with:in

Privacy Policy

Last updated: April 19, 2026

SECTION 01

Who we are

with:in is a personal journaling and wellbeing app available on iOS and Android. This privacy policy explains how we collect, use, protect, and share your information when you use our app and services.

Data controller contact: hi@wi-th-in.com

SECTION 02

What we collect

2.1 Account information

When you create an account, we collect:

- Email address — for authentication and account recovery
- Display name — shown within the app
- Full name (optional) — if you choose to provide it
- About me (optional) — a short personal description

All of these fields are encrypted at rest using AES-256-GCM with keys managed by Google Cloud KMS (see Section 6).

2.2 Journal entries

When you write a reflection, we store:

- The text you write (encrypted at rest)
- The prompt that inspired the entry (title and question)
- Timestamps (created, last edited)

2.3 Preferences and settings

We store your selected wellbeing categories (e.g. self, emotions, connection, purpose, body), language preference, tone preference (e.g. poetic, practical), and notification settings. These are stored as plaintext configuration values and do not contain personally identifiable information.

2.4 Generated content

Based on your journal entries, we generate weekly insights (a summary of patterns from your recent entries) and progress updates (per-category reflections on recurring themes). These are encrypted at rest using the same encryption as your journal entries.

2.5 Prompt feedback

When you indicate whether a daily prompt resonated with you (thumbs up/down), we store that preference to improve future prompts.

2.6 Local data on your device

Your device stores minimal data:

- Journal drafts — saved locally so you don't lose work if the app closes. Drafts are deleted once submitted.
- Firebase SDK cache — managed by the SDK, not by our app code.
- Auth tokens — Firebase authentication tokens stored securely on-device for session management.

No offline database is used. If you are offline, the app displays an offline state and entries cannot be saved until connectivity is restored.

2.7 Analytics

We use Firebase Analytics to collect basic, anonymised usage metrics such as screen views and feature usage. We do not use any other analytics, advertising, or tracking services. We do not track you across apps or websites.

2.8 What we do not collect

- IP addresses (not stored by our backend)
- Location data
- Contacts, photos, or media
- Device identifiers for advertising
- Health or fitness data
- Biometric data
- Browsing history

SECTION 03

How we use your information

PURPOSE	DATA USED
Provide the journaling experience	Journal entries, prompts, preferences
Generate weekly insights	Journal entry text, profile preferences
Generate progress updates	Journal entry text, selected categories

PURPOSE	DATA USED
Personalise daily prompts	Selected categories, tone preference, language, past prompt history
Improve prompt quality	Aggregated, anonymised prompt feedback
Authenticate your account	Email, Firebase Auth tokens
Customer support	Email, display name (authorised support staff only)
Monitor service health	Anonymised performance metrics (latency, error rates)

> *We never use your data for advertising, profiling, or selling to third parties.*

SECTION 04

AI processing

4.1 What gets sent to OpenAI

We use the OpenAI API to generate daily prompts, weekly insights, and progress updates. When this happens, the following is sent to OpenAI's servers:

- Journal entry text — the content of your reflections
- Profile preferences — your selected categories, language, and tone preference

The following is never sent to OpenAI: your email address, your name, or any other account identifiers.

4.2 OpenAI's data handling

As of the date of this policy, OpenAI does not use data submitted via their API to train their models. We do not use OpenAI's fine-tuning services.

4.3 Training consent

We provide an explicit, opt-in consent mechanism for any future use of your data in model training. This consent is never enabled by default — you must actively opt in — and can be revoked at any time through the app. As of this writing, no training pipeline is active.

SECTION 05

Who can access your data

5.1 You

You can access all your own data through the app: journal entries, insights, progress updates, and profile information.

5.2 Customer support staff

Authorised support staff can look up your account by email address to assist with support requests. They can see your user ID, email, display name, selected categories, and language preference.

They cannot access: your journal entries, weekly insights, progress updates, or any personal reflection content. All support lookups are logged in an audit trail.

5.3 No one else

We do not share, sell, or provide your data to any other parties, except as required by law (see Section 10).

SECTION 06

How we protect your data

6.1 Encryption at rest

All personal and sensitive data is encrypted at rest using AES-256-GCM with envelope encryption managed by Google Cloud KMS:

- A unique 256-bit data encryption key (DEK) is generated per document
- Each field is encrypted with a unique nonce
- The DEK is wrapped by a KMS-managed key encryption key (KEK) before storage
- Email addresses use a separate KEK from other personal data
- Email addresses are also hashed (SHA-256) for lookup purposes

6.2 Encryption in transit

All communication between the app and our servers uses HTTPS/TLS. Firebase Cloud Functions enforce TLS for all requests.

6.3 Authentication and authorisation

- All API requests require a valid Firebase Authentication token
- Every request verifies that the token's user ID matches the requested data
- Role-based access control restricts administrative and support functions
- All writes go through server-side Cloud Functions — the app cannot write directly to the database

6.4 Infrastructure

Data is stored in Google Cloud Firestore in the Europe (europe-west1) region. Encryption keys are managed in Google Cloud KMS in the same region. No data is replicated outside the European region by our application.

