

Ekata Data Processing Agreement - Customer (C2C) - BCRs

This Data Processing Agreement (the “**Agreement**”) will become effective at the date the following parties have validly completed and executed it:

- (1) Ekata, Inc., a Delaware corporation with offices at 1301 Fifth Avenue, Suite 1600, Seattle, WA 98101, United States (“**Ekata**”);
- (2) the Company or other applicable counterparty (“**Customer**”); and
- (3) solely with respect to **Annex 2** to this Agreement, Mastercard Europe SA, a company organized under the laws of Belgium with its registered office at Chaussée de Tervuren 198A, 1410 Waterloo, Belgium (“**Mastercard Europe**”).

Ekata and Customer are hereinafter collectively referred to as the “**Parties**” or each individually as a “**Party.**”

BACKGROUND

- (A) Ekata and Customer have entered into a written services agreement, an Order, an enrollment form, or any other relevant agreement (the “**Principal Agreement**”) which involves the Processing of Personal Data of individuals subject to Privacy and Data Protection Law.
- (B) The Parties have agreed to enter into this data processing agreement to govern such Processing of Personal Data.

AGREED TERMS

1. Definitions and interpretation.

Capitalized terms not otherwise defined herein have the meaning given to them in the Principal Agreement. Except as modified below, the terms of the Principal Agreement remain in full force and effect.

The following terms have the meanings set out below for this Agreement:

- 1.1. “**Affiliate**” means in relation to a Party, any other entity which directly or indirectly Controls, is Controlled by, or is under direct or indirect common Control with that Party from time to time. “**Control**”, for the purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.
- 1.2. “**Business Purpose**” (or “**Purpose**”) means the use of Personal Data for Ekata or Customer’s operational purposes, or other notified purposes, provided that the use of Personal Data is reasonably necessary and proportionate to achieve the operational purpose for which the Personal Data was collected or processed or for another operational purpose that is compatible with the context in which the Personal Data was collected.
- 1.3. “**CCPA**” means the California Consumer Privacy Act of 2018 (California Civil Code §§ 1798.100 to 1798.199) and its implementing regulations as amended or superseded from time to time.

- 1.4. “**Customer Data**” means the information submitted by Customer via the Services.
- 1.5. “**Customer Personal Information**” means Personal Information subject to the CCPA that Ekata Processes on behalf of Customer to provide the Services to Customer.
- 1.6. “**Data Protection Rights**” means all rights granted to individuals under Privacy and Data Protection Law, which may include – depending on applicable law – the right to know, the right of access, rectification, erasure, complaint, data portability, restriction of Processing, objection to the Processing, and rights relating to automated decision-making and indemnification against misuse of Personal Data.
- 1.7. “**Data Subject**” means an identified or identifiable natural person whose Personal Data is Processed in the context of the Principal Agreement. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier, such as name, an identification number, location data, an online identifier, or to one or more factors specific to his physical, physiological, genetic, mental, economic, cultural or social identity.
- 1.8. “**Deidentified Data**” means data generated or derived from Customer Data or the Services that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular individual.
- 1.9. “**Ekata Data**” means information that Ekata provides or otherwise makes available to Customer through the Services or pursuant to an Order. Ekata Data includes but is not limited to information from publicly available sources, third-party data providers, and Metadata.
- 1.10. “**EU Data Protection Law**” means all of the following, each as amended and replaced from time to time: the EU General Data Protection Regulation 2016/679 (“**EU GDPR**”) and the e-Privacy Directive 2002/58/EC (as amended by Directive 2009/136/EC) and their respective national implementing legislations; the Swiss Federal Data Protection Act; the Monaco Data Protection Act; the UK Data Protection Act 2018 and UK GDPR (together “**UK Data Protection Law**”); and the Data Protection Acts of the European Economic Area (“**EEA**”) countries; each as applicable.
- 1.11. “**Metadata**” means pseudonymized data that Ekata derives or generates from its analysis of Customer Data. Examples of Metadata include the number of times a data element has been queried in a period of time (velocity) or the last time a data element has been seen (recency) and hashed, encrypted Customer Data. Metadata does not constitute Customer Data.
- 1.12. “**Order**” means a document or online order entered into between Customer and Ekata, or any of their Affiliates, that specifies the Services to be provided by Ekata. By entering into an Order, an Affiliate of Customer agrees to be bound by the terms of this Agreement as if it were an original party.
- 1.13. “**Personal Data**” (or “**Personal Information**”) means any information relating to an identified or identifiable individual, including but not limited to contact information, demographic information, passport number, Social Security number or other national identification number, bank account information, Primary Account Number and authentication information (e.g., identification codes, passwords).

