DATA PROCESSING ADDENDUM

Monetate Services, Including Forte Product

On June 13, 2025, SiteSpect, Inc. was fully acquired by Monetate Intermediate, LLC, operating as Monetate, Inc.. This Data Processing Addendum ("DPA") forms part of the Agreement between Customer and Monetate, Inc.

This DPA consists of:

- **Exhibit A** – Monetate Data Processing Addendum
- **Exhibit B** – SiteSpect Information Security & Data Protection Addendum, applicable to services now provided under the Forte product name.

For clarity:

- All references to "Company" in Exhibit A mean Monetate, Inc.
- All references to "SiteSpect, Inc." or "SiteSpect" in Exhibit B mean Monetate, Inc., acting through its Forte product line.

Application of Exhibits:

- **Exhibit A** governs the Services provided under the Monetate platform.
- **Exhibit B** governs the Services provided under the Forte platform.
- If both apply to the same Service, the more specific provision for that Service controls.

Except as expressly stated above, each Exhibit remains unchanged and in full force and effect.

Execution of the Agreement constitutes execution of both Exhibits.

Exhibit A: Monetate

Data Processing Addendum

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**" and together 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. **"EEA Standard Contractual Clauses"** means Module 2 of the Standard Contractual Clauses for the transfer of Personal Data from a data exporter acting as a Controller to a data importer acting as a Processor, approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021. Where any of the relevant clauses provide for an optional provision or require additional information, the Parties' choices with respect to such optional provisions and the additional information required are set out in Table A of the Appendix to this DPA;
      ii. "**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.
      v. "**UK Addendum**" means the international data transfer addendum to the European Commission's standard contractual clauses for international data transfers (including the Mandatory Clauses, Part 2) issued by the Information Commissioner's Office in accordance with s119A(1) of the Data Protection Act 2018 and which came into force on 21 March 2021;
      vi. "**UK Standard Contractual Clauses**" means the UK Addendum and the EEA Standard Contractual Clauses which are incorporated into this DPA and supplemented by the Tables set out in the Appendix to this DPA;
      vii. "**UK GDPR**" has the meaning set out in the UK Data Protection Act 2018;
      viii. 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**");
      vii. 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;
      viii. 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;
      ix. 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'.

b. 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.

Section 1: EEA 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.

Section 2: UK ADDENDUM

Table 1: Parties

Start date	The date of this DPA	
The Parties	Exporter (who sends the UK Restricted Transfer)	Importer (who receives the UK Restricted Transfer)
Parties' details	Refer to Annex I of this Appendix for details.	Refer to Annex I of this Appendix for details.
Key Contact	Refer to Annex I of this Appendix for details.	Refer to Annex I of this Appendix for details.
Signature	Not applicable	Not applicable

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	The Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:					
Module	**Module in operation**	**Clause 7 (Docking Clause)**	**Clause 11 (Option)**	**Clause 9a (Prior Authorization or General Authorization)**	**Clause 9a (Time period)**	**Is personal data received from the Importer combined with personal data collected by the Exporter?**
2 Controller to Processor	2	The parties agree that Clause 7 shall not apply.	The optional clause under Clause 11(a) shall not apply.	Option 2: General Written Authorization	The parties specify the time period as 60 days.	N/A

Table 3: Appendix Information

"Appendix Information" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: Refer to Annex I of this Appendix for details.
Annex 1B: Description of Transfer: Refer to Annex I of this Appendix for details.
Annex II: Technical and organizational measures including technical and organizational measures to ensure the security of the data:
Annex III: List of Sub Processors (Modules 2 and 3 only): Refer to Annex III of this Appendix for details.

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☐ Importer ☐ Exporter ☒ neither Party

ANNEX I

A. LIST OF PARTIES

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: Chief Information Officer, infosec@monetate.com

Activities relevant to the data transferred under these Clauses: Data Hosting & Processing in the performance of eCommerce Personalization Services pursuant to the Agreement.

B. 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. Data exporter's employees & contractors
2. Data exporter's customers

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. IP addresses
2. Anonymous Cookie Identifiers
3. Personal Data provided by data exporter for use with Monetate (e.g., a frequent buyer ID)
4. Interaction data from a website, or application (Clickstream Data)

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: as needed 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: Data Hosting & Processing in the performance of eCommerce Personalization Services pursuant to the Agreement.
3. The types of Personal Data may include: IP Addresses, Anonymous Cookie Identifiers, Personal Data provided by Company for use with Monetate (e.g., a frequent buyer ID), and/or Interaction data from a website, or application (Clickstream Data)
4. Personal Data may concern the following data subjects:
    - Exporting company employees & contractors
    - Exporting company customers

C. COMPETENT SUPERVISORY AUTHORITY
The EU Member State where data exporter maintains their 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 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) will also be 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 database 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 upon request.

