Data Processing Addendum

Last updated: September 22, 2026

This Data Processing Addendum ("DPA") forms part of the Terms of Service (the "Agreement") between Checkout Page Technologies, Inc., 8 The Green #21601, Dover, DE 19901, United States ("Checkout Page", "Processor") and the customer that has accepted the Agreement ("Customer", "Controller").

It applies automatically whenever Checkout Page processes Customer Personal Data that is subject to the GDPR, UK GDPR or Swiss data protection law. You don't need to sign anything. To keep a copy for your records, save or print this page.

1. Definitions

1.1 "Applicable Data Protection Law" means all laws that apply to the processing of Personal Data under the Agreement, including the EU General Data Protection Regulation 2016/679 ("GDPR"), the GDPR as it forms part of UK law ("UK GDPR"), the Swiss Federal Act on Data Protection ("FADP"), and national laws that implement or supplement them.

1.2 "Controller", "Processor", "Personal Data", "Processing", "Personal Data Breach", "Data Subject" and "Supervisory Authority" have the meanings given in the GDPR.

1.3 "Customer Personal Data" means Personal Data that Checkout Page processes on behalf of Customer to provide the Services, including Personal Data of Customer's end customers and of Customer's authorized users.

1.4 "Services" means the Checkout Page services described in the Agreement.

1.5 "Subprocessor" means any processor that Checkout Page engages to process Customer Personal Data.

1.6 "EEA" means the European Economic Area.

2. Roles and scope

2.1 Customer is the Controller and Checkout Page is the Processor of Customer Personal Data. Where Customer is itself a processor on behalf of a third party, Checkout Page is Customer's subprocessor, and Customer is responsible for passing on this DPA to its controller where required.

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

2.3 Customer is responsible for determining the purposes and means of processing, for giving lawful instructions, and for having a valid legal basis and giving the required notices to Data Subjects.

2.4 If there is a conflict, the following order applies: (i) the Standard Contractual Clauses where they apply under section 11, (ii) this DPA, (iii) the rest of the Agreement.

2.5 Checkout Page processes data about Customer's own account (for example, billing and product usage) as a controller under its Privacy Policy. This DPA does not cover that processing.

3. Instructions

3.1 Checkout Page processes Customer Personal Data only on Customer's documented instructions. The Agreement, this DPA, and Customer's configuration and use of the Services are Customer's complete instructions.

3.2 If the law requires Checkout Page to process Customer Personal Data in another way, Checkout Page will tell Customer before it does so, unless the law prohibits this.

3.3 Checkout Page will tell Customer if, in its opinion, an instruction infringes Applicable Data Protection Law.

4. Confidentiality

Checkout Page ensures that every person authorized to process Customer Personal Data is bound by a duty of confidentiality, by contract or by law.

5. Security

5.1 Checkout Page implements and maintains the technical and organisational measures described in Annex II to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access.

5.2 Checkout Page may update these measures, as long as the update does not materially decrease the overall level of protection.

6. Subprocessors

6.1 Customer gives Checkout Page a general authorization to engage Subprocessors, including those listed on the Subprocessors page (Annex III).

6.2 Checkout Page imposes on each Subprocessor, by written contract, data protection obligations that are no less protective than those in this DPA, and remains responsible to Customer for each Subprocessor's performance.

6.3 At least 30 days before Checkout Page adds or replaces a Subprocessor, it will update the Subprocessors page and email the owner of Customer's account.

6.4 Customer may object to a new Subprocessor on reasonable data protection grounds by emailing security@checkoutpage.com within 14 days of the notice. The parties will work in good faith to resolve the objection. If they cannot, Customer may terminate the affected Services without penalty before the new Subprocessor starts processing Customer Personal Data.

7. Assistance

7.1 Customer can access, export, correct and delete Customer Personal Data in the Checkout Page dashboard. Where Customer cannot fulfil a Data Subject request through the Services, Checkout Page will give reasonable assistance.

7.2 If Checkout Page receives a request directly from a Data Subject about Customer Personal Data, it will pass the request to Customer and will not respond itself unless Customer authorizes it.

7.3 Checkout Page will give Customer reasonable assistance with security of processing, Personal Data Breach notifications, data protection impact assessments and prior consultation with Supervisory Authorities, based on the information available to Checkout Page.

