Legacy — Privacy Policy

Last updated: 27 April 2026

---

1. Who we are

Legacy is operated by **Legacy Vault Technologies Ltd** ("Legacy", "we", "us", "our"), a company registered in England and Wales under company number **16711135**, with its registered office at **167–169 Great Portland Street, London, England, W1W 5PF**.

We are the **data controller** for personal data you give us when using the Legacy app and the website at legacyjournalling.com.

Contact: hello@legacyjournalling.com

---

2. What Legacy is, in privacy terms

Legacy is a private memory preservation app. You record short voice or video memories. Our AI assistant ("Leo") transcribes them, extracts tags (people, places, themes, mood) and lets you search across everything you have ever recorded. Memories are private by default. You can choose to share specific memories into invite-only spaces called "Legacies" with people you select.

We have built Legacy to hold deeply personal content. That has shaped how we handle your data. We minimise what we collect, we are explicit about who we share it with, and we never sell it.

---

3. What data we collect

3.1 Data you give us directly

- **Account data** — email address, password (hashed), display name, profile photo (optional), date of birth, phone number (if you enable SMS features or 2FA).
- **Memory content** — voice recordings, video recordings, photos you attach, written titles, written notes, tags you add or edit.
- **Shared Legacy data** — names of Legacies you create, members you invite (their email addresses or phone numbers), your role within each Legacy.
- **Time Capsule data** — recordings you choose to seal until a future date, recipient details if applicable.
- **Communications** — messages you send to support, feedback you submit.

3.2 Data generated by Legacy

- **Transcripts** — written transcripts of your voice and video recordings, produced by AI (see Section 5).
- **AI tags and entities** — people, places, themes, mood/emotion tags extracted from your memories by AI.
- **Embeddings** — mathematical representations (vectors) of your transcripts that allow semantic search. These are not human-readable but are derived from your content.
- **Memory connections** — relationships between memories that Leo infers (e.g. "this memory is about the same trip as that one").
- **Photo analysis** — if you attach photos, we may extract scene/object tags, colour information, and EXIF metadata.

3.3 Data collected automatically

- **Device data** — device type, operating system version, app version, language and region settings, time zone.
- **Usage data** — features used, screens viewed, session length, crash reports, performance diagnostics.
- **Identifiers** — Apple ID for Sign in with Apple, Google ID for Sign in with Google, anonymous device identifiers, push notification tokens.
- **Subscription data** — purchase receipts, subscription status, trial status (handled via Apple StoreKit, RevenueCat and Superwall — we do **not** see your card details).

3.4 Data we do not collect

We do not collect your contacts, microphone activity outside an active recording session, your camera roll beyond photos you explicitly attach, your precise location (unless you explicitly tag a memory with one), or biometric identifiers used for identification.

---

4. Lawful bases for processing (UK GDPR)

We only process your data where we have a lawful basis to do so:

Activity	Lawful basis
Creating and operating your account	Performance of a contract (our Terms with you)
Storing and serving your memories	Performance of a contract
Transcribing recordings and extracting tags	Performance of a contract — this is the core service you are paying for
Sending invitations to a Legacy	Performance of a contract + your instruction
Push notifications (memory streaks, milestones)	Consent, which you can withdraw in app or device settings
SMS notifications	Consent, which you can withdraw in app settings
Marketing emails (if you opt in)	Consent
Service improvement, debugging, security	Legitimate interests
Preventing fraud and abuse	Legitimate interests + legal obligation
Responding to legal requests	Legal obligation

If a recording happens to contain special category data (for example, detail about your health, religion or political views), our lawful basis for processing it is **Article 9(2)(a) UK GDPR — your explicit consent**, given when you record and save the memory.

---

5. AI processing — how Leo works

This is the part we want to be plainest about, because it is unusual.

When you save a recording:

1. The audio file is encrypted and uploaded to our secure storage on **Supabase**.
2. The audio is sent to **OpenAI's Whisper API** for transcription.
3. The resulting transcript is sent to **OpenAI's GPT-4 API** to extract people, places, themes, mood and significance, and to suggest connections between memories.
4. The transcript is also sent to **OpenAI's Embeddings API** to produce a vector representation that powers semantic search.
5. All AI outputs are stored against your account on Supabase.

OpenAI and your data: Legacy uses OpenAI's API services (not ChatGPT). Under OpenAI's API terms, **OpenAI does not use API content to train its models** and retains data for a limited period

only for abuse monitoring before deletion. OpenAI processes this data on our behalf as a sub-processor (see Section 7).

You can search and filter your memories without sending new data to AI. Once a memory has been processed, day-to-day searches inside the app run against the data we already hold on Supabase.

Accuracy: AI-generated transcripts and tags can be wrong. You can edit any transcript or tag. We do not rely on AI output to make decisions that legally or significantly affect you.