ANNEX III

LIST OF SUB-PROCESSORS

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

Monetate's sub-processors as defined by GDPR are included in the table below:

Sub Processor	Location	Purpose
AWS	USA	Infrastructure as a Service (IaaS) for Monetate's apps and services.

Exhibit B:

Information Security & Data Protection Addendum for Platform: FORTE

1. Introduction

This Addendum governs the manner in which Monetate shall process Customer Personal Data (as defined below) and only applies to the extent Monetate Processes such Customer Personal Data. Except for the changes made by this Addendum, the Agreement remains unchanged and in full force and effect. In the event of a conflict between this Addendum and any other portion of the Agreement, the provision of this Addendum shall control. The parties agree that this Addendum shall replace any existing data processing addendum the parties may have previously entered into in connection with the Services.
Capitalized terms have the meaning given to them in the Agreement, unless otherwise defined below.

2. Definitions

For the purposes of this Addendum, the following terms and those defined within the body of this Addendum apply:

a) "**Applicable Data Protection Law(s)**" means the relevant data protection and data privacy laws, rules, and regulations to which the Customer Personal Data are subject. Applicable Data Protections Law(s) shall include, but not be limited to, the California Consumer Privacy Act of 2018 ("**CCPA**"), the General Data Protection Regulation (EU 2016/679) (the "**GDPR**"), the Swiss Federal Data Protection Act, the Australian *Privacy Act of 1988* (Cth) as amended, and without limitation the *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth) and the United Kingdom Data Protection Act of 2018 or any successor law (the "**UK GDPR**"). "**Controller**" means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the Processing of personal data.

b) "**Customer Personal Data**" means any Personal Data that Customer provides to Monetate and which is necessary for Monetate to provide products and services under the Agreement.

c) "**Personal Data**" shall have the meaning assigned to the terms "personal data" or "personal information" under Applicable Data Protection Law(s).

d) "**Process**," "**Processes**," "**Processing**," "**Processed**" means any operation or set of operations which is performed on data or sets of 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.

e) **"Processor"** means any entity that processes Personal Data under the Controller's instructions.

f) "**Security Incident(s)**" means any accidental, unlawful, or unauthorized access, acquisition, use, modification, disclosure, loss, destruction of, or damage to Customer Personal Data or any other unauthorized Processing of Customer Personal Data.

g) "**Sensitive Personal Data**" shall have the meaning assigned to the terms "sensitive data", "sensitive information", "special categories of personal data", or similar term under Applicable Data Protection Law(s) and, as required by Applicable Data Protection Law(s), shall include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

h) "**EU Standard Contractual Clauses**" means the European Commission Standard Contractual Clauses, which are hereby incorporated by reference and attached hereto as Schedule 3, together with and successors or amendments to such clauses or such other applicable contractual terms adopted and approved under Applicable Data Protection Laws.

i) "**Sub-Processor(s)**" means Monetate authorized contractors, agents, vendors, and third-party service providers that Process Customer Personal Data.

j) "**UK Standard Contractual Clauses**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, completed as set forth in this Addendum.

3. Data Handling and Access

a) Role of the Parties. As between Monetate and Customer, Customer is the Controller of Customer Personal Data, and Monetate shall Process Customer Personal Data only as a Processor acting on behalf of Customer, as such terms are defined in the GDPR. In cases where Customer is a Processor, then Monetate shall Process Customer Personal Data only as a Sub-processor acting on behalf of Customer. For purposes of the CCPA, Customer is a "business" and Monetate is a "service provider," as such terms are defined in the CCPA.

b) General Compliance by Monetate. Customer Personal Data shall be Processed by Monetate solely in compliance with the terms of this Addendum and all Applicable Data Protection Law(s), including the GDPR.

