

DATA PROCESSING ADDENDUM

Version: 1.0

Effective Date: January 1, 2026

This Data Processing Addendum (“DPA”) forms an integral part of the AdMatric Platform Access Agreement entered into by and between DataPoint Technologies LLC (“DataPoint”) and the Platform User (the “Agreement”). Capitalized terms utilized but not explicitly defined in this DPA shall have the meanings ascribed to them in the Agreement or Exhibit B (the “MSA”). If there is an operational conflict between this DPA and the Agreement or the MSA regarding the processing of Personal Data, the provisions of this DPA shall control conclusively.

1. ROLES AND SCOPE OF COMPLIANCE

1.1 Application: This DPA applies strictly and exclusively to Personal Data that DataPoint processes on behalf of the Platform User in connection with the AdMatric software infrastructure during the Term.

1.2 Controller Status: The Platform User acts as the Controller (and, where applicable, the “Business” under U.S. state privacy laws). If an upstream Advertiser client is the true Controller and the Platform User is that Advertiser’s processor, the Platform User is solely and contractually responsible for passing the Advertiser’s lawful instructions to DataPoint. DataPoint shall process that Personal Data as a sub-processor of the Platform User, and DataPoint does not become a party to, or bound by, any external Advertiser Agreement.

1.3 Processor Status: DataPoint acts strictly as the Data Processor (and, where applicable, the “Service Provider” or “Processor” under U.S. state privacy laws, including the FDBR and CCPA).

1.4 Personal Data Boundaries: “Personal Data” means information relating to an identified or identifiable natural person, or “personal information” / “personal data” as defined by Applicable Data Protection Law, that is processed under this DPA. For all purposes under this contract, Personal Data explicitly excludes data that has been completely de-identified, anonymized, or aggregated so it is no longer Personal Data, including any aggregated

performance metrics compiled and retained by DataPoint under the optimization learning parameters set forth in Section 3.4 of Exhibit B (the “MSA”).

1.5 Applicable Data Protection Law Defined: “Applicable Data Protection Law” means, to the extent applicable: the EU GDPR, the UK GDPR, the California Consumer Privacy Act as amended by the CPRA (“CCPA”), the Florida Digital Bill of Rights (“FDBR”), and any other state, federal, or international privacy law that applies to the processing under this DPA.

1.6 Details of processing are itemized in Annex 1 of this Addendum.

2. PLATFORM USER RESPONSIBILITIES

2.1 Data Ingestion Restrictions: The Platform User shall not submit Personal Data to the AdMatric platform except as strictly required to utilize the services, and is absolutely prohibited from submitting special-category data or sensitive personal information unless the Parties have explicitly agreed otherwise in a separate writing.

2.2 Warranties of Consent: The Platform User warrants and covenants that it possesses and will continuously maintain all notices, disclosures, consents, and lawful bases required for DataPoint to process Personal Data as described in the Agreement and this DPA, including mandatory Advertiser and consumer end-user consents where required by law.

2.3 Documented Instructions: The Platform User’s documented processing instructions are limited strictly to the four corners of the front-page Agreement, this DPA, the MSA, and the specific campaign settings the Platform User configures inside the platform dashboard. DataPoint will not process Personal Data except on those explicit instructions unless required to do so by applicable sovereign law, in which case DataPoint will notify the Platform User unless legally prohibited by that authority.

2.4 Compliance Alerts: If DataPoint reasonably believes a processing instruction violates Applicable Data Protection Law, it will notify the Platform User and reserves the absolute right to suspend that specific processing stream until the instruction is confirmed or modified by the Platform User.

3. DATAPOINT OBLIGATIONS

3.1 Processing Covenants: DataPoint shall: (a) process Personal Data only on documented instructions as set out in Section 2.3; (b) ensure persons authorized to process Personal Data are bound by enforceable confidentiality duties; (c) implement the security safeguards set forth in Section 5; (d) engage subprocessors only as permitted by Section 6; (e)

reasonably assist the Platform User, at the Platform User's sole cost except where the need for assistance is caused directly by DataPoint's material breach of this DPA, with data-subject / consumer requests and with the Platform User's obligations under GDPR Articles 32 to 36 or equivalent law, taking into account the nature of processing and information available to DataPoint; (f) delete or return Personal Data as required by Section 8; (g) make available information reasonably necessary to demonstrate compliance with this DPA and allow audits as set out in Section 9; and (h) notify the Platform User if DataPoint determines it can no longer meet its processing obligations under Applicable Data Protection Law.

