Data Processing Addendum

Last modified: January 19th 2023

This Data Processing Addendum (this "DPA"), effective as of the DPA Effective Date (defined below), is entered into by and between ThriveCart LLC (ThriveCart's parent company's registered name; "we", or "us") and YOUNIVERSES ("Customer", or "you").

You have entered into one or more agreements with us (each, as amended from time to time, an "Agreement") governing the provision of the ThriveCart checkout platform, described in further detail at thrivecart.com (the "Service"). This DPA will amend the terms of the Agreement to reflect the parties' rights and responsibilities with respect to the processing and security of YOUNIVERSES's data under the Agreement.

This agreement was signed by Katharina Graff-Haberbosch, a representative of YOUNIVERSES, on Oct 3, 2024.

Definitions

The following definitions apply to this DPA:

- "Alternative Transfer Solution" means a solution, other than the Model Contract Clauses, that enables the lawful transfer of personal data to a third country in accordance with Article 45 or 46 of the GDPR (for example, the EU-U.S. Privacy Shield).
- "Customer Data" means data you submit to, store on, or send to us via the Service.
- "Data Incident" means a breach of ThriveCart's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data on systems that are managed and controlled by ThriveCart. Data Incidents will not include unsuccessful attempts or activities that do not compromise the security of Customer Data, including, without limitation, pings, port scans, denial of service attacks, network attacks on firewall or networked systems, or unsuccessful login attempts.
- "DPA Effective Date" means Oct 3, 2024, the date You signed this agreement.
- "EEA" means the European Economic Area.
- "European Data Protection Legislation" means, as applicable: (a) the GDPR; and/or (b) the Federal Data Protection Act of 19 June 1992 (Switzerland).
- "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, and repealing Directive 95/46/EC.
- "Model Contract Clauses" or "MCCs" means the standard data protection clauses for the transfer of personal data to processors established in third countries that do not ensure an adequate level of data protection, as described in Article 46 of the GDPR.
- "Non-European Data Protection Legislation" means data protection or privacy legislation other than the European Data Protection Legislation.
- "Notification Email Address" means the email address(es) that you designate to receive notifications when you create an account to use the Service. You agree that you are solely responsible for ensuring that your Notification Email Address is current and valid at all times.
- "Personal Data" means any personal data (as that term is defined by European Data Protection Legislation) contained within the Customer Data.
- "Subprocessor" means a third party that we use to process Customer Data in order to provide parts of the Service and/or related technical support.
- "Term" means the period from the DPA Effective Date until the date the Agreement terminates or expires.

The terms "personal data", "sensitive personal data" "data subject", "processing", "controller", "processor" and "supervisory authority" as used in this DPA have the meanings given in the GDPR, and the terms "data importer" and "data exporter" have the meanings given in the MCCs, in each case irrespective of whether the European Data Protection

Legislation or Non-European Data Protection Legislation applies.

Data Processing

Section 1: Roles, Compliance and Authorization

Processor and Controller Responsibilities: If European Data Protection Legislation applies to the processing of Customer's Personal Data, the parties acknowledge and agree as follows: (i) that the subject matter and details of the processing are described in Appendix 1 hereto; (ii) that ThriveCart is a processor of Customer's Personal Data under European Data Protection Legislation; (iii) that you are a controller or processor, as applicable, of the Personal Data under European Data Protection Legislation; and (iv) that each of us will comply with our obligations under applicable European Data Protection Legislation with respect to the processing of the Personal Data.

Authorization by Third Party Controller: If European Data Protection Legislation applies to the processing of Personal Data and you are a processor of the Personal Data, you warrant to us that your instructions and actions with respect to that Personal Data, including your appointment of ThriveCart as another processor, have been authorized by the relevant controller.

Responsibilities Under Non-European Legislation: If Non-European Data Protection Legislation applies to either party's processing of Personal Data, the parties acknowledge and agree that each of us will comply with any applicable obligations under that legislation with respect to the processing of Personal Data.

Section 2: Scope of Processing

Customer Authorization: By entering into this DPA, you hereby authorize and instruct us to process the Personal Data: (i) to provide the Service, and related technical support; (ii) as otherwise permitted or required by your use of the Service and/or your requests for technical support; (iii) as otherwise permitted or required by the Agreement, including this DPA; and (iv) as further documented in any other written instructions that you give us, provided we acknowledge those instructions in writing as constituting processing instructions for the purposes of this DPA. We will not process the Personal Data for any other purpose, unless required to do so by applicable law or regulation.

Authorized Users: By entering into this DPA, if you invite or are invited to join an account as an Authorized User, and you accept the invitation, you are agreeing that certain parts of your information will be shared with the account holder and other members within the account. In particular, the account holder will have access to your name, email address, avatar (if any) and visibility of your products, upsells, downsells and other created content within the Service, and other members may have access to your name, email address and avatar (if any). Any information you create as an Authorized User in an account, including Customer Data or Third-Party Services you link to, will be available to some or all members of that account. You are solely responsible for any information you create in this account, which is posted at your own risk.