- 1.14. **“Personal Data Breach”** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, access to, or other unauthorized Processing of Personal Data transmitted, stored or otherwise Processed.
- 1.15. **“Privacy and Data Protection Law”** means any law, statute, declaration, decree, legislation, enactment, order, ordinance, regulation or rule (as amended and replaced from time to time) which relates to the protection of individuals with regards to the Processing of Personal Data to which the Parties are subject, including but not limited to EU Data Protection Law; the CCPA; the U.S. Gramm-Leach-Bliley Act; the Brazil General Data Protection Act; the South Africa Protection of Personal Information Act; laws regulating unsolicited email, telephone, and text message communications; security breach notification laws; laws imposing minimum security requirements; laws requiring the secure disposal of records containing certain Personal Data; laws governing the portability and/or cross-border transfer of Personal Data; and all other similar international, federal, state, provincial, and local requirements; each as applicable.
- 1.16. **“Processing of Personal Data”** (or **“Processing/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, including any operation defined as “Processing” under applicable Privacy and Data Protection Law.
- 1.17. **“Sensitive Data”** means any Personal Data considered to be sensitive according to applicable Privacy and Data Protection Law and may include data revealing racial or ethnic origin, political opinions, cult, religious or philosophical beliefs, or trade union membership, criminal records, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.
- 1.18. **“Services”** are Ekata’s suite of global identity verification products and fraud detection services provided to Customer under an Order, or pursuant to a free trial, as further defined in the Principal Agreement. Services exclude Ekata Data.
- 1.19. **“User”** means an individual who is authorized by Customer to access or use the Services, and who has been provided a user id and password, or other account credential. For example, Users may include employees, contractors, and agents of Customer.

2. Scope and Applicability

- 2.1. This Agreement regulates the Processing of Personal Data subject to Privacy and Data Protection Law for the Services provided in the Principal Agreement.
- 2.2. In addition, to the extent the Principal Agreement involves the Processing of Personal Data of individuals subject to EU Data Protection Law, the Parties have agreed to the terms set forth in **Annex 2** of the Agreement for the purpose of complying with EU Data Protection Law (the **“EU Addendum”**). To the extent Ekata Processes Customer Personal Information to provide the Services to Customer, Ekata and Customer will comply with their respective obligations pursuant to the terms set forth in **Annex 3** of the Agreement (the **“CCPA Addendum”**).

- 2.3. In the event of a conflict between the terms of the Principal Agreement and this Agreement, the terms of this Agreement will control to the extent of such conflict. In the event of a conflict between the terms of this Agreement and the Value-Added Services Rules, the terms of this Agreement will apply.
- 2.4. The Parties will comply with their respective obligations as laid down in this Agreement, without regard to the residency or location (permanent or otherwise) of any individual to whom any Personal Data relates, the location of a Party's operations, the extent to which it has targeted particular geographic regions or jurisdictions, or any other factors.
- 3. Compliance with Privacy and Data Protection Law.** Both Parties represent and warrant that they will comply with Privacy and Data Protection Law when Processing Personal Data in the context of the Services, and that they will perform their obligations under this Agreement in compliance with Privacy and Data Protection Law.
- 4. Roles of the Parties.** The Parties acknowledge and confirm that each Party is responsible for the Processing of Personal Data for its own Business Purposes in the context of the Services specified in the Principal Agreement, as described below:
- 4.1. Ekata Processes Personal Data for the following Business Purposes: operating, providing, supporting or enabling the Services to Customer and other third parties, including by de-identifying Customer Data and creating Ekata's databases, and for enabling payments, finance and account management, data analysis, benchmarking, technical and customer support, fraud detection and prevention and product development, and for ensuring compliance with applicable laws ("**Ekata Purposes**").
- 4.2. Customer Processes Personal Data for the following Business Purposes: collecting and sharing Customer Data with Ekata; receiving and using Metadata in the context of the Services; and taking any fraud countermeasures based on Metadata ("**Customer Purposes**").
- 5. Obligations of the Parties.** Without prejudice to Section 6 of this Agreement, each Party represents and warrants that, in relation to the Processing of Personal Data for its own Business Purposes in the context of the Services, it will:
- 5.1. provide appropriate notice to and/or seek consent from individuals as required under Privacy and Data Protection Law (Notice and Consent).
- 5.2. ensure that, for any transfers of Personal Data in the context of the Services, the Personal Data will be protected with the same level of protection as provided by this Agreement and it will implement any data transfer mechanism as required under Privacy and Data Protection Law. In particular, in the event Personal Data subject to the Argentina Personal Data Protection Act 25.326 (PDPA) (Ley de Protección de los Datos Personales) is Processed, the Parties undertake to comply with the obligations applicable to a data controller set forth in the model contract titled Contrato Modelo de Transferencia Internacional de Datos Personales con Motivo de Cesión de Datos Personales adopted by the Data Protection Agency of the Republic of Argentina under Disposition 60 — E/2016 (the 'Argentinian SCCs') for the transfer of Personal Data to third countries (Transfers).