7.4 Assistance is given through Checkout Page's standard support channels. If a request needs material engineering work or custom development, the parties will agree the scope and any fees in advance.

8. Personal Data Breach

8.1 Checkout Page will notify Customer without undue delay, and where feasible within 72 hours, after becoming aware of a Personal Data Breach that affects Customer Personal Data. Notice goes to the email address of the owner of Customer's account. Checkout Page will not wait for its investigation to finish before it sends the first notice.

8.2 The notice will include, as far as it is known at the time: 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. Checkout Page will send updates as more information becomes available.

8.3 A notice is not an admission of fault or liability by Checkout Page.

9. Return and deletion

9.1 Customer can export Customer Personal Data from the dashboard at any time before the end of the Agreement.

9.2 When the Agreement ends, Customer has 30 days to export Customer Personal Data or to ask Checkout Page to return it. After those 30 days, Checkout Page deletes the Customer Personal Data it holds for Customer, and confirms the deletion in writing if Customer asks.

9.3 When Customer deletes a store in the dashboard, Checkout Page deletes the Customer Personal Data held for that store within 30 days.

9.4 Sections 9.2 and 9.3 do not apply where the law requires Checkout Page to keep the data. In that case Checkout Page keeps it only for as long as the law requires, and keeps protecting it under Annex II.

9.5 Copies in backups are deleted as the backups expire, and in any event within 3 months of the deletion under 9.2 or 9.3. Until then they stay protected under Annex II and are not accessed except to restore the Services.

9.6 Payment data held by Stripe in Customer's own Stripe account is controlled by Customer and is not affected by deletion in Checkout Page.

10. Audits

10.1 On request, Checkout Page will make available the information reasonably necessary to demonstrate compliance with this DPA, such as its security and privacy documentation and answers to a reasonable written questionnaire, no more than once a year.

10.2 Customer may ask for the information under 10.1 more often than once a year where a Supervisory Authority requires it, after a Personal Data Breach that affects Customer Personal Data, or where there are other indications that Checkout Page is not complying with this DPA.

10.3 Customer may carry out an on-site audit if the information under 10.1 is not enough to demonstrate compliance, or if a Supervisory Authority requires it. Such an audit needs at least 30 days' written notice, or 10 business days after a confirmed Personal Data Breach, or a shorter period where a Supervisory Authority requires it or where a shorter period is reasonably necessary to investigate suspected non-compliance. It is limited to the systems that process Customer Personal Data, must be done by Customer or an independent auditor under confidentiality obligations, must not give access to other customers' data, and is at Customer's cost.

11. International transfers

11.1 Checkout Page processes Customer Personal Data in the United States and the other locations listed on the Subprocessors page.

11.2 **EEA.** For transfers of Customer Personal Data from the EEA to a country without an adequacy decision, the EU Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914 (the "SCCs") are incorporated into this DPA, with Customer as data exporter and Checkout Page as data importer, and completed as follows:

- Module Two (controller to processor) applies. Where Customer is a processor, Module Three (processor to processor) applies.
- Clause 7 (docking clause) does not apply.
- Clause 9(a): Option 2 (general written authorization) applies, with 30 days' notice as in section 6.3.
- Clause 11(a): the optional language does not apply.
- Clause 13: the competent Supervisory Authority is the one that supervises Customer under the GDPR.
- Clause 17: the SCCs are governed by the law of the EU Member State where Customer is established. If that law does not allow third-party beneficiary rights, or Customer is not established in the EU, the law of Ireland applies.
- Clause 18: disputes are resolved by the courts of that same Member State.
- Annexes I, II and III of the SCCs are completed with Annexes I, II and III of this DPA.

11.3 **United Kingdom.** For transfers from the United Kingdom, the SCCs apply as amended by the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner (the "UK Addendum"). This DPA incorporates the Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the Information Commissioner and laid before Parliament in accordance with section 119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses. Table 1 is completed with the parties' details in Annex I, Table 2 with the choices in section 11.2, Table 3 with Annexes I to III, and in Table 4 neither party may end the UK Addendum when the Approved Addendum changes.

