LOTAME DATA PROCESSING ADDENDUM

(Revision February 2021)

This Data Processing Addendum (including its Schedules and Appendices, the "**DPA**") forms a part of the written or electronic agreement into which this DPA is incorporated by reference (the "**Agreement**") between Lotame Solutions, Inc. ("**Lotame**") and the Customer stated in the Agreement ("**Customer**") to reflect the parties' agreement with regard to the Processing of Personal Data under various Privacy Laws.

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

1. Definitions. All capitalized terms not defined in this DPA have the meanings set forth in the Agreement.

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"**Authorized Affiliate**" means any of Company's Affiliate(s) which (a) is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Lotame Services pursuant to the Agreement between Company and Lotame, but has not signed its own Order Form with Lotame and is not a "Company" as defined under this DPA.

"C2C Services" means the following Lotame Services: Lotame Cartographer and the use of Third Party Data.

"C2P Services" means all Lotame Services excluding C2C Services,

"CCPA" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq*., and its implementing regulations.

"Company" means Customer and Authorized Affiliates for the purposes of this DPA only.

"Controller" has the meaning set forth in GDPR.

"Company Data" means what is defined in the Agreement as "Customer Data".

"Data Protection Laws and Regulations" means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland, the United Kingdom and the United States and its states, applicable to the Processing of Personal Data under the Agreement.

"Data Subject" means the identified or identifiable person to whom Personal Data relates.

"**Data Subject Request**" mean an exercise by a Data Subject of their right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, right to opt-out-of sale, or its right not to be subject to an automated individual decision making.

"**GDPR**" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

"Personal Data" means any information relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws and Regulations), where for each (i) or (ii), such data is Company Data.

"Processing" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Processor" means the entity which Processes Personal Data on behalf of the Controller, including as applicable any "service provider" as that term is defined by the CCPA or Subcontractor as that term is defined in the Agreement.

"Lotame Group" means Lotame and its Affiliates engaged in the Processing of Personal Data.

"Standard Contractual Clauses" means Schedule 3 and Schedule 4 attached to and forming part of this DPA pursuant to the European Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC.

"Sub-processor" means any Processor engaged by Lotame or a member of the Lotame Group.

"**Supervisory Authority**" means an independent public authority which is established by an EU Member State pursuant to the GDPR.

2. Legal Effect and Contractual Relationship.

2.1 Contractual Relationship with Company. This DPA will become legally binding between Company and Lotame when Company signs the Agreement. This DPA does not replace any comparable or additional rights relating to Processing of Company Data contained in the Agreement (including any existing data processing addendum to the Agreement).

2.2 Contractual Relationship with Authorized Affiliates and Company Clients. If Company Data includes Personal Data of Authorized Affiliates, to the extent required under applicable Data Protection Laws and Regulations, Company enters into this DPA for its Authorized Affiliates and will ensure that each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. If and to the extent Lotame Processes Personal Data for Company where Company is the Processor for such Personal Data (for example, an Authorized Affiliate or a Company Client is the Controller), Lotame will Process such Personal Data in accordance with this DPA; however, this DPA is not legally binding between Lotame and the Controller of such Personal Data and Lotame, and Lotame is a Processor to Company only. In such cases, Company must have its own data processing addendum or other agreement relating to the Processing of the Controller's Personal Information with such Controller.

2.3 Communication. Company that is the contracting party to the Agreement remains responsible for coordinating all communication with Lotame under this DPA and will make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

2.4 Rights of Authorized Affiliates. Where an Authorized Affiliate becomes a party to this DPA with Lotame under Section 2.2, the Authorized Affiliate is, to the extent required under applicable Data Protection Laws and Regulations, entitled to exercise the rights and seek remedies under this DPA, subject to the following:

(a) Except where applicable Data Protection Laws and Regulations require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against Lotame directly by itself, (i) solely the Company that is the contracting party to the Agreement may exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (ii) the Company that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Authorized Affiliate individually but in a combined manner for itself and all of its Authorized Affiliates together.

(b) Company that is the contracting party to the Agreement shall, when carrying out an on-site audit of the procedures relevant to the protection of Personal Data under this DPA, take all reasonable measures to limit any impact on Lotame and its Sub-Processors by combining, to the extent reasonably possible, several audit requests carried out on behalf of itself and all of its Authorized Affiliates in one single audit.

