

Data Processing Agreement

Shopmark — version 2.1, effective October 6, 2026

This Data Processing Agreement (“DPA”) forms part of the agreement between Shopmark, Inc., with its principal place of business at 838 Walker Road Suite 21-2, Dover, DE 19904 (“Shopmark”), and the merchant that installs or uses the Shopmark application (“Customer”), consisting of the Shopmark Terms of Service, the Shopify App Store listing and any order or plan selected in-app (together, the “Agreement”). It applies whenever Shopmark processes Personal Data on behalf of Customer in providing the Service. In the event of a conflict between this DPA and the Agreement, this DPA prevails with respect to the processing of Personal Data.

This DPA is incorporated into the Agreement and is accepted by Customer on installing or using the Service; no signature is required for it to take effect. The current version is published at <https://shopmark.app/dpa>; questions go to support@shopmark.app.

1. Definitions

1.1 “Data Protection Laws” means all laws applicable to the processing of Personal Data under the Agreement, including the EU General Data Protection Regulation 2016/679 (“GDPR”), the UK GDPR and Data Protection Act 2018, the Swiss Federal Act on Data Protection, and the California Consumer Privacy Act as amended by the California Privacy Rights Act (“CCPA”) and comparable U.S. state privacy laws.

1.2 “Personal Data” means any information relating to an identified or identifiable natural person that Shopmark processes on behalf of Customer under the Agreement. “Customer Data” means all data Customer provides to the Service, or that Shopmark obtains on Customer's behalf in providing the Service, including Personal Data.

1.3 “Service” means the Shopmark application and related services for detecting and acting on unauthorised use of Customer's brand, storefront and product content.

1.4 “Sub-processor” means a third party engaged by Shopmark to process Personal Data on Customer's behalf. “SCCs” means the Standard Contractual Clauses approved by European Commission Decision 2021/914, and the UK International Data Transfer Addendum issued by the UK Information Commissioner.

1.5 “Controller”, “Processor”, “Data Subject”, “processing”, “Personal Data Breach” and “Supervisory Authority” have the meanings given in the GDPR; “Business”, “Service Provider”, “Sell” and “Share” have the meanings given in the CCPA.

1.6 “Confidential Schedules” means the detailed descriptions of Shopmark's security measures and Sub-processors that supplement Annexes 2 and 3. They contain proprietary information about how the Service works and are provided to Customer on request after installation, under the confidentiality terms of the Agreement.

2. Roles and scope

2.1 Customer is the Controller (or, where Customer acts for another controller, a Processor) and Business; Shopmark is a Processor and Service Provider. Shopify Inc., which operates the platform on which the Service is installed, is Customer's own processor under Customer's agreement with Shopify and is not a Sub-processor of Shopmark.

2.2 The subject matter, duration, nature and purpose of processing, and the categories of Data Subjects and Personal Data, are set out in Annex 1.

2.3 Shopmark processes Personal Data only on Customer's documented instructions. The Agreement, Customer's configuration of the Service and this DPA constitute Customer's complete instructions. Shopmark may also process Personal Data where required by applicable law, in which case it will inform Customer of that requirement before processing unless the law prohibits it. Shopmark will inform Customer if, in its opinion, an instruction infringes Data Protection Laws, and may suspend the affected processing until the instruction is confirmed or amended.

2.4 The Service accesses product and theme information from Customer's Shopify store under the permissions granted at installation. It does not access the personal data of Customer's own customers.

3. Shopmark's obligations

3.1 Confidentiality. Shopmark ensures that every person it authorises to process Personal Data is bound by a contractual or statutory duty of confidentiality and processes Personal Data only as instructed.

3.2 Security. Shopmark implements and maintains the technical and organisational measures in Annex 2, which Customer has reviewed and accepts as appropriate to the risk, taking into account the state of the art, the costs of implementation and the nature of the processing. Shopmark may update these measures provided the overall level of protection is not reduced.

3.3 Personal Data Breach. Shopmark will notify Customer without undue delay, and in any case within 72 hours, after becoming aware of a Personal Data Breach affecting Customer's Personal Data. The notice will describe the nature of the breach, the categories and approximate number of Data Subjects and records concerned, the likely consequences, and the measures taken or proposed. Shopmark will provide further information as it becomes available and reasonable assistance with Customer's own notification obligations.