- 5.3. cooperate with the other Party in good faith to fulfil their respective data protection compliance obligations under Privacy and Data Protection Law, including complying with individuals' requests to exercise their Data Protection Rights and replying to investigations and inquiries from regulators (Cooperation and Assistance).
- 5.4. be responsible for compliance with this Agreement and for the compliance of their respective Affiliates and Users.
- 5.5. conduct and review any relevant assessments (including security or privacy impact assessments) as may be required by applicable Privacy and Data Protection Laws for purposes of implementing the Services, and any cross-border transfers of Personal Data.

6. Customer's Obligations.

- 6.1. **Generally.** Customer will use best efforts to prevent unauthorized access to or Processing of Metadata and will notify Ekata without undue delay of any such unauthorized access, or Processing. Customer will use the Services and Metadata only to the extent permitted by the Principal Agreement. Customer is solely responsible for ensuring that its use of the Services and Metadata, including Customer's provision of Customer Data to Ekata as contemplated in the Principal Agreement or this Agreement, does not violate any laws, in particular any applicable Privacy and Data Protection Laws. Any use of the Services in breach of this Agreement by Customer, its Affiliates, or any Users, may result in Ekata's immediate suspension of the Services.
- 6.2. **Customer's Privacy Policy.** Irrespective of Section 5 of this Agreement, Customer will not collect or provide or make available to Ekata any Customer Data that is not collected or stored in accordance with applicable law and Customer's privacy policy (or the privacy policy of Customer's customers, if applicable). Customer represents and warrants that Customer will provide Data Subjects with all notices and obtain from them all rights and consents necessary for the provision and transfer of such data to Ekata, the Processing of such data by or on behalf of Ekata, and Customer's use of Metadata pursuant to this Agreement. As between Customer and Ekata, Customer is solely responsible for providing such notice and obtaining such consent. Customer also confirms and warrants that it will inform Data Subjects in particular of the transfer and storage by Ekata of their Personal Data outside the country in which it was collected (e.g., transfer to and storage in the United States), the ways in which their Personal Data will be Processed by Customer and Ekata, and any other information required by applicable Privacy and Data Protection Laws. Customer will ensure that Customer's privacy policy is readily accessible to anyone from or about whom Customer collects data and, if required by applicable law, Customer will provide those Data Subjects with the ability to exercise rights applicable to their Personal Data under applicable Privacy and Data Protection Laws, such as opting-out of disclosure of their Personal Data by Customer.
- 6.3. **Data Integrity.** Customer is exclusively responsible for the accuracy, completeness, relevance and integrity of all Personal Data provided to Ekata.
- 6.4. **No Automated Decision-Making.** Customer hereby represents and warrants that it will not use the Services to make any automated decisions that produce legal effects concerning Data Subjects or similarly significantly affect Data Subjects.