---

6. Shared Legacies

When you create a Legacy and invite others:

- Memories you choose to add to that Legacy become visible to all current members of that Legacy.
- Members can see who else is in the Legacy.
- Removing a memory from a Legacy stops new viewers from seeing it but does not retract it from anyone who has already viewed or saved it.
- Deleting a Legacy entirely requires unanimous consent from all members.
- If you leave a Legacy, your memories that you previously contributed remain in the Legacy unless you remove them before leaving.

Be intentional about what you share. Once a memory is in a Legacy, the people in that Legacy have effectively seen it.

---

7. Sub-processors and third parties

We use the following service providers ("sub-processors") to deliver Legacy. Each is bound by a data processing agreement and processes your data only on our instructions.

Sub-processor	Purpose	Location
Supabase Inc.	Database, file storage, authentication, real-time updates	United States (East)
OpenAI, L.L.C.	Whisper transcription, GPT-4 analysis, embeddings	United States
Apple Inc.	App distribution, Sign in with Apple, push notifications (APNs), in-app purchase / subscriptions	Ireland / United States
Google LLC	Sign in with Google (optional)	United States
RevenueCat, Inc.	Subscription management and entitlement checks	United States
Superwall, Inc.	Paywall delivery and A/B testing	United States
Stripe, Inc.	Payment processing (web, where applicable)	Ireland / United States
Twilio Inc.	SMS delivery for invitations, notifications and 2FA	Ireland / United States
Vercel Inc.	Web app hosting	United States (with global edge caching)

We do **not sell** your personal data to anyone, ever.

---

8. International transfers

Your personal data, including your memories and transcripts, is stored in the **United States** on Supabase infrastructure, and is processed in the United States by OpenAI for transcription, analysis and embedding generation.

Where we transfer your personal data outside the UK, we rely on:

- the **UK International Data Transfer Agreement (IDTA)** or **UK Addendum to the EU Standard Contractual Clauses**, signed with each relevant sub-processor; and
- additional safeguards including encryption in transit (TLS) and at rest (AES-256), row-level security, and contractual restrictions on use.

You can request a copy of the relevant safeguards by emailing hello@legacyjournalling.com.

---

9. How long we keep your data

Data	Retention
Your memories and account	While your account is active, plus up to 30 days after you delete it (to allow recovery)
Anonymised analytics	Up to 24 months
Subscription / payment receipts	7 years (UK tax law)
Support correspondence	3 years from last contact
Backups	Up to 30 days after deletion

When you delete your account, we **permanently delete** your memories, transcripts, photos, embeddings and AI-generated metadata from our systems within 30 days. Backups are overwritten on rolling cycles within the same window.

If you have contributed memories to a shared Legacy, those memories remain in that Legacy (because other members rely on them) unless you remove them before deleting your account, or unless the Legacy is itself deleted.

---

10. Your rights under UK GDPR

You have the right to:

- **Access** — request a copy of your personal data.
- **Rectification** — correct inaccurate data.
- **Erasure** — ask us to delete your data ("right to be forgotten").
- **Restriction** — ask us to pause processing in certain circumstances.
- **Portability** — receive your data in a structured, machine-readable format.
- **Object** — object to processing based on legitimate interests, including direct marketing.
- **Withdraw consent** — at any time, where consent is the lawful basis.
- **Not be subject to automated decision-making** that produces legal or similarly significant effects (we do not do this).

To exercise any right, email hello@legacyjournalling.com. We will respond within one calendar month.

You also have the right to complain to the **Information Commissioner's Office (ICO)** at ico.org.uk or 0303 123 1113. We would prefer to resolve any concerns directly first, but you do not

need our permission to go to the ICO.

---

11. Security

We protect your data with:

- TLS encryption in transit
- AES-256 encryption at rest (Supabase managed)
- Row-level security policies that prevent users from accessing each other's data
- Hashed passwords (we cannot see your password)
- Restricted internal access on a need-to-know basis
- Regular review of access logs and dependencies

No system is perfectly secure. If we ever experience a personal data breach that is likely to result in a risk to your rights and freedoms, we will notify the ICO within 72 hours and you without undue delay.

---

12. Children

Legacy is not intended for children under **16**. We do not knowingly collect personal data from children under that age. If you believe a child has created an account, contact hello@legacyjournalling.com and we will delete it.

---

13. Cookies and tracking (website only)

The Legacy app itself does not use cookies. The marketing website at legacyjournalling.com may use:

- **Strictly necessary cookies** — for site function.
- **Analytics cookies** — only if you accept them (e.g. Google Analytics or similar).

You can manage cookie preferences through the cookie banner on the website.

---

14. Changes to this policy

We may update this policy. If we make a material change, we will notify you in the app and by email at least 14 days before the change takes effect. The "Last updated" date at the top of this page always reflects the current version.

---

15. Contact

Questions, requests or complaints about your data:

Legacy Vault Technologies Ltd 167–169 Great Portland Street London, England, W1W 5PF
hello@legacyjournalling.com