c) General Compliance by Customer. Customer agrees that (i) it shall comply with its obligations as Controller or Processor under Applicable Data Protection Law(s) in respect of its Processing of Customer Personal Data and any Processing instructions it issues to Monetate and (ii) it has provided notice and obtained (or shall obtain) all consents and rights necessary under Applicable Data Protection Law(s) for Monetate to Process Customer Personal Data and provide the products and services pursuant to the Agreement and this Addendum.

d) Monetate and Sub-Processor Compliance. Monetate agrees to (i) enter into a written agreement with Sub-Processors regarding such Sub-Processors' Processing of Customer Personal Data that imposes on such Third Parties data protection and security requirements for Customer Personal Data that are compliant with Applicable Data Protection Law(s); and (ii) remain responsible to Customer for Monetate's Third Parties' (and their sub-processors if applicable) failure to perform their obligations with respect to the Processing of Customer Personal Data.

e) Authorization to Use Sub-Processors. Monetate does not currently leverage sub-processes. In the event Monetate decides to use them in the future for the purpose of business continuity and fulfilling Customer obligations, the Customer authorizes Monetate to use Monetate's Sub-Processors which will be described on Monetate Subprocessors. Monetate shall inform the Customer of any such Sub-Processor and any intended changes concerning the addition or replacement of Third Parties, thereby giving the Customer the opportunity to object to such changes. If Monetate engages new Third Parties, Monetate will give Customer notice at least 30 calendar days in advance of providing that Sub-Processor with access to Personal Data. If Customer does not object to a new Sub-Processor with such time period, Customer will be deemed to have authorized Monetate's use of the new Sub-Processor and to have waived its right to object. In the event that Customer timely and reasonably objects to Monetate's engagement of a Sub-Processor, the parties shall work together in good faith to resolve such objection. In the event that the objection cannot be overcome after good faith efforts, and if Monetate intends to use the Sub-Processor to whom Customer has objected, Customer shall have the right to terminate the Agreement without liability or penalty as Customer's sole and exclusive remedy. Where Monetate engages a Sub-Processor for carrying out specific processing activities on behalf of Customer, the same data protection obligations as set out in this Addendum shall be imposed on that Sub-Processor by way of a written agreement. Where that Sub-Processor fails to fulfill its data protection obligations, Monetate shall remain fully liable to Customer for the performance of its Sub-Processor obligations. Without limiting the foregoing, Monetate will develop and use reasonable steps to select and retain Third Parties that assist Monetate in performing its obligations under the Agreement that are capable of maintaining security practices consistent with this Addendum and requiring such Third Parties to agree by written contract to comply with terms substantially similar to those contained in this Addendum.

f) Following Instructions. Monetate shall Process Customer Personal Data only in accordance with the written instructions of Customer or as specifically authorized by this Addendum, the Agreement, or any applicable Statement of Work. Monetate will, unless legally prohibited from doing so, inform Customer in writing if it reasonably believes that there is a conflict between Customer's instructions and Applicable Data Protection Laws, applicable laws or otherwise seeks to Process Customer Personal Data in a manner that is inconsistent with Customer's instructions.

g) Confidentiality. Any person authorized to Process Customer Personal Data shall be under an appropriate statutory, professional, or contractual obligation of confidentiality with respect to such.

h) Personal Data Inquiries and Requests. Monetate agrees to comply with all reasonable instructions from Customer related to any requests from individuals exercising their rights in Personal Data granted to them under Applicable Data Protection Law(s) ("**Privacy Request**"). At Customer's request and without undue delay, Monetate agrees to assist Customer in answering or complying with any Privacy Request.

i) Processing of Sensitive Personal Data. Customer agrees that it shall not use the Services to Process Sensitive Personal Data without Monetate's explicit and prior written consent.

j) Sale of Customer Personal Data Prohibited. Monetate is a service provider to Customer and shall not sell Customer Personal Data as the term "service provider" and "sell" are defined by the CCPA.