- 7. Transfers.** Customer acknowledges and agrees that all data including Personal Data Processed in connection with this Agreement will be transferred and stored outside the country in which such Personal Data was collected (e.g., transfer to and storage in the United States), and Customer represents and warrants that it has all necessary consents, authorizations, permissions and/or approvals for such transfer, storage and Processing of all data including Personal Data to a location outside the country in which such Personal Data was collected (including in particular, to the United States), in accordance with applicable Privacy and Data Protection Law.
- 8. Security of the Processing, Confidentiality, and Personal Data Breach Notification.** The Parties agree and warrant that:
- 8.1. they have implemented and maintain a comprehensive written information security program that complies with Privacy and Data Protection Law and **Annex 1** of this Agreement, including appropriate technical, operational and organizational measures to protect from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, access to, or otherwise unauthorized Processing of Personal Data transmitted, stored or otherwise Processed (Information Security Program). A Party's Information Security Program shall comply with the applicable Payment Card Industry Data Security Standards to the extent that Party Processes payment card information.
- 8.2. they have taken steps to ensure that any person or entity acting under its authority, who Processes or in any way has access to Personal Data in the context of the Services (including any entity engaged by a Party or any further sub-contractor) is only granted access to Personal Data on a need-to-know basis and is subject to a duly enforceable contractual or statutory confidentiality obligation (Confidentiality).
- 9. Notification Obligations.** Each Party agree and warrant that it will:
- 9.1. immediately inform the other Party, in writing, of any request, question, objection, complaint, investigation or any other inquiry, received from any individual, regulator or public authority of whatever jurisdiction, that relates to Personal Data Processed in the context of the Services, unless otherwise restricted by applicable law. Each Party will provide the other Party with a copy of any such requests within 48 (forty-eight) hours of receipt (i) for Ekata, by email to TPRM@mastercard.com and SOC@mastercard.com; (ii) for Customer, by email to [insert email address] and will respond to such requests only in accordance with the other Party's prior written authorization, unless otherwise prohibited by applicable law (Notification Obligations).
- 9.2. implements appropriate administrative, technical, operational and organizational measures to ensure, and to be able to demonstrate, that the Processing of Personal Data is performed in accordance with this Agreement and applicable Privacy and Data Protection Law (Accountability).
- 10. Data Disclosures.** The Parties represent and warrant that they will only disclose Personal Data to a third party in accordance with Privacy and Data Protection Law and with this Agreement and Principal Agreement and will require such third party in writing to comply with Privacy and Data Protection Law and with the same obligations as are imposed on each Party by this Agreement, as appropriate and relevant, unless it is not possible to do so, such as where the data recipient is a governmental authority.

11. Liability.

11.1. Each Party agrees that, in relation to the Processing of Personal Data for its own Purposes, it is fully liable towards individuals for the entire damages resulting from a violation of Privacy and Data Protection Law or of this Agreement.

11.2. The Parties agree that if Ekata has paid compensation, damages or fines, Ekata is entitled to claim back from Customer that part of the compensation, damages or fines, corresponding to Customer's part of responsibility for the compensation, damages or fines.

12. Applicable Law and Jurisdiction. The Processing of Personal Data under this Agreement is governed by the law applicable to the Principal Agreement. Any disputes between the Parties relating to the Processing of Personal Data under this Agreement will be subject to the exclusive jurisdiction of the courts in the Principal Agreement.

13. Modification of this Agreement. This Agreement may only be modified by a written amendment signed by each of the Parties.

14. Termination. The Parties agree that this Agreement is terminated upon the termination of the Principal Agreement pursuant to which Customer obtained Personal Data from Ekata.

15. Invalidity and Severability. If any provision of this Agreement is found by any court or administrative body of a competent jurisdiction to be invalid or unenforceable, the invalidity or unenforceability of such provision will not affect any other provision of this Agreement and all provisions not affected by such invalidity or unenforceability will remain in full force and effect.

16. Counterparts. This Agreement may be executed in any number of counterparts, each of which when executed will constitute a duplicate original, but all the counterparts will together constitute the one agreement.

IN WITNESS WHEREOF, Ekata, Mastercard Europe and Customer have executed this Agreement and each acknowledges having received a duly executed copy.

Ekata	
By:	
Name:	
Title:	
Dated:	

[Customer Legal Entity]	
By:	
Name:	[Customer to populate]
Title:	[Customer to populate]
Dated:	

Mastercard Europe	
By:	
Name:	
Title:	
Dated:	

ANNEX 1

TECHNICAL AND ORGANIZATIONAL MEASURES

The Parties will, as a minimum, implement the following types of security measures:

1. Physical access control

Technical and organizational measures to prevent unauthorized persons from gaining access to the data processing systems available in premises and facilities (including databases, application servers and related hardware), where Personal Data are processed, include:

- Establishing security areas, restriction of access paths;
- Establishing access authorizations for employees and third parties;
- Access control system (ID reader, magnetic card, chip card);
- Key management, card-keys procedures;
- Door locking (electric door openers etc.);
- Security staff, janitors;
- Surveillance facilities, video/CCTV monitor, alarm system;
- Securing decentralized data processing equipment and personal computers.

