TRUE FIT

DATA PROCESSING ADDENDUM

This Data Processing Addendum (the "***Addendum***") is entered into by and between **Retailer** and True Fit, LLC ("***True Fit***"), effective as of the date of the applicable Order Form between Retailer and True Fit (the "Effective Date"). Retailer and True Fit may each be referred to as a "***Party***" or together as the "***Parties***".

RECITALS

WHEREAS, the Parties entered into an Order Form and all Exhibits thereto for the provision of True Fit Services (the "***Agreement***");

WHEREAS, pursuant to the Agreement, the Parties have agreed that it may be necessary for True Fit to Process certain Retailer Personal Data (as defined below) on behalf of Retailer, as more fully described in Schedule A attached hereto; and

WHEREAS, in light of this Processing, the Parties have agreed to enter into this Addendum to address the compliance obligations imposed upon Retailer pursuant to Applicable Privacy Law. True Fit is appointed by Retailer, as a Processor (as defined under the GDPR and UK GDPR), to Process Retailer Personal Data on behalf of Retailer to the extent necessary to provide the Services in accordance with the terms of this Addendum and the Master Agreement. For the avoidance of doubt, this Addendum shall not apply to the extent True Fit is operating in the capacity as a Controller (as defined under the GDPR or UK GDPR) or joint Controller of personal data (as defined under the GDPR or UK GDPR), notwithstanding the fact that such data may also constitute Retailer Personal Data hereunder.

NOW THEREFORE, in consideration of the foregoing and the mutual covenants and promises set forth herein, and for other good and valuable consideration, the receipt of which the Parties hereby acknowledge, the Parties hereby agree as follows:

AGREEMENT

1. **Definitions**. In addition to the defined terms specified in the first paragraph, recitals and substantive provisions of this Addendum, the following terms have the meanings set forth below:

1.1 "***Applicable Privacy Law***" means the relevant data protection and privacy law (including GDPR and UK GDPR) to which Retailer is subject, and any guidance or statutory codes of practice issued by the relevant Privacy Authority.

1.2 "***Claim***" means any third party action, claim, assertion, demand or proceeding.

1.3 "***GDPR***" means Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the "General Data Protection Regulation").

1.4 "***Losses***" means any (a) Claim, and (b) direct loss, damage, cost, charge, fine, fees, levies, award or expense. For the avoidance of doubt, Losses shall not include any indirect or consequential losses.

1.5 "***Privacy Authority***" means the relevant supervisory authority with responsibility for privacy or data protection matters in the jurisdiction of Retailer.

1.6 ***"Process", "Processing" or "Processed"*** means any operation or set of operations which is performed upon Retailer Personal Data whether or not by automatic means, including collecting, recording, organising, storing, adapting or altering, retrieving, consulting, using, disclosing, making available, aligning, combining, blocking, erasing and destroying Retailer Personal Data.

1.7 "***Retailer Personal Data***" means any information, provided or made available to True Fit by or on behalf of Retailer in connection with True Fit's performance of the Services, which relates to an identified or identifiable natural person as defined by the Applicable Privacy Law, and including the categories of data listed in the Processing Appendix together with any additional such personal data to which True Fit has access from time to time in performing the Services under this Addendum.

1.8 "***Services***" means the services provided by True Fit in relation to the Processing of Retailer Personal Data as described in the Agreement.

1.9 "***Standard Contractual Clauses***" means the Standard Contractual Clauses set out in the European Commission's Implementing Decision (EU) 2021/914 of 4 June 2021, as may be amended or replaced by the European Commission from time to time.

1.10 "***UK GDPR***" means the UK General Data Protection Regulation, tailored by the Data Protection Act 2018.

1.11 "***UK Addendum***" means the Addendum issued by the UK Information Commissioner's Office in accordance with the Data Protection Act 2018 on 2 February 2022 (as may be amended, updated or superseded from time to time by the UK Government or the Information Commissioner's Office).

2. Processing Requirements.

2.1 True Fit acknowledges and agrees that, for purposes of this Addendum, Retailer is the sole controller of all Retailer Personal Data and only Retailer (including on behalf of its end clients, where applicable) shall have the right to direct True Fit in connection with True Fit's Processing of the Retailer Personal Data.