4. Cross Border Data Transfer

a) Cross-Border Data Transfer Mechanism. Customer will operate as a data Controller and Monetate will operate as a data Processor, Processing Customer Personal Data only as necessary for the limited and specified purposes identified in the Agreement, and in accordance with at least the same level of protection as is required under the Applicable Data Protection Law(s). The Parties acknowledge and agree that to the extent Monetate Processes any Customer Personal Data subject to Applicable Data Protection Laws under the Agreement, any related Orders or Exhibits, any such transfer will be subject to the appropriate Standard Contractual Clauses, as applicable. Customer authorizes Monetate and its Sub-Processors to make international transfers of Customer Personal Data in accordance with this Addendum so long as Applicable Data Protection Laws for such transfers are respected.

b) Cross-Border Data Transfers Under EU Standard Contractual Clauses. With respect to Customer Personal Data transferred from the European Economic Area ("EEA"), the EU Standard Contractual Clauses incorporated herein shall apply, form part of this Addendum, and take precedence over this Addendum. They will be deemed completed as follows:

i) Where Customer is a data exporter and controller, and Monetate is a data importer and processor, Module 2 shall apply. When Customer is a data exporter and processor, and Monetate is a data importer and sub-processor, Module 3 shall apply. References to Modules 1 and 4 in the EU Standard Contractual Clauses shall not apply and language referencing these modules shall not be treated as part of this Addendum.

ii) Clause 7, the "Docking Clause (Optional)", will be deemed incorporated.

iii) Under Clause 9 (Use of sub-processors), the Parties select Option 2 (general written authorization), and the time period for prior notice of addition or replacement of Sub-Processors will be set forth in Section 3(e) of the Addendum.

iv) Under Clause 11 (Redress), the optional requirement that data subjects be permitted to lodge a complaint with an independent dispute resolution body does not apply.

v) Under Clause 17 (Governing law), the Parties choose Option 1 (the law of an EU Member State that allows for third-party beneficiary rights). The Parties select the law of Ireland.

vi) Under Clause 18 (Choice of forum and jurisdiction), the Parties select the courts of Ireland.

vii) Annexes I-II are set forth below.

viii) By entering into this Addendum, the Parties are deemed to be signing the EU Standard Contractual Clauses and its applicable Annexes.

c) Cross-Border Transfers From Switzerland. With respect to Personal Data transferred from Switzerland for which Swiss law (and not the law in any EEA jurisdiction) governs the international nature of the transfer, references to the GDPR in Clause 4 of the EU Standard Contractual Clauses are, to the extent legally required, amended to refer to the Swiss Federal Data Protection Act or its successor instead, and the concept of supervisory authority shall include the Swiss Federal Data Protection and Information Commissioner.

d) Cross-Border Transfers Under UK Standard Contractual Clauses. With respect to Personal Data transferred from the United Kingdom for which United Kingdom law (and not the law in any EEA jurisdiction) governs the international nature of the transfer, the UK Standard Contractual Clauses form part of this Addendum and take precedence over the rest of this Addendum as set forth in the UK Standard Contractual Clauses, unless the United Kingdom issues updates to the UK Standard Contractual Clauses that, upon notice from Customer, will control. Undefined capitalized terms used in this provision shall mean the definitions in the UK Standard Contractual Clauses. For purposes of the UK Standard Contractual Clauses, they shall be deemed completed as follows:

i) Table 1 of the UK Standard Contractual Clauses: (1) the Parties' details shall be the Parties and their Affiliates to the extent any of them is involved in such transfer, including those set forth in Schedule 3; (2) the Key Contact shall be the contacts set forth in Schedule 3.

ii) Table 2 of the UK Standard Contractual Clauses: The Approved EU Standard Contractual Clauses referenced in Table 12 shall be the EU Standard Contractual Clauses as executed by the Parties.

iii) Table 3 of the UK Standard Contractual Clauses: Annex 1A, 1B, and II shall be set forth in Schedule 3.

iv) Table 4 of the UK Standard Contractual Clauses: Monetate may end this Addendum as set out in Section 19 of the UK Standard Contractual Clauses.

v) By entering into this Addendum, the Parties are deemed to be signing the UK Standard Contractual Clauses and its applicable Tables and Appendix Information.

e) Cross-Border Transfers from Australia. With respect to Personal Data transferred from Australia for which Australian law governs the international nature of the transfer, references to the GDPR in Clause 4 of the EU Standard Contractual Clauses are, to the extent legally required, amended to refer to the Australian Data Protection Act or 1988 or its successor instead, and the concept of supervisory authority shall include the appropriate Australian data commission.

f) Statutory Revisions to the Applicable Data Protection Law(s). In the event that the Applicable Data Protection Law(s) require the use of revised standard contractual clauses applicable to this Addendum, such revised standard contractual clauses shall automatically be deemed to replace the current Applicable Data Protection Law(s), as applicable, without the need for any further action, unless Monetate otherwise informs Customer.