3. Processing of Personal Data.

3.1 Roles of the Parties. With regard to the Processing of Personal Data for C2P Services, Company is the Controller, Lotame is the Processor and Lotame may engage Sub-processors pursuant to the requirements set forth in Section 5 "Sub-processors" below. With regard to the Processing of Personal Data for C2C Services, Company and Lotame are independent Controllers.

3.2 Company's Processing of Personal Data. Company shall, in its use of the Lotame Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations and this DPA, including any applicable requirement to provide notice to Data Subjects of the use of Lotame as a Processor. Company has the sole responsibility for (i) the accuracy, quality, and legality of Personal Data and the means by which Company acquired Personal Data and (ii) ensuring that Company's use of the Lotame Services will not violate the rights of any Data Subject that has opted-out from sales or other disclosures of Personal Data, when applicable under Data Protection Laws and Regulations. Company is solely responsible for ensuring that its instructions to Lotame for the Processing of Personal Data complies with Data Protection Laws and Regulations.

3.3 Lotame's Processing of Personal Data. Lotame shall Process Personal Data on behalf of Company in accordance with the requirements of Data Protection Laws and Regulations and this DPA and only as necessary for the following purposes: (i) Processing in accordance with the Agreement; (ii) Processing initiated by Company in its use of the Lotame Services; and (iii) Processing to comply with other documented reasonable instructions provided by Company (e.g., via email) where such instructions are consistent with the terms of the Agreement, Data Protection Laws and Regulations and this DPA.

3.4 Details of the Processing. The subject-matter of Processing of Personal Data by Lotame is the performance of the Lotame Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 2 (Details of the Processing) to this DPA.

4. Rights of Data Subjects. Lotame has created a tool that enables Lotame to respond in an automated fashion to certain Data Subject Requests ("**Data Subject Tool**"). If a Data Subject Request is made by a Data Subject through the Data Subject Tool, then Lotame will automatically respond to such request in accordance with the standard functionality of the Data Subject Tool. If the Data Subject Request is not made via the Data Subject Tool or the Data Subject Tool is not able to respond to the Data Subject Request in an automated fashion, Lotame shall, to the extent legally permitted and the Data Subject makes specific reference to Company, promptly notify Company of the Data Subject Request. Taking into account the nature of the Processing, Lotame shall assist Company by appropriate technical and organizational measures, insofar as this is possible and does not violate Data Protection Laws and Regulations, for the fulfilment of Company's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. To the extent legally permitted, Company shall be responsible for any costs arising from Lotame's provision of such assistance. Company acknowledges that Lotame may not be able to respond to a Data Subject Request using personally identifiable information.

5. Lotame Personnel.

5.1 Confidentiality. Lotame shall ensure that its personnel engaged in the Processing of Personal Data have received appropriate training on their responsibilities and have executed written confidentiality agreements governing the access, use and treatment of Personal Data.

5.2 Limitation of Access. Lotame shall ensure that access to Personal Data is limited to those personnel performing Lotame Services in accordance with the Agreement.

5.3 Data Protection Officer. Lotame has appointed a data protection officer who may be reached at privacy@lotame.com.

6. Sub-Processors

6.1 Appointment of Sub-processors. Company acknowledges that (a) Lotame's Affiliates may be retained as Sub-processors; and (b) Lotame and Lotame's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Lotame Services. Lotame or the Lotame Affiliate has entered into or will enter a written agreement with each Sub-processor containing data protection obligations not less protective than those in the Agreement with respect to the protection of Company Data to the extent applicable to the nature of the Lotame Services provided by such Sub-processor.

6.2 List of Current Sub-processors. Lotame's current Sub-Processors are listed in Schedule 5. Lotame shall provide or make available to Company a list of Sub-processors for the Lotame Services upon request. Such Sub-processor lists will include the identities of those Sub-processors, their country of location, and the processing activities performed for Lotame.

