RevenueHunt Data Processing Agreement

Last updated: June 2025.

This Data Processing Agreement (“DPA”) forms part of the Terms of Service (the “Agreement”) between:

Dairy Capital Limited (“Processor”, “we”, “us”, or “RevenueHunt”) Registered in the United Kingdom

and

You (“Controller”, “Customer”, or “Merchant”) The entity that has agreed to the Agreement

collectively referred to as the “Parties” and each a “Party”.

Merchants who require a signed copy can request one at info@revenuehunt.com.

1. Definitions

1.1 In this DPA, the following terms shall have the meanings set out below:

“Applicable Data Protection Law” means all applicable laws and regulations relating to the processing of Personal Data, including (i) the General Data Protection Regulation (EU) 2016/679 (“GDPR”); (ii) the UK General Data Protection Regulation and Data Protection Act 2018 (“UK GDPR”); (iii) the Swiss Federal Act on Data Protection (“Swiss FADP”); and (iv) any other applicable data protection laws in the jurisdictions where the Services are provided.

“Controller” means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

“Customer Personal Data” means any Personal Data that is Processed by RevenueHunt on behalf of the Customer in connection with the provision of the Services.

“Data Subject” means an identified or identifiable natural person whose Personal Data is Processed.

“Personal Data” means any information relating to an identified or identifiable natural person, as defined under Applicable Data Protection Law.

“Personal Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data.

“Processing” (and its cognates “Process” and “Processed”) means any operation or set of operations performed on Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment, combination, restriction, erasure, or destruction.

“Processor” means a natural or legal person, public authority, agency, or other body which Processes Personal Data on behalf of the Controller.

“Security Incident” means any unauthorized or unlawful access to, or acquisition, alteration, use, disclosure, or destruction of, Customer Personal Data.

“Services” means the Product Recommendation Quiz application and related services provided by RevenueHunt to the Customer under the Agreement.

“Standard Contractual Clauses” or **“SCCs”** means the standard contractual clauses for the transfer of Personal Data to third countries approved by the European Commission, as may be amended or replaced from time to time.

“Sub-processor” means any third party engaged by RevenueHunt to Process Customer Personal Data on behalf of the Customer.

2. Scope and Roles

2.1 Scope. This DPA applies to the Processing of Customer Personal Data by RevenueHunt in connection with the provision of the Services.

2.2 Roles of the Parties. The Parties acknowledge and agree that:

- a. The Customer is the Controller of Customer Personal Data;
- b. RevenueHunt is the Processor of Customer Personal Data, acting on behalf of and under the instructions of the Customer;
- c. RevenueHunt may also act as a Sub-processor where the Customer itself acts as a Processor on behalf of a third-party Controller.

2.3 Customer Responsibilities. The Customer shall:

- a. Ensure that its collection and sharing of Customer Personal Data with RevenueHunt complies with Applicable Data Protection Law;
- b. Provide any required notices to, and obtain any required consents from, Data Subjects for the Processing of their Personal Data as contemplated by this DPA;
- c. Ensure that its instructions to RevenueHunt comply with Applicable Data Protection Law;
- d. Be responsible for the lawfulness of the Processing of Customer Personal Data under this DPA.

3. Processing of Customer Personal Data

3.1 Processing Instructions. RevenueHunt shall Process Customer Personal Data only:

- a. In accordance with the Customer’s documented instructions, including as set forth in the Agreement and this DPA;
- b. As necessary to provide the Services;
- c. As required by Applicable Data Protection Law, in which case RevenueHunt shall inform the Customer of that legal requirement before Processing, unless prohibited by law.

3.2 Details of Processing. The subject matter, duration, nature, and purpose of the Processing, the types of Personal Data Processed, and the categories of Data Subjects are described in **Annex 1** to this DPA.

3.3 Prohibited Processing. RevenueHunt shall not:

- a. Sell Customer Personal Data;
- b. Retain, use, or disclose Customer Personal Data for any purpose other than providing the Services;
- c. Retain, use, or disclose Customer Personal Data outside of the direct business relationship between RevenueHunt and the Customer;
- d. Combine Customer Personal Data with Personal Data received from other sources, except as necessary to provide the Services.

4. Confidentiality

4.1 Personnel Obligations. RevenueHunt shall ensure that any person authorized to Process Customer Personal Data:

- a. Is bound by appropriate confidentiality obligations;
- b. Processes Customer Personal Data only as necessary to provide the Services and in accordance with the Customer's instructions;
- c. Has received appropriate training on data protection requirements.