2.2 True Fit represents and warrants, with respect to all Retailer Personal Data that it Processes on behalf of Retailer, that at all times, unless otherwise expressly permitted under the Agreement:

(a) it shall Process such Retailer Personal Data only for the purposes of providing the Services and as may subsequently be agreed between the Parties in writing and, in so doing, shall act solely on the instructions of Retailer;

(b) it shall not Process, apply, or use, the Retailer Personal Data for any purpose other than as required and necessary to provide the Services; and

(c) it shall not create or maintain identifiable data derived from the Retailer Personal Data, except for the purposes of providing the Services. For the avoidance of doubt, Retailer authorizes True Fit to further process personal data for the purposes of creating aggregate, non-identifiable data which is derived from the Retailer Personal Data. True Fit will implement appropriate safeguards such as the anonymization of the data if this identifying data is not necessary.

2.3 True Fit shall have in place, and maintain, appropriate processes and any associated technical and organizational measures that will ensure that Retailer's reasonable and lawful instructions, as they relate to the Processing of Retailer Personal Data, can be complied with. Such measures are described in Schedule B of this Addendum.

2.4 True Fit shall comply with Applicable Privacy Law, to the extent applicable to True Fit's Processing of the Retailer Personal Data.

2.5 True Fit shall provide to Retailer such co-operation, assistance and information as Retailer may reasonably request to enable it to comply with its obligations under any Applicable Privacy Law and co-operate and comply with the directions or decisions of a relevant Privacy Authority, in each case within such reasonable time as would enable Retailer to meet any time limit imposed by the Privacy Authority. True Fit shall provide Retailer with all reasonable assistance and information with respect to any notifications to, or registration with, Privacy Authorities as required by Applicable Privacy Law.

2.6 The Parties acknowledge and agree that True Fit shall not be entitled to reimbursement of any costs which True Fit may incur as a result of or in connection with complying with Retailer's instructions for the purposes of providing the Services and/or with any of its obligations under this Addendum or any Applicable Privacy Law; provided, however, that Retailer shall reimburse True Fit for its reasonable costs associated with True Fit's compliance with (a) its obligations set forth in Section 2.5 above, and/or (b) the directions or decisions of any Privacy Authority, in each case to the extent such obligations arise as a result of Retailer's failure to comply with Applicable Privacy Law.

2.7 True Fit shall maintain at all times, and provide or make available to Retailer, promptly following receipt of Retailer's written notice, an accurate and complete written record of the Processing of Retailer Personal Data by True Fit on behalf of Retailer (including, without limitation, any Processing undertaken by Sub-Processors).

2.8 To the extent required by Applicable Privacy Law, True Fit shall designate (a) a data protection officer, and (b) a data protection representative in the EU.

3. True Fit Personnel. True Fit shall, and shall require each of its Sub-Processors to:

3.1 restrict access to the Retailer Personal Data to its personnel who need to access it for purposes of providing the applicable outsourced Services;

3.2 instruct its personnel regarding their confidentiality obligations with respect to the Retailer Personal Data; and

3.3 provide its personnel with such information and training as is necessary to ensure that they can Process the Retailer Personal Data in accordance with Applicable Privacy Law and the terms set forth herein.

4. Processing and Storage Locations.

4.1 Retailer acknowledges and agrees that True Fit may Process Retailer Personal Data in the United States.

4.2 To the extent True Fit stores Retailer Personal Data in a cloud environment, True Fit shall require the applicable cloud service provider to comply with industry standard best practices for cloud computing security. Such measures shall, in any event, be as restrictive as those set out in Schedule B of this Addendum.

5. Security of Retailer Personal Data.

5.1 True Fit shall maintain, during the term of the Agreement, appropriate technical and organizational security measures to protect the Retailer Personal Data against accidental or unlawful destruction or accidental loss, damage, alteration, unauthorized disclosure or access and against all other unlawful forms of Processing, as more fully described in the Schedule B attached hereto (the "Security Measures").

5.2 True Fit shall ensure the reliability (as such term is used in the GDPR and UK GDPR) of any employees and Sub-Processor personnel who access the Retailer Personal Data and ensure that such personnel have undergone appropriate training in the care, protection and handling of Retailer Personal Data, and have entered into an agreement, in relation to the Processing of Retailer Personal Data, the terms of which are no less onerous than those found in this Addendum. True Fit will remain liable for any unauthorized access to, Processing, or disclosure of Retailer Personal Data by each such Sub-Processor as if it had undertaken such action itself.

