Data Processing Agreement

This Data Processing Addendum **("DPA")**, forms part of the Master Subscription Agreement, or similarly agreement or other written or electronic agreement pursuant to which Company ("**Company**") sells certain services to the undersigned customer of Company set forth in the Master Subscription Agreement ("**Customer**") (collectively, the "**Service**") provided by Company (**"Agreements**"). Each of Customer and Company may be referred to herein as a "**party**" andtogether as the "**parties**."

The parties have agreed to enter into this DPA in order to ensure that adequate safeguards are put in place with respect to the protection of such Personal Data as required by Global Data Protection Laws. This DPA is an addendum to and forms part of the Agreements. Customer entity signing this DPA must be the same as the Customer entity party to the Agreements.

1. Definitions

a. The following definitions are used in this DPA:
   i. "**Global Data Protection Laws**" means all current laws and regulations applicable to the processing of Personal Data under the Agreements, including, but not limited to, the GDPR, California Consumer Privacy Act (CCPA), as subsequently amended by the California Privacy Rights Act (CPRA), the Privacy Act 1988 California Consumer Privacy Act ("**CCPA**"), as subsequently amended by the California Privacy Rights Act ("**CPRA**"), the Privacy Act 1988, the Colorado Privacy Act, the Connecticut Data Privacy Act, the Utah Consumer Privacy Act, and the Virginia Consumer Data Protection Act ("**VCDPA**").
   ii. "**GDPR**" means the General Data Protection Regulation (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);
   iii. "**Personal Data**" means all data which is defined as "personal data," "personal information," or similar terms under Global Data Protection Laws and which is provided by Customer to Company to process on behalf of Customer;
   iv. The terms "**process**," "**processing**," "**data subject**," "**sub-processor**," "**data protection impact assessment**," etc., shall have the meaning ascribed to them under applicable Global Data Protection Laws.

2. Status of the Parties

a. The type of Personal Data processed pursuant to this DPA and the subject matter, duration, nature, and purpose of the processing, and the categories of data subjects, are as described in Annex 1.
b. Each party warrants in relation to Personal Data that it will comply (and will warrant that any of its personnel comply and use commercially reasonable efforts to warrant that its sub-processors comply), with Global Data Protection Laws. As between the parties, Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data. Specifically, Customer shall have sole

responsibility for complying with any applicable requirements under Global Data Protection Laws to determine the lawful basis for processing, provide data subjects with notice, obtain data subject consent, and respond to data subject requests.

c. In respect of the parties' rights and obligations under this DPA regarding the Personal Data, the parties hereby acknowledge and agree that Customer is the data controller and Company is the data processor.
d. Company it is a “service provider” (as defined in CCPA §1798.140(v)) to Customer under the CCPA.

3. Company Obligations

a. With respect to all Personal Data, Company:
    i. will only process Personal Data in order to provide services under the Agreements, and only in accordance with: (i) this DPA, (ii) the Customer's written instructions as represented by the Agreements and this DPA, and (iii) as required by applicable laws;

    ii. will not retain, use or disclose the Personal Data: (i) for any purpose other than providing services under the Agreements, including any “commercial purpose” (as defined in CCPA §1798.140(f); or (ii) outside of the direct business relationship between Company and Customer;

    iii. will not “sell” (as defined in CCPA §1798.140(t)) the Personal Data;

    iv. certifies that it understands and is willing to abide by the restrictions in California Civil Code Section 1798.140(w)(2)(A), as applicable;

    v. will implement appropriate technical and organizational measures designed to provide a level of security appropriate to the risks that are presented by the processing of Personal Data, and in particular, the risks of accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data. Such measures are set out in Annex II, which Customer has determined are appropriate;

    vi. will take reasonable steps to ensure that only authorized personnel have access to such Personal Data and that any persons whom it authorizes to have access to the Personal Data are under obligations of confidentiality;

    vii. will, no later than 72 hours after becoming aware of a confirmed breach involving Personal Data, notify Customer of any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed by Company (a “**Security Breach**”);

    viii. will, upon Customer’s reasonable request, promptly provide Customer with reasonable cooperation and assistance in respect of a Security Breach and reasonable information in Company’s possession concerning such Security Breach insofar as it affects Customer;

