Data Processing Agreement
(for Lotame Outgoing Data License Agreement)

This Data Processing Agreement (this "**DPA**") is entered into between Lotame Solutions, Inc. ("**Lotame**") and the entity identified as ~~the Customer~~Company 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 Outgoing Data License Agreement between Lotame and ~~Customer~~Company.

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

    "~~**Customer**~~**Company Data**" means ~~Customer's~~Company's proprietary identifier for a User, Application, or Device.

    "**DPA Schedules**" means the schedules for any Applicable Data Protection and Privacy Laws available at https://www.lotame.com/privacy/dpas/dpa-odla/, which include additional requirements applicable to the Processing of ~~Customer~~Company 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~~Company Data, or Company'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~~Company and Lotame.** Upon the signing of ~~this DPA~~the Agreement by both parties this DPA will become legally binding between ~~Customer~~Company 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~~Company 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, Customer~~Company must have its own data processing agreement or other agreement with its Third Party Sources to address the Processing by Lotame of ~~Customer~~Company Data from the Third Party Sources. ~~Customer~~ when required by an Applicable Data Protection and Privacy Law. Company 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~~Company may exercise any such right or seek any such remedy against Lotame on behalf of the Third Party Source, and (ii) ~~Customer~~Company 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~~Company Data or Lotame Data is or includes Personal Data subject to that Applicable Data Protection and Privacy Law. If ~~Customer~~Company 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~~Company Data.**

4.1 **Generally.** ~~Customer~~Company, with respect to its Processing related to the collection and provision of ~~Customer~~Company Data to Lotame, and Lotame, with respect to its Processing of ~~Customer~~Company 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, Customer~~Company 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 Customer Data to Lotame. When required under Applicable Data Protection and Privacy Laws, Customer~~ shall ensure ~~it and~~ each Third Party Source~~:~~ does the same) (a) ~~discloses~~disclosing to Users at the time of collection the Processing of ~~Customer~~Company Data from the Property by Lotame (or by a third-party if Company 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~~Company 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 ~~Customer~~Company obtains ~~Customer~~Company Data from a Third Party Source, ~~Customer~~Company 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 Customer Data. Customer~~.** Company 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~~Company 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*. For any User Rights Requests that ~~Customer~~Company directly receives and forwards to Lotame, Lotame will provide reasonable assistance to ~~Customer~~Company in fulfilling ~~Customer's~~Company's obligations under Applicable Data Protection and Privacy Law to respond to the User Rights Request. To the extent legally permitted, ~~Customer~~Company 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 ~~Customer~~Company 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~~Company, then Lotame will promptly forward the User Rights Request to ~~Customer~~Company and assist ~~Customer~~Company 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 Customer Data and the information available to Lotame)~~ assist ~~Customer~~Company in ensuring compliance with ~~Customer's~~Company's obligations relating to security of ~~Customer~~Lotame's processing of Company 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~~Company 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 ~~Customer~~Company 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 ~~under~~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~~Company by including in the notification such information about the Security Incident as Lotame is able to disclose to enable ~~Customer~~Company 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~~Company is solely responsible for complying with incident notification laws applicable to ~~Customer~~Company 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~~Company's written request, and provided that the parties have an effective non-disclosure or confidentiality agreement in place, Lotame will provide ~~Customer~~Company with (1) a copy of the Report referenced in Section 4.5(b) so that ~~Customer~~Company 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 ~~Customer~~Company 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~~Company or an auditor designated by ~~Customer~~Company (at the ~~Customer's~~Company's sole cost) by making available to ~~Customer~~Company additional documents and information reasonably requested that demonstrates Lotame's compliance with its obligations set forth in this DPA. ~~Customer~~Company shall reimburse Lotame for any costs or expenses incurred by Lotame in completing an audit.

(c) ~~Customer may not conduct any~~Lotame has no obligation to complete an audit ~~more than once in~~if Lotame has completed a Company-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~~Company 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~~Company 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~~Company 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 Customer or its third party auditor seeks to access for any reason other than the good faith fulfillment of Customer's obligations under the Applicable Data Protection and Privacy Laws.~~. Additionally, ~~Customer~~Company 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~~Company Instructions. ~~Customer~~Company acknowledges that certain Platform settings and elections initiated by ~~Customer~~Company through its use of the Services may affect how the Platform Processes ~~Customer~~Company Data ("~~Customer~~**Company Initiated Settings**"). This DPA, the Agreement, and ~~Customer~~Company Initiated Settings constitute ~~Customer's~~Company's documented instructions regarding Lotame's Processing of ~~Customer~~Company Data ("**Documented Instructions**"). Lotame will Process ~~Customer~~Company Data only in accordance with Documented Instructions. ~~Customer~~Company further acknowledges that (a) ~~Customer~~Company 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~~Company's Documented Instructions are likely to violate any Applicable Data Protection and Privacy Law. This section does not negate ~~Customer's~~Company's right to communicate additional instructions to Lotame regarding the Processing of ~~Customer~~Company 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~~Company and Lotame, including agreement on any

additional fees payable by ~~Customer~~Company 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.~~

