Privacy Policy — My Trek Guide

Effective date: May 9, 2026

Last updated: May 9, 2026

This Privacy Policy describes how we collects, uses, stores, and shares information when you use the My Trek Guide mobile application (the “App”) on iOS and Android.

By using the App, you agree to this Privacy Policy. If you do not agree, please do not use the App.

1. Who we are

Data controller: [Amrit Duwal]

Contact: [amritduwal1@gmail.com]

For EU/UK users: you may contact us using the details above. You also have the right to lodge a complaint with your local supervisory authority.

2. Information we collect

2.1 Account and authentication

When you create an account or sign in, we process:

- Email address and password (if you register with email).

- OAuth profile information from Google Sign-In or Sign in with Apple (such as name and email, depending on what you choose to share).

- A Firebase user identifier (UID) and authentication tokens used to keep your session secure.

Authentication is provided by Google Firebase Authentication. Google processes certain technical data as part of providing Firebase. See Google’s privacy documentation for Firebase.

2.2 Profile and app content you provide

When you use profile or related features, our backend API may store information you submit, such as:

- Name, gender, age (if provided).

- Location description and optional home coordinates (latitude/longitude), if you choose to provide them.

- Email and phone (if you enter them in your profile).

- Profile photo (if you upload one).

We also store favorites (e.g., itineraries you save) associated with your account.

2.3 Support, complaints, and in-app chat

If you submit help requests, complaints, or chat messages, we collect the content of those messages and related metadata (such as time sent), and contact details you include (e.g., email or phone), linked to your account identifier where applicable.

2.4 Location

If you grant permission, the App may access approximate or precise device location while you use map or navigation-related features (for example, to show your position on a map). You can disable location access in your device settings; some features may not work fully without it.

2.5 Camera and photos

If you grant permission, the App may access your camera or photo library so you can select or capture images for features such as identifying plants or animals. Images you analyze may be processed on your device using Google ML Kit image labeling where that feature is enabled.

2.6 Push notifications

If you opt in to notifications, we use Firebase Cloud Messaging (FCM) to deliver messages to your device. This involves a device push token and related technical data handled by Google/your platform provider (Apple/Google).

2.7 Maps and geocoding

The App may display maps using Google Maps and/or other map providers. When you interact with maps, your device may send requests (which can include map viewport or location-related parameters) to those providers under their terms and privacy policies.

The App may use geocoding services to convert between addresses and coordinates where that feature is offered.

2.8 Technical and usage data

We and our service providers may automatically collect:

- Device and app information (e.g., OS version, app version, language).

- IP address and network-related data when you call our API or third-party services.

- Diagnostics necessary to operate and secure the App (e.g., error logs where collected).

2.9 Local storage on your device

The App may store tokens, preferences, or cached data locally on your device (for example via platform storage APIs) to remember settings or improve performance.

3. How we use your information

We use the information above to:

- Provide, maintain, and improve the App (including maps, itineraries, identification tools, and support).

- Authenticate users and secure accounts.

- Sync your profile, favorites, and support conversations with our servers.

- Send push notifications you have agreed to receive.

- Respond to inquiries and enforce our Terms of Service.

- Comply with legal obligations and protect rights, safety, and security.

We do not sell your personal information as “sale” is commonly understood in US state privacy laws.

4. Legal bases (EEA/UK/Switzerland)

Where GDPR-style laws apply, we rely on:

- Contract: providing the App and features you request.

- Legitimate interests: security, fraud prevention, improving the App, and support—balanced against your rights.

- Consent: where required (e.g., certain notifications, optional analytics if added later, or non-essential cookies on a website).

- Legal obligation: where the law requires processing.

5. Sharing of information

We share information with:

- Service providers who assist us under instructions, including:

  - Google (Firebase Authentication, Firebase Cloud Messaging, and related infrastructure; ML Kit on-device libraries; Google Maps / Google Sign-In as applicable).

  - Apple (Sign in with Apple; push notification delivery on iOS).

- Hosting/infrastructure for our backend API ([YOUR_API_HOST_DOMAIN] or successor).

- Authorities or third parties if required by law or to protect rights and safety.

Third-party services have their own privacy policies. We encourage you to read Google's and Apple's privacy notices.

6. International transfers

Your information may be processed in countries other than where you live (including the United States), where privacy laws may differ. Where required, we use appropriate safeguards (such as standard contractual clauses).

7. Retention

We retain information as long as needed to provide the App and for legitimate business purposes (e.g., support records, security), unless a longer period is required by law. You may request deletion as described below; some residual copies may persist for a limited time in backups.

8. Security

We use reasonable technical and organizational measures to protect your information. No method of transmission or storage is 100% secure.

9. Your choices and rights

Depending on your location, you may have rights to:

- Access, correct, or delete certain personal data.

- Object to or restrict certain processing.

- Withdraw consent where processing is consent-based.

- Data portability.

- Opt out of certain communications (e.g., push notifications via device settings).

Account deletion: You may be able to delete your profile or account data through the App or by contacting us at **amritduwal1@gmail.com**. Deleting your Firebase authentication account may require using your device/account settings or our support process.

California residents: You may have additional rights under the CCPA/CPRA (e.g., know, delete, correct, opt out of certain sharing). Contact us at the email above.

10. Children's privacy

The App is not directed at children under 13 (or the minimum age in your jurisdiction). We do not knowingly collect personal information from children. If you believe we have, contact us and we will take appropriate steps.

11. Third-party links

The App may open websites or services operated by others. We are not responsible for their privacy practices.

12. Changes to this policy

We may update this Privacy Policy from time to time. We will post the updated version and revise the “Last updated” date. Continued use after changes means you accept the updated policy, unless applicable law requires otherwise.

13. Contact

Questions about this Privacy Policy: amritduwal1@gmail.com