Prohibition on Sensitive Data. You will not submit, store, or send any sensitive data or special categories of Personal Data (collectively, "Sensitive Data") to us for processing, and you will not permit nor authorize any of your employees, agents, contractors, or data subjects to submit, store, or send any Sensitive Data to us for processing. You acknowledge that we do not request or require Sensitive Data as part of providing the Service to you, that we do not wish to receive or store Sensitive Data, and that our obligations in this DPA will not apply with respect to Sensitive Data.

Section 3: Deletion

Deletion During Term: We will enable you to delete Personal Data during the Term in a manner that is consistent with the functionality of the Service. If you use the Service to delete any Personal Data in a manner that would prevent you from recovering the Personal Data at a future time, you agree that this will constitute an instruction to us to delete the Personal Data from our systems in accordance with our standard processes and applicable law. We will comply with this instruction as soon as reasonably practicable, but in all events in accordance with applicable law.

Deletion When Term Expires: When the Term expires, we will either destroy or return to you any Customer Data in our possession or control. This requirement will not apply to the extent that we are required by applicable law to retain some or all of the Customer Data, in which event we will isolate and protect the Customer Data from further processing except

to the extent required by law. You acknowledge that you will be responsible for exporting, before the Term expires, any Customer Data you want to retain after the Term expires.

Section 4: Data Security

Security Measures: We will implement and maintain appropriate technical and organizational measures to protect Customer Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access (collectively, the "Security Measures"). The Security Measures will have regard to the state of the art, the costs of implementation, and nature, scope, context and purposes of the processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. The Security Measures will include, as appropriate: (i) the pseudonymization and/or encryption of Personal Data; (ii) the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of data processing systems and services; (iii) the ability to restore the availability and access to Personal Data in a timely manner, in the event of a Data Incident; and (iv) a process for regularly testing, accessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of data processing. We may update or modify the Security Measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Service.

Security Compliance by our Staff: We will take appropriate steps to ensure that our employees, contractors, and Subprocessors comply with the Security Measures to the extent applicable to their scope of performance, including ensuring that all persons authorized to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligations of confidentiality.

Data Incidents: If we become aware of a Data Incident, we will notify you promptly and without undue delay, and will take reasonable steps to minimize harm and secure Customer Data. Any notifications that we send you will be sent to your Notification Email Address and will describe, to the extent possible, the details of the Data Incident, the steps we have taken to mitigate the potential risks, and any suggestions we have for you to minimize the impact of the Data Incident. We will not assess the contents of any Customer Data in order to identify information that may be subject to specific legal requirements. You are solely responsible for complying with any incident notification laws that may apply to you, and to fulfilling any third party notification obligations related to any Data Incident(s). Our notification of or response to a Data Incident under this Section will not constitute an acknowledgement of fault or liability with respect to the Data Incident.

Your Security Responsibilities: You agree that, without prejudice to our obligations: (i) you are solely responsible for your use of the Service, including making appropriate use of the Service to ensure a level of security appropriate to the risk in relation to Customer Data, securing any account authentication credentials, systems, and devices you use to use the Service, and backing up your Customer Data. You understand and agree that we have no obligation to protect Customer Data that you elect to store or transfer outside of our or our Subprocessors' systems (e.g., offline or on-premise storage). You are solely responsible for evaluating whether the Service and our commitments under this Section meet your needs, including with respect to your compliance with any of your security obligations under European Data Protection Legislation and/or Non-European Data Protection Legislation, as applicable. You acknowledge and agree that – taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing of Personal Data, as well as the risks to individuals – the Security Measures that we implement in this DPA provide a level of security appropriate to the risk in respect to the Customer Data.

Audit Rights: If European Data Protection Legislation applies to the processing of Personal Data, we will allow an internationally-recognized independent auditor that you select to conduct audits to verify our compliance with our obligations in this DPA. You must send any requests for audits under this Section to legal@thrivecart.com. Following our receipt of your request, the parties will discuss and agree in advance on the reasonable start date, scope, duration, and security and confidentiality controls applicable to the audit. You will be responsible for any costs associated with the audit. You agree not to exercise your audit rights more than once in any twelve (12) calendar month period, except (i) if and when required by a competent data protection authority; or (ii) an audit is necessary due to a Data Incident.

Section 5: Data Subject Rights; Data Export

Access; Rectification; Restricted Processing; Portability. During the Term, we will, in a manner consistent with the functionality of the Service, enable you to: (i) access the Customer Data; (ii) rectify inaccurate Customer Data; (iii) restrict the processing of Customer Data; (iv) delete Customer Data; and (v) export Customer Data.

Cooperation; Data Subjects' Rights: We will provide you, at your expense, with all reasonable and timely assistance to enable you to respond to: (i) requests from data subjects who wish to exercise any of their rights under European Data Protection Legislation; and (ii) any other correspondence, enquiry or complaint received from a data subject, regulator or other third party in connection with the processing of the Customer Data. In the event that any such request, correspondence, enquiry or complaint is made directly to us, we will promptly inform you of it via your Notification Email Address and provide you with as much detail as reasonably possible.