SECTION 07

How long we keep your data

DATA TYPE	RETENTION
Account and profile	Until you delete your account
Journal entries	Until you delete the entry or your account
Weekly insights	Until you delete your account
Progress updates	Until you delete your account
Prompt feedback	Until you delete your account
Daily prompts	Until you delete your account
System event logs	Indefinite, but anonymised on account deletion
Local drafts	Automatically cleaned up daily; deleted on submission

SECTION 08

Your rights

Depending on your jurisdiction, you may have some or all of the following rights:

8.1 Right to access

You can view all your personal data through the app at any time.

8.2 Right to rectification

You can edit your profile information and journal entries at any time through the app.

8.3 Right to erasure (right to be forgotten)

You can request complete deletion of your account and all associated data, including all journal entries, insights, progress updates, your user profile, daily prompts, and prompt feedback. System event logs are anonymised.

> *This deletion is irreversible. There is no recovery period.*

8.4 Right to data portability

Contact us at hi@wi-th-in.com to request an export of your data in a machine-readable format.

8.5 Right to restrict processing

You can stop using the app at any time. Your data remains encrypted at rest until you choose to delete your account.

8.6 Right to object

You can object to any processing by contacting us at hi@wi-th-in.com. You can revoke training consent at any time through the app.

8.7 Right to withdraw consent

Where processing is based on consent (such as the optional training consent), you can withdraw consent at any time without affecting the lawfulness of prior processing.

SECTION 09

Device permissions

iOS

The app requests no device permissions. It requires only network access and uses Firebase Authentication for sign-in.

Android

PERMISSION	PURPOSE
INTERNET	Network access for Firebase and API calls
POST_NOTIFICATIONS	Show push notification reminders (runtime prompt on Android 13+)
SCHEDULE_EXACT_ALARM	Schedule daily reminders at the time you choose
RECEIVE_BOOT_COMPLETED	Re-schedule your reminders after a device restart

No permissions are requested for camera, microphone, location, contacts, storage, or any other sensitive capability.

SECTION 10

Legal basis for processing (EEA/UK)

If you are in the European Economic Area or the United Kingdom, our legal bases for processing your data are:

PROCESSING ACTIVITY	LEGAL BASIS
Providing the journaling service	Performance of a contract (Art. 6(1)(b) GDPR)
Generating insights and progress updates	Performance of a contract (Art. 6(1)(b) GDPR)
Sending prompt notifications	Your consent (Art. 6(1)(a) GDPR)
Firebase Analytics	Legitimate interest in service improvement (Art. 6(1)(f) GDPR)
Customer support lookups	Legitimate interest in providing support (Art. 6(1)(f) GDPR)
Future model training (if enabled)	Your explicit consent (Art. 6(1)(a) GDPR)
Compliance with legal obligations	Legal obligation (Art. 6(1)(c) GDPR)

SECTION 11

International data transfers

Your data is stored in Google Cloud's Europe (europe-west1) region. When journal entries are processed by the OpenAI API, that data may be transferred to OpenAI's servers, which may be located in the United States. This transfer is necessary for the performance of our service and is covered by OpenAI's data processing terms.

No personal identifiers (name, email) are included in data sent to OpenAI.

SECTION 12

Children's privacy

with:in is not directed at children under 16. We do not knowingly collect personal information from children under 16. If you believe a child under 16 has provided us with personal data, please contact us at and we will delete it.

SECTION 13

California residents (CCPA/CPRA)

If you are a California resident:

- Right to know: You can request what personal information we collect, use, and disclose (see Sections 2 and 3).
- Right to delete: You can request deletion of your data (see Section 8.3).

- Right to opt out of sale: We do not sell your personal information or share it for cross-context behavioural advertising.
- Right to non-discrimination: We will not discriminate against you for exercising your privacy rights.

SECTION 14

Sub-processors

SERVICE	PURPOSE	DATA ACCESSED
Google Cloud Firestore	Database storage	All data (encrypted at rest)
Google Cloud KMS	Encryption key management	Wrapped encryption keys only
Firebase Authentication	User authentication	Email, auth tokens
Firebase Analytics	Anonymised usage metrics	Screen views, feature usage (no PII)
OpenAI API	Content generation	Journal text, category/language/tone preferences

SECTION 15

Changes to this policy

We may update this privacy policy from time to time. When we make material changes, we will notify you through the app or by other appropriate means. The “last updated” date at the top reflects when this policy was most recently revised.

SECTION 16

Contact us

If you have questions about this privacy policy, want to exercise your rights, or need to report a concern:

Email: hi@wi-th-in.com

Data protection inquiries: hi@wi-th-in.com

If you are in the EEA and are not satisfied with our response, you have the right to lodge a complaint with your local data protection authority.