JAMLOOP

Data Processing Agreement

Version 1.0 | October 23, 2026

This Jamloop Data Processing Agreement ("**DPA**") governs the Processing of Customer Personal Information by Jamloop on behalf of the customer identified in an executed Jamloop Master Services Agreement, accepted Platform Terms and Conditions, Order, or other binding contract document (collectively, the "**Service Agreement**"). This DPA is incorporated into and governed by the Service Agreement.

1. Definitions

1.1 "Aggregated and Deidentified Data" means information derived from Customer Personal Information that Jamloop has aggregated, deidentified, or both, in accordance with Applicable US Data Protection Laws, and does not identify, and cannot reasonably be linked to, any individual, household, or device; provided that Jamloop shall not disclose such data externally in a manner that identifies Customer or individual without the applicable party's authorization.

1.2 "Applicable US Data Protection Laws" means the California Consumer Privacy Act, as amended by the California Privacy Rights Act (together, "**CCPA**"), and other United States state consumer privacy laws that apply to the Processing of Customer Personal Information under this DPA and the Service Agreement. Each law applies only to the extent of its territorial and material scope. References to a defined term include the analogous term under another Applicable US Data Protection Law where appropriate.

1.3 "Customer Personal Information" means Personal Information that Jamloop Processes on behalf of Customer under this DPA. Customer Personal Information does not include information that has been validly deidentified and aggregated in accordance with Applicable US Data Protection Laws or Personal Information for which Jamloop independently determines the purposes and means of Processing, including account administration, billing, security, fraud prevention, and legal compliance.

1.4 "Instructions" means Customer's documented instructions set forth in the Service Agreement, this DPA, an applicable Order or Statement of Work, Platform configuration, or another writing or authenticated electronic instruction agreed to by authorized representatives of the parties.

1.5 "Personal Information" means any information relating to an identified or identifiable individual where such information is protected similarly as personal data, personal information, or personally identifiable information under applicable data protection laws that Jamloop processes on behalf of Customer pursuant to the Service Agreement. Personal Information does not include Aggregated and Deidentified Data as described in this DPA.

1.6 "Platform and Performance Data" means technical, operational, diagnostic, security, and usage information generated through the operation or use of the Services, including system logs, performance metrics, feature-usage information, and information concerning the configuration and administration of Customer's account. Platform and Performance Data does not include Customer Personal Information except to the limited extent necessary for account administration, billing, security, fraud prevention, or legal

compliance. Jamloop may use Platform and Performance Data to operate, maintain, secure, support, and improve the Services and may use or disclose Aggregated and Deidentified Data in accordance with Section 9.2.

1.7 "Security Incident" means a confirmed breach of security resulting in accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Information Processed by Jamloop. Security Incident excludes unsuccessful attempts or activities that do not compromise Customer Personal Information, including pings, port scans, denial-of-service attempts, blocked attacks, and unsuccessful login attempts.

1.8 "Services" means the services described in the Service Agreement and applicable Order or Statement of Work, including the audience activation, measurement, attribution, optimization, reporting, and related services identified in Exhibit A.

Capitalized terms not defined in this DPA shall have the same meaning as set forth in the Service Agreement or Applicable US Data Protection Law.

2. Roles

2.1 Customer.

(a) As an Advertiser. When Customer is an Advertiser, it determines the purposes and means of Processing Customer Personal Information, and acts as a "Business" or "Controller"; Jamloop acts as a "Service Provider" or "Processor".

(b) As an Agency**.** When Customer is an Agency, it acts as a Service Provider or Processor for an Advertiser or other Business or Controller. Customer represents that it is authorized to appoint Jamloop and provide Instructions on that party's behalf. Jamloop acts as Customer's Subprocessor or Service Provider, as applicable, for the processing covered by this DPA. Customer remains responsible for communicating any upstream instructions or restrictions to Jamloop.

(c) As an Enterprise. Where Customer is an Enterprise, it determines the purposes of Processing Customer Personal Information, and acts as a "Business" or "Controller"; Jamloop acts as a "Service Provider or "Processor".

2.2 Jamloop as a Business or Controller. Jamloop acts as a Business or Controller where it independently determines the purposes and means of processing, including the processing of Platform and Performance Data (and any included Personal Information) and Aggregated and Deidentified Data.