Section 6: Data Transfers

Data Storage and Processing Facilities: You agree that we may, subject to Section 6.2, store and process Customer Data in the United States and any other country in which we or our Subprocessors maintain facilities.

Transfers of Data out of the EEA; Your Responsibilities: If the storage and/or processing of Personal Data as described in Section 6.1 involves transfers of Personal Data out of the EEA and European Data Protection Legislation applies to the transfers of such data (collectively, "Transferred Personal Data"), we will, at our sole discretion, either (i) ensure that we (as the data importer) have entered into MCCs with you (as the data exporter), and that the transfers are made in accordance with the MCCs; or (ii) ensure that the transfers are made in accordance with an Alternative Transfer Solution. With respect to Transferred Personal Data, you agree that if we reasonably require you to enter into MCCs with respect to such transfers as required by European Data Protection Legislation, you will promptly do so; similarly, if we reasonably require you to use an Alternative Transfer Solution and we request that you take any action (including, without limitation, execution of documents) required to give full effect to that solution, you will promptly do so.

Section 7: Subprocessors

Consent to Engagement: You specifically authorize us to engage third parties as Subprocessors. Whenever we engage a Subprocessor, we will enter into a contract with that Subprocessor to help ensure that the Subprocessor only accesses and uses Customer Data to the extent required to perform the obligations subcontracted to it, and does so in accordance with the Agreement and this DPA.

List of Subprocessors: A list of our current Subprocessors are:

- Amazon Web Services - data warehousing and hosting
- Bunny - used for caching and performance
- Github - used for issue tracking, which may reference customer names
- PayPal - payment services
- Postmark - transactional emails
- SendGrid - internal email routing
- Slack - internal team communication
- Stripe - payment services
- Zendesk - customer support
- Zapier - used to synchronize data between other subprocessors

We will update this list from time to time upon written notice to you, as our Subprocessors change.

Objections; Sole Remedy: Within ninety (90) days of our engagement of any Subprocessor (as determined by the date that we update the list of Subprocessors described in Section 7.2, above), you have the right to object to the appointment of that Subprocessor by providing documentary evidence that reasonably shows that the Subprocessor does not or cannot comply with the requirements set forth in this DPA (each, an "Objection"). If we do not remedy or provide a reasonable workaround for your Objection within a reasonable time, you may, as your sole remedy and our sole liability for your Objection, terminate the Agreement for your convenience, and without further liability to either party. We will not owe you a refund of any fees you have paid in the event you decide to terminate the Agreement pursuant to this Section.

Section 8: Additional Information

You acknowledge that we are required under European Data Protection Legislation (i) to collect and maintain records of certain information, including, among other things, the name and contact detail of each processor and/or controller on whose behalf we are acting and, where applicable, of such processor's or controller's local representative and data protection officer; and (ii) to make such information available to the supervisory authorities. Accordingly, if European Data Protection Legislation applies to the processing of Personal Data, you will, when requested, provide this additional information to us, and ensure that the information is kept accurate and up-to-date.

Section 9: Data Protection Impact Assessment

If we believe or become aware that our processing of Customer Data is likely to result in a high risk to the data protection rights and freedoms of data subjects, we will promptly inform you of that risk, and provide you with reasonable and timely assistance as you may require in order to conduct a data protection impact assessment and, if necessary, consult with the relevant data protection authority.

Section 10: Miscellaneous

There are no third party beneficiaries to this DPA. Except as expressly provided herein, nothing in this DPA will be deemed to waive or modify any of the provisions of the Agreement, which otherwise remains in full force and effect. Specifically, nothing in this DPA will affect any of the terms of the Agreement relating to ThriveCart's limitations of liability, which will remain in full force and effect. If you have entered into more than one Agreement with us, this DPA will amend each of the Agreements separately. In the event of a conflict or inconsistency between the terms of this DPA and the terms of the Agreement, the terms of this DPA will control.

Appendix 1 to Data Processing Addendum

Subject Matter: ThriveCart's provision of the Service to the Customer, and related technical support.

Processing Duration: Throughout the Term of the Agreement.

Nature and Purpose of the Processing: ThriveCart will process Personal Data submitted to, stored on, or sent via the Service for the purpose of providing the Service and related technical support in accordance with this DPA.

Categories of Data: Personal data submitted to, stored on, or sent via the Service may include, without limitation, the following categories of data: IP addresses, browser agents, email addresses, usernames, full names, browser and operating system identifiers, and any other personal data that Customer chooses to send us related during the course of our provision of the Service and technical support.

Data Subjects: Personal data submitted, stored, sent or received via the Service may concern the following categories of data subjects, without limitation: Customer's employees, contractors, and agents; the personnel of Customer's customers, suppliers and subcontractors; and any other person who transmits data via the Service.

Service User	Service Provider
YOUNIVERSES	ThriveCart LLC
Katharina Graff-Haberbosch	
Date signed: Oct 3, 2024	