DATA PROCESSING AGREEMENT

GDPR Article 28 Compliant with Standard Contractual Clauses

Between:

BodyF1RST, Inc.
("Processor / Data Importer")

And:

[CUSTOMER NAME]
("Controller / Data Exporter")

Effective Date: [DATE]

RECITALS

This Data Processing Agreement ("DPA") forms part of the Master Service Agreement between BodyF1RST, Inc. and Customer. This DPA applies when Personal Data of Data Subjects in the EEA, UK, or Switzerland is processed by BodyF1RST as Processor on behalf of Customer as Controller.

1. DEFINITIONS

"GDPR" Regulation (EU) 2016/679 (General Data Protection Regulation).

"UK GDPR" GDPR as incorporated into UK law by the Data Protection Act 2018.

"Personal Data" Any information relating to an identified or identifiable natural person.

"Special Category Data" Personal Data revealing racial/ethnic origin, health data, biometric data, etc.

"Data Subject" The identified or identifiable natural person to whom Personal Data relates.

"Processing" Any operation performed on Personal Data.

"Sub-processor" Any third party engaged by Processor to process Personal Data.

"SCCs" Standard Contractual Clauses approved by EC Decision 2021/914.

2. SCOPE OF PROCESSING

2.1 Subject Matter. Processor processes Personal Data to provide corporate wellness services.

2.2 Nature and Purpose: Account management, personalized wellness content, activity/nutrition/health tracking, team challenges, analytics.

2.3 Duration. Processing continues for Agreement duration plus data retention period.

2.4 Data Subjects: Customer's employees, contractors, authorized individuals.

2.5 Categories of Data: Identification data, account data, health/fitness data, device/usage data, coach communications.

2.6 Special Category Data. Health and fitness data constitutes Special Category Data under Article 9. Processed based on explicit consent (Art. 9(2)(a)) or occupational medicine (Art. 9(2)(h)).

3. PROCESSOR OBLIGATIONS

3.1 Process Personal Data only on documented Controller instructions or as required by law.

3.2 Ensure authorized persons are bound by confidentiality obligations.

3.3 Implement appropriate technical and organizational security measures.

3.4 Not engage Sub-processors without prior authorization; notify of changes with 30 days' notice.

3.5 Assist Controller with Data Subject requests (Articles 15-21).

3.6 Notify Controller without undue delay of any Personal Data Breach.

3.7 Provide assistance for DPIAs when required.

3.8 Make information available for audits; provide SOC 2 Type II reports.

3.9 Return or delete Personal Data upon termination; provide deletion certification.

4. CONTROLLER OBLIGATIONS

4.1 Provide lawful and complete processing instructions.

4.2 Ensure valid legal basis for Processing.

4.3 Obtain valid explicit consent for Special Category Data.

4.4 Ensure Personal Data provided is accurate and up to date.

5. INTERNATIONAL TRANSFERS

5.1 Transfer Mechanism. Personal Data transfers from EEA/UK to US are governed by Standard Contractual Clauses (Module 2: Controller to Processor).

5.2 UK Transfers. International Data Transfer Addendum to EU SCCs is incorporated.

5.3 Additional Safeguards: End-to-end encryption, strict access controls, data minimization, regular security assessments.

6. ANNEXES

ANNEX I - Standard Contractual Clauses

SCCs (Module 2) approved by EC Decision 2021/914 incorporated by reference. Clause 17: Governing Law - Ireland. Clause 18(b): Forum - Courts of Ireland.

ANNEX II - Technical and Organizational Measures

AES-256 encryption at rest, TLS 1.3 in transit
Role-based access control, MFA, quarterly access reviews
SOC 2 Type II certified infrastructure (Google Cloud)
24/7 security monitoring, intrusion detection
Documented incident response, 24hr breach notification
Data minimization, retention enforcement, automated deletion

ANNEX III - Authorized Sub-processors

Sub-processor	Location	Service	Safeguards
Google Cloud Platform	USA	Hosting, Storage	SCCs, SOC 2, ISO 27001
Stripe	USA	Payments	SCCs, PCI-DSS
SendGrid (Twilio)	USA	Email	SCCs, SOC 2
OneSignal	USA	Push Notifications	SCCs

7. GENERAL PROVISIONS

7.1 Governed by Controller's jurisdiction for EEA matters / UK for UK matters.

7.2 In case of conflict, this DPA prevails for data protection matters.

7.3 Amendments must be in writing signed by both parties.

7.4 Liability governed by Agreement, subject to GDPR Article 82.

SIGNATURES

BodyF1RST, Inc.	**[CUSTOMER NAME]**
Signature: _____	Signature: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

This DPA is compliant with GDPR Article 28. Contact privacy@bodyf1rst.com for questions.