Push Beyond Privacy Policy

Last Updated: October 9, 2026
Version: 1.0
Effective Date: December 1, 2025

---

1. Introduction

Welcome to Push Beyond ("we," "our," or "us"). This Privacy Policy explains how we collect, use, disclose, and safeguard your information when you use our mobile fitness application ("Push Beyond" or "App"). We are committed to protecting your privacy and ensuring transparency about how your data is handled.

Push Beyond is a fitness tracking application that allows you to:

- Track gym workouts and cardio activities
- Monitor personal records and progress
- Connect with friends through social features
- Sync activities from third-party services like Strava
- Receive AI-powered training insights

Contact Information:

- Email: privacy@push-beyond.com
- Website: push-beyond.com

---

2. Data Controller Information

Push Beyond operates as the data controller for personal data processed through the App. For any questions regarding this Privacy Policy or our data practices, please contact us at:

Email: privacy@push-beyond.com

---

3. Information We Collect

3.1 Information You Provide

Account Information:

- Email address
- Username

- Password (stored securely using encryption)
- Profile picture (optional)

Fitness Data:

- Workout records (exercises, sets, reps, weights)
- Activity data (running, cycling, swimming, etc.)
- Personal records and achievements
- Training plans and schedules

Social Content:

- Posts you create
- Comments on posts
- Likes and interactions
- Friend connections

Communication Data:

- Support requests
- Feedback you provide

3.2 Information Collected Automatically

Device Information:

- Device type and model
- Operating system and version
- Unique device identifiers (for push notifications)
- App version

Usage Information:

- Features used within the App
- Time spent in the App
- Crash reports and performance data

Important Note on Location Data: Push Beyond does **not** directly collect GPS or location data. When you view activity routes (from Strava integration), this data is sourced from Strava and displayed within the App. We do not independently track your location.

3.3 Information from Third-Party Services

Strava Integration (Optional): When you connect your Strava account, we may receive:

- Activity data (runs, rides, swims, etc.)
- GPS routes and maps

- Heart rate data (if available)
- Performance metrics
- Athlete profile information

This data is only collected with your explicit consent and can be disconnected at any time.

---

4. Legal Basis for Processing (GDPR)

We process your personal data based on the following legal grounds:

Data Type	Legal Basis
Account data	Contract performance (necessary to provide the service)
Fitness/workout data	Consent (explicit opt-in for health data under GDPR Article 9)
Analytics data	Legitimate interest or consent (depending on jurisdiction)
Marketing communications	Consent
Push notifications	Consent
Third-party integrations	Consent
Safety screening of posts, comments and profile text	Legitimate interest (keeping the community safe)

---

5. How We Use Your Information

We use your information for the following purposes:

5.1 Providing Core Services

- Creating and managing your account
- Recording and displaying your workouts
- Tracking your personal records
- Enabling social features (posts, comments, likes)
- Syncing data from connected services

5.2 Personalization

- Providing personalized workout recommendations
- AI-powered training insights (when enabled)
- Displaying relevant content in your feed

5.3 Communication

- Sending push notifications about friend activities
- Account-related emails
- Important service announcements
- Marketing communications (only with consent)

5.4 Improvement and Analytics

- Analyzing usage patterns to improve the App
- Identifying and fixing bugs
- Developing new features

5.5 Safety and Security

- Detecting and preventing fraud
- Enforcing our Terms and Conditions
- Protecting user safety
- Automatically screening usernames, profile text, posts and comments for hate speech, threats, sexual content and harassment. Text that breaks our rules is refused or hidden. Before text is checked by our AI provider (OpenAI), usernames, email addresses, links and long numbers are removed, and no account details are sent with it. Decisions to remove content or suspend accounts are made by our team.

---

6. Data Sharing and Disclosure

6.1 We Do NOT Sell Your Data

We do not sell, rent, or trade your personal information to third parties for their marketing purposes.

6.2 Service Providers (Subprocessors)

We share data with trusted service providers who help us operate the App:

Provider	Purpose	Location	GDPR Compliant
Supabase Inc.	Database, authentication, storage	EU (Frankfurt)	✅ Yes
Strava Inc.	Activity sync (optional)	United States	✅ Yes (SCCs)
Expo (650 Industries)	Push notifications	United States	✅ Yes (SCCs)

Provider	Purpose	Location	GDPR Compliant
OpenAI	AI features (optional, anonymized); safety screening of posts, comments and profile text (anonymized)	United States	✅ Yes (SCCs)

6.3 Legal Requirements

We may disclose your information if required by law, such as:

- Responding to legal processes or government requests
- Protecting our rights, privacy, safety, or property
- Enforcing our Terms and Conditions

6.4 Business Transfers

In the event of a merger, acquisition, or sale of assets, your information may be transferred. We will notify you of any such change.

---

7. International Data Transfers

Your data is primarily stored on servers located in the **European Union (Frankfurt, Germany)** through our database provider Supabase.

When data is transferred outside the EU (e.g., to Strava in the United States), we ensure adequate protection through:

- **Standard Contractual Clauses (SCCs**) approved by the European Commission
- Verification that recipients maintain appropriate security measures

---

8. Data Retention

We retain your data for as long as necessary to provide our services:

Data Type	Retention Period
Account data	Until account deletion
Workout/activity data	Until account deletion

Data Type	Retention Period
Social content (posts, comments)	Until deleted by you or account deletion
Audit logs	2 years
Consent records	3 years after withdrawal
Anonymized analytics	Indefinitely

Automatic Data Cleanup

- Cached workout data older than 7 days is automatically removed from local device storage
- Expired push notification tokens are periodically cleaned

---

9. Your Rights (GDPR)

Under the General Data Protection Regulation (GDPR), you have the following rights:

9.1 Right to Access (Article 15)

You can request a copy of all personal data we hold about you. Use the **"Export My Data"** feature in Settings > Privacy to download your data in machine-readable format.