4.2 Access Limitations. RevenueHunt shall limit access to Customer Personal Data to those personnel who require such access to perform the Services, following a need-to-know principle.

5. Security Measures

5.1 Security Obligations. RevenueHunt shall implement and maintain appropriate technical and organizational measures to protect Customer Personal Data against unauthorized or unlawful Processing and against accidental loss, destruction, damage, theft, alteration, or disclosure. These measures shall be appropriate to the harm that might result from such unauthorized or unlawful Processing or accidental loss, destruction, or damage, and to the nature of the data to be protected.

5.2 Specific Measures. Without limiting the foregoing, RevenueHunt's security measures shall include those described in **Annex 2** to this DPA.

5.3 Updates to Security Measures. RevenueHunt may update or modify its security measures from time to time, provided that such updates and modifications do not result in a material degradation of the overall security of the Services.

6. Sub-processors

6.1 Authorization. The Customer provides a general authorization for RevenueHunt to engage Sub-processors to Process Customer Personal Data, subject to the requirements of this Section 6.

6.2 Sub-processor List. A list of RevenueHunt's current Sub-processors is set forth in **Annex 3** to this DPA.

6.3 Sub-processor Agreements. RevenueHunt shall enter into a written agreement with each Sub-processor imposing data protection obligations no less protective than those imposed on RevenueHunt under this DPA.

6.4 Notification of Changes. RevenueHunt shall notify the Customer of any intended changes to its Sub-processors by updating the Sub-processor list at least fifteen (15) days before engaging any new Sub-processor.

6.5 Objection Rights. If the Customer has a reasonable objection to a new Sub-processor based on data protection concerns, the Customer may notify RevenueHunt in writing within ten (10) days of receiving notice. The Parties shall work together in good faith to find a mutually acceptable resolution. If no resolution can be reached within thirty (30) days, the Customer may terminate the affected Services without penalty.

6.6 Liability. RevenueHunt shall remain fully liable to the Customer for the performance of its Sub-processors' obligations under this DPA.

7. Data Subject Rights

7.1 Customer Responsibility. The Customer is responsible for responding to requests from Data Subjects to exercise their rights under Applicable Data Protection Law ("Data Subject Requests").

7.2 RevenueHunt Assistance. RevenueHunt shall:

- a. Promptly notify the Customer if it receives a Data Subject Request, unless prohibited by law;
- b. Provide the Customer with self-service functionality through the Services to assist in responding to Data Subject Requests where available;
- c. Provide reasonable assistance to the Customer in responding to Data Subject Requests, to the extent the Customer is unable to respond using the self-service functionality.

7.3 Data Subject Rights Supported. The Services enable the Customer to facilitate the following Data Subject rights:

- a. Right of access to Personal Data;
- b. Right to rectification of inaccurate Personal Data;
- c. Right to erasure of Personal Data;
- d. Right to data portability (export of Personal Data);
- e. Right to object to Processing;
- f. Right to withdraw consent.

7.4 Fees for Assistance. Where assistance under Section 7.2(c) requires effort beyond what is available through the self-service functionality of the Services, RevenueHunt may charge the Customer for such assistance at RevenueHunt's then-current professional services rates. RevenueHunt shall provide an estimate of such fees before commencing the work.

8. Security Incidents

8.1 Notification. RevenueHunt shall notify the Customer without undue delay, and in any event within seventy-two (72) hours, after becoming aware of a Security Incident affecting Customer Personal Data.

8.2 Content of Notification. Such notification shall include, to the extent known:

- a. A description of the nature of the Security Incident, including the categories and approximate number of Data Subjects and Personal Data records concerned;
- b. The name and contact details of a point of contact from whom more information can be obtained;
- c. A description of the likely consequences of the Security Incident;
- d. A description of the measures taken or proposed to address the Security Incident, including measures to mitigate its possible adverse effects.

8.3 Cooperation. RevenueHunt shall cooperate with the Customer and take reasonable steps to assist in the investigation, mitigation, and remediation of any Security Incident.

8.4 No Acknowledgment of Fault. RevenueHunt's notification of or response to a Security Incident shall not be construed as an acknowledgment of any fault or liability.