6.3 Notification of New Sub-processors and Objection Right for New Sub-processors. Lotame shall provide no less than 60 days advance notice to Company before authorizing any new Sub-processor(s) to Process Company's Personal Data in connection with the provision of the Lotame Services. Company may object to Lotame's use of a new Sub-processor to Process Company's Personal Data by notifying Lotame promptly in writing within 30 days after receipt of Lotame's notice. In the event Company objects to a new Sub-processor, as permitted in the preceding sentence, Lotame will use reasonable efforts to make available to Company a change in the Lotame Services or recommend a commercially reasonable change to Company's configuration or use of the Lotame Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening Company. If Lotame is unable to make available such change within a reasonable period of time, which shall not exceed 30 days, Company may terminate only those Lotame Services that cannot be provided by Lotame without the use of the objected-to new Sub-processor by providing written notice to Lotame. Lotame will refund Company any prepaid fees covering the remainder of the term of such Service Order following the effective date of termination with respect to the terminated Lotame Services, without imposing a penalty for such termination on Company. If Company fails to object to Lotame's use of a new Sub-processor within the period set forth in this section, then the new Sub-processor will be deemed approved.

6.4 Liability. Lotame shall be liable for the acts and omissions of its Sub-processors to the same extent Lotame would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

7. Security.

7.1 Controls for the Protection of Company Data. Lotame shall maintain appropriate physical, technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Company Data) and integrity of Company Data. Lotame regularly monitors compliance with these measures. Lotame will not materially decrease the overall security of the Lotame Services during a subscription term.

7.2 Third-Party Certifications. Lotame is ISO27001 certified. Upon Company's written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement, Lotame shall make available to Company that is not a competitor

of Lotame (or Company's independent, third-party auditor that is not a competitor of Lotame) a copy of Lotame's then most recent compliance report.

8. Company Data Incident Management and Notification. Lotame maintains security incident management policies and procedures and shall notify Company without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Company Data, including Personal Data, transmitted, stored or otherwise Processed by Lotame or its Sub-processors of which Lotame becomes aware (a "**Company Data Incident**"). Lotame shall make reasonable efforts to identify the cause of such Company Data Incident and take those steps as Lotame deems necessary and reasonable in order to remediate the cause of such a Company Data Incident to the extent the remediation is within Lotame's reasonable control. The obligations in this section will not apply to Company Data Incidents that are caused by Company or users of Company's account on the Lotame Services.

9. Return and Deletion of Company Data. Lotame shall return Company Data to Company and, to the extent allowed by applicable law, delete Company Data in accordance with the procedures and timeframes specified in its Privacy Policy for the Lotame Services.

10. Limitation of Liability. Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and Lotame, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement. Lotame's and its Affiliates' total liability for all claims from Company and all of its Authorized Affiliates arising out of or related to the Agreement and all DPAs shall apply in the aggregate for all claims under both the Agreement and all DPAs established under the Agreement, including by Company and all Authorized Affiliates, and, in particular, shall not be understood to apply individually and severally to Company and/or to any Authorized Affiliate that is a contractual party to any such DPA.

11. European Specific Provisions.

11.1 GDPR. Lotame will Process Personal Data in accordance with the GDPR requirements directly applicable to Lotame's provision of its Lotame Services.

11.2 Data Protection Impact Assessment. Upon Company's request, Lotame shall provide Company with reasonable cooperation and assistance needed to fulfil Company's obligation under the GDPR to carry out a data protection impact assessment related to Company's use of the Lotame Services, to the extent Company does not otherwise have access to the relevant information, and to the extent such information is available to Lotame. Lotame shall provide reasonable assistance to Company in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to Section 11.2 of this DPA, to the extent required under the GDPR.

11.3 Transfer mechanisms for data transfers. Subject to the additional terms in Schedule 1 to this DPA, Lotame makes available the transfer mechanisms listed below which shall apply to any transfers of Personal Data under this DPA from the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom to countries which do not ensure an adequate level of data protection within the meaning of Data Protection Laws and Regulations of the foregoing territories, to the extent such transfers are subject to such Data Protection Laws and Regulations:

(a) The Controller-to-Processor Standard Contractual Clauses set forth in Schedule 3 to this DPA apply only to the C2P Services, subject to the additional terms in Section 3 of Schedule 1.

(b) The Controller-to-Controller Standard Contractual Clauses set forth in Schedule 4 to this DPA apply only to the C2C Services, subject to the additional terms in Section 3 of Schedule 1.

