

Privacy Policy

This Privacy Policy describes how **Kalmora** ("Kalmora," "we," "our," or "us") collects, uses, and shares information when you use our iOS 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

- **Mood check-ins:** the emotion you select (e.g., anxious, sad, happy) and any optional follow-up text.
- **Chat content:** messages you send and intensity ratings (1–10) you submit during AI-guided sessions.
- **Exercise activity:** which breathing or grounding exercise you start and whether you complete it.
- **Notification preferences:** whether you opt in to morning, evening, or follow-up reminders, and the times you choose.
- **Subscription state:** whether you have an active paid subscription, managed via Apple's In-App Purchase system and our payments provider.

1.2 Information collected automatically

- **Device and usage data:** app version, iOS version, device model, language, time zone, crash logs, and aggregate usage events (screens opened, exercises started/completed, sessions started/ended).
- **Device and app identifiers:** anonymous identifiers that distinguish your device and your installation of the App, and the IP address your requests come from. We do *not* collect Apple's Advertising Identifier (IDFA) — we do not show ads, run attribution, or track you across other apps or websites.
- **Service request logs:** when the App contacts our servers (for AI-guided chat, sleep stories, and similar features), we keep a short log of the request — the identifiers above, app version, and timing — to run the service, prevent abuse, and apply fair-use limits. These logs do not contain your message content.

1.3 Information we do *not* collect

- We do not require an email address, phone number, or real name.

- We do not access your contacts, photos, microphone, or location.
- We do not collect health data from Apple Health.

2. How we use information

- To deliver core features: track exercise sessions, persist mood check-ins, generate AI chat responses, and schedule reminder notifications you've enabled.
- To improve product quality: identify crashes, measure feature adoption, and fix bugs.
- To manage your subscription: confirm entitlement, restore purchases, and prevent fraud.
- To comply with legal obligations.

We do **not** sell your personal information, and we do **not** use your data for cross-context behavioral advertising.

3. Service providers

We share limited information with the third parties below, only as necessary to operate the App. Each provider is contractually limited to using data on our behalf.

Provider	Purpose	Data shared
Google Firebase (Analytics, Crashlytics, Installations) — Google LLC	Aggregate usage analytics and crash diagnostics	Pseudonymous app instance ID, event names & parameters, device info, crash stack traces
RevenueCat, Inc.	Subscription management and entitlement verification	App User ID, purchase receipts, subscription state
Apple — App Store / In-App Purchase	Payment processing and TestFlight distribution	Apple-managed transaction data; we do not see your payment method
Supabase, Inc.	Hosting our servers, processing requests from the App, and storing the service logs and safety records described in Section 4	Anonymous device and app identifiers, IP address, app version; and, for safety records only, message content
OpenAI, L.L.C.	Generating responses during AI-guided chat sessions	Selected emotion, intensity, and the message content of the active conversation

4. Data retention

- **On-device data** (sessions, check-ins, generated sleep stories, preferences) is stored locally on your device and is removed when you delete the App.
- **Service request logs** (identifiers, app version, and timing — no message content) are retained for operational and abuse-prevention purposes.
- **Safety records:** if a message triggers our automated safety or abuse filters, or if you choose to report a conversation to us, the relevant message content is stored on our backend so we can review it, keep users safe, and improve the App's safeguards. Ordinary conversations that do not trigger these filters are not retained on our backend once the AI response has been generated.
- **Analytics events** are retained by Firebase for the period configured in our Firebase Analytics settings (default: 14 months for event-level data).
- **Crash reports** are retained by Firebase Crashlytics per Google's standard retention.
- **Subscription records** are retained as required for billing, tax, and audit purposes.

5. Your rights

Depending on your jurisdiction (including the EU/EEA, UK, California, and other regions with data-protection laws), you may have the right to:

- Access, correct, or delete the information we hold about you.
- Object to or restrict certain processing.
- Receive a portable copy of your data.
- Withdraw consent where we rely on consent.
- Lodge a complaint with your local data-protection authority.

To delete the data stored on your device, delete the App. To request deletion of backend records (such as safety records or request logs), or to exercise any of the rights above, contact us at support@kalmora.app. Because we do not maintain accounts tied to identifying information, we may need additional details to locate any data associated with your device.

6. International data transfers

Our service providers (Firebase, RevenueCat, Apple, Supabase, OpenAI) operate globally. Your information may be processed and stored in the United States and other countries. Where required, we rely on transfer mechanisms such as the EU Standard Contractual Clauses or equivalent safeguards.

7. Children's privacy

Kalmora is not directed to children under 13 (or the equivalent minimum age in your jurisdiction). We do not knowingly collect personal information from children. If you believe a child has used the App, please contact us so we can remove their data.

8. Security

We use industry-standard encryption for data in transit. Data stored on your device — including session history and check-ins — is protected by your device's built-in encryption. Firebase, RevenueCat, Supabase, and Apple maintain their own enterprise-grade security controls. No system is perfectly secure; we will notify users in the event of a breach affecting their data, as required by law.

9. Not a medical service

Kalmora is a wellness application. It is not a medical device, not a substitute for professional mental-health care, and it does not diagnose, treat, or prevent any condition. If you are in crisis, please contact your local emergency services or a crisis hotline immediately. See the in-app "Crisis resources" section for region-specific numbers.

10. Changes to this Policy

We may update this Policy from time to time. The current version will always be available at the URL where this Policy is published. Material changes will be highlighted in the App.

This document is provided as a baseline and should be reviewed by qualified legal counsel for your jurisdiction before publication.