    ix. will, upon receiving any complaint, notice, or communication from any governmental entity (including government access requests or other disclosure orders where permitted by law), relating directly or indirectly to Company’s processing of Personal Data or potential failure to comply with Global Data Protection Laws, to the extent

permitted by law, promptly forward the complaint, notice, or communication to Customer and provide reasonable cooperation and assistance in relation to the same;

x. will promptly notify Customer if it receives a request from a data subject to access, rectify or erase that individual's Personal Data, or if a data subject objects to the processing of, or makes a data portability request in respect of, such Personal Data (each a "**Data Subject Request**"). Company shall not respond to a Data Subject Request without Customer's prior written consent except to confirm that such request relates to Customer, to which Customer hereby agrees. To the extent that Customer does not have the ability to address a Data Subject Request, then upon Customer's request Company shall provide reasonable assistance to Customer to facilitate such

Data Subject Request to the extent able and in line with applicable law. Customer shall cover all costs incurred by Company in connection with its provision of such assistance;

xi. will, other than to the extent required to comply with applicable law, as soon as reasonably practicable following termination or expiry of the Agreements or completion of the Service, delete or return all Personal Data (including copies thereof) processed pursuant to this DPA.

4. Sub-processing

a. Customer grants a general authorization: (a) to Company to appoint other affiliates as sub-processors, and (b) to Company and its affiliates to engage third-party sub-processors for performance of the Service.

5. Audit and Records

a. Where applicable, Company will make available to Customer such information in Company's possession or control as Customer may reasonably request with a view to demonstrating Company's compliance with Global Data Protection Laws in relation to its processing of Personal Data.

6. Data Transfer

Company is headquartered in the United States and only processes data in the United States. As such, to the extent Company will process Personal Data collected outside of the United States, the following provisions apply:

a. To the extent that Personal Data is transferred out of the European Economic Area (EEA) or the United Kingdom (UK), the parties agree that the standard contractual clauses approved by the EU authorities under EU data protection laws and set out in the Appendix (the "**Standard Contractual Clauses**") will apply in respect of that processing, and Company will comply with the obligations of the 'data importer' in the Standard Contractual Clauses and Customer will comply with the obligations of the 'data exporter'.

To the extent that Personal Data is transferred out of Canada or Australia, Company shall offer a "comparable level of protection," meaning protection that can be compared to the level of protection the personal information would receive if it had not been transferred.

7. General

a. This DPA is without prejudice to the rights and obligations of the parties under the Agreements which shall continue to have full force and effect. In the event of any conflict between the terms

of this DPA and the terms of the Agreements, the terms of this DPA shall prevail so far as the subject matter concerns the processing of Personal Data.

b. Company's liability under or in connection with this DPA (including under the Standard Contractual Clauses set out in the Appendix) is subject to the limitations on liability contained in the Agreements.

c. Except for the Standard Contractual Clauses, this DPA does not confer any third-party beneficiary rights, it is intended for the benefit of the parties hereto and their respective permitted successors and assigns only, and is not for the benefit of, nor may any provision hereof be enforced by, any other person.

d. The choice of law and jurisdiction concerning this DPA and any action related thereto shall be consistent with and pursuant to the Agreements. In the absence of choice of law and jurisdiction selection, the parties shall mutually agree upon choice of law and jurisdiction.

e. This DPA is the final, complete and exclusive agreement of the parties with respect to the subject matter hereof and supersedes and merges all prior discussions and agreements between the parties with respect to such subject matter. No modification of, amendment to, or waiver of any rights under the DPA will be effective unless in writing and signed by an authorized signatory of each party. This DPA may be executed in counterparts, each of which shall be deemed to be an original, but all of which, taken together, shall constitute one and the same agreement. Each person signing below represents and warrants that he or she is duly authorized and has legal capacity to execute and deliver this DPA. Each party represents and warrants to the other that the execution and delivery of this DPA, and the performance of such party's obligations hereunder, have been duly authorized and that this DPA is a valid and legally binding agreement on each such party, enforceable in accordance with its terms.

