SURECART

Data Processing Agreement — SureCart Inc.

SureCart · October 2026

Effective date: 26 October 2026

Subject to the SureCart Terms and Conditions (the "Terms" or "Principal Agreement"), SureCart Inc. ("SureCart") processes Personal Data on behalf of merchants who use SureCart to run their online stores ("You", "Merchant" or "Customer"). For that data, SureCart acts as the processor and the Customer acts as the controller under applicable Data Protection Laws. That Personal Data is referred to as "Controller Data", as further described below.

> **Effective date and acceptance.** This DPA forms part of the Terms and is incorporated into them by reference. It applies to all merchants who use SureCart under the Terms, on every plan, with no separate signature and no paid upgrade required. For merchants with an existing account, this DPA takes effect on the effective date shown above, and continued use of the services after that date constitutes acceptance. For new merchants, it takes effect when they accept the Terms. SureCart may update this DPA as described in Section 12.2.

"Data Protection Laws" means all privacy, security and data protection laws and regulations that apply to the Controller Data processed by SureCart under this DPA, including, as applicable, the GDPR, Member State laws implementing the GDPR, the UK GDPR, Swiss DP Law, the California Consumer Privacy Act of 2018 as amended by the California Privacy Rights Act of 2020 (the "CCPA"), the Brazilian General Data Protection Law ("LGPD"), and India's Digital Personal Data Protection Act, 2023, each as amended.

"GDPR" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

"Personal Data" means any information relating to an identified or identifiable natural person, or that is otherwise deemed personal information or personal data (or similar terms) under Data Protection Laws. This includes IP addresses, cookie identifiers, device identifiers and other online identifiers.

"End Customer" means a natural person who browses, buys from, subscribes to, or holds an account with a Customer's store, or who joins a Customer's affiliate programme.

This Data Processing Agreement ("DPA") sets out SureCart's obligations and rights as a processor of Controller Data, and those of the Customer as controller. Everything else is governed by the Principal Agreement.

Out of scope: data SureCart processes as a controller is covered by the SureCart Privacy Policy, not this DPA. That includes merchant and affiliate account data, surecart.com website and marketing data, and optional SureCart Analytics usage data sent from the WordPress plugin.

Terms of the DPA

1. Role of the Parties

1.1 For the processing of Controller Data, SureCart is the processor and the Customer is the controller. References to "processor" and "controller" include any analogous terms under Data Protection Laws (for example, "service provider" and "business" under the CCPA).

1.2 Where SureCart uses Controller Data for its own limited purposes permitted by Data Protection Laws, namely fraud prevention, security of the services, and service improvement using aggregated or de-identified data, SureCart acts as an independent controller for those purposes only, as described in the SureCart Privacy Policy.

2. Scope of Processing

2.1 SureCart shall process Controller Data on behalf of, and in accordance with, the Customer's instructions as specified in Section 2.4. If SureCart is legally required to process Controller Data for another purpose, it will inform the Customer of that requirement unless the law prohibits it.

2.2 SureCart certifies that it will not:

(a) collect, retain, use, disclose or otherwise process Controller Data for any purpose other than performing the services for the Customer;

(b) collect, retain, use or disclose Controller Data for a commercial purpose other than providing the services to the Customer;

(c) process Controller Data outside the direct business relationship between the Customer and SureCart;

(d) combine Controller Data with other personal data SureCart collects, other than as expressly permitted for processors under Data Protection Laws; or

(e) “sell” or “share” (each as defined by the CCPA) Controller Data.

2.3 SureCart processes Controller Data to provide its hosted ecommerce platform to Customers, including checkout, payments orchestration, subscriptions, orders, customer portal, shipping, tax and affiliate features. Controller Data relates to End Customers and the Customer’s own team members. The types of Controller Data and the duration of processing are set out in Schedule 1.

2.4 The Customer’s instructions are, in principle, conclusively set out in this DPA and in the Customer’s configuration of its store. Instructions that deviate from this DPA or impose additional requirements require SureCart’s written agreement. SureCart will promptly inform the Customer if, in its opinion, an instruction infringes Data Protection Laws.