6. Sub-Processors.

6.1 True Fit shall not sub-contract or outsource or otherwise permit any Processing of Retailer Personal Data, or otherwise disclose any Retailer Personal Data, to any other person or entity (each a **"Sub-Processor"**) unless and until:

(a) True Fit has notified Retailer by way of formal written notice of the full name and registered office or principal place of business of the Sub-Processor;

(b) True Fit has provided to Retailer details (including categories) of the processing to be carried out by the Sub-Processor in relation to the Services, and such other information as may be requested by Retailer in order for Retailer to comply with Applicable Privacy Law, including notifying the relevant Privacy Authority;

(c) Retailer has provided prior written approval to such sub-contracting, outsourcing or disclosure;

(d) True Fit has imposed legally binding terms no less onerous than those contained in this Addendum on such Sub-Processor; and

(e) True Fit has, entered into Standard Contractual Clauses with the Sub-Processor, if and to the extent the scope of sub-processing involves the transmission of Retailer Personal Data to, the storage of Retailer Personal Data in, or the Processing of Retailer Personal Data by any other means in, third countries which have not received an adequacy decision under Applicable Laws.

6.2 Retailer acknowledges and agrees that True Fit is authorized to subcontract and outsource Processing of Personal Data to Google and Klaviyo.

7. Breach Notification.

7.1 Unless otherwise prohibited by applicable law, True Fit shall notify Retailer, as soon as is reasonably possible under the circumstances but in any event no later than within 24 hours after becoming aware, of any accidental, unauthorized, or unlawful destruction, loss, alteration, or disclosure of, or access to, Retailer Personal Data (**"Security Breach"**). Such notification shall include (a) a detailed description of the Security Breach, (b) the type of data that was the subject of the Security Breach and (c) the identity of each affected person (or, where not possible, the approximate number of data subjects and of Retailer Personal Data records concerned). True Fit shall communicate to Retailer (i) the name and contact details of True Fit's chief security officer or other point of contact where more information can be obtained; (ii) a description of the likely consequences of the Security Breach; (iii) a description of the measures taken or proposed to be

taken by True Fit to address the Security Breach, including, where appropriate, measures to mitigate its possible adverse effects; and additionally in such notification or thereafter (iv) as soon as such information can be collected or otherwise becomes available, any other information Retailer may reasonably request relating to the Security Breach.

7.2 True Fit shall take prompt action to investigate the Security Breach and shall use industry standard, commercially reasonable, efforts to mitigate the effects of any such Security Breach in accordance with its obligations hereunder and, subject to Retailer's prior written agreement, to carry out, at True Fit's sole cost, any recovery or other action reasonably necessary to remedy the Security Breach. Unless required to do so under Applicable Privacy Law, True Fit shall not release or publish any filing, communication, notice, press release, or report concerning any Security Breach ("**Notices**") without Retailer's prior written approval. True Fit shall provide written notice to Retailer of all corrective actions undertaken by True Fit following a Security Breach.

8. **Privacy Impact Assessment**. True Fit shall, promptly upon receipt of written request by Retailer, make available to the Retailer such information as is reasonably necessary to demonstrate True Fit's compliance with Applicable Privacy Law and shall assist the Retailer, at Retailer's expense, in carrying out such privacy impact assessment of the Services as is reasonable in light of the Retailer Personal Data that is being processed. True Fit shall reasonably cooperate with Retailer to implement such mitigation actions as are reasonably required to address privacy risks identified in any such privacy impact assessment. Unless such request follows a Security Breach, or is otherwise required by Applicable Privacy Law, Retailer shall not make any such request more than once in any 12-month period.

9. **Audit Rights**. True Fit shall permit Retailer and/or its authorized agents to audit its records to the extent reasonably required in order to confirm that True Fit is complying with its obligations under this Addendum or any Applicable Privacy Law, provided always that any such audit does not involve the review of any third party data and that the records and information accessed in connection with such audit is treated as confidential information by Retailer. Retailer shall bear its own costs in relation to such audit, unless the audit reveals any material non-compliance with True Fit's obligations under this Addendum, in which case the costs of the audit shall be borne by True Fit.

10. **Deletion of Retailer Personal Data**. True Fit shall, promptly or within no more 60 days, following receipt of written notice from the Retailer, delete Retailer Personal Data from its records and, upon completion of the Services, comply with all reasonable instructions from the Retailer with respect to the deletion of any remaining Retailer Personal Data.

11. **Third Party Disclosure Requests**.

11.1 Unless prohibited by applicable law, True Fit shall, and shall procure that any Sub-Processor shall, inform Retailer promptly of any inquiry, communication, request or complaint from:

(a) any governmental, regulatory or supervisory authority, including Privacy Authorities or the U.S. Federal Trade Commission; and/or

(b) any data subject,

relating to the Services, any Retailer Personal Data or any obligations under Applicable Privacy Law, and shall provide all reasonable assistance to enable Retailer to respond to such inquiries, communications, requests or complaints and to meet applicable statutory or regulatory deadlines. True Fit shall, and shall require that any Sub-Processor shall, not disclose Retailer Personal Data to any of the persons or entities listed in (a) or (b) above unless it is (i) legally required to do so and has otherwise complied with the obligations in this Section, or (ii) Retailer has expressly authorized it in writing to do so.