List of Schedules

Schedule 1: Additional Terms for Transfer Mechanisms for European Data Transfers

Schedule 2: Details of the Processing

Schedule 3: Controller-to-Processor Standard Contractual Clauses

Schedule 4: Controller-to-Controller Standard Contractual Clauses

Schedule 5: List of Sub-Processors

Schedule 1

Additional Terms for European Data Transfers

1. List of current Sub-processors. Pursuant to Clause 5(h) of Schedule 3, Company acknowledges and expressly agrees that the list of Sub-processors in Schedule 5 are consented to.

2. Notification of New Sub-processors and Objection Right for new Sub-processors. Pursuant to Clause 5(h) of the Standard Contractual Clauses, Company acknowledges and expressly agrees that Lotame may engage new Sub-processors as described in Section 6 of the DPA.

3. Copies of Sub-processor Agreements. The parties agree that the copies of the Sub-processor agreements that must be provided by Lotame to Company pursuant to Clause 5(j) of Schedule 3 may have all commercial information, or clauses unrelated to the Standard Contractual Clauses or their equivalent, removed by Lotame beforehand; and, that such copies will be provided by Lotame, in a manner to be determined in its discretion, only upon request by Company.

4. Audits and Certifications. The parties agree that the audits described in Clause 5(f) and Clause 12(2) of Schedule 3 will be carried out in accordance with the following specifications:

Upon Company's request, and subject to the confidentiality obligations set forth in the Agreement, Lotame shall make available to Company that is not a competitor of Lotame (or Company's independent, third-party auditor that is not a competitor of Lotame) information regarding the Lotame's compliance with the obligations set forth in this DPA in the form of the third-party certifications and audits to the extent Lotame makes them generally available to its customers. Company may contact Lotame in accordance with the "Notices" Section of the Agreement to request an on-site audit of the procedures relevant to the protection of Personal Data. Company shall reimburse Lotame for any time expended for any such on-site audit at the Lotame Group's then-current professional services rates, which shall be made available to Company upon request. Before the commencement of any such on-site audit, Company and Lotame shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Company shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Lotame. Company shall promptly notify Lotame with information regarding any non- compliance discovered during the course of an audit.

5. Certification of Deletion. The parties agree that the certification of deletion of Personal Data that is described in Clause 12(1) of Schedule 3 will be provided by Lotame to Company only upon Company's request.

6. Conflict. In the event of any conflict or inconsistency between the body of this DPA and any of its Schedules (not including the Standard Contractual Clauses), the Standard Contractual Clauses shall prevail.

SCHEDULE 2

Details of The Processing

1. Nature and Purpose of Processing

Lotame will Process Personal Data as necessary to perform the Lotame Services pursuant to the Agreement, as further specified in the Documentation, and as further instructed by Company in its use of the Lotame Services.

2. Duration of Processing

Subject to Section 9 of the DPA, Lotame will Process Personal Data for the duration of the Agreement plus 90 days, unless otherwise agreed upon in writing.

Schedule 3

C2P Services

Standard Contractual Clauses (Processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name and address of the data exporting organization (the data exporter): The entity identified as Customer in the DPA

And

Name and address of the data importing organization (the data importer): Lotame Solutions, Inc.
8850 Stanford Blvd., Suite 4000
Columbia, MD 21045, U.S.A.

each a 'party'; together 'the parties',

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data(note 1);

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of indi- viduals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to

[1] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub- processor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub- processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer([2])

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

[2] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(ii) any accidental or unauthorised access; and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9

Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses (3). Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.
2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data-processing services

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

[3] This requirement may be satisfied by the sub-processor co-signing the contract entered into between the data exporter and the data importer under this Decision.

2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

Appendix 1

to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix

Data exporter

The data exporter is the entity identified as "Customer" in the DPA

Data importer

The data importer is Lotame Solutions, Inc., a provider of enterprise software-as-a-service computing solutions that processes personal data upon the instruction of the data exporter in accordance with the terms of the Agreement for the management of personal data and use in online interest-based behavioral advertising.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

- The extent of the personal data transferred to the data exporter is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to personal data relating to the following categories of data subjects:
    - Prospects, customers, business partners and vendors of data exporter (who are natural persons)
    - Employees and agents of data exporter (who are natural persons) that may use the data importer's services for the benefit of data exporter
    - Data exporter's customers that engage with data exporter online (*e.g.*, through a web browser, mobile application, or direct marketing and advertising activities) or through its services

Categories of data

The personal data transferred concern the following categories of data (please specify):