2.5 The Customer shall comply with its obligations under Data Protection Laws and is responsible for the lawfulness of the processing, including providing notices to and obtaining any consents from End Customers. If a third party asserts a claim against SureCart based on unlawful processing of Controller Data or another violation of Data Protection Laws by the Customer, the Customer shall release SureCart from that claim.

2.6 The Customer shall not submit special categories of personal data (Article 9 GDPR) or criminal-offence data through the services. The Customer shall not submit full payment card numbers or card security codes to SureCart other than through the payment fields provided by its connected payment processor.

2.7 The Customer agrees that SureCart may de-identify or aggregate Controller Data so that it does not identify a natural person, and use it in that form to develop, improve and provide the services. Where such data is “deidentified” under Data Protection Laws, SureCart will take reasonable measures to ensure it cannot be associated with a natural person and will keep it in that form. Data de-identified or aggregated under this Section is no longer Controller Data.

3. Personnel Requirements

3.1 SureCart shall require all personnel engaged in processing Controller Data to keep it confidential.

3.2 SureCart shall ensure that natural persons acting under its authority who have access to Controller Data process it only on SureCart’s instructions.

4. Security of Processing

4.1 SureCart shall implement appropriate technical and organisational measures to protect Controller Data, taking into account the state of the art, implementation costs, the nature, scope, context and purposes of processing, and the likelihood and severity of risk to data subjects.

4.2 SureCart shall establish before processing begins, and maintain throughout the term, the measures in Schedule 2.

4.3 SureCart may modify those measures during the term, provided the modifications do not materially reduce the overall level of protection for Controller Data.

5. Sub-processors

5.1 The Customer authorises SureCart to engage sub-processors to provide the services. No authorisation is required for service providers that only examine or maintain data processing systems, even if access to Controller Data cannot be excluded, provided SureCart takes reasonable steps to protect its confidentiality.

5.2 SureCart shall publish its current sub-processor list at the URL in Schedule 3 and give notice there of any intended addition or replacement. The Customer may object only for important, substantiated reasons. If the Customer does not object within 14 days of the notice date, its right to object to that engagement lapses. If the Customer objects, SureCart may terminate the Principal Agreement on reasonable notice.

5.3 SureCart shall impose on each sub-processor data protection obligations no less protective than those in this DPA. Before transferring Controller Data to a sub-processor outside the European Economic Area, SureCart shall ensure appropriate transfer safeguards are in place.

5.4 SureCart is not a payment processor. Third-party services the Customer connects to its store under its own account and agreement, such as payment processors, email marketing tools, CRMs, learning platforms and webhook endpoints, are engaged by the Customer, not SureCart. SureCart transmits Controller Data to them only on the Customer’s instruction and is not responsible for their processing.

6. Support Obligations

6.1 SureCart shall assist the Customer in meeting its obligations under Data Protection Laws, including, as applicable, Article 28 GDPR.

6.2 End Customers are directed to contact the Customer first to exercise their rights. If SureCart receives such a request directly, it will refer the requester to the Customer where identifiable. The Customer will inform SureCart of any request it needs help with and provide the necessary information. SureCart shall then reasonably support the

Customer, including through dashboard and API tools for access, correction, export and deletion.

6.3 SureCart shall notify the Customer without undue delay after becoming aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Controller Data (a "Security Incident"). The notice shall describe, to the extent known:

(a) the nature of the Security Incident, including where possible the categories and approximate number of data subjects and records affected;

(b) its likely consequences; and

(c) the measures taken or proposed to address it and, where appropriate, to mitigate its possible adverse effects.

6.4 This information may be provided in phases as it becomes available. Where the Customer must inform supervisory authorities or data subjects, SureCart shall assist on request.

6.5 SureCart will take appropriate steps to remediate the cause of a Security Incident and use commercially reasonable efforts to cooperate with the Customer's investigation and remediation.

7. Deletion and Return of Controller Data

7.1 Until termination, the Customer may export Controller Data through the SureCart dashboard or API.

7.2 Within 30 days after the Customer deletes its store or the Principal Agreement terminates, SureCart shall delete all Controller Data, unless law requires SureCart to retain it. Residual copies in backups are overwritten on SureCart's rolling 30–90-day backup cycle and are not restored to active systems in the meantime.