3.4 Data Subject requests. Taking into account the nature of the processing, Shopmark will assist Customer by appropriate technical and organisational measures in responding to requests from Data Subjects to exercise their rights. If Shopmark receives such a request directly, it will refer the Data Subject to Customer (unless legally prohibited) and will not respond on Customer's behalf without Customer's instruction.

3.5 Assistance. Shopmark will provide reasonable assistance with data protection impact assessments and prior consultations with Supervisory Authorities, to the extent required by Articles 35 and 36 GDPR and in light of the information available to Shopmark.

3.6 Records and audits. Shopmark will make available the information reasonably necessary to demonstrate compliance with this DPA, including the Confidential Schedules, and will answer Customer's reasonable written security questionnaires. Where this is insufficient to satisfy a legal requirement, Customer (or an independent auditor bound by confidentiality) may audit Shopmark's relevant controls once in any twelve-month period, on 30 days' written notice, during business hours, in a manner that does not unreasonably disrupt Shopmark's business, and at Customer's expense unless the audit reveals a material breach of this DPA.

4. Sub-processors

4.1 Customer authorises Shopmark to engage Sub-processors in the categories listed in Annex 3. The current list of Sub-processors is a Confidential Schedule provided to Customer on request. Shopmark imposes on each Sub-processor data protection obligations no less protective than those in this DPA, and remains liable to Customer for the performance of its Sub-processors' obligations.

4.2 Shopmark will give Customer at least 30 days' notice by email before authorising a new Sub-processor to process Personal Data. Customer may object on reasonable, documented data protection grounds within

that period. The parties will cooperate in good faith to resolve the objection; if they cannot, Customer may terminate the affected part of the Service, or the Agreement, without penalty and receive a pro-rated refund of prepaid fees for the terminated portion.

5. International transfers

5.1 Shopmark is established in the United States and processes Personal Data there. To the extent Personal Data originating in the European Economic Area, the United Kingdom or Switzerland is transferred to a country without an adequacy decision, the parties agree that the SCCs (Module Two, controller-to-processor, or Module Three where Customer is a processor) are incorporated into this DPA by reference, with: Clause 7 (docking) included; Option 2 of Clause 9 with the 30-day notice period in Section 4.2; Clause 11 optional language omitted; Clause 13 and Clause 17 governed by the law of Ireland and Clause 18 by the courts of Ireland; Annexes I and II completed by Annex 1 and Annex 2 of this DPA; and Annex III by Annex 3 together with the Sub-processor Confidential Schedule. For UK transfers the UK Addendum applies with the parties' details completed as above; for Swiss transfers references to the GDPR are read as references to the Swiss FADP and the competent authority is the Swiss FDPIC.

5.2 Where a Sub-processor is certified under the EU–U.S. Data Privacy Framework, the UK Extension or the Swiss–U.S. DPF, Shopmark may rely on that certification for the onward transfer.

6. CCPA and U.S. state privacy laws

6.1 Shopmark is a Service Provider. Shopmark will not: (a) Sell or Share Personal Data; (b) retain, use or disclose Personal Data for any purpose other than the business purposes specified in Annex 1, including outside the direct business relationship with Customer; (c) retain, use or disclose Personal Data outside the direct business relationship between Shopmark and Customer; or (d) combine Personal Data with personal information it receives from another source, except as permitted for Service Providers by the CCPA regulations.

6.2 Shopmark certifies that it understands the restrictions in Section 6.1 and will comply with them, will notify Customer if it determines it can no longer meet its obligations under the CCPA, will provide the same level of privacy protection as the CCPA requires of Customer, and grants Customer the right to take reasonable steps to stop and remediate unauthorised use of Personal Data.

7. Return and deletion

7.1 Customer may delete Personal Data at any time from within the Service, and may delete all Customer Data by uninstalling the Service. Shopmark deletes Customer Data within 30 days of uninstallation or of Customer's written request, and from backups within a further 30 days, unless retention is required by law. Notices already delivered to third parties on Customer's behalf remain with those recipients.

8. General

8.1 This DPA takes effect when Customer installs or first uses the Service (or on the date above for Customers already using it) and continues until Shopmark has deleted all Personal Data in accordance with Section 7.

