Privacy Policy of the On Trail App

Effective date: March 1, 2026 **Last updated:** March 13, 2026

---

1. Data Controller

The controller of personal data processed within the **On Trail** mobile application (hereinafter: "App") is the owner of the **weiga.pl** service (hereinafter: "Controller"). For matters related to the protection of personal data, please contact us at the e-mail address provided in section 14. Contact.

---

2. Scope of Data Collected

2.1 User Account Data

During registration and use of the App, we collect:

- **Identification data:** first name or username (nick), e-mail address, profile picture (avatar), bio
- **Authentication data:** managed by Firebase Authentication (passwords are not stored by the Controller)
- **Subscription data:** information about active premium packages (SPORT, EXPLORER, HEALTH), Google Play purchase history

2.2 Location Data

The App collects location data for its core functions:

- **Real-time location (GPS):** during activities and navigation – geographic coordinates, altitude above sea level, speed, heading
- **Activity GPS track:** full route recording with timestamps and parameters (distance, elevation, pace)
- **Background location (optional):** access to location while the App runs in the background is used **exclusively** to update home screen widgets (weather, air quality); the user may revoke this permission in the device system settings
- **Real-time location sharing:** optional feature – consciously enabled by the user; visibility can be set to public (for all App users), friends only, or completely disabled

2.3 Physical Activity and Health Data

As part of outdoor activity tracking, we collect:

- Activity type (hiking, cycling, skiing)
- Training parameters: distance, time, speed, elevation gain/loss, cadence, step count
- **Health data (HEALTH package):** heart rate from BLE sensor, heart rate zones, estimated calories burned, user and backpack weight
- Ambient temperature from the device sensor
- Altitude data from barometer (SPORT package)

2.4 Photos and Multimedia

- Photos added to activities and places by the user
- Photo metadata (time, location, if available in the file)
- Photos are visible to accepted friends only by default; the user may change the visibility to public or private
- The user may enable **automatic photo publishing** – a photo is then automatically published only if no person is detected in the photo or at least 5 faces are detected (group photo)
- Detection of the presence and number of persons is performed **exclusively on the user's device** (offline) using **Google ML Kit**; the system does not identify faces or track individuals – it only counts their presence in order to protect user privacy

2.5 Social Content

- Comments and reactions added by the user
- Remarks about trail conditions
- Friends list and connections between accounts
- Search history (stored locally on the device)

2.6 AI Queries and Chat AI Conversation History

As part of the **Chat AI feature (EXPLORER package)**:

- Content of text messages and voice transcriptions sent to the Gemini 2.5 Flash model (Google)
- Conversation history stored in the Controller's database for **30 days from the last activity in the conversation**, after which it is automatically deleted
- All queries are logged in the Controller's database for diagnostic purposes and usage limit enforcement
- At the AI model's request, the following user data may be retrieved and passed to Google: place visit history, activity history, activity statistics
- Optionally: the user's current location (if shared by the user) and the list of installed map regions — passed as context to the model for personalizing responses

2.7 Technical and Device Data

- Device identifier (FCM token) for push notifications
- Diagnostic data and error logs
- Bluetooth connection data when pairing heart rate sensors (BLE)
- Operating system and app version information

---

3. Purpose and Legal Basis for Data Processing

Purpose of processing	Legal basis
Providing App services (activity tracking, navigation, map)	Performance of a contract (Art. 6(1)(b) GDPR)
Managing user account	Performance of a contract (Art. 6(1)(b) GDPR)
Social features (friends, comments, reactions)	Performance of a contract (Art. 6(1)(b) GDPR)
Subscription and payment handling	Performance of a contract and legal obligation (Art. 6(1)(b) and (c) GDPR)
Sending push notifications	Legitimate interest / consent (Art. 6(1)(a) or (f) GDPR)
Processing health data (heart rate, calories)	Explicit user consent (Art. 9(2)(a) GDPR)
Sharing location with friends	Explicit user consent (Art. 6(1)(a) GDPR)
Sharing photos with friends or publicly	Performance of a contract (Art. 6(1)(b) GDPR)
Automatic photo publishing – detecting number of persons (ML Kit, on-device)	Legitimate interest – protecting user privacy (Art. 6(1)(f) GDPR)
Chat AI – query logging and usage limit enforcement	Legitimate interest – security and usage limits (Art. 6(1)(f) GDPR)
Chat AI – storing conversation history	Performance of a contract (Art. 6(1)(b) GDPR)
Service quality improvement and analytics	Legitimate interest (Art. 6(1)(f) GDPR)
Sharing location data with rescue services (GOPR, TOPR) in search and rescue cases	Protection of vital interests of the data subject (Art. 6(1)(d) GDPR)

---

4. Data Sharing

4.1 Publicly Visible Data (by default)

Unless the user changes their privacy settings, the following are publicly visible:

- Name/nick and avatar
- Completed activities marked as public
- Photos marked as public
- Remarks and comments

4.2 Data Visible to Friends

Once a friend request is accepted, the friend may see:

- Activities marked as "friends"
- Photos marked as "friends"
- Real-time location (only if the user enables it)

4.3 Third Parties (Service Providers)

The Controller uses the following data processors:

Provider	Purpose	Privacy Policy
Google Firebase (Authentication, Firestore, Cloud Storage, Cloud Functions, Cloud Messaging)	Backend infrastructure, authentication, database, push notifications	firebase.google.com/support/privacy
Google Gemini AI	Chat AI — multi-turn travel assistant (EXPLORER package)	policies.google.com/privacy
Google ML Kit	Person detection in photos	developers.google.com/ml-kit/terms
Google Play Billing	Payment and subscription handling	play.google.com/about/play-terms
Mapbox	Interactive maps and tiles	mapbox.com/legal/privacy
Meteoblue	Weather forecasts (SPORT package)	meteoblue.com/en/company/legal/privacy-policy
EAWS	Avalanche warnings	avalanches.org

The Controller does not sell users' personal data to third parties.