7.3 Nothing in this Section requires deletion of data that has been de-identified or aggregated under Section 2.7.

8. Evidence and Audits

8.1 SureCart shall process Controller Data in line with this DPA, comply with its obligations as a processor under Data Protection Laws, and provide the level of privacy protection those laws require. SureCart shall notify the Customer within five business days after determining that it can no longer meet its obligations under the CCPA.

8.2 SureCart shall document its implementation of this DPA and provide appropriate evidence at the Customer's reasonable request.

8.3 At the Customer's reasonable request, SureCart shall demonstrate compliance by providing a report from an independent auditor or a suitable IT security or data protection certification relating to its processing systems.

9. Transfer of Controller Data

SureCart's primary servers are in the United States, and Controller Data may also be accessed from India. When Controller Data is transferred outside the European Union, the United Kingdom or Switzerland, SureCart will rely on the mechanisms below, in this order.

9.1 **Data Privacy Framework.** SureCart Inc. is certified under the EU-U.S. Data Privacy Framework, the UK Extension and the Swiss-U.S. Data Privacy Framework. Transfers to SureCart in the United States rely on that certification while it remains valid.

9.2 **EU Standard Contractual Clauses.** For transfers from the EU to a Third Country not covered by Section 9.1 or an adequacy decision, the parties agree to the Standard Contractual Clauses as set out in Schedule 4. "Standard Contractual Clauses" means the clauses adopted by Commission Implementing Decision (EU) 2021/914 of 4 June 2021. "Third Country" means a country the EU has not recognised as providing an adequate level of protection.

9.3 **UK Addendum.** For transfers subject to the UK GDPR, the parties agree to the UK Addendum as set out in Schedule 4. "UK Addendum" means the International Data Transfer Addendum to the Standard Contractual Clauses issued by the UK Information Commissioner, in force 21 March 2022. "UK GDPR" means the GDPR as incorporated into UK law by the Data Protection Act 2018, as amended.

9.4 **Swiss transfers.** For transfers subject to Swiss DP Law, the parties agree to the Standard Contractual Clauses with the Swiss modifications in Schedule 4. "Swiss DP Law" means the Swiss Federal Act on Data Protection, as amended.

9.5 If the mechanism relied on is invalidated, SureCart will move to the next applicable mechanism without the need for further agreement.

10. Liability

10.1 Each party's liability under this DPA is subject to the limitations in the Principal Agreement, except where Data Protection Laws do not permit such limitation with respect to data subject rights.

11. Term

11.1 This DPA remains in force for as long as SureCart processes Controller Data on the Customer's behalf under the Principal Agreement.

11.2 Provisions that by their nature should survive termination, including Sections 7, 9 and 12, survive.

12. General

12.1 This DPA is governed by the laws of the State of Delaware, United States, except where Data Protection Laws require otherwise. The parties submit to the exclusive jurisdiction of the Delaware courts, except as required by the Standard Contractual Clauses in Schedule 4.

12.2 This DPA may be amended only by a written instrument signed by both parties, or by SureCart updating it on its legal page with at least 30 days' prior notice.

12.3 If any provision is held unenforceable, the remaining provisions stay in full force.

12.4 This DPA, its Schedules and the Principal Agreement are the entire agreement on processing Controller Data and supersede prior agreements on the same subject. If this DPA conflicts with the Principal Agreement on data protection, this DPA prevails; if it conflicts with the Standard Contractual Clauses, the Clauses prevail.

Schedule 1 — Processing Details

This Schedule sets out the specifics of processing Controller Data, as required by Article 28(3) GDPR.

