BrandPay Data Processing Addendum

This Data Processing Addendum (the “DPA”) forms part of the agreement between True Ample Limited (Hong Kong company no. 3065248), trading as BrandPay (“BrandPay”) and the customer named in that agreement (the “Customer”) for the BrandPay platform (the “Agreement”). It applies automatically when the Customer accepts the Agreement and applies for as long as BrandPay processes Customer Personal Data. A countersigned copy is available on request at privacy@brandpay.io.

1. Definitions

1.1 “Applicable Data Protection Law” means the laws on the protection of personal data that apply to the processing under this DPA, including the UK GDPR, the Data Protection Act 2018, Regulation (EU) 2016/679 (“EU GDPR”) and the Australian Privacy Act 1988 (Cth).

1.2 “Customer Personal Data” means personal data that BrandPay processes on behalf of the Customer as a processor, as described in Annex I.

1.3 “Sub-processor” means a third party engaged by BrandPay to process Customer Personal Data. “Security Incident” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data.

1.4 “Standard Contractual Clauses” means the clauses annexed to European Commission Implementing Decision (EU) 2021/914. “UK Addendum” means the International Data Transfer Addendum to the Standard Contractual Clauses, version B1.0, issued by the UK Information Commissioner under section 119A of the Data Protection Act 2018.

1.5 “Controller”, “processor”, “data subject”, “personal data” and “processing” have the meanings given in Applicable Data Protection Law.

2. Roles and scope

2.1 For Customer Personal Data, the Customer is the controller (or, where it acts for another controller, a processor) and BrandPay is the processor (or sub-processor).

2.2 BrandPay is an independent controller, not a processor, for personal data of consumers who register for and take part in BrandPay rewards, including account, social account verification, reward participation, redemption, device, location and fraud prevention data. BrandPay processes that data under its Privacy Policy and shares it with participating merchants as that policy describes. Each party complies with Applicable Data Protection Law for the personal data it controls. This DPA does not apply to that data, except clause 7 where a transfer to BrandPay occurs.

2.3 Annex I describes the subject matter, nature, purpose and duration of the processing, the types of personal data and the categories of data subjects.

3. Instructions

3.1 BrandPay processes Customer Personal Data only on the Customer's documented instructions, which are the Agreement, this DPA, and the Customer's use and configuration of the platform, unless required by law to do otherwise. In that case BrandPay informs the Customer before processing unless the law prohibits this.

3.2 BrandPay tells the Customer without undue delay if it believes an instruction infringes Applicable Data Protection Law. BrandPay may suspend the instruction until the Customer confirms or amends it.

4. Confidentiality

4.1 BrandPay ensures that everyone authorised to process Customer Personal Data, including contractors, is bound by a duty of confidentiality and has access only to the extent needed to provide the services.

5. Security

5.1 BrandPay implements and maintains the technical and organisational measures in Annex II, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing.

5.2 BrandPay may update those measures, provided it does not materially reduce the overall level of security.

6. Sub-processors

6.1 The Customer gives BrandPay general written authorisation to engage Sub-processors. The current list is published at #subprocessors of the BrandPay privacy page, and forms Annex III.

6.2 BrandPay gives at least 30 days' notice of any addition or replacement of a Sub-processor, by email to subscribers of the update list and by updating the published list. The Customer can subscribe at any time using the form on that page. Where a Sub-processor itself gives BrandPay less than 30 days' notice of a change, BrandPay passes the notice on within seven days of receiving it.

6.3 The Customer may object on reasonable grounds relating to data protection, in writing within 30 days of the notice. The parties then discuss the objection in good faith. If it is not resolved, the Customer may terminate the affected services by written notice and BrandPay refunds prepaid fees for the period after termination. This is the Customer's sole remedy for an objection.

6.4 BrandPay may replace a Sub-processor at short notice where needed to protect the security or availability of the services, and gives notice as soon as reasonably practicable.