2. Virtual access control

Technical and organizational measures to prevent data processing systems from being used by unauthorized persons include:

- User identification and authentication procedures;
- ID/password security procedures (special characters, minimum length, change of password);
- Automatic blocking (e.g. password or timeout);
- Monitoring of break-in-attempts and automatic turn-off of the user ID upon several erroneous passwords attempts;
- Creation of one master record per user, user master data procedures, per data processing environment.

3. Data access control

Technical and organizational measures to ensure that persons entitled to use a data processing system gain access only to such Personal Data in accordance with their access rights, and that Personal Data cannot be read, copied, modified or deleted without authorization, include:

- Internal policies and procedures;
- Control authorization schemes;
- Differentiated access rights (profiles, roles, transactions and objects);
- Monitoring and logging of accesses;
- Disciplinary action against employees who access Personal Data without authorization;
- Reports of access;
- Access procedure;
- Change procedure;
- Deletion procedure.

4. Disclosure control

Technical and organizational measures to ensure that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media (manual or electronic), and that it can be verified to which companies or other legal entities Personal Data are disclosed, include:

- Tunneling
- Logging
- Transport security

5. Entry control

Technical and organizational measures to monitor whether data have been entered, changed or removed (deleted), and by whom, from data processing systems, include:

- Logging and reporting systems;
- Audit trails and documentation.

6. Control of instructions

Technical and organizational measures to ensure that Personal Data are processed solely in accordance with the Instructions of the Controller include:

- Unambiguous wording of the contract;
- Formal commissioning (request form);
- Criteria for selecting the Processor

7. Availability control

Technical and organizational measures to ensure that Personal Data are protected against accidental destruction or loss (physical/logical) include:

- Backup procedures;
- Mirroring of hard disks (e.g. RAID technology);
- Uninterruptible power supply (UPS);
- Remote storage;
- Anti-virus/firewall systems;
- Disaster recovery plan.

8. Separation control

Technical and organizational measures to ensure that Personal Data collected for different purposes can be processed separately include:

- Separation of databases;
- "Internal client" concept / limitation of use;
- Segregation of functions (production/testing);
- Procedures for storage, amendment, deletion, transmission of data for different purposes.

ANNEX 2 EUROPEAN DATA PROCESSING ADDENDUM

Customer, Ekata, and Mastercard Europe agree that the terms and conditions set out below are added as a European Data Processing Addendum (“**EU Addendum**”) to, and form an integral part of, the Agreement to which it is attached. This EU Addendum regulates the Processing of Personal Data of Data Subjects subject to EU Data Protection Law.

In the event of a conflict between the terms of this EU Addendum and the Agreement with respect to the subject matter of this EU Addendum, the terms of this EU Addendum will control to the extent of such conflict.

1. Definitions.

Capitalized terms not otherwise defined herein have the meaning given to them in the Agreement. Except as modified below, the terms of the Agreement remain in full force and effect.

The following terms have the meanings set out below for this EU Addendum:

- 1.1. The terms “**Binding Corporate Rules**”, “**Controller**”, “**Data Subject**”, “**Personal Data**”, “**Personal Data Breach**”, “**Processing/Process of Personal Data**”, “**Processor**”, and “**Supervisory Authority**” shall have the meanings given to them under EU Data Protection Law.
- 1.2. “**Europe**” means the European Economic Area, Switzerland, Monaco and the United Kingdom.
- 1.3. “**EEA Mastercard Binding Corporate Rules**” (or “**EEA Mastercard BCRs**”) means the Mastercard Binding Corporate Rules as approved by the EEA data protection authorities and available at <https://www.mastercard.us/content/dam/mccom/en-us/documents/mastercard-bcrs-february-2017.pdf>.
- 1.4. “**UK Mastercard Binding Corporate Rules**” (or “**UK Mastercard BCRs**”) means the Mastercard Binding Corporate Rules as approved by the UK data protection authority and available at <https://www.mastercard.us/content/dam/mccom/en-us/documents/mastercard-bcrs-february-2017.pdf>.

2. Roles of the Parties. For the purpose of the Principal Agreement and the Agreement, the Parties acknowledge and confirm that each Party is a Controller for the Processing of Personal Data for its own Purposes (as specified in Section 4 of the Agreement) in the context of the Services. The Parties further confirm that neither Party acts as a Processor on behalf of the other Party; that each Party is an independent Controller; and that the Agreement does not create a joint-Controllership or a Controller-Processor relationship between the Parties.

