

Push Beyond Data Processing Agreement

Last Updated: October 8, 2026

Version: 1.0

Effective Date: December 1, 2025

1. Introduction

This Data Processing Agreement (“DPA”) forms part of the Terms and Conditions between Push Beyond (“Processor,” “we,” “us”) and users of the Push Beyond mobile application (“Controller,” “you,” “user”).

This DPA outlines how we process personal data on your behalf and ensures compliance with:

- General Data Protection Regulation (EU) 2016/679 (“GDPR”)
- UK General Data Protection Regulation (“UK GDPR”)
- Other applicable data protection laws

Contact Information:

- Email: privacy@push-beyond.com
-

2. Definitions

Term	Definition
Personal Data	Any information relating to an identified or identifiable natural person
Special Category Data	Personal data revealing racial origin, political opinions, religious beliefs, genetic data, biometric data, health data, or sex life/orientation
Processing	Any operation performed on personal data (collection, storage, use, disclosure, deletion)
Data Controller	The entity that determines the purposes and means of processing personal data

Term	Definition
Data Processor	The entity that processes personal data on behalf of the controller
Subprocessor	A third party engaged by the processor to process personal data
Data Subject	The individual whose personal data is being processed

3. Roles and Responsibilities

3.1 Push Beyond as Processor

When you use Push Beyond to track your fitness activities, we act as a **Data Processor** processing your personal data according to your instructions (your use of the app and consent choices).

3.2 User as Controller

As a user, you act as the **Data Controller** for your personal data. You determine:

- What data to input into the app
- Which consent options to enable
- Which third-party services to connect
- When to delete your data

3.3 Joint Controller Scenarios

For certain social features (sharing posts, comments), we may act as **Joint Controllers** as we both determine purposes of processing.

4. Data Processing Details

4.1 Subject Matter

Processing of personal data through the Push Beyond mobile application for fitness tracking, social features, and related services.

4.2 Duration

Processing continues for the duration of your use of the Push Beyond application and until deletion of your account plus any legally required retention periods.

4.3 Nature and Purpose

Purpose	Nature of Processing
Account Management	Collection, storage, authentication
Fitness Tracking	Collection, storage, analysis, display
Social Features	Collection, storage, sharing, display
Third-Party Sync	Collection, import, storage
Analytics	Collection, aggregation, analysis
Push Notifications	Collection, transmission
AI Features	Collection, anonymization, transmission, analysis

4.4 Categories of Data Subjects

- Registered users of Push Beyond aged 16 and older

4.5 Types of Personal Data

Standard Personal Data:

- Account data (email, username, profile information)
- Usage data (app interactions, preferences)
- Device data (device type, OS, push tokens)
- Social data (posts, comments, likes, friend connections)

Special Category Data (GDPR Article 9):

- Health and fitness data (workouts, activities, personal records)
 - Biometric data (if imported from Strava: heart rate)
-

5. Processor Obligations

5.1 Lawful Processing

We process personal data only:

- In accordance with your documented instructions (app usage and consent)
- As required by applicable law
- With appropriate legal basis (consent, contract performance)

5.2 Confidentiality

We ensure that persons authorized to process personal data:

- Have committed to confidentiality

- Are bound by appropriate confidentiality obligations
- Receive data protection training

5.3 Security Measures

We implement appropriate technical and organizational measures:

Technical Measures:

Measure	Implementation
Encryption in Transit	HTTPS/TLS 1.2+ for all data transmission
Encryption at Rest	AES-256 encryption for sensitive data
Token Encryption	Encrypted storage of third-party tokens
Secure Storage	Platform-specific secure storage (Keychain/Keystore)
Password Security	Industry-standard hashing algorithms
Access Controls	JWT-based authentication with expiration

Organizational Measures:

- Regular security assessments
- Access control policies
- Incident response procedures
- Security training for personnel

5.4 Subprocessor Engagement

Before engaging subprocessors, we:

- Conduct due diligence on data protection practices
- Ensure contractual obligations equivalent to this DPA
- Maintain an updated list of subprocessors (see Section 7)

5.5 Data Subject Rights

We assist you in responding to data subject requests:

Right	How We Support
Access	Export My Data feature (Settings > Privacy)
Rectification	Profile editing within app

Right	How We Support
Erasure	Delete My Account feature
Portability	JSON/CSV data export
Restriction	Consent management controls
Objection	Consent withdrawal options

5.6 Data Breach Notification

In case of a personal data breach, we will:

- Notify you without undue delay (within 72 hours where feasible)
- Provide details: nature of breach, data affected, likely consequences, measures taken
- Document all breaches and actions taken

5.7 Audit and Inspection

Upon reasonable request, we will:

- Provide information necessary to demonstrate compliance
- Allow for audits by you or an authorized auditor
- Cooperate with supervisory authorities

5.8 Data Return and Deletion

Upon termination of services or request:

- Export your data in portable format
- Delete personal data within 30 days of account deletion
- Retain only data required by law with documented justification

6. Controller Obligations

As a user (Controller), you are responsible for:

6.1 Lawful Instructions

- Ensuring your use of the app complies with applicable laws
- Providing accurate personal data
- Not uploading unlawful content

6.2 Consent

- Providing valid consent for data processing
- Obtaining any necessary third-party consents before sharing their data

6.3 Data Subject Rights

- Responding to data subject requests using provided tools
- Contacting us if additional assistance is needed

7. Subprocessors

7.1 Authorized Subprocessors

We currently use the following subprocessors:

Subprocessor	Purpose	Location	Data Types
Supabase Inc.	Database, authentication, file storage	EU (Frankfurt)	Account data, workout data, social data
Strava Inc.	Activity sync (when connected)	United States	Activity data, GPS routes, performance metrics
Expo (650 Industries)	Push notification delivery	United States	Device tokens, notification content
OpenAI	AI features (optional); safety screening of user text	United States	Anonymized workout summaries; anonymized post, comment and profile text

7.2 Subprocessor Requirements

All subprocessors are required to:

- Implement appropriate security measures
- Process data only as instructed
- Comply with applicable data protection laws
- Maintain confidentiality obligations

7.3 International Transfers

For transfers outside the EEA, we use:

- **Standard Contractual Clauses (SCCs)** approved by the European Commission
- Additional safeguards where required (encryption, anonymization)

7.4 Updates to Subprocessors

We will notify you of any intended changes to subprocessors:

- Through updates to this DPA
 - Via app notifications for significant changes
 - You may object to new subprocessors within 14 days
-

8. International Data Transfers

8.1 Primary Data Location

Your data is primarily stored in the **European Union (Frankfurt, Germany)** through Supabase.

8.2 Transfer Mechanisms

When data is transferred outside the EU/EEA:

Destination	Mechanism	Additional Safeguards
United States (Strava)	Standard Contractual Clauses	Optional integration only
United States (Expo)	Standard Contractual Clauses	Limited to push tokens
United States (OpenAI)	Standard Contractual Clauses	Data anonymization

8.3 Transfer Impact Assessment

We have assessed that transfers to the United States are appropriate because:

- SCCs provide adequate legal protection
 - Subprocessors maintain robust security measures
 - Sensitive data is encrypted or anonymized
 - You have control over which integrations to enable
-

9. Data Retention

9.1 Retention Periods

Data Category	Retention Period	Justification
Account data	Until account deletion	Contract performance
Workout/activity data	Until account deletion	Contract performance
Social content	Until deleted or account deletion	Contract performance
Consent records	3 years after withdrawal	GDPR compliance (Art. 7)
Audit logs	2 years	Security and legal compliance
Anonymized analytics	Indefinitely	Legitimate interest

9.2 Automatic Cleanup

- Cached workout drafts: 7 days
- Expired push tokens: Periodic cleanup
- Session data: Upon logout

9.3 Post-Deletion Retention

After account deletion:

- Personal data deleted within 30 days
- Anonymized data may be retained for analytics
- Legal holds may extend retention where required by law

10. Security Incident Response

10.1 Incident Classification

Severity	Description	Response Time
Critical	Data breach affecting multiple users	Immediate
High	Unauthorized access attempt	Within 4 hours
Medium	Security vulnerability discovered	Within 24 hours
Low	Minor security improvement needed	Within 7 days

10.2 Breach Response Process

1. **Detection:** Identify and contain the incident
2. **Assessment:** Determine scope and severity
3. **Notification:** Notify affected users and authorities as required

4. **Remediation:** Fix vulnerability and restore security
5. **Review:** Document lessons learned and improve processes

10.3 Your Notification

In case of a breach affecting your data:

- Notification within 72 hours
 - Description of breach nature
 - Contact information for questions
 - Recommended protective measures
-

11. Data Protection Impact Assessment

For high-risk processing activities, we conduct Data Protection Impact Assessments (DPIAs):

Current DPIAs completed for:

- Health/fitness data processing (GDPR Article 9)
- Third-party data sharing (Strava integration)
- AI processing features

DPIA considerations include:

- Necessity and proportionality of processing
 - Risks to data subjects
 - Measures to address risks
 - Consultation with DPO where required
-

12. Data Protection Officer

While we may not be legally required to appoint a Data Protection Officer, privacy inquiries should be directed to:

Privacy Contact:

This contact handles:

- Data subject requests
 - Privacy inquiries
 - Complaint handling
 - Regulatory communication
-

13. Amendments

This DPA may be updated to reflect:

- Changes in data processing activities
- New subprocessors
- Legal or regulatory requirements
- Security improvements

Significant changes will be notified through the app. Continued use after notification constitutes acceptance.

14. Governing Law

This DPA shall be governed by:

- For EU users: Laws of the European Union (GDPR) and the laws of Belgium
- For UK users: Laws of the United Kingdom (UK GDPR)
- For other users: Laws of Belgium

Disputes shall be resolved in the courts of the judicial district where the Data Controller is established.

15. Contact Information

For questions about this Data Processing Agreement:

Email: privacy@push-beyond.com

Website: push-beyond.com

Supervisory Authority: EU users may lodge complaints with their local data protection authority.

16. Annexes

Annex A: Technical and Organizational Measures

A.1 Physical Security

- Data centers with 24/7 security (via Supabase in Frankfurt)
- Access controls and monitoring
- Environmental controls

A.2 Network Security

- Firewall protection
- Intrusion detection systems
- DDoS protection
- TLS/HTTPS encryption

A.3 Application Security

- Secure development practices
- Regular security testing
- Code review processes
- Dependency vulnerability scanning

A.4 Access Management

- Role-based access controls
- Multi-factor authentication for systems
- Regular access reviews
- Audit logging

A.5 Data Protection

- Encryption at rest and in transit
- Secure key management
- Regular backups
- Data minimization practices

Annex B: Data Subject Request Procedures

Request Types:

1. Access Request → Use “Export My Data” feature
2. Rectification → Edit profile in app
3. Erasure → Use “Delete My Account” feature
4. Portability → Use data export (JSON/CSV)
5. Restriction → Adjust consent settings
6. Objection → Contact

Response Timeline:

- Acknowledgment: Within 3 business days
 - Completion: Within 30 days (may extend to 60 days for complex requests)
-

This Data Processing Agreement was last updated on October 8, 2026.