g) Prior Consultation. Monetate agrees to provide reasonable assistance at Customer's expense to Customer where, in Customer's reasonable judgment, the type of Processing performed by Monetate is likely to result in a high risk to the rights and freedoms of natural persons (e.g., systematic and extensive profiling, Processing sensitive Personal Data on a large scale and systematic monitoring on a large scale, or where the Processing uses new technologies) and thus requires a data protection impact assessment and/or prior consultation with the relevant data protection authorities.

h) Demonstrable Compliance. Monetate agrees to keep records of its Processing in compliance with Applicable Data Protection Law(s) and provide such records to Customer upon reasonable request to assist Customer with complying with supervisory authorities' requests.

i) Notice of Non-Compliance. Monetate shall promptly notify Customer's Designated POC (as defined below) if it can no longer meet its obligations under this Section 4. Monetate shall have the opportunity to cure within a commercially reasonable timeframe (not less than thirty (30) days). If Monetate is unable to cure, Customer shall have the right to terminate the Agreement without liability or penalty as Customer's sole and exclusive remedy.

5. California Privacy Rights Act (CPRA) Compliance

For any personal information subject to the CPRA Customer makes available to Monetate that is not subject to this Addendum, the following provisions apply: (1) Monetate may process that personal information solely to improve and provide its products and services; (2) Monetate shall comply with applicable obligations under the CPRA applicable to such personal information, including any privacy protections afforded by the CPRA; (3) Customer may take reasonable and appropriate steps to help ensure that Monetate uses such personal information in a manner consistent with Customer's obligations under the CPRA; (4) Monetate shall notify Customer if it makes a determination it can no longer meet its obligations under the CPRA for such personal information; and (5) Customer may, with notice, take reasonable and appropriate steps to stop and remediate unauthorized use of such personal information. Monetate shall have the opportunity to cure within a commercially reasonable timeframe (not less than thirty (30) days). If Monetate is unable to cure, shall have the right to terminate the Agreement without liability or penalty as Customer's sole and exclusive remedy.

6. Information Security Program

Monetate agrees to implement appropriate technical and organizational measures designed to protect Customer Personal Data as required by Applicable Data Protection Law(s) (the "**Information Security Program**"). Further, Monetate agrees to regularly test, assess, and evaluate the effectiveness of its Information Security Program to ensure the security of the Processing.

7. Audits

Upon request from Customer, Monetate agrees to reasonably cooperate with Customer for the purpose of verifying Monetate's compliance with Applicable Data Protection Law(s). In such case, any audit conducted under this Addendum shall consist of examination of the most recent reports, certificates and/or extracts prepared by an independent auditor bound by confidentiality provisions no less protective than those set out in the Agreement. In the event that provision of the same is not sufficient under Applicable Data Protection Law(s), Customer may at its own expense conduct a more extensive audit which will be (a) limited in scope to matters specific to Customer and agreed in advance with Monetate, (b) carried out during local business hours and upon reasonable notice which shall not be less than thirty (30) days unless a Security Incident has arisen in which case an audit may be performed promptly upon notice; (c) conducted in a way which does not interfere with Monetate's day-to-day business; and (d) undertaken no more than once in any 12 month period except where required by a competent supervisory authority or where an audit is required due to a Security Incident. Customer's representatives performing an audit shall protect the confidentiality of all information obtained through such audits in accordance with the Agreement, may be required to execute an enhanced mutually agreeable nondisclosure agreement and shall abide by Monetate's security policies while on Monetate's premises. Upon completion of an audit, Customer will promptly furnish to Monetate any written audit report or, if no written report is prepared, to promptly notify Monetate of any non-compliance discovered during the course of the audit. All audit reports, and information and records observed or otherwise collected or generated in the course of the audit, are Confidential Information of Monetate under the terms of the Agreement. If no non-compliance issues are identified, Customer will reimburse Monetate for its time

expended in connection with an audit at Monetate's then-current professional service rates, which shall be reasonable taking into account the time and effort required by Monetate.

If any non-compliance issues are identified, upon notice, Monetate shall have the opportunity to cure within a commercially reasonable timeframe (not less than thirty (30) days). If Monetate is unable to cure, Customer shall have the right to terminate the Agreement without liability or penalty as Customer's sole and exclusive remedy.

