Data Processing Agreement

Applies to every client of the Cartful platform

Effective date: December 1, 2026

This Data Processing Agreement ("DPA") is between Cartful Solutions, Inc. ("Cartful") and the customer that signs a Statement of Work referencing the Cartful Master Services Agreement (the "Client"). It forms part of the agreement between them for the Cartful platform: the Cartful Master Services Agreement cited in the Statement of Work, and each Statement of Work under it (together, the "Agreement"). It applies without a separate signature. Signing a Statement of Work is agreement to this DPA.

It has three parts: Part 1 sets out Cartful's terms. Part 2 incorporates the European Commission's Standard Contractual Clauses and the UK Addendum. The Annexes describe the processing, Cartful's security measures and its sub-processors.

Part 1. Terms

1. Roles and scope

The Client is the controller and Cartful is the processor of the personal data Cartful processes on the Client's behalf to provide the platform ("Client Personal Data"). The processing is described in Annex I. Account details of the Client's own team members who log in to the platform are handled by Cartful as a controller under its Platform Privacy Policy and are outside this DPA.

2. Instructions

Cartful processes Client Personal Data only on the Client's documented instructions. The Agreement, this DPA and the settings the Client chooses in the platform (such as which features run, which questions are asked and which integrations are connected) are those instructions. Cartful will tell the Client promptly if it believes an instruction breaks data protection law.

3. Confidentiality

Only authorized personnel of Cartful who need access to provide, secure or support the service can access Client Personal Data, and each of them is bound by a duty of confidentiality.

4. Security

Cartful applies at least the measures in Annex II. Cartful may update them over time, provided the overall level of protection does not go down.

5. Sub-processors

The Client gives Cartful general written authorisation to use the sub-processors in Annex III. Before adding or replacing a sub-processor, Cartful will notify the Client in writing at least 30 days in advance, with the information the Client needs to decide whether to object. The Client may object in writing within that period. If the Client objects and the parties cannot resolve it, the Client's remedy is to end the affected services.

Cartful engages each sub-processor under a written contract with data protection terms that protect Client Personal Data at least as well as this DPA, and Cartful remains responsible to the Client for each sub-processor's performance.

6. Personal data breaches

Cartful will notify the Client without undue delay after becoming aware of a personal data breach affecting Client Personal Data, with the information Clause 8.6 of the SCCs requires.

7. Shopper requests and other assistance

If a shopper contacts Cartful directly to exercise a data protection right, Cartful will pass the request to the Client promptly and will not respond to it unless the Client asks it to. Cartful will help the Client respond to shopper requests, taking into account what data Cartful holds and how it is stored. Most Client Personal Data expires automatically on

the schedule in Annex I. Cartful will also give the Client reasonable help with data protection impact assessments and consultations with supervisory authorities about the processing.

8. Audits

On request, and under appropriate confidentiality terms, Cartful will provide its most recent SOC 2 Type II report and answer reasonable written security and privacy questionnaires. The Client will consider these first. The Client, or an independent auditor it appoints who is bound by confidentiality, may also audit Cartful at reasonable intervals (normally no more than once in 12 months) or where there are indications of non-compliance, on reasonable notice (normally 30 days) and during business hours. An audit beyond the SOC 2 report and written questionnaires is at the Client's expense and must not give access to other clients' data.

9. End of the Agreement

When the Agreement ends, Cartful will make the Client Personal Data it then holds available for the Client to export for 30 days, and will then delete it. Cartful will delete it straight away if the Client asks it to skip the export, and will confirm deletion in writing on request (as Section 7(c) of the Master Services Agreement sets out). Where one Statement of Work ends and another continues, this applies to the Client Personal Data used only for the one that ended. Copies in encrypted backups are deleted on the normal backup cycle and stay protected under this DPA until then. Cartful may keep data only where law requires it to.

10. International transfers

Cartful is established in the United States. Personal data of shoppers in the European Economic Area and the United Kingdom is stored and processed in the European Union. Cartful staff and some sub-processors may access it from outside the EEA. Those transfers are covered by Part 2.

11. US state privacy laws

For personal information covered by the California Consumer Privacy Act and similar US state privacy laws, Cartful acts as the Client's service provider or processor. Cartful will not sell or share that personal information (including for cross-context behavioral advertising); will not retain, use or disclose it outside its direct business relationship with the Client or for any purpose other than providing the services under the Agreement; and will not combine it with personal information it receives from anyone else, except as those laws allow. Cartful will give it the level of protection those laws require and will tell the Client if it can no longer meet these obligations. The Client may take reasonable steps to stop and fix any unauthorised use.