- The extent of the personal data transferred to the data exporter is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to personal data relating to the following categories of data:
    - Business contract information
    - Demographic Information
    - Online Behavioral Information
    - Technical Identifiers (such as IP address, Lotame cookie ID, or mobile device IDFA or AAID)
    - Event-level data (such as http headers, user agent string, time date stamp)

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

- The data exporter will not send special categories of data to the data importer.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

- Data importer will process personal data as necessary to perform the Lotame Services pursuant to the Agreement and as may be further instructed by data exporter in its use of the Lotame Services. Additionally, data importer processes personal data for the following purposes for data exporter:
    - Interest based advertising
    - Cross device matching
    - Personalized content delivery

- Campaign analytics and insights
- ID syncing
- Market research

Appendix 2

to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

1. Systems. Data importer shall maintain appropriate technical and organizational policies, procedures and safeguards for protection of personal data, including protection against unauthorized Processing, and against destruction, loss, alteration, damage, or unauthorized disclosure of or access to, Personal Data.

1.1 Data Transmission: All customer interactions with the data importer's services are encrypted in transit with Secure Sockets Layer (SSL) technology using industry standard encryption practices.

1.2 Application Security: All user access to the data importer's services is protected by granular user privileges, including distinct read/write privileges. These privileges are packaged into reusable and customizable roles. Individual users are granted any number of roles, thus providing the capability to control specific responsibilities and access levels within a customer's organization.

1.3 Development Practices: Data importer's services utilizes industry-standard source code management systems to manage the introduction of new code into the product suite. Access to the code repositories is granted on an as needed basis only to employees within the Technology and Engineering organizations.

1.4 Hosting Infrastructure: Data importer's production infrastructure is hosted in a combination of Amazon Web Services (AWS) and Equinix co-location facilities. Both are top tier hosting providers with hardened and redundant facilities management practices. Data importer does not maintain any physical access to the AWS facilities, and remote access is restricted to named operations staff on as needed basis. Equinix is a top tier data center with multiple layers of physical security, including on site security personnel, photo id requirements for all on site visits, and multiple layers of biometric access restrictions. They provide a fully redundant and fault tolerant infrastructure, including on site power generation in the event of the failure of a public utility. Data importer's footprint within the facilities is itself internally fault tolerant and fully redundant at the hardware, software, and connectivity layers.

1.5 Configuration Management: Data importer utilizes automated configuration management tools to manage application runtimes and configuration parameters across our infrastructure, with access restricted to staff 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

2. Confidentiality. Data importer shall ensure that all personnel responsible for processing personal data enter into customary confidentiality agreements that governs the access, use and treatment of personal data by data importer.

3. Access by Data Importer's Employees. Data importer shall limit access to personal data to those individuals that require access to personal data in order to provide data importer's services to data exporter.

4. Personal Data Incident Notifications. Data importer shall maintain personal data incident management policies and procedures and shall, without undue delay and in accordance with the timelines required by the applicable data protection law, notify data exporter of any personal data incidents that result in the unauthorized or illegal destruction, loss, alteration, disclosure of, or access to, personal data that is stored or processed by data importer. Data importer will take prompt action to mitigate any harm to data exporter or personal data.

Schedule 4

SET II

Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to controller transfers)

Data transfer agreement

between

The entity identified as Customer in the DPA
(hereinafter "data importer")

and

Lotame Solutions, Inc.
8850 Stanford Blvd., Suite 4000, Columbia, MD 21045, U.S.A.
(hereinafter "data exporter")

each a "party"; together "the parties".

Definitions

For the purposes of the clauses:

(a) "personal data", "special categories of data/sensitive data", "process/processing", "controller", "processor", "data subject" and "supervisory authority/authority" shall have the same meaning as in Directive 95/46/EC of 24 October 1995 (whereby "the authority" shall mean the competent data protection authority in the territory in which the data exporter is established);

(b) "the data exporter" shall mean the controller who transfers the personal data;

(c) "the data importer" shall mean the controller who agrees to receive from the data exporter personal data for further processing in accordance with the terms of these clauses and who is not subject to a third country's system ensuring adequate protection;

(d) "clauses" shall mean these contractual clauses, which are a free-standing document that does not incorporate commercial business terms established by the parties under separate commercial arrangements.

