Ava — Privacy Policy

Operated by beacon2

Effective Date: May 8, 2026

This Privacy Policy describes how beacon2 ("we," "us," or "our") collects, uses, stores, and protects your personal information when you use the Ava mobile application ("the App") and our marketing website at avajournal.app ("the Site"). By using the App or the Site, you agree to the practices described in this policy.

1. INFORMATION WE COLLECT

1.1 Information You Provide

- **Account information:** When you sign up via Apple Sign-In or Google Sign-In, we receive your email address (or Apple's private relay email) and, on first Apple sign-in only, your name. We do not receive or store your SSO password.
- **Display name:** A preferred name you enter during onboarding (e.g., "Kev"). This is encrypted at rest using per-user encryption keys.
- **Voice recordings:** Audio files (up to 2 minutes each) that you record within the App. These are stored encrypted on our servers.
- **Transcripts:** Text generated from your voice recordings using on-device speech-to-text (Apple Speech Framework). Transcripts are encrypted at rest using per-user encryption keys.
- **Mood selections:** Your mood check-in choices (Happy, Sad, or Mixed).
- **Preferences:** Settings such as Face ID preference, notification opt-in, and preferred notification time.

1.2 Information Generated by the App

- **AI-generated summaries:** Natural-language summaries of your voice entries, generated by AI from your transcripts. Encrypted at rest with an additional per-user layer of protection.
- **Sentiment classifications:** Automated mood/sentiment labels derived from your transcripts by AI processing. Stored in cleartext to support future trend features.

1.3 Information Collected Automatically

- **Analytics events:** We collect anonymous usage events such as screen views, feature engagement (e.g., toggling a setting), and session data. Each event includes basic technical metadata like app version and iOS version. These events are **not linked to your identity** and never include journal content, mood data tied to your identity, voice recordings, transcripts, or audio metadata. An anonymous account identifier (a random ID with no connection to your name or email) is used solely to measure retention and distinguish unique users — it cannot be used to identify you personally.
- **Error and crash reports:** We collect crash and error reports from the App and our server functions to help us fix bugs. These may include device type, OS version, and error details. An anonymous account identifier may be attached to group related errors, but no journal content, mood data, transcripts, audio, or personally identifiable information is ever included. We strip any identifying details before reports leave your device.

- **Notification token:** If you opt in to notifications, we receive a token from Apple's notification service so we can send you reminders and processing updates.

1.4 Information We Do NOT Collect (in the App)

The Ava iOS App does not collect:

- Location data
- Contacts or address book
- Photos, camera, or microphone access beyond voice recording within the App
- Health or fitness data from HealthKit or similar frameworks
- Advertising identifiers (IDFA)
- Browsing history

For information collected on our marketing website, see Section 1.5 below.

1.5 Information Collected on Our Marketing Site (avajournal.app)

Separate from the App, our marketing website uses two third-party tools to measure how visitors find and use the site. **These tools only operate on our marketing website. They are not present in the iOS App.**

- **Google Analytics 4 (GA4):** Collects IP-anonymized usage data including pages visited, referring URL, approximate (city-level) location, browser/device type, and a randomly generated client identifier stored in cookies (`_ga`, `_gid`). GA4 helps us understand which marketing channels bring visitors to the Site. IP anonymization is enabled.
- **Meta Pixel:** Collects page views and waitlist sign-up events ("Lead" events) and transmits this data to Meta Platforms, Inc. (Facebook/Instagram) for advertising measurement and audience matching. Meta Pixel sets cookies (`_fbp`, `_fbc`) and may match your visit to your Meta account if you are signed in. This enables us to measure the effectiveness of paid Meta advertising and to build similar-audience targeting for future campaigns.

Your choices on the marketing site:

- **Browser-level controls:** You can block these trackers via browser settings, an ad blocker (e.g., uBlock Origin), or built-in anti-tracking features (Safari Intelligent Tracking Prevention, Firefox Enhanced Tracking Protection).
- **Google Analytics opt-out:** Install Google's official opt-out browser add-on at https://tools.google.com/dlpage/gaoptout.
- **Meta opt-out:** Adjust your Meta ad preferences at https://www.facebook.com/ads/preferences. iOS users can also enable "Ask App Not to Track" via Settings > Privacy & Security > Tracking.
- **Clear cookies:** Clearing your browser cookies removes all marketing-site identifiers; you will appear as a new visitor on subsequent visits.