8.2 Each party's liability under this DPA is subject to the limitations and exclusions of liability in the Agreement, which apply in aggregate across the Agreement and this DPA. Nothing in this DPA limits either party's liability to Data Subjects or Supervisory Authorities where such limitation is prohibited by Data Protection Laws.

8.3 This DPA is governed by the law governing the Agreement, Delaware, except where Section 5 provides otherwise. Shopmark may update this DPA to reflect changes in Data Protection Laws or the Service, provided the changes do not reduce the protections for Personal Data; material changes will be notified 30 days in advance.

8.4 The Confidential Schedules are Shopmark's confidential information. Customer may use them only to assess Shopmark's compliance with this DPA and Data Protection Laws, may share them with its advisers and auditors bound by confidentiality, and may not publish them or use them for any other purpose.

Annex 1 — Details of processing

Item	Description
Subject matter	Provision of the Service: detecting unauthorised use of Customer's brand, storefront and product content, and supporting Customer's enforcement against it.
Duration	The term of the Agreement, plus the deletion period in Section 7.
Nature and purpose	Collecting, storing, analysing and reporting information about Customer's store and about websites and listings suspected of infringing Customer's rights; preparing and delivering enforcement notices on Customer's behalf; and communicating with Customer about the Service.
Categories of Data Subjects	Customer's personnel and authorised users of the Service; Customer's designated rights-holder contact; and operators of websites and listings suspected of infringing Customer's rights.
Categories of Personal Data	Merchant Data: name, business name, email address, telephone number, business address and store identifiers. Enforcement Data: names, business and contact details, domain and hosting records, and correspondence relating to suspected infringers, obtained from publicly available sources and from the parties themselves. Technical Data: standard web request information relating to suspected infringing sites.
Special categories	None.
Frequency	Continuous, for the term of the Agreement.

Annex 2 — Technical and organisational measures

Shopmark maintains the following measures. The specific technologies, providers and configurations used to implement them are proprietary and are described in the Security Confidential Schedule, available to Customer on request.

- **Infrastructure.** The Service is hosted on managed infrastructure from a major cloud provider. Each customer's data is logically segregated and accessible only through authenticated requests scoped to that customer.
- **Encryption.** Data is encrypted in transit and at rest. Credentials and access tokens are held in a managed secrets store.
- **Access control.** Access to production systems is limited to named personnel on a least-privilege basis and protected by multi-factor authentication.
- **Data minimisation.** The Service collects and retains the data needed to provide it, and requests only the Shopify permissions it requires. Network addresses received by the Service are pseudonymised before storage.

- **Sub-processor controls.** Each Sub-processor is bound by written data protection terms and receives only the data needed for its purpose. AI providers are contractually prohibited from using Customer Data to train models.
- **Logging and monitoring.** Operational logs are retained for a short rolling window. Changes to records in the Service are recorded in an audit trail.
- **Backups and resilience.** Production data is backed up with point-in-time recovery, and stored evidence is replicated by the provider.
- **Deletion.** Customer Data is deleted in accordance with Section 7.
- **Secure development.** Source code is kept in a private repository; changes are reviewed and tested before deployment; dependencies are kept up to date; secrets are never committed to source control.
- **Incident response.** Security incidents are triaged, contained and notified to affected customers under Section 3.3, followed by a post-incident review.

Storefront scripts. Where the Service places a script on Customer's storefront, it serves only to detect unauthorised copies of the storefront. It does not collect information about Customer's visitors on Customer's own domains.

Annex 3 — Sub-processors

Shopmark engages Sub-processors in the following categories, established in the United States and bound by written data processing terms, SCCs and, where applicable, Data Privacy Framework certification. The named providers are listed in the Sub-processor Confidential Schedule, provided to Customer on request after installation and updated under Section 4.2.

Category	Purpose	Personal Data involved
Cloud infrastructure	Hosting, storage and processing	Merchant Data, Enforcement Data and Technical Data (Annex 1)
AI and analysis provider	Automated analysis and document drafting	Enforcement Data; product content; rights-holder contact details
Image search provider	Image matching	Product images
Email delivery provider	Email delivery and receipt	Merchant Data; rights-holder contact details; message content

Shopify Inc. is Customer's platform provider, not a Sub-processor of Shopmark.