12. Order of precedence, liability and term

- This DPA takes effect when the Client signs a Statement of Work, and needs no separate signature. Where the parties have signed a separate data processing agreement, that agreement applies in place of this DPA. For the processing of personal data, the Standard Contractual Clauses and UK Addendum in Part 2 prevail over the rest of this DPA, and this DPA prevails over the rest of the Agreement, including Sections 6 (Data Security) and 7(c) (Effect of termination) of the Master Services Agreement and any Statement of Work.
- Each party's total liability arising out of or relating to this DPA, including Part 2, is subject to the liability caps in Section 9 of the Master Services Agreement, to the extent the law allows. Nothing in this DPA limits the rights of data subjects under Part 2.
- Part 1 is governed by the law that governs the Agreement. Part 2 is governed as set out there.
- This DPA applies for as long as Cartful processes Client Personal Data.

Part 2. Standard Contractual Clauses

EU Standard Contractual Clauses

Where Client Personal Data is subject to the EU General Data Protection Regulation (GDPR), the parties incorporate **Module Two (controller to processor)** of the standard contractual clauses in the Annex to Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (the "SCCs"). The Client is the data exporter and Cartful is the data importer. The SCCs also meet the requirements of Article 28(3) and (4) GDPR (recital 9 of that Decision). The parties choose these options:

Clause	Selection
Clause 7 (docking clause)	Not used.
Clause 9(a) (sub-processors)	Option 2, general written authorisation. The time period is 30 days. The agreed list is Annex III.
Clause 11(a) (redress)	The optional independent dispute resolution language is not used.
Clause 13(a) (supervision)	The alternative that applies to the data exporter. The supervisory authority is set out in Annex I.C.
Clause 17 (governing law)	Option 2. The law of the EU Member State where the data exporter is established. Where that law does not allow third-party beneficiary rights, or the data exporter is not established in an EU Member State, the law of Ireland.
Clause 18(b) (forum)	The courts of the EU Member State whose law governs the SCCs under Clause 17.
Annexes I, II and III of the SCCs	Annexes I, II and III of this DPA.

Sections 5, 6 and 8 of Part 1 describe how Cartful carries out Clauses 9, 8.6 and 8.9 of the SCCs. They add to the SCCs and do not change them.

Signing a Statement of Work counts as each party signing the SCCs, the UK Addendum and Annex I, on the effective date of that Statement of Work.

UK Addendum

Where Client Personal Data is subject to the UK GDPR, the parties incorporate the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (version B1.0) issued by the UK Information Commissioner under section 119A(1) of the Data Protection Act 2018 (the "UK Addendum"). Its Part 1 tables are completed as follows, and its Part 2 is: Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

UK Addendum table	Completed as
Table 1 (parties)	The parties in Annex I.A. Start date: the effective date of the Client’s first Statement of Work.
Table 2 (selected SCCs)	The Approved EU SCCs, including the Appendix Information, with only these provisions brought into effect: Module 2 in operation; Clause 7 (docking clause) not used; Clause 11 option not used; Clause 9(a) general authorisation; Clause 9(a) time period 30 days.
Table 3 (appendix information)	Annex 1A: Annex I.A of this DPA. Annex 1B: Annex I.B. Annex II: Annex II. Annex III: Annex III.
Table 4 (ending the Addendum when the Approved Addendum changes)	Neither party.

Switzerland

Where Client Personal Data is subject to the Swiss Federal Act on Data Protection (FADP), the SCCs apply with these changes: references to the GDPR include the FADP; the Swiss Federal Data Protection and Information

Commissioner is a competent supervisory authority for transfers under the FADP; and "Member State" does not prevent data subjects in Switzerland from bringing claims where they habitually reside.

Annex I. Parties and description of the processing

A. List of parties

Data exporter (controller)

Name	The Client named in the Statement of Work
Address	The Client's address for notices under the Agreement
Contact person	The Client's contact for notices under the Agreement
Activities	Uses the Cartful platform on the websites named in the Statement of Work.
Role	Controller
Signature and date	Signed by signing the Statement of Work, on its effective date.

Data importer (processor)

Name	Cartful Solutions, Inc.
Address	PO Box 520, New York, NY 10024, USA
Contact person	Timothy Petrella, President & CEO, privacy@cartfulsolutions.com
Activities	Provides the Cartful platform: product guidance features on the client's websites, including interactive quizzes (Studio), product page guidance (Affinity), product recommendations (Lineup) and the shared product logic behind them (the Library).
Role	Processor
Signature and date	Signed by signing the Statement of Work, on its effective date.

B. Description of the processing and transfer

Data subjects	Visitors and shoppers on the Client's websites who use Cartful features.
Categories of personal data	Answers and choices in Cartful features, and products viewed or clicked in them. What shoppers type to describe their needs on a product page (used once and not stored by Cartful). Contact and profile details, only if the Client turns on their collection and the shopper provides them: email address, name, phone number, date of birth or age, gender, postal code, country or language, and marketing preferences. Identifiers from the Client's own connected systems, if connected (for example an email platform profile ID). Technical data: IP address, approximate location, browser and device details, a random visitor and session ID kept in the shopper's browser storage, pages viewed, ad click IDs and consent choices.
Sensitive data	None is required. Cartful's features do not ask for sensitive data. The Client chooses the questions in its features and is responsible for the lawful basis and any consent for a question that could reveal sensitive data. All personal data gets the safeguards in Annex II.
Frequency of transfer	Continuous, while Cartful features are live on the client's websites.
Nature of the processing	Collection, storage, structuring, analysis, transmission to the Client's connected systems, and deletion.
Purposes	Running the features and showing shoppers relevant products. Measuring how the features perform, for the Client's analytics dashboards, following the Client's consent settings.