8. Deletion of Data

Upon request by Customer any time after termination of the provision of the Services, Monetate shall within a reasonable destruction period, delete all Customer Personal Data. Notwithstanding the foregoing, Monetate may retain Customer Personal Data to the extent that it is required or authorized to do so under applicable law and/or regulation or this Agreement or to the extent it already had this data or if it is archived on Monetate's back-up systems where it is not regularly accessed or used and deleted in accordance with Monetate's separate retention timeframes for archival media, in which case Monetate will securely protect such data from any further processing, except to the extent required by applicable law and/or regulation.

9. Security Incident

a) Security Incident Procedure. Monetate will deploy and follow policies and procedures to detect, respond to, and otherwise address Security Incidents including using reasonable commercial efforts to (i) identify and respond to Security Incidents, mitigate harmful effects of Security Incidents, document Security Incidents and their outcomes, and (ii) restore the availability or access to Customer Personal Data in a timely manner.

b) Notice. Monetate agrees to provide prompt written notice within seventy-two (72) hours or such other time frame required under Applicable Data Protection Law(s) to Customer's Designated POC if it confirms that a Security Incident has taken place. Such notice will include all available details required under Applicable Data Protection Law(s) for Customer to comply with its own notification obligations to regulatory authorities or individuals affected by the Security Incident.

c) No Assessment of Customer Personal Data. Monetate will not assess the contents of Customer Personal Data in order to identify information subject to any specific legal requirements.

d) No Acknowledgment of Fault. Monetate's notification of or response to a Security Incident under this Section 9 shall not be construed as an acknowledgment by Monetate of any fault or liability with respect to the Security Incident.

10. Contact Information

- Monetate and the Customer agree to designate a point of contact for urgent security issues (a "**Designated POC**"). The Designated POC for both parties are:

Monetate Designated POC	privacy@monetate.com
Customer Designated POC email	

11. LIMITATION OF LIABILITY

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

Schedule 1 to the Addendum

DESCRIPTION OF PROCESSING

1.1 Subject Matter of Processing	Data Hosting & Processing in the performance of eCommerce Personalization Services pursuant to the Agreement.
1.2 Duration of Processing	The Processing will continue as needed 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.
1.3 Categories of Data Subjects	Includes the following: - Data exporter's employees & contractors - Data exporter's customers
1.4 Nature and Purpose of Processing	Data Hosting & Processing in the performance of eCommerce Personalization Services pursuant to the Agreement.
1.5 Types of Personal Information	Includes: - IP addresses - Anonymous Cookie Identifiers - Personal Data provided by data exporter for use with Monetate (e.g., a frequent buyer ID) - Interaction data from a website, or application (Clickstream Data)
1.6 Sensitive Personal Data Transferred	N/A - Data exporter will not submit sensitive personal data
1.7 Frequency of Transfer of Data	Continuous
1.8 Period for which Personal Data will be retained	The period for which the Personal Data will be retained is more fully described in the Agreement, Addendum, and accompanying applicable Orders.
1.9 Obligations and Rights of Customer	The obligations and rights of Customer as a controller are set out in the Agreement and this Addendum.

Schedule 2 to the Addendum

TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

Monetate reserves the right to update its security program from time to time; provided, however, any update will not materially reduce the overall protections set forth in this schedule.