11.4 **Switzerland.** For transfers from Switzerland, the SCCs apply with these changes. References to the GDPR are read as references to the FADP, except where a transfer is also subject to the GDPR, in which case the GDPR references stay and the changes in this section apply in addition. The Swiss Federal Data Protection and Information Commissioner is the competent Supervisory Authority for transfers subject to the FADP. The term "Member State" does not stop a Data Subject who lives in Switzerland from bringing proceedings in Switzerland under Clause 18(c).

12. Payment data

Checkout Page does not store full card numbers, CVV codes or magnetic stripe data. Stripe processes payments. Checkout Page stores only limited payment metadata, such as card brand, last four digits, card country, payment status and transaction identifiers.

13. Liability

Each party's liability under this DPA is subject to the exclusions and limitations of liability in the Agreement, except where Applicable Data Protection Law or the SCCs do not allow such a limitation.

14. Changes to this DPA

Checkout Page may update this DPA to reflect changes in law, in its Subprocessors or in the Services. An update will not materially decrease the protection of Customer Personal Data. The "Last updated" date at the top of this page shows the current version.

15. Contact

Questions about data protection or this DPA go to security@checkoutpage.com.

Annex I: Details of processing

Parties. Data exporter: Customer, as identified by the name, address and email address in its Checkout Page account, acting as controller (or as processor for its own controller). Its activity is selling products, services, events or subscriptions through the Services. Data importer: Checkout Page Technologies, Inc., 8 The Green #21601, Dover, DE 19901, United States, contact security@checkoutpage.com, acting as processor. Its activity is providing checkout, payment and subscription software. Each party accepts this Annex by entering into the Agreement.

Categories of Data Subjects. Customer's end customers and prospective customers whose data is submitted through the Services, and Customer's employees, contractors and other authorized users of its account.

Categories of Personal Data.

- Identity and contact: name, email address, phone number, billing and shipping address, and other fields Customer chooses to collect.
- Account: user IDs, authentication data, account settings.
- Orders: order identifiers, products and plans, amounts, currency, timestamps, refund and charge status.
- Payment metadata: card brand, last four digits, card country, payment status, Stripe transaction identifiers. No full card numbers or CVV codes.
- Technical data: IP address, device and browser information, event and security logs.

Special categories of data. Not intended to be processed. Customer must not collect special category data through the Services unless agreed in writing.

Frequency. Continuous, for as long as Customer uses the Services.

Nature and purpose. Collection, storage, retrieval, use, transmission to Subprocessors, and deletion of Customer Personal Data to provide the checkout flow, payments, subscriptions, emails to Customer's end customers and to Customer, customer support, and the security of the Services.

Duration and retention. For the term of the Agreement, then deletion as described in section 9.

Competent Supervisory Authority. As set out in section 11.2.

Annex II: Technical and organisational measures

- **Access control.** Access to production systems is role-based, limited to the staff who need it, and removed promptly when no longer needed. Administrative access uses strong authentication.
- **Encryption.** Data is encrypted in transit with TLS and at rest in databases and file storage.
- **Secrets.** Credentials and API keys are kept in secrets management and not in source code.
- **Logging and monitoring.** System events are logged, and monitoring alerts on availability problems and suspicious activity. Access to logs is restricted.
- **Vulnerability management.** Systems and dependencies are patched regularly, and security issues are fixed in order of severity.
- **Secure development.** Code is kept in version control with code review, and development and test environments are separate from production.
- **Backups.** Backups are made on a fixed schedule and deleted under a consistent retention cycle. Checkout Page can restore data after a physical or technical incident.
- **Incident response.** A documented process covers identification, containment, recovery and review of incidents, and Customer is notified under section 8.
- **Staff.** Everyone with access to Customer Personal Data is bound by confidentiality obligations.
- **Subprocessors.** Subprocessors are reviewed before use and bound by written data protection terms.
- **Analytics.** Session replay never runs on checkout or payment pages. In the seller dashboard it masks all text and input fields, and analytics receive no page addresses that could carry search terms.

Annex III: Subprocessors

The current list of Subprocessors, with their purpose, location and the data they process, is on the Subprocessors page.

Signatures

This DPA applies without signature. These lines are for Customers whose records need a countersigned copy.

Checkout Page Technologies, Inc. (Processor)
Name: Sander Visser
Title: Founder
Signature: 
Date: 23 September 2026

Customer (Controller)
Legal entity: _____
Name: _____
Title: _____
Signature: _____
Date: _____