11.2 Unless prohibited by applicable law, in the event that True Fit or any Sub-Processor is required by law, court order, warrant, subpoena, or other legal judicial process ("Legal Request") to disclose any Retailer Personal Data to any person or entity other than Retailer, True Fit shall, and shall procure that any Sub-Processor shall, notify Retailer promptly and shall provide all reasonable assistance to Retailer to enable Retailer to respond or object to, or challenge, any such demands, requests, inquiries or complaints and to meet applicable statutory or regulatory deadlines. True Fit shall, and shall procure that any Sub-Processor shall, not disclose Retailer Personal Data pursuant to a Legal Request unless it is required to do so and has otherwise complied with the obligations in this Section.

12. **Transfers of Retailer Personal Data Outside of the European Economic Area**. Where Retailer Personal Data originating in the European Economic Area and/or the United Kingdom is Processed by True Fit outside the European Economic Area and/or the United Kingdom, in a territory that has not been designated by the European Commission or the United Kingdom relevant authority (as applicable) as ensuring an adequate level of protection pursuant to Applicable Privacy

Law, True Fit and Retailer agree that the transfer will be subject to the applicable Standard Contractual Clauses and UK Addendum (as applicable) which shall be deemed to apply in respect of such Processing.

13. **Indemnity**. True Fit shall indemnify Retailer (and each of its respective officers, employees and agents), against all Losses arising out of or in connection with any material breach by True Fit (and by any Sub-Processor) of the provisions of this Addendum. Notwithstanding anything to the contrary in the Agreement, in no event shall either party's liability under this DPA exceed, in the aggregate, the total fees paid or payable by Retailer to True Fit under the Agreement during the twelve (12) months preceding the date on which the claim arose. Retailer shall promptly notify True Fit, in writing, of any such alleged breach and Retailer shall not incur any costs or liabilities with respect to the same and with respect to which it would be indemnified by True Fit hereunder, without the prior written consent of True Fit, such consent not to be unreasonably delayed or withheld.

14. **Term**. This Addendum shall commence on the Effective Date and shall continue in full force and effect until the later of (a) the termination or expiration of the Agreement, or (b) completion of the last of the Services to be performed pursuant to the Agreement.

15. **Governing Law**. This Addendum shall be governed by and construed in accordance with the laws of the United States and shall be subject to the exclusive jurisdiction of the Courts of the Commonwealth of Massachusetts.

16. **Counterparts**. This Addendum may be executed in any number of counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument.

TRUE FIT

Schedule A

Summary of Processing

1. Subject Matter: The context for the Processing of Retailer Personal Data is TrueFit's provision of the Services under the Agreement(s).

2. Duration of Processing: True Fit will Process Retailer Personal Data until expiration or termination of the Agreement(s).

3. Nature and Purpose of Processing: True Fit will Process Personal Data for the purpose of providing Services in accordance with the Agreement(s).

4. Categories of Data Subjects: True Fit will Process Personal Data that relates to any and all data subjects about whom Retailer transfers Personal Data to True Fit to provide services under the Agreement(s). True Fit only receives pseudonymized User IDs linked to Transactional Data.

5. Types of Personal Data Processed: Transactional Data (e.g., sales transaction data.)

6. Contact Details of True Fit's Privacy Contact: For questions related to security and privacy please email privacy@truefit.com.

7. Approved Subcontractors and Data Transfers

Subcontractor Name	Purpose of Subcontracting	Physical Location
Google Cloud Platform (GCP)	Site hosting, data storage, analytics	USA
Klaviyo, Inc.	Email delivery services, professional services	USA

TRUE FIT

Schedule B

True Fit Security Measures

All security measures are implemented in support of a robust Data Protection and Security Policy that includes several safeguards including controls on who is allowed to access customer information, where and how customer information is stored, and definitions of how customer information must be destroyed.

Operational Security

True Fit Operations Team is responsible for operational security. This includes network and data security, as well as the patching and monitoring of True Fit's computing resources.

Organizational Security

All True Fit employees sign a document acknowledging receipt and understanding of True Fit's security policies and procedures. Security training is required and provided annually.

All employees undergo background checks as part of the onboarding process.

Physical Security

True Fit utilizes best in breed cloud hosting facilities. These facilities are certified in various levels of ISO, PCI, and SOC compliance. Specific certifications are available on request. Access to infrastructure is tightly controlled as per SAS 70 requirements and guidelines.