3.2 Processing Prohibitions: DataPoint shall not: (a) sell or share Personal Data (as "sell" and "share" are defined under the CCPA); (b) retain, use, or disclose Personal Data for any purpose other than the specific business purposes specified in Annex 1, the Agreement, and this DPA, including any commercial purpose other than those business purposes; (c) retain, use, or disclose Personal Data outside the direct business relationship with the Platform User; or (d) combine Personal Data with personal information received from or on behalf of another person, except to perform the services or as otherwise permitted for service providers / processors under Applicable Data Protection Law.

3.3 Aggregated Learnings Safe Harbor: Section 3.2 does not restrict, limit, or prohibit DataPoint from compiling, retaining, and utilizing de-identified, anonymized, or aggregated data logs as described in Section 3.4 of Exhibit B (the MSA).

4. FDBR AND OTHER U.S. STATE PROCESSOR TERMS

Where the FDBR or another U.S. state privacy law applies to the platform traffic, DataPoint shall comply with the processor / service-provider obligations of that law, including cooperating with reasonable assessments and flowing equivalent data duties to approved downstream subprocessors. The Platform User remains solely and exclusively responsible for executing its controller / business obligations under those laws.

5. SECURITY MEASURES & BREACH SLA

5.1 Technical and Physical Safeguards: DataPoint shall maintain commercially reasonable administrative, technical, and physical safeguards designed to protect Personal Data, consistent with the cybersecurity baseline set forth in Section 3.6.1 of Exhibit B (the MSA) and appropriate to the risk under GDPR Article 32 where GDPR applies.

5.2 Personal Data Breach Notifications: Contractual Security Incident notifications under this DPA follow the email delivery channels set forth in Section 3.6 of Exhibit B (the "MSA").

“Personal Data Breach” for GDPR purposes means a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data DataPoint processes under this DPA. DataPoint shall notify the Platform User without undue delay after becoming aware of a verified Personal Data Breach, and shall provide information reasonably available to DataPoint to help the Platform User meet any legal notification duty. Electronic mail sent to the Platform User’s registered Notice Email satisfies DataPoint’s contractual notice obligations under this Section 5.2.

5.3 Notice Disclaimer and Burden Shift: Deliver of a Notice under this Section 5 is strictly an administrative update and under no circumstances constitutes an admission of fault or legal liability by DataPoint. Each Party remains responsible for notifications that applicable law requires that specific Party to send. The Platform User retains sole, exclusive responsibility for executing notices directed to its Advertisers and consumer end users unless a sovereign law requires DataPoint to notify a regulator directly.

6. SUBPROCESSORS

6.1 Authorized Ingestions: The Platform User authorizes DataPoint to engage subprocessors to process Personal Data for the purposes detailed in Annex 1. DataPoint’s current subprocessors are listed in Annex 3 of this Addendum or at a secure digital platform link DataPoint provides to the Platform User.

6.2 Flow-Down Duties: DataPoint shall impose written terms on each subprocessor that are no less protective of Personal Data than this DPA, and shall remain responsible to the Platform User for the subprocessor’s performance of those obligations.

6.3 Objection Mechanics: DataPoint shall give the Platform User prior notice of a new subprocessor (including by updating the list or URL). The Platform User may object on reasonable data-protection grounds within fifteen (15) days of posting. If the Parties cannot resolve the objection, the Platform User may stop using the affected feature or terminate the Agreement for convenience under Section 6.1 of the Agreement, completely bypassing the standard sixty (60) day convenience notice period.

7. INTERNATIONAL TRANSFERS

7.1 Processing Locations: DataPoint may process and transfer Personal Data in the United States and other countries where DataPoint or its subprocessors maintain active technical operations.

7.2 Standard Contractual Clauses (SCCs): If a transfer of Personal Data from the EEA, UK, or Switzerland requires a transfer mechanism under applicable law, the Parties are deemed to enter into: (a) the EU Commission Standard Contractual Clauses, Module Two (controller to processor), or Module Three (processor to processor) if the Platform User is itself a processor, including the 2021 SCCs and any required annexes completed by Annexes 1–3 of this DPA; and (b) the UK International Data Transfer Addendum to the EU SCCs, where the UK GDPR applies.

7.3 Transfer Hegemony: For purposes of those Clauses: DataPoint is “data importer,” the Platform User is “data exporter,” the governing law and clause-17/18 choices are Ireland for EU transfers, and Annex I–III of the Clauses are populated by this DPA’s Annexes. If the Clauses conflict with this DPA, the Clauses control for that specific international transfer.

8. RETURN AND DELETION

8.1 Terminal Purge Track: After termination or expiration of the Agreement, and after the complete closure of the wind-down window set forth in Section 8.1 of Exhibit B (the MSA), DataPoint shall, at the Platform User’s written election, delete or return Personal Data in DataPoint’s possession, except for: (a) copies retained as required by applicable law, or for strict legal, regulatory, or archival backup purposes, which copies remain subject to this DPA; and (b) de-identified, anonymized, or aggregated data blocks retained under Section 3.4 of Exhibit B (the MSA).