	Passing details a shopper provides to the Client's own email, marketing or customer systems, when the Client connects them. Keeping the service secure and fixing problems. Improving the features, using de-identified data only.
AI	Some features use AI models hosted inside Cartful's cloud providers (Annex III). They receive product information and what a shopper types to describe their needs. Cartful does not send AI models the contact details a shopper enters in contact fields. The free-text field is for describing a need, and Cartful does not use it to collect contact details. No data is used to train AI models. Cartful turns off optional storage at these providers. A provider may hold inputs briefly under its own abuse-prevention process. AI features that process shopper input are offered for shoppers in the US and Canada.
Where data is stored	EEA and UK shopper data is stored and processed in the European Union. US and Canadian shopper data is stored and processed in the United States.
Retention	Contact details: none kept after successful delivery to the client's system. Failed deliveries are held encrypted for up to 72 hours to retry, then deleted. If the client asks Cartful to sync contact details to its own CRM, they are kept encrypted in analytics for up to 6 months and decrypted only to deliver them. Answers, choices and technical data: 6 months, then aggregated so they no longer identify anyone. What shoppers type to describe their needs: not stored by Cartful. Security and operations logs: up to 90 days. Encrypted backups: deleted data ages out on the normal backup cycle.
Transfers to sub-processors	As listed in Annex III, for the purposes and in the locations shown there, for the term of the Agreement.

C. Competent supervisory authority

The supervisory authority that Clause 13(a) of the SCCs identifies for the Client. Where the Client is established in an EU Member State, that is the authority of that Member State.

Annex II. Technical and organisational measures

Certification and testing	SOC 2 Type II, audited yearly by an independent firm (Security, Availability and Confidentiality criteria). Independent penetration testing every year.
Encryption	TLS for all data in transit. Encryption at rest for all stored data. Personal data is envelope-encrypted with managed encryption keys from the first point it enters Cartful's systems and stays encrypted in storage. IP addresses are stored encrypted. Integration credentials are stored encrypted.
Access control	Role-based access on a least-privilege basis, limited to staff who need it. Access is removed when a role changes or ends.
Monitoring and logging	Continuous security monitoring of the cloud environment. Application logs and error monitoring are configured to exclude personal data, including what shoppers type to describe their needs. Logs are kept up to 90 days.
Availability and recovery	Hosting on major cloud providers. Encrypted backups kept in the same region as the data.
Data minimisation	Collection of contact details is off unless the client turns it on. Contact details are deleted after delivery. What shoppers type to describe their needs is used once and not stored by Cartful. Stored IP addresses are used only for security and troubleshooting.
Retention and deletion	Automated deletion on the schedule in Annex I.B. Return or deletion at the end of the Agreement (Part 1, Section 9).
Regional separation	EEA and UK shopper data is stored and processed in the EU; US and Canadian shopper data in the US.
Physical security	Cartful runs no data centres of its own. Data is hosted with the cloud providers in Annex III, whose facilities are independently audited (for example SOC 2 and ISO/IEC 27001).
Staff	Confidentiality obligations for everyone with access. Security training for staff.
Sub-processors	Written contracts with data protection terms; providers chosen for their security certifications.
Assistance to the controller	A privacy contact (privacy@cartfulsolutions.com) for requests and incidents. Help with shopper requests, breach notices and impact assessments as described in Part 1, Sections 6 and 7.

Annex III. Sub-processors

The Client authorises the following sub-processors. Each is engaged for the term of the Agreement. Cartful publishes its current list at cartful.com/legal/subprocessors.

Sub-processor	Address	Purpose	Data location
Amazon Web Services, Inc.	410 Terry Ave N, Seattle, WA 98109, USA	Cloud hosting, storage, analytics and email delivery; AI models via Amazon Bedrock	EU (EEA and UK data); US (US and Canadian data)
Google LLC (Google Cloud Platform)	1600 Amphitheatre Pkwy, Mountain View, CA 94043, USA	Cloud infrastructure; AI models via Vertex AI	EU; US
Cloudflare, Inc.	101 Townsend St, San Francisco, CA 94107, USA	Content delivery, DNS and DDoS protection	Global edge network
Functional Software, Inc. (Sentry)	45 Fremont St, 8th Floor, San Francisco, CA 94105, USA	Error monitoring; configured to receive no personal data	US

Contact for each sub-processor: its published privacy contact, or through Cartful at privacy@cartfulsolutions.com.