9. Data Protection Impact Assessments and Consultations

9.1 Taking into account the nature of the Processing and the information available to RevenueHunt, RevenueHunt shall provide reasonable assistance to the Customer in:

- a. Conducting data protection impact assessments in relation to the Processing of Customer Personal Data, where required under Applicable Data Protection Law;
- b. Consulting with supervisory authorities in relation to such data protection impact assessments, where required under Applicable Data Protection Law.

9.2 Fees. RevenueHunt may charge the Customer for assistance provided under this Section 9 at RevenueHunt's then-current professional services rates. Such assistance is time-intensive and may include document preparation, technical analysis, and coordination with the Customer's legal and compliance teams.

10. Audit Rights

10.1 Audit Information. RevenueHunt shall make available to the Customer all information reasonably necessary to demonstrate compliance with this DPA and Applicable Data Protection Law.

10.2 Audit Methods. The Customer's audit rights may be satisfied through:

- a. RevenueHunt's completion of a security questionnaire or similar documentation upon reasonable request;

- b. Review of RevenueHunt's certifications and third-party audit reports (such as SOC 2, penetration testing reports, or similar);
- c. An on-site audit, subject to the conditions in Section 10.3.

10.3 On-Site Audits. On-site audits shall be subject to the following conditions:

- a. The Customer shall provide at least thirty (30) days' prior written notice;
- b. Audits shall be conducted during normal business hours and shall not unreasonably interfere with RevenueHunt's operations;
- c. Audits shall be limited to once per twelve (12) month period, unless required by a supervisory authority or following a Security Incident;
- d. The Customer shall bear the costs of any such audit;
- e. The Customer and its auditors shall be bound by confidentiality obligations.

10.4 Professional Services Fees. The Customer acknowledges that audit-related activities require significant resources and personnel time. The following fees shall apply:

Service	Fee
Security Questionnaire Completion	Charged at professional services rates (minimum $1,200)
Custom Security Documentation	Charged at professional services rates based on scope
Third-Party Audit Report Access	Available upon request; administrative fee may apply
On-Site Audit Coordination	Charged at professional services rates plus travel and accommodation expenses
Expedited Requests	Requests requiring response within 5 business days incur a 50% expedite fee

RevenueHunt's current professional services rate is **$600 USD per hour**. RevenueHunt shall provide a fee estimate and obtain Customer approval before commencing any chargeable audit-related work. Fees are payable in advance or within thirty (30) days of invoice.

11. International Data Transfers

11.1 Transfer Mechanisms. Where Customer Personal Data is transferred from the European Economic Area ("EEA"), United Kingdom, or Switzerland to a country not recognized as providing an adequate level of data protection, RevenueHunt shall ensure that appropriate safeguards are in place, including:

- a. Standard Contractual Clauses approved by the European Commission;
- b. The UK International Data Transfer Addendum, where applicable;
- c. Any other transfer mechanism recognized under Applicable Data Protection Law.

11.2 Standard Contractual Clauses. The Parties agree that the Standard Contractual Clauses set forth in **Annex 4** shall apply to transfers of Customer Personal Data to countries outside the EEA, United Kingdom, or Switzerland that are not recognized as providing an adequate level of data protection.

11.3 Data Location. Customer Personal Data may be Processed in the United States and other countries where RevenueHunt or its Sub-processors maintain facilities. A list of data processing locations is included in **Annex 3**.

12. Data Retention and Deletion

12.1 Retention. RevenueHunt shall retain Customer Personal Data for the duration of the Agreement and for such period thereafter as necessary to comply with Applicable Data Protection Law or as otherwise agreed by the Parties.

12.2 Deletion or Return. Upon termination or expiration of the Agreement, or upon the Customer's written request, RevenueHunt shall:

- a. Return Customer Personal Data to the Customer in a commonly used, machine-readable format; or
- b. Delete Customer Personal Data and all copies thereof.

12.3 Deletion Timeline. RevenueHunt shall complete deletion within ninety (90) days of the termination of the Agreement or the Customer's request, except where retention is required by Applicable Data Protection Law.

12.4 Certification. Upon request, RevenueHunt shall provide written certification of the deletion of Customer Personal Data.

13. General Provisions

13.1 Order of Precedence. In the event of any conflict between this DPA and the Agreement, this DPA shall prevail with respect to the Processing of Customer Personal Data.

13.2 Amendment. RevenueHunt may update this DPA from time to time to reflect changes in Applicable Data Protection Law or RevenueHunt's data processing practices. Material changes will be notified to the Customer.