3. Permitted Processing; Restrictions; Personnel; AI Features

3.1 Permitted Processing. Jamloop shall Process Customer Personal Information solely: (a) to provide the Services described in the Service Agreement, applicable Order, or Statement of Work; (b) on behalf of and for the business purposes of Customer or the applicable Advertiser; (c) in accordance with Instructions; and (d) as otherwise permitted for a service provider, contractor, or processor under Applicable US Data Protection Laws. Instructions shall not require Jamloop to violate Applicable US Data Protection Laws. A description of the Processing is in Exhibit A.

3.2 Restrictions and Data Integration.

3.2.1 Restrictions. Except as expressly permitted by Applicable US Data Protection Laws, Jamloop shall not: (a) Sell Customer Personal Information for monetary or other valuable consideration; (b) Share Customer Personal Information for cross-context behavioral advertising or use it to provide targeted advertising for a person other than Customer or the applicable Advertiser; (c) retain, use, or disclose Customer Personal Information outside the direct business relationship between Customer and Jamloop, as described in the Service Agreement; (d) combine Customer Personal Information with Personal Information received from or on behalf of another person, or collected from Jamloop's own interaction with

a Consumer, except as permitted under subsection 3.2.2; or (e) attempt to reidentify information maintained as Aggregated and Deidentified except as permitted by law or expressly authorized in writing by Customer.

3.2.2 Data Integration. Subject to Customer's Instructions and Applicable US Data Protection Laws, Jamloop may match, combine, transform, analyze, or otherwise Process Customer Personal Information with data received from service providers, subprocessors, advertising-supply partners, measurement providers, identity-resolution providers, or other authorized sources identified in the Service Agreement or Customer's documented Instructions solely to provide the Customer-specific Services. Such Processing may include: (a) audience onboarding, matching, segmentation, and activation; (b) identity resolution and cross-device or household-level matching; (c) ad selection, delivery, frequency management, optimization, and fraud prevention; (d) attribution based on website activity, campaign events, offline transactions, or visits to permitted physical locations; (e) analytics, reporting, and reconciliation; and (f) security, troubleshooting, quality assurance, and verification of the Services.

Jamloop shall not use data integration permitted under this subsection to build or materially enrich a profile or audience for the independent benefit of Jamloop, another customer, or a third party, except through Aggregated and Deidentified Data maintained and used in accordance with Section 9.2.

3.2.3 Independent-Controller Processing. Processing for which Jamloop independently determines the purposes and means is outside the scope of the service-provider and processor restrictions in this Section 3.2 and shall be governed by Section 2.2 and Jamloop's applicable privacy notice, as applicable.

3.3 Authorized Personnel and Advisers. Jamloop shall ensure that any person it authorizes to Process Customer Personal Information has agreed to protect it in accordance with Jamloop's confidentiality obligations or is otherwise under a legal duty of confidentiality. Jamloop may disclose Customer Personal Information to advisers, auditors, and other third parties as reasonably required to perform its obligations, subject to applicable confidentiality and data-protection requirements.

3.4 AI Features. To the extent Jamloop makes available any artificial intelligence, machine-learning, or similar functionality as part of the Services ("AI Features"), any Personal Information included in Customer's prompts, inputs, configurations, or other materials submitted to an AI Feature ("AI Inputs"), or contained in responses, recommendations, analyses, or other results generated by an AI Feature ("AI Outputs"), shall constitute Customer Personal Information and remain subject to this DPA.

4. Compliance; Certification

4.1 Compliance. Jamloop shall comply with obligations applicable to it under Applicable US Data Protection Laws and shall provide the same level of protection for Customer Personal Information as is required under Applicable US Data Protection Laws applicable to Customer.

4.2 Certification. Jamloop certifies that it understands and will comply with the restrictions and obligations set forth in this DPA and Applicable US Data Protection Laws.

5. Advertising Services; Consumer Choice; Customer Warranties; Customer Indemnity

5.1 Customer-Specific Advertising Services. Jamloop Processes Customer Personal Information as Customer's service provider, contractor, processor, or subprocessor, as applicable, when Jamloop performs Customer-specific audience activation, identity matching, ad delivery, frequency management, fraud prevention, campaign optimization, website-pixel attribution, offline-sales attribution, foot-traffic attribution, analytics, reporting, or related Services, as described in the Service Agreement.

The parties intend that Customer's disclosure of Customer Personal Information to Jamloop, and Jamloop's disclosure of such information to an authorized service provider, subprocessor, or advertising-supply partner solely to provide the Customer-specific Services, will not constitute a Sale for monetary or other valuable consideration or Sharing for cross-context behavioral advertising, to the extent

permitted by Applicable US Data Protection Laws. The legal characterization of each activity shall depend on the actual data flow, purpose, recipient, contractual restrictions, and Applicable US Data Protection Laws.