1A. SureCart Merchant Stores

Processor: SureCart Inc. · Servers: United States

Field	Detail
Subject matter	Operation of the SureCart hosted ecommerce platform for the Customer's store: checkout, payments orchestration, one-time and subscription billing, orders, invoices, refunds, customer portal, shipping and fulfilment, tax calculation, product reviews, and transactional email.
Nature of processing	Collection, storage, use, transmission to Customer-connected services, and deletion of End Customer data on behalf of the Customer.
Purposes	Processing checkouts and orders; passing payment details to the Customer's connected payment processor; managing subscriptions, renewals and dunning; providing the customer portal; calculating US sales tax and shipping rates; generating shipping labels; generating PDF receipts and invoices; moderating merchant-customised email templates; sending order, receipt and subscription emails; fulfilment and download delivery; fraud and abuse screening; support at the Customer's request.
Types of Personal Data	Contact data: name, email address, phone number, billing and shipping addresses, business name and tax ID where provided. Order data: products purchased, prices, discounts, order and subscription history, invoices, refunds. Payment data: payment method type, last four digits, card brand and expiry, and processor tokens. Full card numbers and card security codes are never received or stored by SureCart. Technical data: IP address, browser and device data captured at checkout for fraud prevention and tax location. Customer portal login credentials. Product reviews and any custom checkout fields the Customer configures.
Categories of data subjects	End Customers (shoppers, buyers, subscribers, and customer-portal users). The Customer's own staff who use the dashboard.
Retention	Store data: for the life of the store, then deleted within 30 days of store deletion or termination (Section 7). Order and transaction records: up to 7 years where required for accounting and tax, unless the Customer deletes the store earlier. Security logs: 12 months. Backups: 30–90 days rolling.
Controller responsibility	The Customer is responsible for the lawful basis for processing End Customer data, for its own store privacy notice, and for consent to any marketing it sends.

Merchant Stores Note: SureCart is not a payment processor. The Customer connects its own payment processor (such as Stripe, PayPal, Mollie, Razorpay or Paystack) under its own agreement with that processor, and payment card data is entered directly into that processor's fields; SureCart receives only tokens and non-sensitive card metadata. Shipping rates and labels are generated through Shippo, US sales tax through TaxJar, and PDF receipts and invoices through URL Box. Merchant-customised email templates are screened for abuse by OpenAI's moderation service. Integrations the Customer enables (email marketing, CRMs, LMS, membership plugins, webhooks and the WordPress plugin sync) send End Customer data to destinations the Customer selects and controls. SureCart does not control those destinations.

1B. SureCart Merchant Affiliate Programmes

Processor: SureCart Inc. · Servers: United States

Field	Detail
Subject matter	Operation of the affiliate programme features the Customer runs through SureCart: affiliate sign-up, referral tracking, commission calculation and payout records.
Nature of processing	Collection, storage, use and deletion of affiliate and referral data on behalf of the Customer.
Purposes	Managing the Customer's affiliates; attributing referred visits and orders; calculating commissions; recording payouts; affiliate portal access.
Types of Personal Data	Affiliate contact data: name, email address, website, and payout details (such as a PayPal email). Referral data:

	referral links and codes, click events, IP address and browser data on referred visits, attributed orders. Commission and payout history.
Categories of data subjects	People who apply to or join the Customer's affiliate programme. End Customers whose visits or orders are attributed to an affiliate.
Retention	For the life of the store, then deleted under Section 7. Payout records: up to 7 years where required for accounting and tax.
Controller responsibility	The Customer is responsible for its affiliate terms, for notice to visitors about referral tracking, and for any consent needed for tracking cookies.

Affiliate Note: This Schedule covers affiliate programmes run by Customers. SureCart's own affiliate programme is a controller activity covered by the SureCart Privacy Policy.

Schedule 2 — Technical and Organisational Measures

These measures apply to Controller Data processed under this DPA and may be updated under Section 4.3.

1. Encryption

1.1 Controller Data is encrypted at rest using industry-standard encryption. Customer-portal and dashboard passwords are hashed with industry-standard one-way algorithms and are never stored in plain text.

1.2 API keys and tokens are cryptographically hashed. Payment-processor credentials and integration secrets are encrypted at rest.

1.3 All data in transit is encrypted using TLS. Unencrypted connections are not supported.

2. Payment Data

2.1 Card numbers and security codes are captured directly by the Customer's PCI DSS–compliant payment processor through hosted fields or redirects. They never reach SureCart's servers.

2.2 SureCart stores only processor tokens and non-sensitive card metadata (brand, last four digits, expiry).

3. Access Controls

3.1 Role-based access control limits SureCart personnel access to Controller Data to those with a documented business need.

3.2 Multi-tenant architecture enforces strict isolation between stores: no Customer can access another Customer's data.

3.3 Customers control their own team access through dashboard roles. SureCart applies secure authentication, session management, and additional verification for sensitive account changes.