13.3 Severability. If any provision of this DPA is found to be invalid or unenforceable, the remaining provisions shall remain in full force and effect.

13.4 Governing Law. This DPA shall be governed by the laws specified in the Agreement, except that the Standard Contractual Clauses shall be governed by the law of the EU Member State specified therein.

13.5 Term. This DPA shall remain in effect for the duration of the Agreement and shall automatically terminate upon the termination of the Agreement, except that the obligations relating to the deletion of Customer Personal Data shall survive termination.

Annex 1: Details of Processing

A. Categories of Data Subjects

Customer Personal Data may concern the following categories of Data Subjects:

- End users (quiz takers) of the Customer's e-commerce store
- Customer's employees and authorized users
- Customer's business contacts

B. Categories of Personal Data

The following categories of Personal Data may be Processed:

Category	Data Elements
Contact Information	Email address, phone number, first name, last name
Quiz Response Data	Quiz answers, selected choices, preference scores, tags
Commerce Data	Product recommendations, cart contents, order information
Technical Data	IP address, browser type, device type, operating system
Location Data	Country, region, city (derived from IP address)
Marketing Data	UTM parameters, referral source, landing page
Consent Records	Marketing consent status, consent timestamps

C. Special Categories of Personal Data

The Services are not designed to Process special categories of Personal Data (e.g., health data, racial or ethnic origin, religious beliefs). If the Customer configures quizzes to collect such data, the Customer is solely responsible for ensuring a lawful basis for such Processing.

D. Purpose of Processing

Customer Personal Data is Processed for the following purposes:

- Providing the Product Recommendation Quiz services
- Generating personalized product recommendations
- Delivering quiz results to end users

- Syncing Customer Personal Data to Customer's integrated third-party services (e.g., email marketing platforms, CRM systems)
- Analytics and reporting on quiz performance
- Technical support and service improvement
- Compliance with legal obligations

E. Duration of Processing

Customer Personal Data shall be Processed for the duration of the Agreement between RevenueHunt and the Customer.

F. Frequency of Processing

Processing occurs on a continuous basis whenever:

- An end user interacts with the Customer's quiz
- The Customer accesses the RevenueHunt dashboard
- Data is synchronized with integrated third-party services
- Analytics and reports are generated

Annex 2: Technical and Organizational Security Measures

RevenueHunt implements the following technical and organizational measures to protect Customer Personal Data:

A. Access Control

Measure	Description
Authentication	JWT-based authentication with HMAC-SHA256 signing
Multi-Factor Authentication	Required for RevenueHunt employee access to production systems
Role-Based Access	Access to Customer Personal Data limited to personnel who require it
Need-to-Know Principle	Staff access restricted based on job responsibilities
Session Management	Secure session handling with appropriate timeouts

B. Data Protection

Measure	Description
Encryption in Transit	TLS/HTTPS for all data transmissions
Encryption at Rest	Database-level encryption for stored data
API Key Security	Sensitive credentials stored securely and masked in user interfaces
Parameter Filtering	Sensitive data (passwords, tokens, secrets) filtered from logs

C. Network Security

Measure	Description
Firewalls	Network firewalls protecting production infrastructure
Rate Limiting	Protection against abuse (100 requests/minute per IP)
DDoS Protection	Cloud-based DDoS mitigation

D. Infrastructure Security

Measure	Description
Cloud Hosting	Services hosted on Amazon Web Services (AWS)
Data Center Security	AWS data centers with physical security controls
Redundancy	Geographic redundancy and backup systems
Monitoring	Continuous monitoring of infrastructure and services

E. Application Security

Measure	Description
Secure Development	Secure coding practices and code review
Vulnerability Testing	Annual penetration testing and security assessments
Dependency Management	Regular updates to address security vulnerabilities
Error Monitoring	Application error tracking with sensitive data redaction

F. Organizational Measures

Measure	Description
Confidentiality Agreements	All personnel bound by confidentiality obligations
Security Training	Regular security awareness training for staff
Incident Response	Documented incident response procedures
Business Continuity	Disaster recovery and business continuity plans
Vendor Management	Security assessment of Sub-processors

G. Data Subject Rights Support

Measure	Description
Data Export	CSV export functionality for quiz responses
Data Deletion	Account deletion and data redaction capabilities
Consent Management	Integration with Shopify Customer Privacy API
Configurable Tracking	Merchant controls for analytics and pixel tracking