4.9 ~~Customer~~Contractors.

(a) Company generally authorizes Lotame to engage the ~~Subcontractors~~contractors listed in Schedule 2 of this DPA in connection with the provision of the Services, which ~~Subcontractors~~contractors may process ~~Customer~~Company Data. When engaging ~~any Subcontractor~~a contractor, 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~~Company Data and (ii) that the ~~Subcontractor~~contractor will only access and use ~~Customer~~Company Data to the extent required to perform the obligations ~~Subcontracted~~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~~contractor.

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

5. **Processing of Lotame Data.**

5.1 **Generally.** Lotame, with respect to its Processing related to the provision of Lotame Data to ~~Customer~~Company, and ~~Customer~~Company, 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~~Company 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~~Company directly receives, ~~Customer will forward the User Rights Request to Lotame and~~ Lotame will assist ~~Customer~~Company in fulfilling ~~Customer's~~Company's obligations, if any, under Applicable Data Protection and Privacy Laws to respond to the User Rights Request. If Company receives a User Rights Request that specifically references Lotame, Company 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 Company for the submission of User Rights Requests.

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

5.5 **Security Incident Notification.** If Company has determined that a Security Incident has occurred, Company 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. Company's obligation to report a Security Incident under this section is not and will not be construed as an acknowledgement by Company of any fault or liability with respect to the Security Incident. Company will cooperate with and provide reasonable assistance to Lotame by including in the notification such information about the Security Incident as Company 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 Company, 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 Company 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.   **Audits to Verify Compliance with this DPA.** At Lotame's written request, and provided that the parties have an effective non-disclosure or confidentiality agreement in place, Company will provide Lotame with (1) a copy of the Report referenced in Section 5.4 so that Lotame can verify Lotame's compliance with its obligations under this DPA and (2) any other documents and information Lotame deems necessary to demonstrate Company's compliance with its obligations set forth in this DPA. Lotame will not request any audit more than once in a 12-month period. Except for audits conducted at Company's premises or physical facilities, Lotame shall provide Lotame with no less than 30 days' prior notice before commencing an audit. Audits may be conducted at Company'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, Lotame shall provide Company with no less than 45 days' prior notice, carry out the audit only during Company's standard business hours, and cause minimal disruption to Company's operations. Under no circumstances will Company provide Lotame or its auditor with access to any facilities of its Vendors, or any information that, in Company's reasonable opinion, would not assist Lotame in verifying Company's compliance with its obligations under this DPA or that could: (1) compromise the security of Company's systems or premises; or (2) cause Company to breach its obligations under Applicable Data Protection and Privacy Laws, or (3) its security and/or privacy obligations to any third party.

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 ~~Customer~~Company 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.   ~~**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.~~

8.   **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~~Company's data protection officer/privacy point of contact is stated in the Agreement.

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

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

Contractors

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
~~Roq.ad, Inc.~~	~~2600 El Camino Real Palo Alto, CA 94306~~	~~Device and Identifier graphing provider~~	~~As set forth in the DPA or applicable DPA Schedule. See also https://www.roq.ad/privacy-policy-roqad/~~
~~FullContact, Inc.~~	~~1624 Market Street Suite 226PMB 45057 Denver, Colorado 80202-2523~~	~~Data onboarding services (U.S.A.)~~	~~As set forth in the DPA or applicable DPA Schedule.~~
~~Killi Limited~~	~~1306-80 John Street Toronto, ON, M5V 3X4~~	~~Data onboarding services (U.S.A., Canada, and the following countries in the Asia-Pacific region: Singapore, Taiwan, South Korea, China, Japan, Australia, New Zealand, Hong Kong, Vietnam, Malaysia, Indonesia, Philippines, Thailand, India and other Southeast Asia countries)~~	~~As set forth in the DPA or applicable DPA Schedule.~~