6.5 BrandPay has a written agreement with each Sub-processor that requires it to protect Customer Personal Data to a standard no less protective than this DPA, and remains liable to the Customer for the Sub-processor's performance.

7. International transfers

7.1 BrandPay is based in Hong Kong and its hosting and personnel are in several countries, including Indonesia, Singapore, India, Sri Lanka, the United Kingdom and Vietnam. The Customer authorises these transfers, subject to this clause.

7.2 Where Applicable Data Protection Law requires a transfer mechanism for Customer Personal Data transferred by the Customer to BrandPay, the Standard Contractual Clauses are incorporated and apply as follows: Module Two (controller to processor), or Module Three (processor to processor) where the Customer acts as a processor; clause 7 (docking clause) does not apply; in clause 9(a) Option 2 (general written authorisation) applies with the notice period in clause 6.2; the optional wording in clause 11 does not apply; in clause 17 the law of Ireland governs; in clause 18(b) the courts of Ireland have jurisdiction; and for clause 13 the competent supervisory authority is the one that supervises the Customer. Annexes I to III to the Standard Contractual Clauses are Annexes I to III to this DPA.

7.3 For transfers subject to the UK GDPR, the UK Addendum is incorporated. Table 1 to 3 information is in this DPA and its Annexes, and in Table 4 neither party may end the UK Addendum when it changes. The UK Addendum is governed by the law of England and Wales.

7.4 BrandPay transfers Customer Personal Data to Sub-processors outside the UK and the European Economic Area only under a mechanism that Applicable Data Protection Law recognises, such as an adequacy decision, the EU-US Data Privacy Framework (and its UK Extension), the Standard Contractual Clauses or the UK International Data Transfer Agreement. The Sub-processor list states the mechanism for each.

7.5 If the Standard Contractual Clauses or the UK Addendum conflict with this DPA or the Agreement, they prevail.

8. Assistance

8.1 BrandPay forwards to the Customer, within five business days, any request it receives from a data subject about Customer Personal Data, and does not respond other than to say it has passed the request on, unless instructed.

8.2 Taking into account the nature of the processing, BrandPay assists the Customer with appropriate technical and organisational measures to respond to data subject requests, and with its obligations on security, breach notification, data protection impact assessments and prior consultation, so far as these relate to Customer Personal Data. BrandPay may charge reasonable costs for assistance that goes beyond what the platform provides.

9. Security Incidents

9.1 BrandPay notifies the Customer without undue delay, and in any case within 72 hours, after becoming aware of a Security Incident affecting Customer Personal Data.

9.2 The notice describes, as far as known, the nature of the incident, the categories and approximate numbers of data subjects and records, the likely consequences, and the measures taken or proposed. BrandPay provides further information as it becomes available and takes reasonable steps to contain and remediate the incident.

10. Deletion and return

10.1 On termination or expiry of the Agreement, or on the Customer's request, BrandPay deletes Customer Personal Data within 30 days, or returns it on request, unless the law requires it to be kept. Merchant-order data, such as Shopify order line items, is deleted when the Customer leaves the platform.

10.2 Copies in backups are deleted in the ordinary backup cycle. Until then BrandPay continues to protect them under this DPA and does not use them.

11. Information and audit

11.1 BrandPay makes available the information reasonably necessary to show compliance with this DPA, including a completed security questionnaire once in any 12 months and, on request, the available audit reports and certifications of its Sub-processors.

11.2 Where that is not enough, or where a regulator or the Standard Contractual Clauses require it, the Customer may audit BrandPay's compliance on 30 days' written notice, during business hours, no more than once a year (unless a Security Incident or regulator requires otherwise), subject to confidentiality, and at the Customer's cost.

12. Liability

12.1 Each party's liability under this DPA is subject to the limits and exclusions of liability in the Agreement.

12.2 Nothing in this DPA limits either party's liability to data subjects under the Standard Contractual Clauses or Applicable Data Protection Law, or any liability that cannot lawfully be limited.