5.2 Consumer Choice. To the extent required by Applicable US Data Protection Laws, Customer shall: (a) provide required notices at or before collection and in its public-facing privacy policy; (b) obtain and maintain rights, permissions, and authorizations necessary to disclose Customer Personal Information to Jamloop; (c) provide any legally required methods to opt out of Sale, Sharing, or targeted advertising; (d) recognize and honor qualifying opt-out preference signals, including Global Privacy Control; (e) not disclose to Jamloop Customer Personal Information for which a Consumer has exercised an applicable right unless the disclosure and Processing remain legally permitted; and (f) provide timely, accurate, and technically usable suppression instructions reasonably necessary for Jamloop to honor applicable Consumer choices. Jamloop shall have no liability for Processing where Customer fails to provide a valid suppression instruction.

5.3 Customer Warranties. Customer represents and warrants that: (a) its Instructions and disclosure of Customer Personal Information comply with Applicable US Data Protection Laws; (b) it has provided any and all required notices and obtained any and all required consents to provide Customer Personal Information to Jamloop for Processing; (c) it will not instruct Jamloop to Process information for a prohibited purpose; (d) Customer Personal Information will not include information prohibited by Exhibit A or Applicable US Data Protection Laws; and (e) it will promptly notify Jamloop of a Consumer choice, regulator direction, or change in law that affects the lawfulness of the Services. Jamloop may suspend affected Processing on reasonable notice if it reasonably determines continued Processing would violate Applicable US Data Protection Laws.

5.4 Customer Indemnity. Customer will defend, indemnify, and hold harmless Jamloop and its Affiliates, and their officers, directors, employees, and agents, from third-party claims, regulatory investigations or proceedings, damages, fines, penalties, liabilities, costs, and expenses, including reasonable attorneys' fees, to the extent arising from Customer's breach of its obligations in Section 5.2 or Section 5.3, except to the extent caused by Jamloop's breach of this DPA, violation of Applicable US Data Protection Laws, gross negligence, or willful misconduct.

6. Consumer Requests and Assistance

6.1 Assistance. To the extent legally required, Jamloop shall provide reasonable assistance to Customer to enable Customer to respond to verifiable Consumer requests, including access, deletion, correction, opt-out of Sale or Sharing (where applicable), and limitation of use or disclosure of Sensitive Personal Information.

6.2 Requests Received by Jamloop. If Jamloop receives a Consumer request directly that identifies Customer, Jamloop shall promptly notify Customer and refrain from responding except to direct the Consumer to Customer, unless Customer directs Jamloop to respond in writing or applicable law requires it.

7. Notice of Inability to Comply; Remediation

7.1 Notice. Jamloop shall promptly notify Customer if it determines that it can no longer meet its obligations under Applicable US Data Protection Laws or this DPA.

7.2 Remediation. Upon notice, Customer may direct Jamloop to take reasonable and appropriate steps to stop and remediate unauthorized Processing. Jamloop shall cooperate in good faith to implement remediation.

8. Service Providers or Subprocessors

8.1 Notice. Jamloop may engage service providers or subprocessors to Process Customer Personal Information on Customer's behalf with prior written notice to Customer. Jamloop's current service providers are listed in Exhibit B. Notice may be provided by email or through a maintained online subprocessor list identified in the Service Agreement.

8.2 Objection. Customer may object to a new service provider within ten (10) business days after notice solely on reasonable, documented data-protection grounds. The parties shall work in good faith to address the objection. If no commercially reasonable resolution is available, Jamloop may elect not to use the proposed provider for Customer or permit Customer to terminate only the affected Service without penalty for future unused Services.

8.3 Data Protection Obligations; Responsibility. Jamloop shall impose written data-protection obligations on its service providers and subprocessors consistent with applicable requirements of this DPA and remains liable for their acts and omissions to the extent required by Applicable US Data Protection Laws.

9. Security; Aggregated and Deidentified Data

9.1 Security. Jamloop shall implement and maintain reasonable administrative, technical, and physical safeguards appropriate to the nature of Customer Personal Information and risks presented by Processing, including access controls, encryption in transit and at rest where commercially reasonable, vulnerability management, personnel confidentiality obligations, incident-response procedures, vendor-management controls, and secure disposal.

9.2 Aggregated and Deidentified Data. Jamloop may create Aggregated and Deidentified Data from Customer Personal Information processed in connection with the Services, and Jamloop may use and disclose such data for its lawful business purposes, including to operate, maintain, secure, analyze, develop, and improve its products and services; conduct research and analytics regarding the performance of the Services; and generate industry insights and benchmarking reports. Any such Aggregated and Deidentified Data shall be maintained and used in accordance with Applicable US Data Protection Laws and Jamloop will implement appropriate technical safeguards, business processes, and public commitments that reasonably prevent reidentification. Jamloop shall not use or disclose any Aggregated and Deidentified Data in a manner that identifies Customer or any individual and shall not attempt to re-identify Aggregated and Deidentified Data, except as permitted by applicable law or expressly authorized in writing by Customer.

10. Security Incident Notification and Response

10.1 Notification. Jamloop shall notify Customer in writing without undue delay after confirming, based on reasonably available information, a Security Incident affecting Customer Personal Information. Notice shall include information reasonably available concerning the nature and scope of the Security Incident, affected data categories, mitigation measures, and a Jamloop contact. Jamloop may provide information in phases as it becomes available. Jamloop's notice or cooperation does not constitute an admission of fault or liability.

10.2 Response. Jamloop shall take reasonable steps to contain, investigate, and remediate the Security Incident and reasonably cooperate with Customer. Customer is responsible for determining whether notice to End Consumers or regulators is required and for issuing notice, except to the extent Jamloop has an independent legal obligation.

10.3 Incident Plan. Jamloop shall maintain an incident-response plan and reasonably coordinate with Customer on incident-response activities.

11. Assessments; Audit and Monitoring

11.1 Compliance Information. At Customer's reasonable request, Jamloop shall make available information necessary to demonstrate compliance with this DPA and Applicable US Data Protection Laws. Jamloop may satisfy the request through current independent audit reports, certifications, summaries, or questionnaires.

11.2 Audit. If those materials are reasonably insufficient, Customer may conduct one audit in any rolling twelve-month period, except following a confirmed material Security Incident or a legally binding request. An audit must be conducted on at least thirty (30) days' notice, during normal business hours, without unreasonable interference, and subject to confidentiality, security, privilege, and other appropriate protections. Customer bears audit costs unless the audit identifies Jamloop's material breach of this DPA.

12. Return or Deletion

12.1 Deletion or Return. Except where Jamloop is acting as an independent Business or Controller, upon termination or expiration of applicable Services, or Customer's written request where required by Applicable US Data Protection Laws, Jamloop shall delete Customer Personal Information from its active production systems within thirty (30) days, unless retention is permitted or required by applicable law or this DPA. At Customer's written request submitted before such deletion, Jamloop shall make Customer Personal Information available for return in a commonly used format supported by the Services, to the extent technically feasible.

12.2 Backup and Archival Systems. Customer Personal Information stored in backup, archival, disaster-recovery, logging, or other systems not reasonably accessible in the ordinary course shall not be subject to immediate deletion or return. Jamloop may retain such information until it is deleted or overwritten in accordance with Jamloop's standard retention and backup cycles. If retained information is restored to an active system, Jamloop shall apply the deletion requirements of Section 12.1.

12.2 Other Permitted Retention. Jamloop may retain Customer Personal Information to the extent and for the period reasonably necessary for legal or regulatory compliance, legal holds, security, fraud prevention, dispute resolution, or the establishment, exercise, or defense of legal claims. Retained information remains protected under this DPA, shall not be used for another purpose, and shall be deleted when the retention basis expires. Jamloop may retain Deidentified and Aggregated Data maintained in accordance with applicable law.

13. EEA, UK or Swiss Data Subjects.

The parties agree that if Personal Information of Data Subjects located in European Economic Area, United Kingdom or Switzerland are to be processed by Jamloop, the parties will enter into an appropriate GDPR Data Processing Agreement or other contract document to authorize the Processing. Customer shall notify Jamloop before enabling any Processing reasonably expected to involve such Personal Information.

14. Liability and Precedence

14.1 Liability. Except to the extent prohibited by Applicable US Data Protection Laws, all liability arising out of or relating to this DPA is subject to the indemnification, exclusions, and limitations of liability in the Service Agreement.

14.2 Conflict. If the Service Agreement and this DPA conflict, this DPA controls solely with respect to Processing of Customer Personal Information; otherwise, the Service Agreement controls.

15. Term

15.1 Term. This DPA commences on the effective date of the Service Agreement and continues for so long as Jamloop Processes Customer Personal Information on Customer's behalf, including any permitted retention period.

EXHIBIT A — DESCRIPTION OF PROCESSING

Processing Item	Description
Subject of Processing	Providing the Services described in the Jamloop Master Services Agreement, accepted Platform Terms and Conditions, Order, or other binding contract document.
Nature and Purpose	Operating, securing, supporting, measuring, optimizing, and reporting CTV and related advertising Campaigns, including audience activation, data matching or combining, ad delivery, frequency management, fraud prevention, website-pixel attribution, offline-sales attribution, foot-traffic attribution, analytics, and customer support.
Categories of Data Subjects	● Customer's employees and other authorized persons ● SSP (supply-side provider) advertisement viewers ● End Consumers (i.e., persons who purchase an advertised product from the Customer and devices associated with visits to Customer-designated physical locations)
Types of Personal Information	● Customer's employees and other authorized persons: name, business address, email, phone number, IP address ● SSP advertisement viewers: IP address, device mobile advertising ID, geolocation information (e.g., ZIP code, latitude/longitude, device-derived location and/or geographic-IP lookup, if provided by Customer, service provider or data provider) ● End Consumers: name, physical addresses, phone number; email, IP address, mobile device advertising ID, tracking cookies and pixels, IFAs, impression and campaign-event data, and direct identifiers supplied by Customer for offline identity resolution (e.g., name, address, IP address, email and/or CRM ID, if provided by Customer, service provider or data provider)
Sensitive Data	N/A - Not permitted unless separately approved in writing after legal review. Excluded categories include payment-card authentication data, account credentials, government identifiers, health or consumer-health information, biometric data, , children's data, and other information not expressly listed.
Sensitive Locations	No Processing relating to End Consumers' visits to healthcare or reproductive-health facilities, places of worship, addiction-treatment centers, shelters, correctional facilities, educational institutions primarily serving children, or other locations designated by Jamloop, unless separately approved in writing after legal review.
Duration	For the period stated in the Service Agreement plus permitted backup, legal-retention, security, fraud-prevention, and dispute periods.
Frequency	Continuous, periodic, or Campaign-based, as configured by Customer or stated in an Order.

EXHIBIT B — SERVICE PROVIDERS / SUBPROCESSORS

Name	Description of Processing	Contact	Location
AWS	Cloud storage and infrastructure	aws-security@amazon.com	United States
Snowflake	Data warehousing, data engineering, and secure data sharing	privacy@snowflake.com / dpo@snowflake.com	United States
Clerk	User authentication and management	privacy@clerk.dev	United States

Name	Description of Processing	Contact	Location
Vercel	Developer tools and cloud infrastructure	privacy@vercel.com	United States
Cloudflare	Cybersecurity, performance optimization, and serverless computing	dpo@cloudflare.com	United States
HubSpot	Customer relationship management	privacy@hubspot.com	United States
Salesforce	Customer relationship management	privacy@salesforce.com	United States
PostHog	Developer and product analytics	privacy@posthog.com	United States
Experian (TapAd)	Digital identity resolution and cross-device marketing	privacy@experian.com	United States
Semcasting	Digital identity and first-party data enhancement	privacychoice@semcasting.com	United States
OnSpot	Provisioning and processing of location and point-of-interest–based data	nfo@onspotdata.com	United States
Echo Analytics	Provisioning and processing of location and point-of-interest–based data	https://www.echo-analytics.com/contact	France
Evorra	Digital identity and first-party data enhancement	privacy@evorra.com	United States
Aristotle International, Inc.	Digital identity and first-party data enhancement	info@aristotle.com	United States
PDI (Political Data Inc.)	Provisioning and processing of California voter file segments	Info@politicaldata.com	United States
Jounce Media	Programmatic supply path optimization (SPO), inventory quality verification, publisher authorization analysis, and adtech analytics services	contact@jouncemedia.com	United States
TransUnion	Digital identity matching, audience data onboarding, segment enrichment, and cross-channel media activation services	privacy@transunion.com	United States
Intuizi	Location intelligence analytics, point-of-interest (POI) visitation measurement, behavioral signal aggregation, and privacy-compliant audience activation	security@intuizi.com	United States
GepEdge - Five Media Marketing Ltd. d/b/a GeoEdge)	Ad security, ad verification, malvertising protection and ad quality monitoring services,	Privacy@geoedge.com	Israel