8.2 Deletion Timelines: Deletion shall occur within thirty (30) days after the Platform User’s written request or, if no request is made, within thirty (30) days after complete closure of the wind-down window, subject to backup-cycle deletion in the ordinary course of technical operations.

9. INFORMATION AND AUDITS

9.1 Compliance Overviews: Upon written request, no more than once per consecutive twelve (12) month period unless a Personal Data Breach or a sovereign regulator requires more, DataPoint shall provide a summary of relevant security documentation reasonably sufficient to demonstrate compliance with this DPA (for example, a security overview or third-party report if available).

9.2 Narrow Audit Scope: If that summary information is not reasonably sufficient, the Platform User may conduct a narrowly scoped audit of DataPoint’s controls relevant to Personal Data under this DPA, on thirty (30) days’ written Notice, during normal business

hours, subject to strict confidentiality under Section 5 of Exhibit B (the MSA), and without access to other customers' data or to DataPoint pricing, Deal IDs, or supply terms. DataPoint may require the audit to be performed by an independent professional bound by enforceable confidentiality duties. The Platform User bears its own audit costs unless the audit reveals a material breach of this DPA by DataPoint.

10. RISK AND LIABILITY CAPS

Liability under this DPA is strictly subject to the aggregate caps set forth in Section 7.1 of the Front Agreement. This DPA does not expand DataPoint's indemnity beyond Section 7.2 of Exhibit B (the MSA) or remove or limit the Platform User's primary indemnity under Section 7.1 of the MSA for Personal Data, Advertiser Data, or consents the Platform User failed to obtain.

11. DPA TERM

This DPA starts on the Effective Date and lasts until DataPoint ceases processing Personal Data under the Agreement, including any permitted archival retention under Section 8.

12. UNILATERAL UPDATE MECHANISMS & DPA URL CONTROL

This DPA is the DataPoint Data Processing Addendum published at datapoint.tech/legal/DPA (the "DPA URL"). The version published at the DPA URL on the Effective Date of the Agreement applies as of that date. DataPoint may update this DPA by publishing a new dated version at the DPA URL. No email, mail, signature, click-accept, or other Platform User approval is required to execute an update; publication at the DPA URL is the sole notice method for DPA updates and satisfies Section 1.2 of the Agreement for that purpose. Each updated DPA applies only to data processing that occurs on or after its specific posting date. An update published only at the DPA URL may not expand DataPoint's permitted use of Personal Data beyond Sections 3.4.1 and 3.4.4 of Exhibit B (the MSA) and Annex 1 of this DPA. Any such expansion requires an amendment executed under Section 9.2 of the MSA. This DPA forms part of the Agreement. If there is a conflict between this DPA and the Agreement on the processing of Personal Data, this DPA controls. Section 1.1 of the front-page Agreement is satisfied by this DPA at the DPA URL.

Annex 1 — Details of processing

Subject matter: Providing the AdMatric platform and related services under the Agreement (plan, activate, manage curated PMP/PG deals; reporting; billing; optimization; Partner Data if elected).

Duration: The Term plus wind-down and the retention in Section 8.

Nature and purpose: Storage, hosting, transmission, logging, reporting, delivery, fraud/IVT filtering, optimization, and support of campaigns configured by Platform User. Types of Personal Data (as submitted by Platform User): Account and user identifiers of Platform User personnel (name, email, login). Campaign instructions and targeting parameters. Advertiser brand and creative assets if they contain Personal Data. If Platform User uploads or activates it: first-party audience data, customer-match identifiers, cookie or device identifiers, IP address, coarse or precise location, and similar online identifiers. Log and performance data generated by delivery of those campaigns. DataPoint does not require special-category data. Platform User shall not upload it without prior written agreement.

Categories of data subjects: Platform User personnel; Advertiser personnel if included in account data; end users / consumers whose Personal Data Platform User or an Advertiser submits or whose identifiers are processed in ad delivery. Processing operations: As described in Exhibit B, §§ 1.1.2, 3.4.1, and 3.4.4.

Annex 2 — Security measures (summary)

DataPoint maintains, at a minimum:

- access controls and unique user authentication for production systems;
- encryption in transit for platform connections over public networks;
- encryption at rest for production datastores where commercially reasonable;
- logging and monitoring of production access;
- employee confidentiality obligations;
- vendor due diligence for subprocessors that process Personal Data;

- backup and restoration procedures;
- a process to assess and notify Security Incidents / Personal Data Breaches as provided in Section 5.

This Annex 2 is a summary, not a warranty of uninterrupted security.

Annex 3 — Subprocessors

Subprocessor	Purpose	Location
AWS	Hosting and storage	US East Region
AWS	Operational notices and support	US East Region