APPENDIX

This Appendix applies to only to the data of data subjects governed by the GDPR.

STANDARD CONTRACTUAL CLAUSES

Controller to Processor

Introduction

Both parties have agreed on the following Contractual Clauses (the "**Clauses**") in order to adduce adequate safeguards with respect to 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 Annex 1.

Agreed Terms

https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj

In response to Clause 9

Use of sub-processors

(a) OPTION 2: The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s).

In response to Clause 17

Governing Law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the EU Member State where data exporter maintains its main place of business in the EU.

In response to Clause 18

Choice of forum and jurisdiction

(b) The Parties agree that those shall be the courts of the EU Member State where data exporter maintains its main place of business in the EU.

ANNEX I

A. LIST OF PARTIES

B. Data exporter(s): The Company set forth in the Master Subscription Agreement.

Data importer(s):

Name: Monetate, Inc.
Address: 325 N. Saint Paul Street, Suite 3100, PMB #4759, Dallas, TX 75201, USA

Contact person's name, position, and contact details: KC Attaya, CFO, kc.attaya@monetate.com

Activities relevant to the data transferred under these Clauses: Processing data exporter's data for purposes set forth in the Agreements.

C. DESCRIPTION OF TRANSFER

Data Exporter:

The data exporter is (i) the legal entity that has entered into a contract with Company for provision of Services and executed the Clauses as a data exporter and (ii) all affiliates of such entity established within the EEA, which have purchased services from Company.

Data importer:

The data importer is Company, which processes Personal Data upon the instruction of the data exporter in accordance with the terms of the agreement between the data exporter and Company.

Data Subjects:

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

The data exporter may submit Personal Data to Company, the extent of which 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:

1. Prospective customers, customers, suppliers, authorized agents, minors, subscribers, and vendors of the data exporter (who are natural persons);
2. Employees or contact persons of the data exporter's prospective customers, customers, subcontractors, business partners, and vendors (who are natural persons);
3. Natural persons authorized by the data exporter to use the services provided by Company to the data exporter.

Categories of data:

The personal data transferred concern the following categories of data:

The data exporter may submit Personal Data to Company, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to, the following categories of Personal Data:

1. Names, titles, position, employer, contact information (email, phone, fax, physical address etc.), identification data, professional life data, personal life data, connection data, or localization data (including IP addresses).

Special categories of data (if appropriate):

The parties do not anticipate the transfer of special categories of data.

Processing operations

The objective of the processing of Personal Data by Company is to provide the Service, pursuant to the Agreements. The personal data transferred will be subject to the following basic processing activities:

1. The duration of the processing will be: until the earliest of (i) expiry/termination of the Agreements, or (ii) the date upon which processing is no longer necessary for the purpose of either party performing its obligations under the Agreements (to the extent possible).

2. The purpose(s) of the processing is/are: as necessary for the provision of the Service pursuant to the Agreements.

3. The types of Personal Data may include: names, titles, position, employer, contact information (email, phone, fax, physical address etc.), identification data, professional life data, personal life data, connection data, or localization data (including IP addresses).

4. Personal Data may concern the following data subjects:

    - Prospective customer, customers, vendors of Customer (who are natural persons), suppliers, authorized agents, and subscribers;

    - Employees or contact persons of Customer's prospective customers and Customer's current customers, subcontractors, business partners, and vendors (who are naturalpersons); and/or

    - Natural persons authorized by Customer to operate on their behalf.

D. COMPETENT SUPERVISORY AUTHORITY

The EU Member State where data exporter maintains its main place of business in the EU.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Data importer/sub-processor has implemented and shall maintain a security program in accordance with industry standards and Global Data Protection Laws. More specifically, data importer/sub-processor's security program shall include:

Access Control of Processing Areas

Data importer/sub-processor implements suitable measures in order to prevent unauthorized persons from gaining access to the data processing equipment (namely telephones, database and application servers and related (hardware) where the personal data are processed or used, including:

- Establishing security areas;
- Protection and restriction of access paths;
- establishing access authorizations for employees and third parties, including the respective documentation;
- all access to the data center and/or operation center where personal data are hosted is logged, monitored, and tracked; and
- the data center and/or operation center where personal data are hosted is secured by a security alarm system, and other appropriate security measures.