Network Security

True Fit follows industry standard best practices regarding the hardening of servers, and communication protocols against attacks and exploits and are audited monthly. All production systems are built from a standard system images that are closely audited and tested. True Fit allows only specific traffic from known services to communicate with its applications and servers; extraneous services are disabled and required ports are whitelisted. Applications are run with restricted privileges, and passwords are rotated.

True Fit leverages on and off-host network access control lists (ACLs) to actively protect against application layer attacks. These systems are configured to pass only HTTPS (TLS) traffic and other limited ports required for proper application operation.

Access control policies are enforced based on server roles and kept in a known state. True Fit's in-house security team audits the currently enforced policies on a regular basis to maintain effective security controls.

Access to network administration controls are restricted to audited roles. These roles, network tools, protocols, and configuration are reviewed and evaluated as part of ongoing internal audits.

Data Security

Personal data is always transferred over SSL connections, and is stored in encrypted form at rest. Data is encrypted using GPG public/private key encryption using a 2048-bit key. Encryption keys are stored offline to avoid loss in a catastrophic event. Access to offline encryption keys is protected by authenticated, multi-factor-based access.

Role based controls restrict access to personal data. Roles are centrally managed by True Fit Operations team and access rights are actively maintained. True Fit Operations performs ongoing reviews of all privileges within its systems to ensure that entitlements align with the roles defined in the organization.

Requests for changes to a user's entitlements are tracked via a Case Management system, which logs the requestor, approver and executor. Cases are stored indefinitely.

Changes to user entitlements are logged with the date, roles added/revoked, and the username of the user administering the change. Logs are retained for one year.

Patching

Vulnerabilities and patches are reviewed and evaluated on a monthly basis, and as required by True Fit's in-house security team. Patches are verified in a staging environment that matches production, before applying them to production. Operating system changes are tested and deployed in conjunction with major software releases to ensure testing and compatibility before releasing to production.

Infrastructure Monitoring

True Fit's Operations team utilizes best of breed & industry standard utilities to monitor all system and network-level activities. True Fit uses host-based Intrusion Detection Systems that are integrated with its monitoring and alerting system.

Server logs are maintained in storage one year and are transferred via encrypted protocols. In addition, log forging countermeasures are employed in the application layer to avoid false log entries.

Secure Software Development Process

True Fit utilizes a web framework that is designed to address the OWASP Top 10 vulnerabilities. True Fit also combines automated Static Analysis Security Testing (SAST) with 100% peer code review to identify potential security- related flaws.

Data is validated on both client and server side before use in the True Fit ecosystem. Data input and output routines are architected to prevent both CSS and SQL injection as well as other data corruption.

User credentials to True Fit applications are stored using a one-way hashing function with salt added. The True Fit software enforces minimum password requirements for length, complexity, and age, and account locks after several failed logon attempts. In addition, inactive user sessions are locked after a period of inactivity.

Release Management

All production builds are produced on a controlled build system that pulls code directly from True Fit's source code repository and all code changes are tagged by developers and traceable back to individual engineers. Changes to production systems are verified in a staging environment that is a clone of production. Only builds that have been marked as tested by QA are eligible to be deployed to production.

The release management team reviews tested builds to assess timing and risk of production releases. Access controls allow only authorized individuals to initiate changes to production environment via True Fit's managed deployment system.

Data Retention

Retailer-provided sales and returns data is retained for 5 years.

User registration data is retained indefinitely. Once a user has been inactive for a period of 5 years, that user's data is anonymized.

Backup Policy

Data backups are performed nightly and stored encrypted at rest in True Fit's hosting provider's cloud storage solution. True Fit utilizes strong GPG encryption prior to transmission off-site. Private encryption keys are stored offline.

Backup restore tests are executed at least quarterly.

Internal Audits

True Fit's in-house security team performs monthly security audits. These audits comprise a triage of non-critical internal alerts and a review of public CVE reports occurring since the last audit. Any issues requiring remediation are assigned and scheduled into the standard change management process.

Third Party Audits

True Fit works with independent security vendors to perform independent testing of its service and infrastructure. Network penetration and application penetration tests are performed annually or in conjunction with major architectural changes.

Threat Management Practices

Threats and vulnerabilities are managed through ongoing internal and 3rd party audits and a risk management program owned by True Fit's in-house security team.

Critical internal alerts and public CVE reports are triaged and assessed immediately and remediated as appropriate.

A formal Incident Response Policy is in place to govern the processes and procedures for responding to a security incident. Notifications are executed within 72 hours to appropriate parties.