Ava — Privacy Policy

Operated by beacon2

Effective Date: April 7, 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"). By using the App, 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 Anthropic's Claude API. Encrypted at rest using per-user encryption keys.
- **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 use PostHog (US Cloud) to collect anonymous usage events such as screen views, feature engagement (e.g., toggling a setting), and session data. Each event includes basic technical metadata: app version, build number, 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 opaque account identifier (a random UUID 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 use Sentry to collect crash reports, error logs, and diagnostic data from the App and our server functions. These may include device type, OS version, error class names, and stack traces. An opaque 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 actively scrub any identifying patterns (such as file paths containing account identifiers) before reports

leave your device.

- **Device token:** If you opt in to notifications, we receive your Apple Push Notification Service (APNs) device token to send you reminders and processing updates.

1.4 Information We Do 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

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 transcript text (not audio) to Anthropic's Claude API for summarization and sentiment analysis
Authenticate your identity	Verify your account via Apple or Google Sign-In; issue and manage session tokens
Send notifications	Deliver daily reminder nudges and processing-complete alerts via APNs
Improve the App	Analyze anonymous usage patterns (via PostHog) and fix bugs (via Sentry)
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

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 on S3)

Provider	Purpose	Data Shared
Anthropic (Claude API)	AI summarization	Transcript text only (not audio, not your name or email). Processed per Anthropic's data processing terms. Not used for model training.
Apple (Sign-In, APNs, Speech)	Auth, notifications, transcription	SSO credentials (to Apple only), device token (for push), audio (on-device only for speech-to-text — never sent to Apple's servers)
Google (Sign-In)	Authentication	SSO credentials (to Google only)
PostHog (US Cloud)	Analytics	Anonymous usage events and an opaque account identifier. No journal content, no identity-linked mood data, no audio metadata, no name or email.
Sentry (US)	Error tracking	Crash reports, stack traces, device metadata, and an opaque 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 Supabase's managed infrastructure, which uses AWS for database hosting and S3 for audio file storage. Our Supabase project is hosted in the US East region. Analytics data is processed by PostHog on US Cloud servers. Error reports are processed by Sentry on US servers.

4.2 How Your Data Is Protected

- **Encryption at rest:** All stored data is encrypted using AES-256. Audio files are encrypted via S3 server-side encryption (SSE).
- **Per-user encryption:** Sensitive fields (your display name, transcripts, and AI summaries) are additionally encrypted using per-user symmetric keys via PostgreSQL's pgcrypto extension. Each user's key is itself encrypted with a server master key stored securely outside the database.
- **Encryption in transit:** All network communication uses TLS. Audio uploads use time-limited presigned URLs for direct-to-storage transfer.
- **Row-level security (RLS):** Database policies ensure that every query is scoped to the authenticated user. No user can access another user's data, even through direct database queries.
- **Access tokens:** Your access token (JWT) is held in memory only and never written to disk. Your refresh token is stored in the iOS Keychain with "after first unlock" protection and is not synced to iCloud.
- **Face ID (optional):** If enabled, Face ID acts as an on-device privacy gate using the Secure Enclave. No biometric data is ever transmitted to our servers or any third party.
- **Analytics privacy safeguards:** Before error reports are transmitted, we automatically strip any email addresses, usernames, or display names from the data, and redact file paths that could contain account identifiers. Analytics events are designed to capture only the action taken (e.g., "recorded a voice note"), never the content of the action.

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 (PostHog)	Retained per PostHog's US Cloud data retention policy (anonymized, not linked to identity)
Error reports (Sentry)	Retained per Sentry's standard retention policy (typically 90 days)
Anonymized deletion log	Retained indefinitely. Contains no personally identifiable information — only a one-way hashed identifier, 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. Error reporting (Sentry) captures crash and error data to ensure app stability. When you delete your account, your opaque 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 ava-feedback@beacon2.com 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):

- **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.
- **Right to opt out of sale:** We do not sell your personal information to third parties.
- **Right to non-discrimination:** We will not discriminate against you for exercising your privacy rights.

To exercise any of these rights, contact us at ava-feedback@beacon2.com. 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 (Supabase) is hosted in the United States (US East region). 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 provider (PostHog) and error tracking provider (Sentry) both process data on US servers.

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: ava-feedback@beacon2.com

App Store Listing: Available on the Apple App Store

We aim to respond to all inquiries within 30 days.