Annex 3: Sub-processors

RevenueHunt engages the following Sub-processors to Process Customer Personal Data:

A. Infrastructure Sub-processors

Sub-processor	Purpose	Location
Amazon Web Services (AWS)	Cloud hosting and infrastructure	United States

B. Integration Sub-processors

The following Sub-processors may Process Customer Personal Data when the Customer enables the respective integration:

Sub-processor	Purpose	Location	Customer-Enabled
Klaviyo	Email marketing integration	United States	Yes
Omnisend	Email marketing integration	United States	Yes
HubSpot	CRM integration	United States	Yes

Sub-processor	Purpose	Location	Customer-Enabled
Zapier	Workflow automation	United States	Yes
Recharge	Subscription management	United States	Yes
Shopify	E-commerce platform	United States/Canada	Yes

C. Analytics and Monitoring Sub-processors

Sub-processor	Purpose	Location
Sentry	Error monitoring and performance	United States
Google Analytics	Analytics (when enabled by Customer)	United States

D. Customer-Configured Sub-processors

Customers may configure additional integrations that transmit Customer Personal Data to third-party services, including:

- Meta (Facebook Pixel)
- TikTok (TikTok Pixel)
- Custom webhook endpoints

The Customer is responsible for ensuring appropriate data processing agreements are in place with any Customer-configured Sub-processors.

E. Sub-processor Updates

The authoritative list of Sub-processors is maintained in this Annex 3. RevenueHunt shall update this DPA when Sub-processors are added or removed, in accordance with Section 6.4 of this DPA.

Customers may subscribe to notifications of Sub-processor changes by contacting info@revenuehunt.com.

Annex 4: Standard Contractual Clauses

A. European Economic Area Transfers

For transfers of Customer Personal Data from the European Economic Area to countries not recognized as providing an adequate level of data protection, the Parties agree to be bound by the Standard Contractual Clauses approved by European Commission Implementing Decision (EU) 2021/914.

Module Two (Controller to Processor) shall apply where the Customer is the Controller and RevenueHunt is the Processor.

Module Three (Processor to Processor) shall apply where the Customer is a Processor acting on behalf of a third-party Controller and RevenueHunt is a Sub-processor.

The following provisions shall apply to the Standard Contractual Clauses:

Clause	Selection
Clause 7 (Docking clause)	Included
Clause 9 (Use of sub-processors)	Option 2: General written authorization
Clause 11 (Redress)	Optional language not included
Clause 17 (Governing law)	Laws of Ireland
Clause 18 (Choice of forum and jurisdiction)	Courts of Ireland

Annex I.A (List of Parties): As set forth in the preamble of this DPA.

Annex I.B (Description of Transfer): As set forth in Annex 1 of this DPA.

Annex I.C (Competent Supervisory Authority): The Irish Data Protection Commission.

Annex II (Technical and Organizational Measures): As set forth in Annex 2 of this DPA.

B. United Kingdom Transfers

For transfers of Customer Personal Data from the United Kingdom, the Parties agree to be bound by the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (Version B.1.0) issued by the UK Information Commissioner's Office.

The following provisions shall apply:

Table	Selection
Table 1 (Parties)	As set forth in the preamble of this DPA
Table 2 (SCCs, Modules and Clauses)	Module Two or Module Three as applicable
Table 3 (Appendix Information)	As set forth in Annexes 1, 2, and 3 of this DPA
Table 4 (Ending the Addendum)	Neither Party may end the Addendum

C. Switzerland Transfers

For transfers of Customer Personal Data from Switzerland, the Standard Contractual Clauses shall apply with the following modifications:

- References to “Regulation (EU) 2016/679” shall be interpreted as references to the Swiss Federal Act on Data Protection (FADP);
- References to “EU”, “Union”, and “Member State” shall not be interpreted to exclude Data Subjects in Switzerland;
- The competent supervisory authority shall be the Swiss Federal Data Protection and Information Commissioner.

Contact Information

For questions about this DPA or to exercise rights under this DPA, please contact:

Dairy Capital Limited Email: info@revenuehunt.com Website: https://revenuehunt.com

For Data Protection inquiries: Email: info@revenuehunt.com

This Data Processing Agreement is effective as of the date the Customer agrees to the Terms of Service or, for existing Customers, upon publication of this DPA.