13. Term, precedence and law

13.1 This DPA continues for as long as BrandPay processes Customer Personal Data. Clauses that by nature survive, including 10 and 12, continue after that.

13.2 If there is a conflict, the Standard Contractual Clauses and the UK Addendum prevail over this DPA, and this DPA prevails over the Agreement on the processing of personal data. BrandPay may update this DPA to reflect changes in law or in the mechanisms in clause 7, giving 30 days' notice.

13.3 This DPA is governed by the law that governs the Agreement, except that the Standard Contractual Clauses and the UK Addendum are governed as stated in clause 7.

13.4 Questions about this DPA go to privacy@brandpay.io. BrandPay has not appointed a data protection officer; this contact is its privacy contact.

Annex I. Description of the processing

A. Parties

Data exporter: the Customer named in the Agreement (controller, or processor where it acts for another controller). Contact details are in the Agreement.

Data importer: True Ample Limited (Hong Kong company no. 3065248), trading as BrandPay, 6/F, 44 Wyndham Street, Central, Hong Kong SAR, China (processor or sub-processor). Contact: privacy@brandpay.io.

B. Description of processing

Data subjects: the Customer's staff who use the platform; the Customer's end customers whose purchase or gift card data is made available through the Customer's connected store, point of sale or loyalty system.

Types of personal data: name, email address, phone number, user account details, order and transaction data (such as order line items, gift card codes and redemption records). No special category data is intended to be processed.

Frequency: continuous, for as long as the Customer uses the platform.

Nature and purpose: hosting, storage, retrieval, matching and display of the data to deliver rewards, redemption and reporting for the Customer, and deletion.

Retention: for the term of the Agreement. Merchant-order data is deleted when the Customer leaves the platform, and other Customer Personal Data within 30 days after termination (clause 10).

Sub-processors: as listed in Annex III, for hosting, storage, email and message delivery, authentication, payment collection and monitoring.

C. Competent supervisory authority

For the Standard Contractual Clauses: the authority that supervises the Customer. For the UK Addendum: the UK Information Commissioner's Office.

Annex II. Technical and organisational measures

- Access control. Staff sign in to core systems with accounts on the company domain. Multi-factor authentication is required for staff access to Google Workspace, Supabase, Cloudflare, Stripe, Postmark, Mixpanel, GitHub, Bitbucket, Jira and Apollo, and sign-in to Sentry is through company Google accounts. All other tools, including analytics, workflow and monitoring tools sit behind Cloudflare Access and admit company accounts only.

- Least privilege. Access rights are reviewed and reduced where excessive. For example, owner roles on our authentication platform were reduced from five to one in October 2026, and expired invitations and former staff logins are removed.
- Authentication of platform users. Sign-in uses one-time codes sent by email, WhatsApp or SMS. Repeated wrong codes trigger a temporary lockout.
- Encryption. Traffic to our services is encrypted in transit. Our hosting providers encrypt stored data by default.
- Payments. Card details are entered on Stripe-hosted pages. BrandPay does not receive full card numbers for merchant payments.
- Monitoring and data minimisation. We monitor errors and performance with Sentry and Grafana. Error monitoring is configured not to receive IP addresses, cookies, request headers, names, email addresses, social handles, location or login codes. Session recordings are made only when an error occurs, with text, inputs and images masked.
- Sub-processor management. We keep a register of vendors, hold a data processing agreement with each Sub-processor, and check its transfer mechanism and data location before use.
- AI tools. Where we use AI services on personal data, we use business accounts with model training turned off and a data processing agreement in place.
- Personnel. Everyone with access to Customer Personal Data is bound by confidentiality obligations.
- Hosting. Production data is hosted on Google Cloud in Jakarta, Indonesia, with other systems in Singapore. Physical security of data centres is provided by our hosting providers.

Annex III. Sub-processors

See the sub-processor table on the BrandPay privacy page.