3. Obligation of the Parties. Without prejudice to Section 6 of the Agreement, each Party represents and warrants that, in relation to the Processing of Personal Data for its own Purposes in the context of the Services, it acts as a Controller and that it:

- 3.1. complies with EU Data Protection Law in respect of Processing of Personal Data (Lawfulness of processing);
- 3.2. relies on a valid legal ground under EU Data Protection Law for each of its own Purposes, including obtaining Data Subjects' appropriate consent if required or appropriate under EU Data Protection Law (Legal ground);
- 3.3. provides appropriate notice to the Data Subjects regarding the Processing of Personal Data for its own Purposes, in a timely manner and at the minimum with the elements required under EU Data Protection Law (Notice);
- 3.4. takes reasonable steps to ensure that Personal Data is accurate, complete and current; adequate, relevant and limited to what is necessary in relation to the Purposes for which they are processed; and kept in a form which permits identification of Data Subjects for no longer than is necessary for the Purposes for which the Personal Data are processed unless a longer retention is required or allowed under applicable law (Accuracy, data minimization and data retention);
- 3.5. implements appropriate technical and organizational measures to ensure, and to be able to demonstrate, that the Processing of Personal Data is performed in accordance with EU Data Protection Law (Accountability);
- 3.6. responds to Data Subject requests to exercise their any rights granted to individuals under EU Data Protection law, including but not limited to the right of (a) access, (b) rectification, (c) erasure, (d) data portability, (e) restriction of Processing, and (f) objection to the Processing in accordance with EU Data Protection Law (Data Subjects' Rights); and
- 3.7. cooperates with the other Party to fulfil their respective data protection compliance obligations under EU Data Protection Law (Cooperation).

4. International Data Transfers.

- 4.1. Customer may transfer the Personal Data Processed in connection with the Services outside of Europe in accordance with EU Data Protection Law, provided that the Personal Data are transferred to a country which provides an adequate level of protection under EU Data Protection Law or to a recipient which has implemented adequate safeguards under EU Data Protection Law such as approved Binding Corporate Rules or standard contractual clauses.
- 4.2. Ekata may transfer the Personal Data Processed in connection with the Services outside of the European Economic Area, Switzerland, Monaco in accordance with the EEA Mastercard BCRs and outside of the UK in accordance with the UK Mastercard BCRs or with any other lawful data transfer mechanism that provides an adequate level of protection under EU Data Protection Law. Ekata represents and warrants that it will abide by the EEA or the UK Mastercard BCRs when Processing Personal Data for its own Purposes in the context of the Services.

- 4.3. If either Party's compliance with EU Data Protection Law applicable to transfers of Personal Data is affected by circumstances outside of either Party's control, including if a legal instrument for transfers is invalidated, amended, or replaced, then the Parties will work together in good faith to reasonably resolve such non-compliance.
- 4.4. Notwithstanding anything to the contrary in the Agreement, Customer shall promptly and no later than 48 hours from becoming aware inform Ekata in writing to euprivacy@ekata.com, with the subject line "Data Processing Agreement Notification", if (1) it has reason to believe that it is or has become subject to laws or practices that prevent the Customer from fulfilling its obligations under this EU Addendum. Customer shall provide the description of the non-compliance and the reasons for the non-compliance, and its impact or likely impact on Ekata or Ekata's customers.
- 5. Data Disclosures.** The Parties represent and warrant that they will only disclose Personal Data Processed to a third party in the context of the Services in accordance with EU Data Protection Law and will require such third party in writing to comply with EU Data Protection Law as well as the same obligations as are imposed by this EU Addendum, as appropriate and relevant, unless it is not possible to do so, such as where the data recipient is a governmental authority. Customer will not disclose any Metadata to third parties.
- 6. Security of the Processing, Confidentiality, and Personal Data Breach Notification.**
- 6.1. The Parties must implement and maintain a comprehensive written information security program with appropriate technical and organizational measures to ensure a level of security appropriate to the risk, and as appropriate: (a) the pseudonymization and encryption of Personal Data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing. In assessing the appropriate level of security, the Parties must take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing of Personal Data as well as the risk of varying likelihood and severity for the rights and freedoms of Data Subjects and the risks that are presented by the Processing of Personal Data, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed.
- 6.2. The Parties must take steps to ensure that any person acting under their authority who has access to Personal Data is subject to a duly enforceable contractual or statutory confidentiality obligation, and if applicable Process Personal Data in accordance with the Controller's instructions.
- 6.3. Each Party must notify the other Party of a Personal Data Breach that relates to Personal Data Processed in the context of the Service and for which the other Party is a Controller, without undue delay, and not later than forty-eight (48) hours after having become aware of a Personal Data Breach. The Parties will assist each other in complying with their obligations to notify a Personal Data Breach. The Party which becomes aware of a Personal Data Breach will notify, without undue delay and, where feasible, not later than 72 hours after having become aware of it, the competent Supervisory Authority, where required by EU Data Protection Law. When the Personal Data Breach is likely to result in a high

risk to the rights and freedoms of Data Subjects or upon the competent Supervisory Authority's request to do so, such Party must communicate the Personal Data Breach to the Data Subject without undue delay, where required by EU Data Protection Law.