The details of the transfer (as well as the personal data covered) are specified in Annex B, which forms an integral part of the clauses.

I. Obligations of the data exporter

The data exporter warrants and undertakes that:

(a) The personal data have been collected, processed and transferred in accordance with the laws applicable to the data exporter.

(b) It has used reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses.

(c) It will provide the data importer, when so requested, with copies of relevant data protection laws or references to them (where relevant, and not including legal advice) of the country in which the data exporter is established.

(d) It will respond to enquiries from data subjects and the authority concerning processing of the personal data by the data importer, unless the parties have agreed that the data importer will so respond, in which case the data exporter will still respond to the extent reasonably possible and with the information reasonably available to it if the data importer is unwilling or unable to respond. Responses will be made within a reasonable time.

(e) It will make available, upon request, a copy of the clauses to data subjects who are third party beneficiaries under clause III, unless the clauses contain confidential information, in which case it may remove such information. Where information is removed, the data exporter shall inform data subjects in writing of the reason for removal and of their right to draw the removal to the attention of the authority. However, the data exporter shall abide by a decision of the authority regarding access to the full text of the clauses by data subjects, as long as data subjects have agreed to respect the confidentiality of the confidential information removed. The data exporter shall also provide a copy of the clauses to the authority where required.

II. Obligations of the data importer

The data importer warrants and undertakes that:

(a) It will have in place appropriate technical and organisational measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.

(b) It will have in place procedures so that any third party it authorises to have access to the personal data, including processors, will respect and maintain the confidentiality and security of the personal data. Any person acting under the authority of the data importer, including a data processor, shall

be obligated to process the personal data only on instructions from the data importer. This provision does not apply to persons authorised or required by law or regulation to have access to the personal data.

(c) It has no reason to believe, at the time of entering into these clauses, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under these clauses, and it will inform the data exporter (which will pass such notification on to the authority where required) if it becomes aware of any such laws.

(d) It will process the personal data for purposes described in Annex B, and has the legal authority to give the warranties and fulfil the undertakings set out in these clauses.

(e) It will identify to the data exporter a contact point within its organisation authorised to respond to enquiries concerning processing of the personal data, and will cooperate in good faith with the data exporter, the data subject and the authority concerning all such enquiries within a reasonable time. In case of legal dissolution of the data exporter, or if the parties have so agreed, the data importer will assume responsibility for compliance with the provisions of clause I(e).

(f) At the request of the data exporter, it will provide the data exporter with evidence of financial resources sufficient to fulfil its responsibilities under clause III (which may include insurance coverage).

(g) Upon reasonable request of the data exporter, it will submit its data processing facilities, data files and documentation needed for processing to reviewing, auditing and/or certifying by the data exporter (or any independent or impartial inspection agents or auditors, selected by the data exporter and not reasonably objected to by the data importer) to ascertain compliance with the warranties and undertakings in these clauses, with reasonable notice and during regular business hours. The request will be subject to any necessary consent or approval from a regulatory or supervisory authority within the country of the data importer, which consent or approval the data importer will attempt to obtain in a timely fashion.

(h) It will process the personal data, at its option, in accordance with:

(i) the data protection laws of the country in which the data exporter is established, or

(ii) the relevant provisions (note 1) of any Commission decision pursuant to Article 25(6) of Directive 95/46/EC, where the data importer complies with the relevant provisions of such an authorisation or decision and is based in a country to which such an authorisation or decision pertains, but is not covered by such authorisation or decision for the purposes of the transfer(s) of the personal data (note 2), or

(iii) the data processing principles set forth in Annex A.

Data importer to indicate which option it selects: clause (iii)

Initials of data importer: Agreed by data importer by signing the Agreement

(i) It will not disclose or transfer the personal data to a third party data controller located outside the European Economic Area (EEA) unless it notifies the data exporter about the transfer and

(i) the third party data controller processes the personal data in accordance with a Commission decision finding that a third country provides adequate protection, or

(ii) the third party data controller becomes a signatory to these clauses or another data transfer agreement approved by a competent authority in the EU, or

(iii) data subjects have been given the opportunity to object, after having been informed of the purposes of the transfer, the categories of recipients and the fact that the countries to which data is exported may have different data protection standards, or

(iv) with regard to onward transfers of sensitive data, data subjects have given their unambiguous consent to the onward transfer

III. Liability and third party rights

(a) Each party shall be liable to the other parties for damages it causes by any breach of these clauses. Liability as between the parties is limited to actual damage suffered. Punitive damages (i.e. damages intended to punish a party for its outrageous conduct) are specifically excluded. Each party shall be liable to data subjects for damages it causes by any breach of third party rights under these clauses. This does not affect the liability of the data exporter under its data protection law.

