Privacy Policy — *MyMemoir AI*

Effective date: *August 25, 2025*
Contact: *jql61122@gmail.com*

Summary

- We collect microphone **audio** that you choose to record, and we generate **transcripts** and **AI-authored text** for you.
- Processing happens through our server on **AWS Lambda** and the **OpenAI API**.
- We don't use your data for ads or tracking.
- We keep data **only as long as needed** to provide the feature and maintain security; by default we do **not** persist transcripts on our servers.
- You can request deletion or ask questions anytime at *jql61122@gmail.com*.

---

1) What this policy covers

This policy explains what we collect, why we collect it, how we use it, who we share it with, and your choices.

---

2) Data we collect

2.1 Data you provide

- **Audio recordings.** When you tap record, the App captures microphone audio to transcribe and generate summaries/memoir text.
- **Text you type or paste.** Prompts, edits, and any notes you enter.

Sensitive content: You might include sensitive information in audio or text (e.g., health, race, sexual orientation). We don't ask for this, but if you include it, it's processed to fulfill your request.

2.2 Device & app info (minimal)

- A **random app user/device ID** (e.g., a UUID) used only for rate-limiting, abuse prevention, and debugging.
- **Diagnostics** (e.g., time, HTTP status code, endpoint URL, and a short error body) when a request fails, to help us fix issues.
- **Basic device information** that iOS provides with network calls (OS version, model) and **crash reports** if you enable them with Apple.

We do **not** collect precise location, contact list, advertising identifiers, or behavioral analytics.

---

3) How we use your data

- **App functionality.** Transcribe audio, generate summaries, extra questions, and long-form memoir drafts.
- **Quality & reliability.** Troubleshoot errors, prevent spam/abuse, and maintain service availability.
- **Support.** Respond to your requests if you contact us.

We do **not** sell your data or use it for cross-app tracking or targeted advertising.

---

4) Where processing happens (our providers)

We act as the **controller** of your data for the App. We use the following **processors** solely to provide the features:

- **Amazon Web Services (AWS)** — We run a small proxy on **AWS Lambda** (and API Gateway / Function URL) to add authentication and forward your requests. Temporary server logs (e.g., error details) are stored in **CloudWatch** with limited retention (see §7).
- **OpenAI** — We send your transcript and prompts to the **OpenAI API** to generate summaries and memoir text. OpenAI acts as our processor for this purpose.

We don’t allow our processors to use your data for advertising or independent purposes.

---

5) Storage & retention

- **On your device.** Your recordings, transcripts, and generated text may be stored locally in the app’s storage (and, if you enable it, in device backups like iCloud).
- **On our servers.** By default we **do not persist** transcripts or generated content on our servers beyond what’s necessary to process the request and maintain security.
- **Logs.** We keep limited operational logs (e.g., timestamp, status code, truncated error text) for up to **14 days** to detect abuse and debug issues, after which they are deleted or anonymized.

If you contact support and share information, we keep that communication as long as necessary to address your inquiry.

---

6) Security

We use **HTTPS/TLS** for data in transit. AWS encrypts environment variables at rest. Access to systems is limited to personnel who need it for operations. No method of transmission or storage is 100% secure, but we apply reasonable safeguards appropriate to the App's scope.

---

7) Your choices & rights

- **Permissions.** You can grant/deny microphone and speech recognition permissions in iOS Settings at any time.
- **Export & deletion.** You can delete recordings and generated text on your device. You may also request that we delete any server-side data associated with your support interactions or diagnostic logs (subject to legal/operational obligations).
- **Opt-out of diagnostics.** If you prefer not to send error details, do not submit diagnostics to us and contact support for assistance.

GDPR/UK & other regions

If you are in the EEA/UK, our legal bases include **contract** (to provide the service you request) and **legitimate interests** (fraud/abuse prevention, debugging). You may have rights to access, correct, delete, or port your data, and to object or restrict certain processing. Contact us at *jql61122@gmail.com* to exercise rights; we may ask for information to verify your request.

California (CPRA)

We **do not sell or share** personal information as defined by CPRA. You may request access/deletion and to limit use of sensitive personal information (we don't use it for purposes beyond the App's functionality).

---

8) Children

The App is not directed to children under **13** (or the minimum age in your jurisdiction). We don’t knowingly collect personal data from children. If you believe a child provided data, contact us to delete it.

---

9) International transfers

We may process data in the **United States** or other countries where our providers operate. Where required, we rely on appropriate safeguards (e.g., Standard Contractual Clauses).

---

10) Third-party content & links

If you export, share, or use content with third-party apps, those apps’ terms and privacy policies apply. We’re not responsible for third-party practices.

---

11) Changes to this policy

We may update this policy to reflect changes to the App or law. We’ll post the new version with an updated **Effective date**. Material changes will be highlighted in-app or via other reasonable notice.