- 6.4. The Parties will use their best efforts to reach an agreement on whether and how to notify persons or entities of a Personal Data Breach, and must document all Personal Data Breaches, including the facts relating to the Personal Data Breach, its effects and the remedial action taken.
- 7. Data Protection and Security Audit.** Each Party commits to conduct audits on a regular basis to control compliance with EU Data Protection Law, including the security measures provided in Section 6 of this EU Addendum and **Annex 1** of the Agreement. Upon prior written request, each Party agrees to cooperate and within reasonable time provide the requesting Party with: (a) a summary of the audit reports demonstrating its compliance with EU Data Protection Law obligations and the Agreement; and (b) confirmation that the audit has not revealed any material vulnerability, or to the extent that any such vulnerability was detected, that such vulnerability has been fully remedied.
- 8. Liability Towards Data Subject.** Subject to the limitation of liability clauses in the Agreement, each Party agrees that it will be held liable towards Data Subjects for the entire damage resulting from a violation of EU Data Protection Law for its own Purposes as specified in Section 4 of the Agreement. Where the Parties are involved in the same Processing and where they are responsible for any damage caused by the Processing of Personal Data, both Customer and Ekata may be held liable for the entire damage in order to ensure effective compensation of the Data Subject. If Ekata paid full compensation for the damage suffered, it is entitled to claim back from Customer that part of the compensation corresponding to Customer's part of responsibility for the damage.
- 9. Applicable Law and Jurisdiction.** The Parties agree that this EU Addendum and the Processing of Personal Data will be governed by the law of Belgium and that any dispute will be submitted to the Courts of Brussels.

The Parties are signing this EU Addendum on the Effective Date as defined in the Principal Agreement.

ANNEX 3 CCPA ADDENDUM

This CCPA Addendum (“**CCPA Addendum**”) forms part of the Agreement and sets forth the additional terms in respect of the Parties’ compliance with the CCPA. In the event of a conflict between the terms of this CCPA Addendum and the Agreement with respect to the subject matter of this CCPA Addendum, the terms of this CCPA Addendum will control to the extent of such conflict.

In this CCPA Addendum, the capitalized terms (i) “**Aggregate Consumer Information**,” “**Business**,” “**Business Purpose**,” “**Commercial Purpose**,” “**Deidentified**,” “**Personal Information**,” “**Processing**,” “**Sell**,” and “**Service Provider**” are defined as set forth in the CCPA and (ii) “**Metadata**” and “**Services**” are defined as set forth in the Agreement.

WHEREAS, pursuant to the Agreement, Ekata provides to Customer certain Services in support of one or more Business Purposes.

WHEREAS, the Parties intend for the terms of this CCPA Addendum to apply to the extent Ekata collects, receives, or otherwise, Processes Personal Information on Customer’s behalf to provide the Services to Customer.

NOW THEREFORE, for good and other valuable consideration, the Parties hereby agree as follows:

1. **Roles of the Parties.** The Parties agree that Customer is the Business and Ekata is a Service Provider with respect to any Customer Personal Information. Each Party will comply with its respective obligations under the CCPA. For the avoidance of doubt, Ekata’s collection, retention, use, disclosure, sale, or other Processing of Personal Information for its own purposes independent of Customer’s use of the Services specified in the Agreement are outside the scope of this CCPA Addendum.
2. **Processing of Client Personal Information**
 - 2.1. Ekata will collect, use, retain, disclose, and otherwise Process Customer Personal Information (i) to perform the Services, including in support of its internal operations and to identify and protect against fraudulent or illegal activity; (ii) as set forth in the Agreement and this CCPA Addendum; (iii) to comply with legal or contractual obligations; and (iv) as otherwise permitted by the CCPA.
 - 2.2. Ekata may disclose Customer Personal Information to, and permit the Processing of Customer Personal Information by, its Service Providers who perform services on behalf of Ekata. Ekata will take steps to ensure that such Service Providers are subject to contractual requirements with respect to the processing of Customer Personal Information at least as protective as those to which Ekata is subject pursuant to the Agreement and this CCPA Addendum. Ekata may retain, use, or disclose Customer Personal Information to detect data security incidents or protect against fraudulent or illegal activity. Further, Ekata may retain and use Customer Personal Information (and combine it with Personal Information from other customers) to build or improve the quality of its fraud detection and identity verification services, provided Ekata does not: (i) build or modify profiles to use in providing services to another business; or (ii) correct or augment data acquired from another source.
 - 2.3. With respect to Customer Personal Information, the Parties acknowledge and agree that:
 - (a) Ekata does not receive Customer Personal Information as consideration for any of the Services;

