

# Data Processing Addendum

Capconvert Agency Engagement

Between **Capconvert, LLC.** (the “Processor”)  
and the **Customer** named in Annex 1A (the “Controller”)

Form effective: May 26, 2026

## 1. Background & Application

---

This Data Processing Addendum (the “**Agency DPA**”) supplements and forms part of the Capconvert Master Service Agreement (the “MSA”) and any Statements of Work executed under it between Capconvert, LLC., a limited liability company with an address in San Francisco, California, United States (“**Capconvert**”) and the Customer identified in Annex 1A (the “**Customer**”; together with Capconvert, the “**Parties**”).

This Agency DPA reflects the Parties’ agreement on the Processing of Personal Data by Capconvert on behalf of the Customer in connection with the agency services provided under the MSA. It applies to the extent and only to the extent Capconvert Processes Personal Data subject to the EU General Data Protection Regulation (Regulation (EU) 2016/679, “EU GDPR”), the UK General Data Protection Regulation (“UK GDPR”), the Swiss Federal Act on Data Protection (“FADP”), the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act (“CCPA/CPRA”), or other applicable data protection laws of comparable scope (each, a “**Data Protection Law**”).

Where the engagement also includes Cortex SaaS access, the Cortex Data Processing Addendum (available at <https://www.capconvert.com/cortex/dpa>) governs the Cortex surface; this Agency DPA governs the agency services. In the event of conflict between the body of this Agency DPA and its Annexes, the body controls.

## 2. Definitions

---

### **Agency Services**

The search marketing services provided by Capconvert to the Customer under the MSA and any executed SOW, including SEO, GEO, CRO, PPC, content production, technical audit, and analytics implementation services.

### **Authorised Sub-processor**

Any third party engaged by Capconvert to Process Customer Personal Data on Capconvert’s behalf in connection with the Agency Services, as listed at <https://www.capconvert.com/subprocessors>.

### **Customer Personal Data**

Personal Data Processed by Capconvert on behalf of the Customer in the course of providing the Agency Services, as further described in Annex 1B.

### **Data Subject Request**

A request made by or on behalf of a Data Subject under a Data Protection Law to exercise their rights, including access, rectification, erasure, restriction, portability, objection, or non-discrimination.

### **Personal Data Breach**

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data Processed by Capconvert or an Authorised Sub-

processor.

### **Restricted Transfer**

A transfer of Customer Personal Data from the European Economic Area, the United Kingdom, or Switzerland to a country that has not been recognised by the relevant Supervisory Authority as providing an adequate level of protection.

### **Standard Contractual Clauses (“SCCs”)**

The standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679, as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, including any subsequent amendments.

### **UK IDTA Addendum**

The International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, version B.1.0, in force 21 March 2022.

Capitalised terms not otherwise defined in this Agency DPA have the meanings given to them in the applicable Data Protection Law.

## **3. Roles & Scope of Processing**

---

With respect to the Processing of Customer Personal Data under this Agency DPA, the Customer is the Controller and Capconvert is the Processor. Under CCPA/CPRA, Capconvert acts as a Service Provider on behalf of the Customer (as Business).

The subject matter, duration, nature and purpose of the Processing, the types of Personal Data, and the categories of Data Subjects are set out in **Annex 1B**.

Capconvert will Process Customer Personal Data only on the documented instructions of the Customer (which are deemed to include those instructions necessary for Capconvert to provide the Agency Services in accordance with the MSA), and as required by applicable law. Capconvert will not Sell or Share Customer Personal Data, will not retain Customer Personal Data outside the direct business relationship with the Customer, will not combine Customer Personal Data with Personal Data from other sources except as permitted, and will not use Customer Personal Data to train any AI or ML model offered to third parties.

## **4. Confidentiality**

---

Capconvert ensures that each person authorised to Process Customer Personal Data is subject to written confidentiality obligations or a statutory duty of confidentiality at least as protective as those in this Agency DPA, and Processes Customer Personal Data only as necessary to perform their role.

## 5. Security

---

Capconvert has implemented and will maintain appropriate technical and organisational measures designed to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to such data, as described in **Annex 2**. Capconvert may update those measures from time to time, provided updates do not materially decrease overall security.

## 6. Sub-processors

---

The Customer authorises Capconvert to engage Authorised Sub-processors, including those listed at <https://www.capconvert.com/subprocessors> and reproduced for the effective date at **Annex 3**, to Process Customer Personal Data for the purposes of providing the Agency Services.

