Data Processing Agreement
(for Lotame Master Services Agreement)

This Data Processing Agreement (this "**DPA**") is entered into between Lotame Solutions, Inc. ("**Lotame**") and the entity identified as Customer in the Agreement (individually "**a party**" and collectively "**the parties**") and forms a part of and is incorporated by reference into the Agreement. This DPA memorializes the parties' agreement regarding the Processing of Personal Data (defined in the Agreement) under Applicable Data Protection and Privacy Laws.

The parties agree to comply with the following provisions with respect to the Processing of Personal Data, each acting reasonably and in good faith.

1. **Definitions.** Capitalized words used but not defined in this DPA have the meanings given in the Agreement.

"**Agreement**" means the Lotame Master Services Agreement between Lotame and Customer.

"**Applicable Data Protection and Privacy Law**" means a Data Protection and Privacy Law that is applicable to the Processing of Customer Data, Sightings Data, or Lotame Data.

"**DPA Schedules**" means the schedules for any Applicable Data Protection and Privacy Laws available at https://www.lotame.com/privacy/dpas/dpa-msa/, which include additional requirements applicable to the Processing of Customer Data, Sightings Data, and Lotame Data by the parties under Applicable Data Protection and Privacy Laws.

"**Security Incident**" means a breach of Lotame's security leading to the unauthorized disclosure of, or access to, Customer Data, or Customer's security leading to the unauthorized disclosure of, or access to, Lotame Data.

"**Supervisory Authority**" means a governmental agency that can regulate or investigate a party under any law or an independent public authority that is established by or pursuant to an Applicable Data Protection and Privacy Law to regulate and enforce that law.

"**User Rights Request**" means a request from a User to exercise rights provided to them under an Applicable Data Protection and Privacy Law.

2. Contractual Relationship.

2.1 **Contractual Relationship between Customer and Lotame.** Upon the signing of the Agreement by both parties this DPA will become legally binding between Customer and Lotame as of the effective date of the Agreement. Except as expressly stated in this DPA, this DPA does not modify or replace any obligations contained in the Agreement.

2.2 **Contractual Relationship with Third Party Sources.** If Customer Data or Sightings Data includes any Personal Data from Third Party Sources:

(a) This DPA is not a binding agreement between Lotame and any Third Party Sources. Customer must have its own data processing agreement or other agreement with its Third Party Sources to address the Processing by Lotame of Customer Data and Sightings Data from the Third Party Sources when required by an Applicable Data Protection and Privacy Law. Customer is responsible for coordinating all communication from Third Party Sources addressed to Lotame in relation to this DPA.

(b) Except where an Applicable Data Protection and Privacy Law requires that Third Party Sources be permitted to exercise a right or seek any remedy under this DPA against Lotame directly, (i) solely Customer may exercise any such right or seek any such remedy against Lotame on behalf of the Third Party Source, and (ii) Customer shall exercise any such rights under this DPA in a combined manner for itself and all of its Third Party Sources together and not individually.

3. **Incorporation of DPA Schedules.** A DPA Schedule for an Applicable Data Protection and Privacy Law will be incorporated by reference into this DPA *only when* Customer Data, Sightings Data, or Lotame Data is or includes Personal Data subject to that Applicable Data Protection and Privacy Law. If Customer Data, Sightings Data, or Lotame Data is not or does not include any Personal Data subject to an Applicable Data Protection and Privacy Law, then the DPA Schedule for that Applicable Data Protection and Privacy Law is not applicable and will not be incorporated into this DPA.

4. Processing of Customer Data and Sightings Data.

4.1 **Generally.** Customer, with respect to its Processing related to the collection and provision of Customer Data and Sightings Data to Lotame, and Lotame, with respect to its Processing of Customer Data and Sightings Data received under the Agreement, shall

comply with all Applicable Data Protection and Privacy Laws, this DPA, and the DPA Schedules for the Applicable Data Protection and Privacy Laws.

4.2 Providing Notices to Users and Obtaining Consents from Users. Without limiting the generality of the obligations under Section 4.1, Customer has the sole responsibility for (and shall ensure each Third Party Source does the same) (a) disclosing to Users at the time of collection the Processing of Customer Data and Sightings Data from the Property by Lotame (or by a third-party if Customer prefers to not specifically name Lotame) for the purposes contemplated by the Agreement and, if Lotame Code is used, the usage of third-party technology to collect Customer Data and Sightings Data from the Property when required under Applicable Data Protection and Privacy Laws, and (b) obtaining Users' consent to the Processing of their Personal Data for the purposes contemplated by the Agreement when required under Applicable Data Protection and Privacy Laws. Where Customer obtains Customer Data and Sightings Data from a Third Party Source, Customer may discharge the obligations in this section through a data processing or other agreement with the Third Party Source containing substantially similar requirements as set forth in this section.

4.3 Cross-Border Transfers. Customer acknowledges that Lotame's primary Processing activities take place in the United States. When an Applicable Data Protection and Privacy Law has requirements related to the cross-border transfers of Personal Data, the parties will comply with the Applicable Data Protection and Privacy Law and the provisions in the applicable DPA Schedule related to the transfer of Customer Data and Sightings Data to the United States.

4.4 Responding to User Rights Requests. This section describes how Lotame handles User Rights Requests in general. If an Applicable Data Protection and Privacy Law has additional or different requirements than what is described in this section, the applicable DPA Schedule will supersede this section.

(a) *User Rights Requests Received by Lotame from Customer*. For any User Rights Requests that Customer directly receives and forwards to Lotame, Lotame will provide reasonable assistance to Customer in fulfilling Customer's obligations under Applicable Data Protection and Privacy Law to respond to the User Rights Request. To the extent legally permitted, Customer shall be responsible for any costs arising from Lotame's provision of such assistance. Lotame may make available an API or other mechanism to Customer for the submission of User Rights Requests.

(b) *User Rights Requests Received by Lotame Directly from a User.* Lotame has created a tool and uses third party services to enable a User to exercise their rights under any Data Protection and Privacy Laws, which can be accessed at https://www.lotame.com/privacy/privacy-manager/ ("**Privacy Tools**"). If Lotame receives a User Rights Request through a Privacy Tool and the User Rights Request specifically references Customer, then Lotame will promptly forward the User Rights Request to Customer and assist Customer as set forth in Section 4.4(a).

4.5 Security.

(a) Lotame shall (and shall require its Subcontractors to) employ appropriate physical, technical and organizational measures to protect against a Security Incident in accordance with industry standards, the requirements in an Applicable Data Protection and Privacy Law, and any applicable DPA Schedule ("**Lotame Security Measures**," which are attached as Schedule 1 to this DPA).

(b) Lotame's Information Security Management System is ISO/IEC 27001:2013 certified. Lotame uses external auditors to verify the adequacy of its security measures and controls, including the security of its Subcontractors. This audit: (a) will be performed annually; (b) will be performed according to ISO/IEC 27001:2013 standards or such other alternative standards that are substantially equivalent to ISO/IEC 27001:2013; (c) will be performed by independent third-party security professionals; and (d) will result in the generation of an audit report ("**Report**"), which will be Lotame's Confidential Information.

(c) Lotame will assist Customer in ensuring compliance with Customer's obligations relating to security of Lotame's processing of Customer Data and Security Incidents under Applicable Data Protection and Privacy Laws by:

(1) implementing and maintaining the Lotame Security Measures while this DPA is in effect;

(2) complying with the terms of Section 4.6 (Security Incident Notification); and

(3) providing Customer with the documents and information described in Section 4.7 (Audits to Verify Compliance with this DPA).

(d) Lotame has no obligation to protect Customer Data that Customer elects to transfer outside of Lotame's and its Subcontractors' systems.

4.6 Security Incident Notification. If Lotame has determined that a Security Incident has occurred, Lotame will (1) notify Customer of the Security Incident without undue delay but no later than the timeframes set forth in an Applicable Data Protection and Privacy Laws, and (2) promptly take appropriate measures to address the Security Incident, including measures to mitigate any adverse

effects resulting from the Security Incident in accordance with its established procedures. Lotame's reporting of a Security Incident in accordance with this section is not and will not be construed as an acknowledgement by Lotame of any fault or liability with respect to the Security Incident. Lotame will cooperate with and provide reasonable assistance to Customer by including in the notification such information about the Security Incident as Lotame is able to disclose to enable Customer to notify Supervisory Authorities or Users (as applicable) of the Security Incident as may be required under an Applicable Data Protection and Privacy Law, taking into account the information available to Lotame, and any restrictions on disclosing the information related to the Security Incident. Notification of Security Incidents will be delivered to the Data Protection/Privacy Contact identified in the Agreement via email. It is each party's sole responsibility to ensure it maintains accurate contact information at all times. Customer is solely responsible for complying with incident notification laws applicable to Customer and fulfilling any third-party notification obligations related to any Security Incident (for example, to Third Party Sources).

4.7 Audits to Verify Compliance with this DPA.

(a) At Customer's written request, and provided that the parties have an effective non-disclosure or confidentiality agreement in place, Lotame will provide Customer with (1) a copy of the Report referenced in Section 4.5(b) so that Customer can verify Lotame's compliance with its obligations under this DPA and (2) any other documents and information Lotame deems necessary to demonstrate Lotame's compliance with its obligations set forth in this DPA.

(b) In response to a request by Customer that the Report, documents, or information provided in Section 4.7(a) do not sufficiently demonstrate Lotame's compliance, Lotame will allow for and contribute to an audit, conducted by Customer or an auditor designated by Customer (at the Customer's sole cost) by making available to Customer additional documents and information reasonably requested that demonstrates Lotame's compliance with its obligations set forth in this DPA. Customer shall reimburse Lotame for any costs or expenses incurred by Lotame in completing an audit.

(c) Lotame has no obligation to complete an audit if Lotame has completed a Customer-requested audit during the previous 12-month period ending on the date of the most recent request. Except for audits conducted at Lotame's premises or physical facilities, Customer shall provide Lotame with no less than 30 days' prior notice before commencing any audit. Audits may be conducted at Lotame's premises or physical facilities only when an Applicable Data Protection and Privacy Law allows for such in-person audits, and in such a case, Customer shall provide Lotame with no less than 45 days' prior notice, carry out the audit only during Lotame's standard business hours, and cause minimal disruption to Lotame's operations. Under no circumstances will Lotame provide Customer or its auditor with access to any facilities of its Subcontractors, any data of any other customer of Lotame, any of Lotame's internal accounting or financial information, any trade secret of Lotame, any information that, in Lotame's reasonable opinion, is not relevant to verifying Lotame's compliance with its obligations under this DPA or that could: (1) compromise the security of Lotame's systems or premises; or (2) cause Lotame to breach its obligations under Applicable Data Protection and Privacy Laws, or (3) its security and/or privacy obligations to another customer or any third party. Additionally, Customer shall take all reasonable measures to combine all audits into one single audit on behalf of itself and all of its Third Party Sources.

4.8 Customer Instructions. Customer acknowledges that certain Platform settings and elections initiated by Customer through its use of the Services may affect how the Platform Processes Customer Data ("**Customer Initiated Settings**"). This DPA, the Agreement, and Customer Initiated Settings constitute Customer's documented instructions regarding Lotame's Processing of Customer Data ("**Documented Instructions**"). Lotame will Process Customer Data only in accordance with Documented Instructions. Customer further acknowledges that (a) Customer is solely responsible for ensuring that its Documented Instructions complies with all Applicable Data Protection and Privacy Laws and, when applicable, its agreements with Third Party Platforms and Third Party Sources and (b) Lotame will not verify that Customer's Documented Instructions are likely to violate any Applicable Data Protection and Privacy Law. This section does not negate Customer's right to communicate additional instructions to Lotame regarding the Processing of Customer Data; however, with respect to any other instructions, such instructions must be provided to Lotame in writing and may require prior written agreement between Customer and Lotame, including agreement on any additional fees payable by Customer to Lotame for carrying out such instructions. Lotame is under no obligation to modify the Services or the Platform to accommodate such additional instructions.

4.9 Subcontractors.

(a) Customer generally authorizes Lotame to engage the Subcontractors listed in Schedule 2 of this DPA in connection with the provision of the Services, which Subcontractors may process Customer Data. When engaging a Subcontractor, Lotame will (1) ensure via a written contract, which will include terms (i) no less protective than those in this DPA related to the processing of Customer Data and (ii) that the Subcontractor will only access and use Customer Data to the extent required to perform the obligations contracted to it and in accordance with Applicable Data Protection and Privacy Laws and (2) remain fully liable for all obligations subcontracted to, and all acts and omissions of, the Subcontractor.

(b) Lotame will, when required by Applicable Data Protection and Privacy Laws, provide Customer with at least 60 days advance notice of new Subcontractors that will process Customer Data. Lotame will provide an opportunity for Customer to object to such new Subcontractors where required by Applicable Data Protection and Privacy Laws. If Customer objects to a new Subcontractor, Lotame will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid the processing of Customer Data by the objected-to new Subcontractor without unreasonably burdening Customer. If Lotame is unable to make available such a change within 30 days, Customer may terminate only those Services that cannot be provided by Lotame without the use of the new Subcontractor by providing written notice to Lotame. If Customer fails to object to Lotame's use of a new Subcontractor within the period set forth in this section, then the new Subcontractor will be deemed accepted by Customer.

5. Processing of Lotame Data.

5.1 Generally. Lotame, with respect to its Processing related to the provision of Lotame Data to Customer, and Customer, with respect to its Processing of Lotame Data received under the Agreement, shall comply with all Applicable Data Protection and Privacy Laws, this DPA, and the DPA Schedules for the Applicable Data Protection and Privacy Laws.

5.2 Notices and Consents. When required under an Applicable Data Protection and Privacy Law, Lotame will contractually require that its licensors of Lotame Data: (a) disclose to Users the purposes for the Processing of their Personal Data and (b) obtain Users' consent to the Processing of their Personal Data by Lotame and Customer for the purposes contemplated by the Agreement. Lotame's Services Privacy Notice related to its Processing of Lotame Data is located at https://www.lotame.com/privacy/privacy-notices/services/.

5.3 User Rights Requests. For any User Rights Requests related to Lotame Data that Customer directly receives, Lotame will assist Customer in fulfilling Customer's obligations, if any, under Applicable Data Protection and Privacy Laws to respond to the User Rights Request. If Customer receives a User Rights Request that specifically references Lotame, Customer shall promptly forward the User Rights Request to Lotame and assist Lotame in fulfilling Lotame's obligations under Applicable Data Protection and Privacy Laws to respond to the User Rights Request. Lotame may make available an API or other mechanism to Customer for the submission of User Rights Requests.

5.4 Security. Customer shall (and shall require its Vendors) employ appropriate physical, technical and organizational measures to protect against a Security Incident in accordance with industry standards, the requirements in Applicable Data Protection and Privacy Laws, and any applicable DPA Schedule ("**Customer Security Measures**"). Customer shall audit the adequacy of its Customer Security Measures, including its Vendors, at least annually. This audit: (a) will be performed according to ISO/IEC 27001:2013 standards or such other alternative standards that are substantially equivalent to ISO/IEC 27001:2013; (b) will be performed by independent third-party security professionals; and (c) will result in the generation of an audit report, which will be Customer's Confidential Information.

5.5 Security Incident Notification. If Customer has determined that a Security Incident has occurred, Customer shall (1) notify Lotame of the Security Incident without undue delay but no later than the timeframes set forth in an Applicable Data Protection and Privacy Laws, and (2) promptly take appropriate measures to address the Security Incident, including measures to mitigate any adverse effects resulting from the Security Incident in accordance with its established procedures. Customer's obligation to report a Security Incident under this section is not and will not be construed as an acknowledgement by Customer of any fault or liability with respect to the Security Incident. Customer will cooperate with and provide reasonable assistance to Lotame by including in the notification such information about the Security Incident as Customer is able to disclose to enable Lotame to notify Supervisory Authorities or its customers (as applicable) of the Security Incident as may be required under an Applicable Data Protection and Privacy Law, taking into account the information available to Customer, and any restrictions on disclosing the information related to the Security Incident. Notification of Security Incidents will be delivered to Lotame at privacy@lotame.com and to Customer at the Data Protection/Privacy Contact identified in the Agreement via email. It is each party's sole responsibility to ensure it maintains accurate contact information at all times. Lotame is solely responsible for complying with incident notification laws applicable to Lotame and fulfilling any third-party notification obligations related to any Security Incident (for example, to its customers).

6. Processing of Personal Data by Customer that is Provided by a Collaboration Data Provider.

Lotame's Platform provides functionality whereby Customer can create or analyze Audiences using Personal Data shared by another Lotame customer ("**Collaboration Data Provider**"). Customer acknowledges that (a) it is obtaining Personal Data directly from the Collaboration Data Provider, (b) Lotame is only facilitating the access to the Personal Data of the Collaboration Data Provider; (c) Customer is solely responsible for evaluating any risks related to its use of Personal Data of the Collaboration Data Provider and entering into any agreement with the Collaboration Data Provider as it deems necessary or that is required under any Applicable Data Protection and Privacy Laws; and (d) Lotame has no control over, and will have no liability for, any violations of Applicable Data Protection and Privacy Laws with respect to the provision of or use of the Personal Data of the Collaboration Data Provider.

7. **Impact Assessments.** Upon a party's request: (1) the other Party shall provide the requesting party with reasonable cooperation and assistance needed for the requesting party to fulfil its obligations under any Applicable Data Protection and Privacy Law to complete any required impact assessments related to the Processing of Customer Data, Sightings Data, or Lotame Data, to the extent the requesting party does not otherwise have access to the relevant information, and to the extent such information is available to the other party and (2) the other party shall provide reasonable assistance to the requesting party for any inquiry or investigation by a Supervisory Authority related to a party's performance under the Agreement or this DPA.

8. **Training; Confidentiality.** Lotame shall ensure that its personnel engaged in the Processing of Customer Data have received appropriate training regarding the access, use and treatment of Personal Data under Data Protection and Privacy Laws and have executed written confidentiality agreements governing the access, use and treatment of Customer Data.

9. **Data Protection/Privacy Point of Contact.** Lotame's employee responsible for handling any inquiries related to this DPA or Applicable Data Protection and Privacy Laws may be reached at privacy@lotame.com. Customer's data protection officer/privacy point of contact is stated in the Agreement.

10. **Duration and Termination of this DPA.** This DPA will continue in force until the later of (i) the termination of all Agreements into which it is incorporated, (ii) Lotame is no longer Processing Customer Data and Sightings Data, and (iii) Customer is no longer Processing Lotame Data. Lotame will delete, deidentify, or render useless Customer Data no later than 90 days after termination of the Agreement and Customer will delete Lotame Data no later than 6 months after the termination or expiration of the Agreement unless a longer retention period is required by law, in which case Customer may continue to Process Lotame Data no longer than the applicable law requires.

11. **Previous DPAs; Conflict.** This DPA cancels any previous data processing agreements or addendums that may have been attached to or entered into under the Agreement by the parties. Except as supplemented by this DPA, the Agreement is not modified. If there is a conflict between the Agreement, this DPA and a DPA Schedule, this DPA will control over the Agreement, and an applicable DPA Schedule will control over this DPA and the Agreement.

Schedule 1

Technical and Organizational Security Measures

Description of the technical and organizational security measures implemented by Lotame:

1. Systems' Access Controls. Lotame maintains appropriate technical and organizational policies, procedures, and safeguards to limit access to its platform and services to only those individuals that require access, including protection against unauthorized processing, loss, or unauthorized disclosure of or access to Personal Data. Access to Personal Data within Lotame's platform is governed by role-based access control (RBAC) and can be configured to define granular access privileges, including distinct read/write privileges. These privileges are packaged into reusable and customizable roles to support various permission levels for employees and users (owner, admin, agent, end-user, etc.). Individual users are granted any number of roles, thus providing the capability to control specific responsibilities and access levels within Lotame's organization. Lotame's information security management system is ISO/IEC 27001:2013 certified and is audited annually by an independent third party. Lotame's ISO/IEC 27001:2013 certificate is available upon request.

2. Physical & Environmental Controls – Hosting Infrastructure. Lotame's production infrastructure is hosted by Amazon Web Services (AWS). Lotame does not maintain any physical access to the AWS facilities, and remote access is restricted to named operations staff on an as needed basis. For more information about AWS security, refer to https://aws.amazon.com/security/.

3. Physical & Environmental Controls – Corporate Offices. While Personal Data is not hosted at Lotame's corporate offices, its technical, administrative, and physical controls for its corporate offices are covered by its ISO/IEC 27001:2013 certification and include, but are not limited to, the following:

    - Physical access to the corporate offices are controlled at office ingress points;
    - Badge access is required for all personnel and badge privileges are reviewed regularly;
    - Visitors are required to be escorted by employees; and
    - Cameras.

4. Data Transmission and Storage. All Personal Data in transit is encrypted using TLS 1.2 or better. Personal Data is also encrypted at rest.

5. Development Practices. Lotame utilizes industry-standard source code, build, and deployment processes and systems to manage the introduction of new code into its platform and services. Access to the code repositories is granted on an as needed basis only to employees within Lotame's technology and engineering organizations. A member of Lotame's privacy team is also part of product and service development to ensure privacy by design and default considerations are taken into account.

6. Configuration Management. Lotame utilizes automated configuration management tools to manage application runtimes and configuration parameters across its infrastructure, with access restricted to employees that support releases and operations. Within the configuration management information architecture, credentials used by automated systems (*e.g.*, database logins) are isolated from general application configuration parameters to further limit access to such credentials.

7. Data Minimization and Pseudonymization. Lotame's services do not actively monitor what is sent in as a behavior to Lotame – Customer is responsible for determining what behaviors are collected. Lotame's platform will process all data regardless of its nature as long as it fits the predefined characteristics that allow it to be processed. Lotame does not make any data-based decisions other than following customers' instructions as they configure Lotame's data collection tools to perform their desired operations. Personal Data may be associated with pseudonymous IDs assigned by Lotame or device-based pseudonymous IDs. If Personal Data includes un-hashed deterministic identifiers (for example, email addresses), Lotame tokenizes such deterministic identifiers and segregates them from all other data, and uses technical and organizational measures and controls to maintain that separation, prevent use of those deterministic identifiers during processing within the platform, and prevent access and viewing of deterministic identifiers except by limited operations leadership for troubleshooting purposes and compliance with applicable laws.

9. Confidentiality. All Lotame employees and contractors enter into customary confidentiality agreements that governs the access, use and treatment of all Personal Data that is processed.

10. Personal Data Incident Notifications and Mitigation. Lotame maintains data incident management policies and procedures that it tests annually. Lotame will, without undue delay and in accordance with the timelines required by applicable Data Protection and Privacy Laws, notify data exporter of any incidents that result in the unauthorized or illegal destruction, loss, alteration, disclosure

of, or access to, their Personal Data. Lotame will take prompt action to mitigate continued harm to data exporter or personal data.

11. Vulnerability Detection and Management.

- *Anti-Virus and Vulnerability Detection*: Lotame leverages threat detection tools to monitor and alert it to suspicious activities, potential malware, viruses and/or malicious computer code.
- *Penetration Testing and Vulnerability Detection*: Lotame engages an independent third party to conduct penetration tests of its platform and services annually.
- *Vulnerability Management*: Vulnerabilities meeting defined risk criteria trigger alerts and are prioritized for remediation based on their potential impact to the Platform and Services.

Schedule 2

Subcontractors

Processor	Address	Subject Matter and Nature of the Processing	Duration of Processing
Amazon Web Services, Inc.	410 Terry Avenue North Seattle, WA 98109-5210	Infrastructure and hosting provider for the Lotame Platform and all Lotame products and services.	As set forth in the DPA or applicable DPA Schedule.
Tapad, Inc.	1177 6th Avenue 5th Floor New York, NY 10036	Device and Identifier graphing provider	As set forth in the DPA or applicable DPA Schedule. See also https://www.tapad.com/privacy