(b) The parties agree that a data subject shall have the right to enforce as a third party beneficiary this clause and clauses I(b), I(d), I(e), II(a), II(c), II(d), II(e), II(h), II(i), III(a), V, VI(d) and VII against the data importer or the data exporter, for their respective breach of their contractual obligations, with regard to his personal data, and accept jurisdiction for this purpose in the data exporter's country of establishment. In cases involving allegations of breach by the data importer, the data subject must first request the data exporter to take appropriate action to enforce his rights against the data importer; if the data exporter does not take such action within a reasonable period (which under normal circumstances would be one month), the data subject may then enforce his rights against the data importer directly. A data subject is entitled to proceed directly against a data exporter that has failed to use reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses (the data exporter shall have the burden to prove that it took reasonable efforts).

[1] "Relevant provisions" means those provisions of any authorisation or decision except for the enforcement provisions of any authorisation or decision (which shall be governed by these clauses).

[2] However, the provisions of Annex A.5 concerning rights of access, rectification, deletion and objection must be applied when this option is chosen and take precedence over any comparable provisions of the Commission Decision selected.

IV. Law applicable to the clauses

These clauses shall be governed by the law of the country in which the data exporter is established, with the exception of the laws and regulations relating to processing of the personal data by the data importer under clause II(h), which shall apply only if so selected by the data importer under that clause.

V. Resolution of disputes with data subjects or the authority

(a) In the event of a dispute or claim brought by a data subject or the authority concerning the processing of the personal data against either or both of the parties, the parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.

(b) The parties agree to respond to any generally available non-binding mediation procedure initiated by a data subject or by the authority. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

(c) Each party shall abide by a decision of a competent court of the data exporter's country of establishment or of the authority which is final and against which no further appeal is possible.

VI. Termination

(a) In the event that the data importer is in breach of its obligations under these clauses, then the data exporter may temporarily suspend the transfer of personal data to the data importer until the breach is repaired or the contract is terminated.

(b) In the event that:

(i) the transfer of personal data to the data importer has been temporarily suspended by the data exporter for longer than one month pursuant to paragraph (a);

(ii) compliance by the data importer with these clauses would put it in breach of its legal or regulatory obligations in the country of import;

(iii) the data importer is in substantial or persistent breach of any warranties or undertakings given by it under these clauses;

(iv) a final decision against which no further appeal is possible of a competent court of the data exporter's country of establishment or of the authority rules that there has been a breach of the clauses by the data importer or the data exporter; or

(v) a petition is presented for the administration or winding up of the data importer, whether in its personal or business capacity, which petition is not dismissed within the applicable period for such dismissal under applicable law; a winding up order is made; a receiver is appointed over any of its assets; a trustee in bankruptcy is appointed, if the data importer is an individual; a company voluntary arrangement is commenced by it; or any equivalent event in any jurisdiction occurs

then the data exporter, without prejudice to any other rights which it may have against the data importer, shall be entitled to terminate these clauses, in which case the authority shall be informed where required. In cases covered by (i), (ii), or (iv) above the data importer may also terminate these clauses.

(c) Either party may terminate these clauses if (i) any Commission positive adequacy decision under Article 25(6) of Directive 95/46/EC (or any superseding text) is issued in relation to the country (or a sector thereof) to which the data is transferred and processed by the data importer, or (ii) Directive 95/46/EC (or any superseding text) becomes directly applicable in such country.

(d) The parties agree that the termination of these clauses at any time, in any circumstances and for whatever reason (except for termination under clause VI(c)) does not exempt them from the obligations and/or conditions under the clauses as regards the processing of the personal data transferred.

VII. Variation of these clauses

The parties may not modify these clauses except to update any information in Annex B, in which case they will inform the authority where required. This does not preclude the parties from adding additional commercial clauses where required.