- (b) Ekata will not Sell Customer Personal Information provided by Customer to Ekata for the provision of the Services to Customer; and
 - (c) Except as otherwise permitted by the CCPA, Ekata will not use, retain, or disclose Customer Personal Information except as necessary to perform the Services and as set forth herein, and not for any Commercial Purpose.
- 2.4. Customer represents and warrants that it has provided notice that the Customer Personal Information is being used or shared consistent with Cal. Civ. Code 1798.140(t)(2)(C)(i). Customer acknowledges and agrees that it is responsible for compliance with all notice, consent, opt out, and privacy policy requirements under the CCPA, as well as for complying with all requests from individuals with respect to Customer Personal Information (including but not limited to requests to know, requests to delete, and requests to opt out), as may be required by applicable law (“**Consumer Requests**”).
- 2.5. Upon request, Ekata will provide reasonable assistance, as necessary, to permit Customer to respond to Consumer Requests to the extent required by the CCPA. Upon direction by Customer, and in any event no later than thirty (30) days after receipt of a written request from Customer, Ekata shall delete the Customer Personal Information as directed by Customer without undue delay.
 - 2.5.1. Ekata shall not be required to delete any Customer Personal Information to comply with a Customer’s request directed by Customer if Ekata’s retention of such information is required to comply with Cal. Civ. Code 1798.105(d), in which case Ekata shall promptly inform Customer of the exceptions relied upon under 1798.105(d) and Ekata shall not use the Customer Personal Information retained for any other purpose than provided for by that exception.
- 2.6. Notwithstanding any provision to the contrary of the Agreement or this Addendum, the terms of this Addendum shall not apply to Ekata’s processing of Customer Personal Information that is exempt from the CCPA, including under Cal. Civ. Code 1798.145(a).

3. **Processing of Metadata**

- 3.1. Customer acknowledges and agrees that Ekata may Process Metadata derived or generated from Customer Personal Information for its Business Purposes, such as to identify and protect against fraudulent or illegal activity. For clarity, Metadata does not include identifiers that indicate Customer as the source of Metadata. As between Ekata and Customer, Ekata exclusively will own rights, title, and interest in and to Metadata.

4. **Deidentified Data and Aggregated Data**

- 4.1. Customer acknowledges and agrees that Ekata may Process Aggregate Consumer Information and De-identified data (together, “**Deidentified Data**”) relating to, derived, or generated from Customer Personal Information or derived from the Services, for any lawful purpose. As between Ekata and Customer, Ekata exclusively will own rights, title, and interest in and to Deidentified Data. Customer further acknowledges and agrees that Deidentified Data does not constitute Customer Personal Information pursuant to the Agreement and this CCPA Addendum, and Ekata may use, maintain, disclose, and otherwise Process such Deidentified Data for any lawful purpose.
- 4.2. In the event that either Party shares Deidentified Data with the other Party, the receiving Party warrants that it: (i) has implemented technical safeguards designed to prohibit reidentification of the Consumer to whom the Deidentified Data may pertain; (ii) has implemented business processes designed to specifically prohibit reidentification of the Deidentified Data; (iii) has implemented business processes

designed to prevent inadvertent release of the Deidentified Data; and (iv) will make no attempt to reidentify Deidentified Data.

- 5. Changes in Data Protection Laws.** If any modification to this CCPA Addendum is required as a result of a change in data protection laws or regulations, then either Party may provide written notice to the other Party of that change in law. The Parties will discuss and negotiate in good faith any necessary amendments to this CCPA Addendum to address such change. If Customer gives notice under this Section 5, the Parties shall without undue delay discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in Customer's notice as soon as is reasonably practicable.