DATA PROCESSING AGREEMENT

THIS DATA PROCESSING AGREEMENT, including its Schedules and Appendices (the "**DPA**"), forms part of the Master Services Agreement and all applicable Orders between Ekata, Inc. ("**Ekata**" "**we**" or "**us**") and you ("**Customer**" or "**You**") and your applicable Affiliates, for the purchase and license of online services and data from Ekata. All capitalized terms used herein, which are not defined herein, shall have the definition set forth in the Master Services Agreement, applicable Orders, or any agreement for similar services that require Processing of Personal Data.

SECTION 1. DEFINITIONS.

1.1 "**European Data Protection Laws**" means the EU General Data Protection Regulation 2016/679 (as amended or replaced from time to time) ("**GDPR**") and the Member State laws implementing or supplementing the GDPR), the GDPR as amended and incorporated into UK law under the UK European (Withdrawal) Act 2018 ("UK GDPR"), and UK Data Protection Act 2018 (each as amended and replaced from time to time).

1.2 "**Personal Data**" means any information relating to an identified or identifiable natural person (a "**Data Subject**").

1.3 "**Processing**" or "**Process**" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated 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.

SECTION 2. DATA TRANSFER.

2.1 **Transfer Mechanism.** This DPA applies to the Processing of Personal Data subject to European Data Protection Laws and transferred by or on behalf of Customer to Ekata. You acknowledge that Ekata Processes Personal Data in the United States. Ekata and Customer confirm that each will comply with all applicable requirements under the European Data Protection Laws with regard to the transfer of Personal Data from the European Economic Area ("**EEA**"), the United Kingdom ("**UK**"), or Switzerland to the United States, and that this DPA incorporates by this reference, the Standard Contractual Clauses (2004/915/EC) attached as Addendum A to this DPA, to the extent applicable to the data flows and Personal Data transferred hereunder.

2.2 **Assessment.** Taking into account (i) the circumstances of the transfer, (ii) the supplementary measures Ekata has put into place, which include encryption of Personal Data in transit and at rest, and (iii) Ekata is not an "electronic communication service provider" as defined by 50 U.S.C. § 1881(b)(4) ("FISA 702"), compliance with the Standard Contractual Clauses ensures appropriate safeguards for such cross-border transfers. Ekata shall notify Customer if it becomes unable to comply with the Standard Contractual Clauses.

SECTION 3. PROCESSING DETAILS.

3.1 **Purpose.** The purposes for which Personal Data will be Processed pursuant to this DPA are for identify verification, fraud detection, and the development of identity verification and fraud prevention solutions, as set forth in the Master Services Agreement and any applicable Order.

3.2 **Roles.** As between the parties, each party is an independent data controller.

3.3 **Categories of Data Subjects and Types of Personal Data.** Customer and its Users may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects: customers, potential customers, employees, agents and contractors of Customer (who are natural persons) and Customer's Users authorized by Customer to use the Services. The Personal Data Processed include the following types of non-sensitive data: first and last name, employer, physical address, phone, email address, and IP address. The parties shall Process no sensitive data hereunder.

SECTION 4. EUROPEAN DATA LAW OBLIGATIONS

4.1 **Data Subject Rights.** Each party will comply with its obligations under European Data Laws, including but not limited to GDPR Articles 12-15 (inclusive), to provide information and communications relating to Processing of Personal Data pursuant to this DPA, as well as complying with its obligations under European Data Laws, including but not limited to GDPR Articles 15-22 relating to Data Subject rights. You represent that you comply with your obligations under European Data Laws, including but not limited to GDPR Articles 13 and/or 14, as applicable, to provide information and communications to Data Subjects relating to the Processing of Personal Data pursuant to this DPA. Taking into account the nature of the Processing, at your request, we will provide reasonable assistance, in so far as possible, to you for the fulfilment of your obligation to respond to Data Subject requests where such Data Subject requests come through the Customer. Otherwise, each party will reasonably assist the other party with any legitimate requests from data subjects or authorities regarding Personal Data.

4.2 **Security and Data Protection.** Taking into account the nature of the Processing, each party shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk as set out under European Data Laws, including but not limited to GDPR Article 32, and otherwise as set out under GDPR Articles 33-36 .

4.3 **Other Obligations.** Each party shall comply with its respective obligations under European Data Protection Laws with regard to the Personal Data transferred by or on behalf of Customer to Ekata.

SECTION 5. ENTIRE AGREEMENT.

This DPA, together with the Master Services Agreement, applicable Order(s), and documentations referenced therein, constitutes the entire understanding of the parties with respect to the subject matter thereof. In the event of inconsistency or conflict between the Master Services Agreement, applicable Order(s), or other documents incorporated in the Agreement, and this DPA, the terms and conditions of this DPA shall govern and control. The terms set forth in this DPA shall not release a Party of its obligations and covenants set forth in the Agreement that accrued prior to the DPA Effective Date.

SECTION 6. REPRESENTATIONS AND WARRANTIES.

Each party represents and warrants that: (i) it has obtained any necessary and requisite approvals, consents and authorizations of third parties and governmental authorities to enter into this DPA and to perform and carry out its obligations hereunder; (ii) the persons executing this DPA on behalf of each party have express authority to do so, and, in so doing, to bind the parties thereto; (iii) the execution, delivery and performance of this DPA does not violate any provision of any bylaw, charter, regulation, or any other governing authority of the party; and (iv) the execution, delivery and performance of this DPA has been duly authorized by all necessary partnership or corporate action and is a valid and binding obligation of such party, enforceable in accordance with its terms.

WHEREFORE, the parties have executed this DPA as of the effective date of the applicable Order.

Ekata, Inc.

By: _____

Name: _____

Title: _____

Date: _____

Customer

By: *[Incorporated by reference and signed via execution of an applicable Order]*

ADDENDUM A

DATA TRANSFER AGREEMENT

between

Customer

hereinafter “data exporter”

and

Ekata, Inc.
1301 Fifth Avenue, Suite 1600
Seattle, WA USA 98101
legal@ekata.com

hereinafter “data importer”

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 organizational measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized 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 authorizes 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 authorized 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 organization authorized 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 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 authorization or decision and is based in a country to which such an authorization or decision pertains, but is not covered by such authorization or decision for the purposes of the transfer(s) of the personal data, or

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

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

Initials of data importer: ____

(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).

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.

Dated: *[as of the effective date of the applicable Order]*

FOR DATA IMPORTER

By: _____

Name: _____

Its: _____

FOR DATA EXPORTER

By: *[Incorporated by reference and signed via execution of an applicable Order]*

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 authorized 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 organizational 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, unauthorized 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 organization 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 organizations 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 organization 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: Exporter's customers and potential customers, employees, agents and contractors (who are natural persons).

Purposes of the transfer(s)

The transfer is made for the following purpose(s): To provide identity verification, fraud detection and fraud prevention solutions.

Categories of data

The personal data transferred concern one or more of the following categories of non-sensitive data: First and last name, employer, physical address, phone number, email address, and IP address. The parties shall transfer no sensitive data hereunder.

Data protection registration information of data exporter (where applicable)

Contact points for data protection enquiries

Data importer:

euprivacy@ekata.com

Attn: EU privacy officer