VIII. Description of the Transfer

The details of the transfer and of the personal data are specified in Annex B. The parties agree that Annex B may contain confidential business information which they will not disclose to third parties, except as required by law or in response to a competent regulatory or government agency, or as required under clause I(e). The parties may execute additional annexes to cover additional transfers, which will be submitted to the authority where required. Annex B may, in the alternative, be drafted to cover multiple transfers.

ANNEX A

DATA PROCESSING PRINCIPLES

1. Purpose limitation: Personal data may be processed and subsequently used or further communicated only for purposes described in Annex B or subsequently authorised by the data subject.

2. Data quality and proportionality: Personal data must be accurate and, where necessary, kept up to date. The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.

3. Transparency: Data subjects must be provided with information necessary to ensure fair processing (such as information about the purposes of processing and about the transfer), unless such information has already been given by the data exporter.

4. Security and confidentiality: Technical and organisational security measures must be taken by the data controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the data controller.

5. Rights of access, rectification, deletion and objection: As provided in Article 12 of Directive 95/46/EC, data subjects must, whether directly or via a third party, be provided with the personal information about them that an organisation holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the data exporter. Provided that the authority has given its prior approval, access need also not be granted when doing so would be likely to seriously harm the interests of the data importer or other organisations dealing with the data importer and such interests are not overridden by the interests for fundamental rights and freedoms of the data subject. The sources of the personal data need not be identified when this is not possible by reasonable efforts, or where the rights of persons other than the individual would be violated. Data subjects must be able to have the personal information about them rectified, amended, or deleted where it is inaccurate or processed against these principles. If there are compelling grounds to doubt the legitimacy of the request, the organisation may require further justifications before proceeding to rectification, amendment or deletion. Notification of any rectification, amendment or deletion to third parties to whom the data have been disclosed need not be made when this involves a disproportionate effort. A data subject must also be able to object to the processing of the personal data relating to him if there are compelling legitimate grounds relating to his particular situation. The burden of proof for any refusal rests on the data importer, and the data subject may always challenge a refusal before the authority.

6. Sensitive data: The data importer shall take such additional measures (e.g. relating to security) as are necessary to protect such sensitive data in accordance with its obligations under clause II.

7. Data used for marketing purposes: Where data are processed for the purposes of direct marketing, effective procedures should exist allowing the data subject at any time to "opt-out" from having his data used for such purposes.

8. Automated decisions: For purposes hereof "automated decision" shall mean a decision by the data exporter or the data importer which produces legal effects concerning a data subject or significantly affects a data subject and which is based solely on automated processing of personal data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. The data importer shall not make any automated decisions concerning data subjects, except when:

(a) (i) such decisions are made by the data importer in entering into or performing a contract with the data subject, and

(ii) (the data subject is given an opportunity to discuss the results of a relevant automated decision with a representative of the parties making such decision or otherwise to make representations to that parties.

or

(b) where otherwise provided by the law of the data exporter.

ANNEX B

DESCRIPTION OF THE TRANSFER

Data subjects

The personal data transferred concern the following categories of data subjects:

- Persons viewing and/or interacting with the online properties (including advertisements) which have been tagged by or on behalf of data exporter.

Purposes of the transfer(s)

The transfer is made for the following purposes:

- Data analysis and creation of segments
- Targeting of ad campaigns

Categories of data

The personal data transferred concern the following categories of data:

- Online identifiers (*e.g.*, cookie ID, mobile device advertising ID (e.g., Apple IDFA, Google AD ID);
- IP address;
- Event-level data; and
- Data exporter proprietary identifiers

The event-level data collected includes information in http headers (for example, URL, web page title, and referring page information), user-agent, timestamps, etc. A full list of event-level data collected is available upon request.

Recipients

The personal data transferred may be disclosed only to the following recipients or categories of recipients:

- Data importer (or its subsidiaries and affiliates) employees
- Data importer subcontractors;
- Data importer customers
- Other technology providers involved in the purchasing of digital ad inventory / DSPs / Ad networks or exchanges;

Sensitive data (if appropriate)

The personal data transferred concern the following categories of sensitive data (special categories of data):

- The data exporter will not send sensitive data to the data importer.

Additional useful information (storage limits and other relevant information)

- See the Agreement

Contact points for data protection inquiries:

Data exporter
General Counsel and Chief Privacy Officer
See address in the agreement

Data importer
The data exporter's privacy and security point of contact stated in a Service Order for the Lotame Services