Capconvert will (a) enter into a written agreement with each Authorised Sub-processor imposing data protection obligations substantially similar to those in this Agency DPA, (b) maintain a current list of Authorised Sub-processors at the URL above, and (c) provide at least fifteen (15) calendar days' prior notice of the addition of a new Authorised Sub-processor that will materially Process Customer Personal Data, during which the Customer may object on reasonable grounds. If no resolution can be reached, the Customer may terminate the affected Services on written notice. Capconvert remains responsible for the acts and omissions of its Authorised Sub-processors.

## 7. Assistance with Data Subject Requests

---

Taking into account the nature of the Processing, Capconvert assists the Customer by appropriate technical and organisational measures, insofar as possible, for the fulfilment of the Customer's obligation to respond to Data Subject Requests. If Capconvert receives a Data Subject Request directly relating to Customer Personal Data, Capconvert will, without undue delay, forward the request to the Customer and will not respond directly other than to confirm receipt and refer the Data Subject to the Customer.

## 8. Personal Data Breach Notification

---

Capconvert will notify the Customer without undue delay, and in any event within seventy-two (72) hours, after becoming aware of a Personal Data Breach affecting Customer Personal Data. The notification will, to the extent the information is available, describe the nature of the breach (including the categories and approximate number of Data Subjects and records concerned), the likely consequences, the measures taken or proposed to address it, and the Capconvert contact point. Capconvert will provide further information as it becomes available.

## **9. Data Protection Impact Assessments and Prior Consultation**

---

Capconvert provides reasonable assistance to the Customer (at the Customer's cost where the assistance falls outside the routine support included with the Agency Services) in connection with the Customer's data protection impact assessments and prior consultations with Supervisory Authorities.

## **10. Return and Deletion of Customer Personal Data**

---

On termination or expiry of the Agency Services, or earlier on the Customer's written request, Capconvert will, at the Customer's choice, return or delete all Customer Personal Data in its possession or control (including copies held by Authorised Sub-processors) within ninety (90) calendar days, except to the extent applicable law requires continued retention. Backup copies that are routinely overwritten on Capconvert's standard cycle do not require active deletion and will be deleted in the ordinary course.

## **11. Audits and Compliance Information**

---

Capconvert will make available to the Customer all information reasonably necessary to demonstrate compliance with this Agency DPA. On the Customer's prior written request (not more than once per calendar year, except in connection with a Personal Data Breach or Supervisory Authority directive), Capconvert will respond to a reasonable written audit questionnaire concerning the security of the Agency Services. Capconvert may satisfy this obligation by providing the most recent third-party audit report applicable to its operations.

## **12. International Data Transfers**

---

Where the Processing of Customer Personal Data under this Agency DPA involves a Restricted Transfer from the EEA, the Parties incorporate by reference Module Two (Controller to Processor) of the SCCs, as completed in **Annex 4**. Where the Processing involves a Restricted Transfer from the United Kingdom, the Parties incorporate the UK IDTA Addendum. Where the Processing involves a Restricted Transfer from Switzerland, references in the SCCs to the EU GDPR are interpreted as references to the FADP, and the competent Supervisory Authority is the Swiss Federal Data Protection and Information Commissioner.

## **13. CCPA/CPRA-Specific Terms**

---

For Customer Personal Data subject to the CCPA/CPRA, Capconvert acknowledges that it is a Service Provider acting on behalf of the Customer (Business), will not Sell or Share Personal Information, will not retain, use, or disclose Personal Information for any purpose other than the specific business purpose of providing the Agency Services, will not combine Personal Information received from the Customer with Personal Information from another source or collected from its own interactions with Data Subjects (except as permitted), and will comply with all applicable CCPA/CPRA requirements. Capconvert will notify the Customer if it determines that it can no longer meet its CCPA/CPRA obligations.

## 14. Liability

---

The liability of each Party under or in connection with this Agency DPA is subject to the limitations of liability in the MSA, except that nothing in this Agency DPA, the MSA, or any other agreement between the Parties limits or excludes either Party's liability for (a) death or personal injury caused by negligence, (b) fraud or wilful misconduct, or (c) any other liability that cannot be excluded under applicable law.