4. Infrastructure and Availability

4.1 Primary application servers are in the United States. Encrypted backups run regularly, are kept on a 30–90-day rolling cycle, and have restricted access.

4.2 CDN, WAF and DDoS mitigation protect availability and filter malicious traffic. Application performance, errors and logs are monitored with dedicated observability tools.

5. Organisational Measures

5.1 Personnel with access to Controller Data are bound by confidentiality obligations. Production access is restricted, logged and requires justification.

5.2 SureCart maintains an incident response plan and tests its breach notification procedures. Security patches are applied promptly, dependencies are monitored for known vulnerabilities, and SureCart runs a public bug bounty programme.

5.3 Sub-processors are bound by data protection obligations at least as protective as this DPA.

Schedule 3 — Sub-processor List

The current list of SureCart sub-processors is maintained at **https://surecart.com/legal/sub-processors/**. SureCart will update that page and give notice of material changes under Section 5.2. Customers should check it regularly.

Where a sub-processor is outside the European Economic Area, SureCart shall ensure appropriate transfer safeguards, such as the Standard Contractual Clauses, are in place before transferring Controller Data to it.

Schedule 4 — Standard Contractual Clauses

For Controller Data transferred outside the European Union: the parties agree to be bound by Module Two (controller to processor) of the Standard Contractual Clauses, which are incorporated into this DPA with the following selections.

Section reference	Concept	Selection by the parties
Clause 7	Docking clause	The option under Clause 7 shall not apply
Section II, Clause 9	Approval of sub-processors	Option 2: general written authorisation, with notice under Section 5.2 of this DPA
Section IV, Clause 17	Governing law	The laws of Ireland
Section IV, Clause 18(b)	Choice of forum and jurisdiction	The courts of Ireland
Annex I.A	List of parties	Data exporter: the Customer, as identified in the Principal Agreement. Data importer: SureCart Inc., 2055 Limestone Rd, STE 200-C, Wilmington, Delaware 19808, United States; support@surecart.com
Annex I.B	Description of transfer	Data subjects, personal data and purposes as described in Schedule 1. Frequency: continuous. Nature: collection, storage, use, transmission and deletion. Duration: the term of the Principal Agreement
Annex I.C	Competent supervisory authority	Irish Data Protection Commission
Annex II	Technical and organisational measures	Schedule 2 of this DPA
Annex III	List of sub-processors	Schedule 3 of this DPA

For Controller Data transferred outside the United Kingdom: the parties agree to the UK International Data Transfer Addendum, which is incorporated into this DPA with the following selections.

Section reference	Concept	Selection by the parties
Clause 7	Docking clause	The option under Clause 7 shall not apply
Clause 11	Redress	The option under Clause 11 shall not apply
Section II, Clause 9(a)	Approval of sub-processors	Option 2: general written authorisation
Section IV, Clause 17	Governing law	The laws of England and Wales, insofar as the transfer is governed by UK data protection law
Section IV, Clause 18(b)	Choice of forum and jurisdiction	The courts of England and Wales have exclusive jurisdiction
Annex I.A	List of parties	As set out in the EU table above
Annex I.B	Description of transfer	As set out in the EU table above
Annex I.C	Competent supervisory authority	UK Information Commissioner’s Office
Annex II	Technical and organisational measures	Schedule 2 of this DPA
Annex III	List of sub-processors	Schedule 3 of this DPA
Section 19 of UK Addendum	Ending the Addendum when the Approved Addendum changes	Neither party may end the UK Addendum under Section 19, except as set out in the Principal Agreement

For Controller Data transferred outside Switzerland: the parties agree to the Standard Contractual Clauses above, with these modifications.

Amended provision	Modification
Clause 13 and Annex I.C — competent supervisory authority	The Swiss Federal Data Protection and Information Commissioner (FDPIC)
Processing standard	The parties will apply the GDPR standard to all processing of Controller Data governed by Swiss DP Law
Meaning of “Member State”	Not interpreted to exclude data subjects habitually resident in Switzerland from bringing proceedings there under Clause 18(c)
References to the GDPR	Read as references to Swiss DP Law insofar as the transfer is subject to it

END OF DATA PROCESSING AGREEMENT

SureCart Inc. · October 2026