9.2 Right to Rectification (Article 16)

You can update your profile information directly in the App at any time.

9.3 Right to Erasure (Article 17)

You can delete your account and all associated data using the **"Delete My Account"** feature in Settings > Privacy. If you signed up with Google or Apple, you confirm with a code we send to your email address. This action is irreversible.

Deleting your account removes your profile, workouts and activities, posts, comments and likes, photos and videos, followers and following, your conversations with Luca, your training plans, and data from connected services. We keep only:

- Audit logs and consent records, for the periods listed in section 8
- Reports you made or that were made about you, without your account details, so our team can still act on abuse
- Our moderation log, which records which rule was triggered but no text you wrote

9.4 Right to Restriction (Article 18)

You can restrict certain processing by adjusting your consent preferences in Settings > Privacy > Manage Consent.

9.5 Right to Data Portability (Article 20)

You can export your data in a portable format (JSON/CSV) through the App.

9.6 Right to Object (Article 21)

You can opt-out of certain processing activities by adjusting your consent settings.

9.7 Right to Withdraw Consent (Article 7)

You can withdraw consent at any time through Settings > Privacy > Manage Consent. Withdrawal does not affect the lawfulness of processing before withdrawal.

To exercise these rights, contact us at: privacy@push-beyond.com

---

10. Children's Privacy (GDPR Article 8)

Push Beyond is not intended for anyone under the age of 16, and we do not knowingly collect personal data from them.

Age Requirement

- You must be at least 16 years old to create an account
- During registration, you confirm that you meet this age requirement
- We do not ask for or store your date of birth

If we learn that an account belongs to someone under 16, we will delete the account and its data promptly. If you believe someone under 16 is using Push Beyond, please contact us at privacy@push-beyond.com.

---

11. Health Data (GDPR Article 9)

Fitness and workout data may constitute "special category data" under GDPR. We handle this data with extra care:

- **Explicit Consent:** We require explicit opt-in consent before collecting health/fitness data
- **Purpose Limitation:** Health data is only used for providing fitness tracking features
- **No Third-Party Sharing:** We do not share health data with advertisers or marketers
- **Revocable:** You can withdraw health data consent at any time without deleting your account

---

12. Security Measures

We implement industry-standard security measures to protect your data:

Technical Measures

- **Encryption in Transit:** All data transmitted using HTTPS/TLS 1.2+
- **Encryption at Rest:** Sensitive data encrypted using AES-256
- **Token Encryption:** Third-party tokens (Strava) are encrypted before storage
- **Secure Storage:** Passwords hashed using industry-standard algorithms

Organizational Measures

- Regular security audits
- Access controls and authentication
- Employee security training
- Incident response procedures

Mobile App Security

- Secure token storage using platform-specific secure storage
- Certificate pinning for API communications
- No sensitive data in local logs

---

13. Cookies and Tracking

Mobile App

The Push Beyond mobile app does not use traditional cookies. However, we use equivalent technologies:

- **Functional Storage:** Required for app operation (authentication tokens, preferences)
- **Analytics (Optional):** Usage analytics to improve the App
- **Marketing (Optional):** Only with your consent

You can manage these preferences in Settings > Privacy > Manage Consent.

Web Components

When you authenticate with third-party services (like Strava) through in-app browsers:

- First-party cookies may be used for authentication
- These are essential for the OAuth process

---

14. Push Notifications

We send push notifications for:

- Friend activity updates
- Comments on your posts
- Likes on your content
- Personal record achievements

You can:

- Disable notifications in Settings > Notifications
- Manage notification permissions in your device settings

Device tokens are:

- Cached for 7 days to reduce API calls
- Automatically refreshed when expired
- Deleted when you disable notifications

---

15. AI Features

Push Beyond offers optional AI-powered features for training insights and recommendations.

How AI Data is Processed

- Workout summaries are **anonymized** before processing
- No personally identifiable information is sent to AI providers
- You can disable AI features at any time

AI Disclaimer

AI-generated content is for informational purposes only and does not constitute medical advice. Always consult healthcare professionals before starting new exercise programs.

---

16. Changes to This Privacy Policy

We may update this Privacy Policy from time to time. We will notify you of any changes by:

- Posting the new Privacy Policy in the App
- Updating the “Last Updated” date
- Sending a notification for significant changes

We recommend reviewing this Privacy Policy periodically.

---

17. Contact Us

If you have questions about this Privacy Policy or our data practices, please contact us:

Email: privacy@push-beyond.com
Website: push-beyond.com

Supervisory Authority

If you are located in the European Union and believe we have not adequately addressed your concerns, you have the right to lodge a complaint with your local data protection authority.

---

18. Additional Information for Specific Regions

European Economic Area (EEA)

This Privacy Policy is designed to comply with the General Data Protection Regulation (GDPR). All rights described in Section 9 are available to EEA residents.

United Kingdom

Following Brexit, we comply with the UK GDPR. UK residents have the same rights as EEA residents.

California (CCPA/CPRA)

California residents have additional rights under the California Consumer Privacy Act:

- Right to know what personal information is collected
- Right to delete personal information
- Right to opt-out of sale of personal information (we do not sell data)
- Right to non-discrimination for exercising privacy rights

This Privacy Policy was last updated on October 8, 2026.