest 1, 5, 10 or 20 local recordings regardless of their age. Eligible older audio is removed from this Mac or moved to a destination you configured, according to your setting; the meeting, its transcript and its summary stay. A recording of a meeting that was never transcribed is not removed this way, because it is the only copy that meeting has
A speaker question you have not answered	You answer it, or 7 days
Saved voices	Forget Person, or 90 days without a confirmation
Capture leftovers the app can no longer use	Swept after 7 days; an unfinished recording is recovered instead of deleted. This staging area is the one place on disk that is not encrypted, and the sweep is what empties it
The technical log of what the app did	7 days, swept while the app runs. A zip you exported from it is a file of yours, and is kept until you delete it
Events read from the Google accounts you connected	Only in the app's memory while it runs, never written to disk. Quitting clears them all; removing a connection clears its copy
Calendar connection details: refresh token, display label, account email when available, connection status and workspace choices	In a separate item for each connection in this Mac's keychain until you replace or remove that connection. Remove from This Mac removes the local item; Disconnect also asks Google to revoke access
Which calendar event a recording started during	You delete the meeting. It is an identifier of the event, stored encrypted with the meeting, never its title or its guests

Deleting a meeting is permanent: it is removed from Recordstead and cannot be recovered there. Files you exported, and your own backups such as Time Machine or iCloud, are outside the app's reach and are not touched.

13. AI-generated content

Transcripts are produced by automatic speech recognition and are labelled *Automatic transcription* in the app. Summaries, suggested titles, tasks found in your transcripts and Ask answers are generated by a language model; the app labels them *AI-generated. Review for accuracy.* and tells you which model and destination Ask uses before your first question. They can be wrong, and they are not a verbatim record.

An exported summary carries a machine-readable provenance record at the end of the file, stating that the content was machine-generated, by which model, where, and when. An exported transcript carries no such record: it is a verbatim record of what was said, not text a model wrote for you. If you publish or circulate generated text, any duty to say it was AI-generated is yours as the one publishing it; keep the provenance record in place, or label the text yourself.

The models that run on your Mac are published by third parties under their own licences, listed in the app under Help › Third-Party Licenses. We are not the developer of those models.

14. Google Calendar, if you connect it

Recordstead can show your next meeting on its Home screen and open the recording of the last time you had the same meeting. This needs the calendar of one or more of your Google accounts and is off until you choose *Connect* in *Settings > Calendar* or on Home.

Signing in. *Connect* opens Google's own sign-in page in your browser, and *Add Account…* does the same for another Google account. You sign in to Google and grant access there; Recordstead never sees your Google password. The access you grant is read-only and covers events on calendars you own. The app reads only the main calendar of each account you connect, never changes or creates an event, and does not read your other calendars, your contacts or your mail.

What is read. While connected, and every few minutes while the app runs, your Mac asks Google for the events of each connected account's main calendar from now to seven days ahead. For each event the app uses its title, start and end time, the names or addresses of the people invited, Google's identifier for the event, and the link to the call, from which it keeps only which call service it is (for example Zoom or Google Meet). The app also reads the calendar's title and, when available, the email on event entries that Google identifies as belonging to that calendar. It uses these to label the connection and uses the email to check whether a reconnect returns the same account. The editable calendar title is not used for that check. An event's location and description are read only to find the call link and are not kept. Cancelled events, events you declined and all-day events are not shown.

Where it goes. The app's requests to Google use HTTPS, which encrypts data in transit. They go directly from your Mac to Google, with no Recordstead server in between. This integration does not send us your events, your account addresses or the sign-ins that let the app read them. Google sees the requests under your Google account and its own
privacy policy.

Sharing and disclosure. The Google Calendar integration does not send data obtained through Google APIs, your connected account addresses or your OAuth tokens to Recordstead-operated servers or to third-party service providers. This includes Cloudflare, Paddle, Resend and any external AI provider you configure. The app communicates directly with Google to authorize access, refresh or revoke tokens, and read your calendar. Data obtained through Google APIs is not supplied to external or on-device language models. If you separately choose to include calendar information in a support message, we receive what you send and handle it as support correspondence under section 6; the calendar integration does not send it for you.

What is kept, and where. Each connection has a separate item in your Mac's keychain containing the refresh token Google gives it, its display label, the account email when available, whether it needs a new sign-in and its workspace choices. These items are for this Mac only and are not synced to your other devices. The short-lived access tokens are held only in the app's memory. The events themselves are also held only in memory and are not written to disk. When a recording starts during an event, the app stores that event's identifier with the meeting, in the encrypted database, so that the next time the same meeting comes up Home can open this recording. It stores the identifier only, never the event's title or guests, and deleting the meeting deletes it.

How it is used. Calendar data is used to show your next meeting, link a recording to its calendar event, check the account when reconnecting and apply your workspace choices. An account's events appear in the workspaces you select, or in all workspaces if you choose *All Workspaces*. New connections default to *All Workspaces*.

When an automatic recording starts, the app matches it to an event by time and call service. It saves the recording in the event's workspace only when there is one matching event and all connected accounts holding that event point to the same single workspace. Otherwise it keeps the active workspace. A recording you start manually keeps the workspace chosen for that recording. These choices are made on your Mac.

If a reconnect returns a different account, or the app cannot confirm it is the same one, it asks you to choose workspaces again. *All Workspaces* also requires an explicit choice. Until you confirm, the new token and events remain only in memory and are not used to show meetings or choose a recording's workspace. Canceling discards them and keeps the previous connection. Connections are not merged or deleted automatically, even when their account emails match.

Calendar data is not used for advertising, not sold, not passed to any language model, including the one that runs on your Mac, and not used to train any model. Data obtained through Google Workspace APIs is not used to develop, improve, or train generalized AI or machine-learning models. Recordstead's use and transfer of information received from Google APIs adheres to the Google API Services User Data Policy, including the Limited Use requirements.

Removing a connection. *Remove from This Mac*, in the connection's menu in *Settings > Calendar*, deletes that connection's keychain item, including its workspace choices, and clears its events from memory. It does not revoke access at Google or remove other connections, including another connection to the same Google account.

Disconnect removes the same local data and also asks Google to revoke the app's access. Google's revocation can invalidate other connections to the same Google account, so the app asks you to confirm. If Google cannot be reached, the local connection is still removed and the app tells you that revocation was not confirmed. If the keychain item cannot be deleted, either removal action keeps the connection and reports the error; it does not revoke access.

Canceling or failing a sign-in discards the new tokens without asking Google to revoke them, because revocation could affect another connection to that account. You can remove the app's access in your Google Account at any time (Third-party apps with account access). The app asks you to sign in again when Google refuses a stored grant. Event identifiers already stored with your meetings stay until you delete those meetings.

For the calendar data handled locally by this integration, Recordstead is neither a controller nor a processor: the integration keeps that data between your Mac and your Google account, and you decide whether it is read at all. Information you separately choose to send to support is handled by Recordstead as a controller of support correspondence, as described in sections 6 and 7.