The waitlist email address you submit on the Site is stored in our database (Supabase) and used solely to notify you about Ava's launch. We do not sell or share waitlist email addresses with third parties.

2. HOW WE USE YOUR INFORMATION

We use your information solely to provide, maintain, and improve the App:

Purpose	Details
Provide the journaling service	Store and display your entries, play back recordings, show summaries
Generate AI summaries	Send your transcript (not your audio) to our AI provider for summarization and sentiment analysis
Authenticate your identity	Verify your account via Apple or Google Sign-In and keep you signed in
Send notifications	Deliver daily reminder nudges and processing-complete alerts
Improve the App	Analyze anonymous usage patterns and fix bugs
Enforce rate limits	Track your daily entry count (5 per day) to manage service costs
Comply with legal obligations	Respond to valid legal requests; enforce our Terms of Service

For the specific service providers we work with — and exactly what data we share with each — see Section 3.

We do NOT use your data for: advertising, selling to third parties, training AI models, profiling for purposes unrelated to the App, or any purpose beyond providing the App's services to you.

3. HOW WE SHARE YOUR INFORMATION

We do not sell your personal information. We share data only with the following service providers, solely to operate the App:

Provider	Purpose	Data Shared
Supabase	Backend infrastructure	Account data, encrypted entries, encrypted transcripts and summaries, audio files (encrypted at rest)
Anthropic	AI summarization	Transcript text only (not audio, not your name or email). Not used to train AI models.
Apple	Sign-In, notifications, on-device transcription	SSO credentials (to Apple only), notification token, audio (on-device only — never sent to Apple's servers)
Google	Authentication	SSO credentials (to Google only)
PostHog (US Cloud)	Analytics	Anonymous usage events and an anonymous account identifier. No journal content, no identity-linked mood data, no audio metadata, no name or email.

Provider	Purpose	Data Shared
Sentry (US)	Error tracking	Crash and error reports, device metadata, and an anonymous account identifier. No journal content, no name or email.

We may also disclose information if required by law, subpoena, or other legal process, or if we believe disclosure is necessary to protect our rights, your safety, or the safety of others.

4. DATA STORAGE AND SECURITY

4.1 Where Your Data Is Stored

Your data is stored on managed cloud infrastructure located in the United States. Analytics data and error reports are also processed in the United States. See Section 3 for the specific service providers we work with.

4.2 How Your Data Is Protected

- **Encryption everywhere:** Your data is encrypted both when stored on our servers and when it moves between your device and our servers.
- **Extra protection for sensitive content:** Your transcripts, AI summaries, and display name receive an additional layer of per-user encryption — so even within our own systems, this content cannot be read without your account's key.
- **Account isolation:** You can only see your own data. Our backend is configured so that no user can access another user's content, even by mistake.
- **Session security:** Your sign-in session is stored securely on your device and is not backed up to iCloud.
- **Face ID (optional):** If you enable Face ID, biometric verification happens entirely on your device using Apple's Secure Enclave. No biometric data is ever sent to us or to any third party.
- **No personal content in analytics:** Analytics events and error reports are designed not to include journal content, voice recordings, transcripts, or anything that could identify you. We also strip identifying details before any error report leaves your device.

No security system is impenetrable. While we implement industry-standard protections, we cannot guarantee absolute security of your data.

5. DATA RETENTION

Data Type	Retention Period
Journal entries, transcripts, summaries	Retained until you delete the entry or your account
Voice recordings (audio files)	Retained until you delete the entry or your account
User profile and preferences	Retained until you delete your account
Analytics events	Retained per our analytics provider's policy (anonymized, not linked to identity)

Data Type	Retention Period
Error reports	Retained per our error tracking provider's policy (typically 90 days)
Anonymized deletion log	Retained indefinitely. Contains no personally identifiable information — only an anonymous identifier (which cannot be traced back to you), a timestamp, and whether the account had entries.

6. YOUR RIGHTS AND CHOICES

6.1 Access and Deletion

- **View your data:** All your journal entries, recordings, and summaries are accessible within the App at any time.
- **Delete individual entries:** You can permanently delete any entry (including its transcript, summary, and audio recording) from within the App. Deletion is immediate and irreversible.
- **Delete your account:** You can permanently delete your entire account and all associated data via Settings > Delete Account. This erases all entries, audio files, your profile, and your authentication credentials from our servers. Account deletion requires re-authentication for security. See Section 11 of our Terms of Service for details.