4.4 Rescue Services

The Controller may share a user's location data with mountain rescue services — **Górskie Ochotnicze Pogotowie Ratunkowe (GOPR)** and **Tatrzańskie Ochotnicze Pogotowie Ratunkowe (TOPR)** — exclusively in justified cases where the user is being searched for by these services and there is a risk to their life or health. The legal basis for such sharing is the protection of the vital interests of the data subject (Art. 6(1)(d) GDPR).

---

5. Data Transfers Outside the EEA

The use of Google services (Firebase, Gemini AI, ML Kit, Google Play) may involve the transfer of data to the United States. Google applies Standard Contractual Clauses (SCCs) approved by the European Commission as a data transfer mechanism, ensuring an adequate level of protection in compliance with GDPR.

---

6. Data Retention

Data category	Retention period
User account data	Until the account is deleted by the user
Activity and GPS track data	Until deleted by the user or account deletion

Data category	Retention period
Photos	Until deleted by the user or account deletion
Health data (heart rate, calories)	Until deleted by the user or account deletion
Chat AI conversation history	30 days from the last message in the conversation (automatic TTL)
AI query logs	Maximum 12 months from the date of query
Push notification tokens (FCM)	Until logout or app uninstallation
Payment data	As required by law (minimum 5 years)

After account deletion, data is permanently removed from the Controller's systems within **30 days**, except for data required to be retained by law.

---

7. User Rights (GDPR)

Every user is entitled to the following rights:

- **Right of access** – the right to obtain information about processed data
- **Right to rectification** – correction of inaccurate or completion of incomplete data
- **Right to erasure** ("right to be forgotten") – deletion of data when there is no legal basis for processing
- **Right to restriction of processing** – the right to request a suspension of processing in specific situations
- **Right to data portability** – receipt of data in a structured format (e.g. GPX for routes)
- **Right to object** – objection to processing based on legitimate interest
- **Right to withdraw consent** – withdrawal of consent at any time (e.g. for health data, location sharing)
- **Right to lodge a complaint** – filing a complaint with a supervisory authority (in the EU: your local data protection authority; in Poland: UODO, uodo.gov.pl)

Most rights can be exercised directly in the App settings (deleting activities, photos, or the account). For other requests, please contact the Controller (see section 14).

---

8. App Permissions

The App may request access to the following system permissions:

Permission	Purpose
Precise location (GPS)	Activity tracking, navigation, map, real-time location sharing
Background location	Home screen widget updates (weather, air quality)
Camera	Taking photos for activities and places
Storage / files	GPX file export/import, offline map storage
Microphone	Voice search and voice input in Chat AI (EXPLORER package)
Bluetooth	Pairing and communicating with BLE heart rate sensors (HEALTH package)
Notifications	Activity alerts, social notifications, weather alerts
Physical activity	Step and cadence detection via accelerometer

Users can manage permissions in the device's system settings. Revoking selected permissions may limit App functionality.

---

9. Activity, Photo and GPS Data Privacy

Activity Privacy Settings

Each activity can be marked as: - **Public** – visible to all users - **Friends** – visible only to accepted friends - **Private** – visible only to the owner

Photo Privacy Settings

Each photo can be marked as: - **Public** – visible to all App users - **Friends** – visible only to accepted friends (**default**) - **Private** – visible only to the owner

Automatic photo publishing is an optional feature that the user may enable in the settings. Once enabled, a photo is automatically published only if at least one of the following conditions is met: - No person is detected in the photo, or - At least 5 faces are detected in the photo (group photo)

Detection is performed entirely on the user's device (offline) using Google ML Kit and does not involve identifying or tracking individuals.

Real-Time Location

The real-time location sharing feature is **disabled by default**. The user may consciously choose one of the following visibility levels: - **Disabled (private)** – location not visible to others (**default**) - **Friends** – visible only to accepted friends - **Public** – visible to all App users

The user may change this setting at any time in the App settings.

---

10. Data Security

The Controller applies the following technical and organizational measures:

- Data encryption in transit (HTTPS/TLS)
- Data encryption at rest within Firebase/Google Cloud infrastructure
- Token-based authorization via Firebase Authentication
- Input sanitization (protection against prompt injection attacks in the AI feature)
- Firestore security rules restricting data access
- API usage limits (rate limiting) for AI features

---

11. Children's Privacy

The **On Trail** App is not intended for children under the age of 13. We do not knowingly collect personal data from persons under 13 years of age. If you become aware that a child has provided us with data without parental/guardian consent, please contact us – we will delete such data.

---

12. Cookies and Tracking Technologies

The mobile App does not use browser cookies. It may use local data storage on the device solely for the purpose of ensuring App functionality (e.g. map cache, search history, settings).

---

13. Changes to This Privacy Policy

The Controller reserves the right to amend this Privacy Policy. Users will be informed of material changes via a message displayed upon launching the App.

Continued use of the App after the changes take effect constitutes acceptance of the updated Privacy Policy.

14. Contact

For matters related to personal data protection, exercising GDPR rights, or account deletion, please contact us:

E-mail: weiga.apps@gmail.com **Website:** weiga.pl

We respond to personal data inquiries within **30 days** of receiving the request.

This Privacy Policy has been prepared in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR).