

Data Processing Agreement (for Lotame Incoming Data License Agreement)

This Data Processing Agreement (this “DPA”) is entered into between Lotame Solutions, Inc. (“Lotame”) and the entity identified as ~~the~~ Data Provider 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 Incoming Data License Agreement between Lotame and Data Provider.

“**Applicable Data Protection and Privacy Law**” means a Data Protection and Privacy Law that is applicable to the Processing of Data Provider Data, Sightings Data, ~~and/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-idla/>, which include additional requirements applicable to the Processing of Data Provider Data, Sightings Data, and Lotame Data by the parties under Applicable Data Protection and Privacy Laws.

“**Lotame Data**” means (1) a cookie ID assigned by Lotame to a User’s browser or (2) Lotame’s pseudonymous proprietary universal identifier (branded as the Lotame Panorama ID) that is linked to a profile of other pseudonymous IDs (predicted to be the same User) in the Lotame Panorama Graph.

“**Security Incident**” means a breach of Lotame’s security leading to the unauthorized disclosure of, or access to, Data Provider Data, or Data Provider’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 Data Provider and Lotame. Upon the signing of ~~this DPA~~ the Agreement by both parties this DPA will become legally binding between Data Provider 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 Data Provider Data or Sightings Data includes any ~~User~~ Personal Data from Third Party Sources:

(a) This DPA is not a binding agreement between Lotame and any Third Party Sources. ~~When required by an Applicable Data Protection and Privacy Law,~~ Data Provider must have its own data processing agreement or other agreement with its Third Party Sources to address the Processing by Lotame of Data Provider Data and Sightings Data from the Third Party Sources. ~~when required by an Applicable Data Protection and Privacy Law.~~ Data Provider 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 Data Provider may exercise any such right or seek any such remedy against Lotame on behalf of the Third Party Source, and (ii) Data Provider 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* Data Provider Data, Sightings Data, or Lotame Data is or includes Personal Data subject to that Applicable Data Protection and Privacy Law. If Data Provider 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 Data Provider Data and Sightings Data.

4.1 Generally. Data Provider, with respect to its Processing related to the collection and provision of Data Provider Data and Sightings Data to Lotame, and Lotame, with respect to its Processing of Data Provider 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, and Opt-outs from Users.~~ Without limiting the generality of the obligations under Section 4.1, ~~as between the parties,~~ Data Provider has the sole responsibility for ~~compliance with Applicable Data Protection (and Privacy Laws with respect to the collection of Customer Data and Sightings Data and the provision of Data Provider Data and Sightings Data to Lotame. When required under Applicable Data Protection and Privacy Laws, Data Provider shall ensure it and each Third Party Source: does the same)~~ (a) ~~discloses/disclosing~~ to Users at the time of collection the Processing of Data Provider Data and Sightings Data from the Property by Lotame (or by a third-party if Data Provider 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 Data Provider Data and Sightings Data from the Property when required under Applicable Data Protection and Privacy Laws, and (b) ~~obtain~~obtaining Users' consent to the Processing of their Personal Data ~~by Lotame~~ for the purposes contemplated by the Agreement when required under Applicable Data Protection and Privacy Laws. Where Data Provider obtains Data Provider Data and Sightings Data from a Third Party Source, Data Provider 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 of Data Provider Data and Sightings Data.~~ Data Provider 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 Data Provider 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 specifies~~has~~ additional or different requirements than what is described in this section, the applicable DPA Schedule will supersede ~~any conflicting obligations in this section related to the handling of User Rights Requests~~this section.

(a) *User Rights Requests Received by Lotame from ~~Company~~Data Provider.* For any User Rights Requests that Data Provider directly receives and forwards to Lotame, Lotame will provide reasonable assistance to Data Provider in fulfilling Data Provider's obligations under Applicable Data Protection and Privacy Law to respond to the User Rights Request. To the extent legally permitted, Data Provider shall be responsible for any costs arising from Lotame's provision of such assistance. Lotame may make available an API or other mechanism ~~available~~ to Data Provider 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 Data Provider, then Lotame will promptly forward the User Rights Request to Data Provider and assist Data Provider as set forth in Section 4.4(a).

4.5 Security.

(a) Lotame shall (and shall require its ~~Subcontractors~~contractors 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 ~~sub-processors~~contractors. 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 (taking into account the nature of the processing of Data Provider Data and the information available to Lotame)~~Lotame will assist Data Provider in ensuring compliance with Data Provider's obligations relating to security of Lotame's processing of Data Provider 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 Data Provider}~~ with the documents and information described in Section 4.7 (Audits to Verify Compliance with this DPA).

4.6 Security Incident Notification. If Lotame has determined that a Security Incident has occurred, Lotame will (1) notify Data Provider 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 ~~obligation to report~~ reporting of a Security Incident ~~underin 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 Data Provider by including in the notification such information about the Security Incident as Lotame is able to disclose to enable Data Provider 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. Data Provider is solely responsible for complying with incident notification laws applicable to Data Provider 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 Data Provider's written request, and provided that the parties have an effective non-disclosure or confidentiality agreement in place, Lotame will provide Data Provider with (1) a copy of the Report referenced in Section 4.5(b) so that Data Provider can ~~reasonably~~ 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 Data Provider 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 Data Provider or an auditor designated by Data Provider (at the Data Provider's sole cost) by making available to Data Provider additional documents and information reasonably requested that demonstrates Lotame's compliance with its obligations set forth in this DPA. Data Provider 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~~ Data Provider ~~may not conduct any requested~~ audit ~~more than once in a 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, Data Provider 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, Data Provider 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 Data Provider or its auditor with access to any facilities of its ~~Subcontractors~~ contractors, 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 ~~the~~ Applicable Data Protection and Privacy Laws, or (3) its security and/or privacy obligations to another customer or any third party, or any information that Data Provider or its third party auditor seeks to access for any reason other than the good faith fulfillment of Data Provider's obligations under the Applicable Data Protection and Privacy Laws. Additionally, Data Provider shall take all reasonable measures to combine all audits into one single audit on behalf of itself and all of its Third Party Sources.

5. Processing of Lotame Data.

5.1 Generally. Lotame, with respect to its Processing related to the provision of Lotame Data to Data Provider, and Data Provider, 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 Data Provider 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 Data Provider directly receives, Lotame will assist Data Provider in fulfilling Data Provider's obligations, if any, under Applicable Data Protection and Privacy Laws to respond to the

User Rights Request. If Data Provider receives a User Rights Request that specifically references Lotame, Data Provider 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 Data Provider for the submission of User Rights Requests.

5.4 Security. Data Provider 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 ("**Data Provider Security Measures**"). Data Provider shall audit the adequacy of its Data Provider 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 Data Provider's Confidential Information.

5.5 Security Incident Notification. If Data Provider has determined that a Security Incident has occurred, Data Provider 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. Data Provider's obligation to report a Security Incident under this section is not and will not be construed as an acknowledgement by Data Provider of any fault or liability with respect to the Security Incident. Data Provider will cooperate with and provide reasonable assistance to Lotame by including in the notification such information about the Security Incident as Data Provider 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 Data Provider, 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 Data Provider 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).

5.6. Processing of Lotame Data by Data Provider.

5.16.1 Generally. Lotame, with respect to its Processing related to the provision of Lotame Data to Data Provider, and Data Provider, 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.

5.26.2 User Rights Requests. Data Provider shall notify Lotame of any User Rights Requests related to Lotame Data. Lotame will provide reasonable assistance to Data Provider in fulfilling Data Provider'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 ~~available~~ to Data Provider for the submission of User Rights Requests.

6.7. 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 Data Provider 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.

7.8. Training; Confidentiality. Lotame shall ensure that its personnel engaged in the Processing of Data Provider 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 Data Provider Data.

8.9. 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. Data Provider's data protection officer/privacy point of contact is stated in the Agreement.

9.10. 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 Data Provider Data and Sightings Data, and (iii) Data Provider is no longer Processing Lotame Data. Lotame will delete, deidentify, or render useless Data Provider Data no later than 90 days after termination of the Agreement and Data Provider 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 Data Provider may continue to Process Lotame Data no longer than the applicable law requires.

10.11.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-Provider Data~~. Access to ~~Data-Provider~~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 ~~Data-Provider~~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 ~~Data-Provider~~Personal Data in transit is encrypted using TLS 1.2 or better. ~~Data-Provider~~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 ~~Data-Provider to limit~~ what ~~personal data~~ is ~~collected by Lotame's code or sent to us via~~ as a file ~~behavior to Lotame~~ – Data Provider 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. ~~Data-Provider~~Personal Data may be associated with pseudonymous IDs assigned by Lotame or device-based pseudonymous IDs. If ~~Data-Provider~~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 ~~Data-Provider~~Personal Data that ~~we process~~ 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 ~~Data-Provider~~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.