Access Control to Data Processing Systems

Data importer/sub-processor implements suitable measures to prevent their data processing systems from being used by unauthorized persons, including:

- use of adequate encryption technologies;
- identification of the terminal and/or the terminal user to the data importer/sub-processor and processing systems;
- automatic temporary lock-out of user terminal if left idle, identification and password required to reopen;
- automatic temporary lock-out of the user ID when several erroneous passwords are entered, log file of events,
- monitoring of break-in-attempts (alerts); and
- all access to data content is logged, monitored, and tracked.

Access Control to Use Specific Areas of Data Processing Systems

Data importer/sub-processor commits that the persons entitled to use their data processing system are only able to access the data within the scope and to the extent covered by their respective access permission (authorization) and that personal data cannot be read, copied or modified or removed without authorization. This shall be accomplished by various measures including:

- employee policies and training in respect of each employee's access rights to the personal data;
- allocation of individual terminals and /or terminal user, and identification characteristics exclusive to specific functions;
- monitoring capability in respect of individuals who delete, add or modify the personal data;

- release of data only to authorized persons, including allocation of differentiated access rights and roles;
- use of adequate encryption technologies; and
- control of files, controlled and documented destruction of data.

Availability Control

Data importer/sub-processor implements suitable measures to ensure that personal data are protected from accidental destruction or loss, including:

- infrastructure redundancy; and
- backup is stored at an alternative site and available for restore in case of failure of the primary system.

Transmission Control

Data importer/sub-processor implements suitable measures to prevent the personal data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media. This is accomplished by various measures including:

- use of adequate firewall, VPN and encryption technologies to protect the gateways and pipelines through which the data travels;
- certain highly confidential Personal data (e.g., personally identifiable information such as National ID numbers, credit or debit card numbers) is also encrypted within the system; and
- providing user alert upon incomplete transfer of data (end to end check); and
- as far as possible, all data transmissions are logged, monitored and tracked.

Input Control

Data importer/sub-processor implements suitable input control measures, including:

- an authorization policy for the input, reading, alteration and deletion of data;
- authentication of the authorized personnel;
- protective measures for the data input into memory, as well as for the reading, alteration and deletion of stored data;
- utilization of unique authentication credentials or codes (passwords);
- providing that entries to data processing facilities (the rooms housing the computer hardware and related equipment) are kept locked;
- automatic log-off of user ID's that have not been used for a substantial period of time;
- proof established within data importer/sub-processor's organization of the input authorization; and
- electronic recording of entries.

Separation of Processing for Different Purposes

Data importer/sub-processor implements suitable measures to ensure that data collected for different purposes can be processed separately, including:

- access to data is separated through application security for the appropriate users;

- modules within the data importer/sub-processor's data base separate which data is used for which purpose, i.e. by functionality and function;
- at the database level, data is stored in different normalized tables, separated per module, per Controller Customer or function they support; and
- interfaces, batch processes and reports are designed for only specific purposes and functions, so data
- collected for specific purposes is processed separately.

Documentation

Data importer/sub-processor will keep documentation of technical and organizational measures in case of audits and for the conservation of evidence. Data importer/sub-processor shall take reasonable steps to ensure that persons employed by it, and other persons at the place of work concerned, are aware of and comply with the technical and organizational measures set forth in this Appendix Annex II.

Monitoring

Data importer/sub-processor shall implement suitable measures to monitor access restrictions to data importer/sub-processor's system administrators and to ensure that they act in accordance with instructions received. This is accomplished by various measures including:

- individual appointment of system administrators;
- adoption of suitable measures to register system administrators' access logs to the infrastructure and keep them secure, accurate and unmodified for at least six months;
- yearly audits of system administrators' activity to assess compliance with assigned tasks, the instructions received by the data importer/sub-processor and applicable laws;
- keeping an updated list with system administrators' identification details (e.g. name, surname, function or organizational area) and tasks assigned and providing it promptly to data exporter uponrequest.

ANNEX III

LIST OF SUB-PROCESSORS

The controller has authorized the use of the following sub-processors: https://monetate.com/sub-processor-statement/