## 15. Term, Termination & Survival

---

This Agency DPA takes effect on the date the Customer executes the MSA (or, where the Customer requests a DPA after the MSA is in place, the date Capconvert counter-signs) and remains in effect for so long as Capconvert Processes Customer Personal Data on behalf of the Customer. Sections that by their nature should survive termination (Section 4 (Confidentiality), Section 10 (Return and Deletion), Section 11 (Audits), Section 12 (International Transfers), Section 14 (Liability), Section 16 (Governing Law)) will survive.

## 16. Governing Law & Jurisdiction

---

This Agency DPA is governed by and construed in accordance with the laws of the State of California, without regard to its conflict of laws provisions, except that the SCCs incorporated under Section 12 are governed by the law of Ireland. Disputes are subject to the exclusive jurisdiction of the state and federal courts located in San Francisco County, California, except that suits arising from the SCCs may be brought before the courts of Ireland.

## 17. General

---

This Agency DPA, together with the MSA, constitutes the entire agreement of the Parties with respect to the Processing of Customer Personal Data in connection with the Agency Services and supersedes any prior data processing terms. Any modification of this Agency DPA must be in writing and signed by both Parties. If any provision is held to be unenforceable, the remaining provisions continue in full force and effect. Neither Party may assign this Agency DPA without the prior written consent of the other, except in connection with a merger, reorganisation, or sale of substantially all of its assets.

### Capconvert, LLC.

\_\_\_\_\_  
Authorised signature

\_\_\_\_\_  
Print name

### Customer

\_\_\_\_\_  
Authorised signature

\_\_\_\_\_  
Print name

Title

---

Date

Title

---

Date

## Annex 1A - List of the Parties

---

### Data Exporter (Controller / Customer)

<b>Name</b>	_____
<b>Address</b>	_____
<b>Contact person's name, position, contact details</b>	_____
<b>Activities relevant to the data transferred</b>	Procurement of search marketing agency services from the Data Importer (Capconvert).
<b>Role</b>	Controller (or Processor where the Customer is itself acting on behalf of an upstream Controller)

### Data Importer (Processor)

<b>Name</b>	Capconvert, LLC.
<b>Address</b>	San Francisco, California, United States
<b>Contact person</b>	Legal, help@capconvert.com
<b>Activities relevant to the data transferred</b>	Provision of search marketing agency services (SEO, GEO, CRO, PPC, content, audit, analytics).
<b>Role</b>	Processor (Service Provider under CCPA/CPRA)

## **Annex 1B - Description of Processing**

---

### ***Categories of Data Subjects***

- The Customer's end customers and prospects whose visits to the Customer's digital properties are reflected in connected Google Search Console, Google Analytics, ad-platform, or first-party data sources.
- The Customer's employees and contractors who interact with Capconvert during the engagement (typically through email, Slack, calls, and shared documents).
- Third-party content authors, public figures, or business contacts identified in publicly available data the Customer instructs Capconvert to research.

### ***Categories of Personal Data***

- Names, business email addresses, business phone numbers, and roles of the Customer's personnel involved in the engagement.
- Aggregated or pseudonymised search analytics (query strings, landing pages, country, device, dates), advertising performance (campaigns, keywords, click-through, spend), and analytics metrics (sessions, conversions, source/medium) retrieved from connected platforms.
- Publicly available information about people connected to brand entities under analysis (authors, founders, team members surfaced in brand discovery workflows).
- Customer-supplied notes, attachments, and other inputs to project planning surfaces.

### ***Special Categories of Personal Data***

None contemplated. The Customer agrees not to submit special-category data to Capconvert without first agreeing additional terms in writing.

### ***Frequency of the Transfer***

Continuous, for the duration of the engagement.

### ***Nature of the Processing***

Collection, organisation, storage, retrieval, consultation, analysis, alignment or combination, restriction, erasure, and destruction of Customer Personal Data for the purpose of providing the Agency Services.

### ***Purpose of the Processing***

Producing audits, recommendations, plans, content, and other deliverables for the Customer's use in its search marketing operations.

### ***Period for Which Personal Data Will Be Retained***

For the duration of the engagement and thereafter per Section 10 of this Agency DPA and Capconvert's Data Retention Policy.

***Transfers to (Sub-) Processors***

As listed in Annex 3 and at <https://www.capconvert.com/subprocessors>.

## **Annex 2 - Technical and Organisational Security Measures**

---

### **1. Access control**

- Multi-factor authentication required for all Capconvert personnel with access to systems Processing Customer Personal Data.
- Role-based access control with least-privilege defaults; access reviewed at least quarterly.
- Production credentials are rotated on personnel changes and on suspected compromise.
- Customer Personal Data is logically segregated by Customer identifier.