6.2 Analytics and Error Reporting

The App collects anonymous analytics and error reports as described in Section 1.3 to help us improve the App and fix bugs. This data is not linked to your identity and never includes journal content, mood data, transcripts, or audio. When you delete your account, your anonymous identifier is disassociated from all analytics and error data.

6.3 Notifications

You can enable or disable daily reminder notifications in the App's Settings or through your device's iOS notification settings.

6.4 Face ID

You can enable or disable the Face ID privacy gate at any time in the App's Settings. Disabling Face ID does not affect your data or account security — it only removes the on-device biometric check when opening the App.

7. CHILDREN'S PRIVACY

Ava is not directed at children under 13 years of age. We do not knowingly collect personal information from children under 13. If you are a parent or guardian and believe your child under 13 has provided personal information to us, please contact us at privacy@avajournal.app and we will promptly delete that information.

If you are between 13 and 18 years of age, you should review this Privacy Policy with your parent or legal guardian before using the App.

8. CALIFORNIA PRIVACY RIGHTS

If you are a California resident, you have additional rights under the California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA):

- **Right to know:** You may request information about the categories and specific pieces of personal information we have collected about you.
- **Right to delete:** You may request deletion of your personal information. The in-app account deletion feature (Settings > Delete Account) fulfills this right immediately for App data.
- **Right to correct:** You may request that we correct inaccurate personal information we hold about you.
- **Right to opt out of sale:** We do not sell your personal information to third parties for monetary or other valuable consideration.
- **Right to opt out of sharing for cross-context behavioral advertising:** Our marketing website (avajournal.app) uses Meta Pixel, which transmits Site activity to Meta for advertising measurement and audience matching as described in Section 1.5. Under the CPRA, this data flow may qualify as "sharing" for cross-context behavioral advertising. **To opt out:** (1) use the browser-level controls, Google Analytics opt-out, or Meta opt-out described in Section 1.5, or (2) email us at privacy@avajournal.app and we will honor your opt-out request. The iOS App itself does not engage in cross-context behavioral advertising.
- **Right to non-discrimination:** We will not discriminate against you for exercising your privacy rights.

To exercise any of these rights, contact us at privacy@avajournal.app. We will respond to verifiable requests within 45 days.

9. APP STORE PRIVACY LABEL

In accordance with Apple's App Store requirements, here is a summary of our data practices as they relate to the App Store privacy nutrition label:

Data Type	Purpose	Linked to Identity	Used for Tracking
Contact Info (email)	App Functionality	Yes (linked to account)	No
User Content (audio, transcripts)	App Functionality	Yes (linked to account)	No
User Content (mood selections)	App Functionality	Yes (linked to account)	No
Identifiers (user ID)	App Functionality, Analytics	Yes (linked to account)	No
Usage Data (analytics events)	Analytics	No (not linked to identity)	No
Diagnostics (crash reports)	App Functionality	No (not linked to identity)	No

10. ON-DEVICE PROCESSING

To protect your privacy, the following processing happens entirely on your device and never involves sending data to external servers:

- **Speech-to-text transcription:** Your voice recordings are transcribed using Apple's Speech Framework, which runs entirely on-device. Audio data for transcription is never transmitted to Apple's servers or any third party.
- **Face ID authentication:** Biometric verification is performed by the iOS Secure Enclave. No biometric data leaves your device.
- **Local data caching:** Recent entries are cached on-device for performance. The cloud remains the source of truth.

11. INTERNATIONAL DATA TRANSFERS

Our backend infrastructure is hosted in the United States. If you access the App from outside the United States, your data will be transferred to and processed in the United States. By using the App, you consent to this transfer. Our analytics and error tracking providers also process data in the United States.

12. CHANGES TO THIS PRIVACY POLICY

We may update this Privacy Policy from time to time. If we make material changes, we will notify you through the App or by other reasonable means before the changes take effect. Your continued use of the App after changes are posted constitutes acceptance of the revised policy.

The effective date at the top of this document indicates when the current version took effect.

13. CONTACT US

If you have any questions, concerns, or requests regarding this Privacy Policy or our data practices, please contact us at:

Email: privacy@avajournal.app

App Store Listing: Available on the Apple App Store

We aim to respond to all inquiries within 30 days.