### **2. Encryption**

- Customer Personal Data in transit is encrypted using TLS 1.2 or higher.
- Customer Personal Data at rest is encrypted using AES-256 or equivalent.

### **3. Network & application security**

- Production services are deployed behind Cloudflare with bot management and rate limiting; origin servers are not directly addressable.
- Code changes are reviewed prior to deployment and subjected to automated static analysis.
- A vulnerability disclosure programme is published at <https://www.capconvert.com/security> with a safe-harbour commitment to good-faith security researchers.

### **4. Logging, monitoring & incident response**

- Application, access, and infrastructure logs retained for at least ninety days; reviewed for anomalies on an automated basis.
- Documented incident response plan with defined severities, escalation paths, and notification procedures consistent with Section 8 of this Agency DPA.

### **5. Personnel**

- Personnel with access to Customer Personal Data are subject to written confidentiality obligations and receive periodic data-protection and security training.
- Background checks are conducted on personnel with access to production systems, to the extent permitted by applicable law.

### **6. Sub-processor diligence**

- Capconvert assesses each Authorised Sub-processor for security, privacy, and regulatory compliance prior to engagement and on a recurring basis.

- Each Authorised Sub-processor is required to maintain technical and organisational measures substantially equivalent to those described here.

## **7. Business continuity & backups**

- Customer-state databases are backed up on the infrastructure provider's standard schedule with point-in-time recovery available.
- Documented business continuity plan covering loss of access to primary infrastructure providers.

### Annex 3 - Authorised Sub-processors (as of the effective date)

The current authoritative list is published at <https://www.capconvert.com/subprocessors> and is updated in accordance with Section 6 of this Agency DPA.

Sub-processor	Role	Location
Google LLC (Workspace, Drive)	Corporate email, calendar, deliverable storage	United States
Slack Technologies, LLC	Internal + Customer-facing collaboration channels	United States
Notion Labs, Inc.	Internal knowledge base and project notes	United States
Fathom Inc.	Call transcription for internal note-taking (recorded with consent)	United States
Loom, Inc.	Screen recordings for walkthroughs and async updates	United States
Vercel, Inc.	Application hosting for Customer-facing dashboards	United States
Neon, Inc.	Managed Postgres database	United States
Cloudflare, Inc.	CDN, DNS, bot management, edge security	Worldwide
Amazon Web Services, Inc.	Underlying infrastructure for managed services	United States
Anthropic, PBC	Claude AI APIs for audit + recommendation authoring	United States
OpenAI, L.L.C.	ChatGPT API for GEO + citation auditing	United States
Ahrefs Pte. Ltd.	SEO and backlink data, site audit, GSC connector	Singapore
Brave Software, Inc.	Brave Search API for SERP retrieval	United States
Stripe, Inc.	Payment processing	United States
Twilio (SendGrid)	Transactional email delivery	United States

<b>Sub-processor</b>	<b>Role</b>	<b>Location</b>
Mailchimp Transactional (Mandrill)	Backup transactional email delivery	United States
Klaviyo, Inc.	Marketing email lifecycle communications	United States

## **Annex 4 - Standard Contractual Clauses Annex**

---

### **Module & Roles**

Module Two (Controller to Processor) of the SCCs for Restricted Transfers from the EEA. Where the Customer is itself acting as a Processor on behalf of an upstream Controller, Module Three (Processor to Processor) applies instead.

### **Clause 7 - Docking Clause**

Not applicable.

### **Clause 9 - Use of Sub-processors**

Option 2 (General written authorisation), with a notice period of fifteen (15) calendar days, as described in Section 6.

### **Clause 17 - Governing Law of the SCCs**

Ireland.

### **Clause 18 - Choice of Forum and Jurisdiction**

Courts of Ireland.

### **UK IDTA Addendum**

For Restricted Transfers from the United Kingdom, the Parties incorporate the UK IDTA Addendum (version B.1.0). Tables 1, 2, and 3 are populated from the corresponding entries in this Agency DPA and its Annexes. Table 4 is set so the Importer may not end the Addendum.

### **Swiss FADP**

For Restricted Transfers from Switzerland subject to the FADP, references in the SCCs to the EU GDPR are interpreted as references to the FADP, references to the European Union as references to Switzerland, the competent Supervisory Authority is the Swiss Federal Data Protection and Information Commissioner, and the governing law is Swiss law.