1. **Compliance**
   Monetate will comply with all applicable state and federal data security regulations and shall abide by all required security controls as stated herein, based upon the nature of the Services provided, the data involved and/or the location where such Services are rendered.
2. **Security Certification**
   Monetate holds the following security-related certifications from independent third-party auditors: **PCI 4.0**.
3. **Information Security Program**
   Monetate maintains a formal information security program that is supported by written information security policies, approved by management, published, and communicated to staff. The information security program is based on a recognized security framework designed to protect the confidentiality and integrity of data, and appropriate to the nature, scope, context and purposes of processing and the risks involved in the processing for the data subjects.
4. **Organization of Information Security**
   Monetate will delegate an accountable party for information security intended to provide executive-level oversight and approval for security and compliance initiatives and planning through various actions. The delegate(s) will be required to review, recommend edits or changes, and accept internal information security policy and processes.
5. **Access Control**
   Monetate shall have in place formal processes and procedures to support the secure creation, amendment, and deletion of user accounts of personnel, consultants, and subcontractors, as well as systems and software, which contain, or otherwise have access to Customer Personal Data. Furthermore, Monetate takes it upon itself to carry out the following measures:
   - Monitor redundant and inactive accounts
   - Ensure that all user accounts privileges are allocated on “a-need-to-use-basis”
   - Ensure that access control mechanisms based on reasonably secure passwords are enforced
   - Ensure, where possible, Monetate’s internal system access authentication is using two-factor authentication
6. **Data Center Architecture and Security**
   Data centers must be designed and managed in compliance with regulations, standards, and best practices, such as PCI, SOC 2, ISO 27001, CSA, and FIPS 140-2. The data center must implement physical and environmental controls designed to secure the facility and protect equipment from damage. Monetate must exercise regular oversight of the data center
   supplier’s ability to meet these controls by reviewing current independent third-party reports of compliance and/or industry standard certifications.
7. **Network Architecture and Security**
   Monetate networks must span multiple availability zones that are physically separated and isolated, connected through low-latency, high-throughput, and highly redundant networking. Networks or applications that contain Controller data must be separated from public networks by a firewall to prevent unauthorized access from the public network.
8. **Availability and Continuity**
   a. Service Availability. Monetate employs service clustering and network redundancies to eliminate single points of failure. Monetate maintains a publicly available system-status webpage, which includes system availability details, scheduled maintenance, and service incident history, found at: Forte Status
   b. Backups. Customer data is backed up daily using policy-based scheduling.
   c. Disaster Recovery and Business Continuity. Monetate has a disaster recovery plan that outlines roles and responsibilities for key personnel involved in business continuity, our plan to activate and respond to a disaster, target timelines, and testing requirements.

9. **Information Security Incident Management**

   Monetate will have a documented Incident Response Plan that is approved by management. The key components must include:

   - Classify the severity of the incident using an initial analysis
   - Limit the immediate impact of the incident
   - Take corrective action to contain the impact
   - Investigate and collect evidence
   - Inform the relevant authorities (where applicable)
   - Inform impacted customers

10. **Software Development**

    Monetate shall have appropriate governance processes in place to supervise and monitor software development (e.g., implement an SDLC) and ensure security requirements are included in the requirements for new information systems or enhancements to existing information systems.

11. **Security Testing**

    At least quarterly vulnerability scanning will be performed against all public-facing applications. At least annually, Monetate will engage a third-party security expert to perform a penetration test. Critical and high-risk vulnerabilities identified during the scanning will be promptly remediated.

12. **Personnel Security**

    Monetate performs pre-employment background checks of all personnel with exposure to Controller data, in accordance with applicable local laws. These personnel must receive security training upon hire and at least annually thereafter.
    Personnel must be bound by written confidentiality agreements.

13. **Encryption Controls**

    Monetate implements reasonable measures to ensure data cannot be read, copied, modified, or removed without authorization during electronic transmission or transport. Data is encrypted in transit over public networks via industry standard HTTPS/TLS (TLS 1.2 or higher).

    Data at rest is encrypted in storage in databases, storage buckets and backup files using AES-256-bit encryption.

Additional Technical and Organizational Security Measures

a. **Measures of encryption of personal data.** Monetate has taken the following measures in the Subscription Services designed to convert clearly legible Transferred Data into ciphertext by means of a cryptographic process:
Transferred Data transmitted via TLS can be encrypted with TLS 1.2 or stronger protocol.

b. **Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services.**

i. Monetate has taken the following measures designed to ensure that Transferred Data is accessed only by authorized personnel and prevents the intrusion by unauthorized persons into Monetate's systems and applications used for the processing of Transferred Data:

- Two-factor or two-step authentication is required.
- All Transferred Data is subject to the encryption measures identified above.
- Development and test environments are logically separated from production environments by design.
- Monetate maintains administrative controls which govern access under the principle of least privilege.
- Privileged access is not granted by default.

ii. Monetate has taken the following measures designed to ensure that Transferred Data cannot be read, copied, modified, or removed without authorization during electronic transmission or transport, and that it is possible to check and establish whether and by whom Transferred Data has been input into data processing systems, modified, or removed:

- All Transferred Data is subject to the encryption measures identified above.
- Monetate must maintain tools in place for audit trails, event notifications, and logs for application and cloud systems.

iii. Monetate has taken the following measures designed to ensure that Transferred Data is protected from accidental destruction or loss due to internal or external influences, and ensure the ability to withstand attacks or to quickly restore systems to working order after an attack):

- Alerting is set up for specified thresholds and a team with experienced personnel monitors system availability and overall health.
- High availability infrastructure is used as appropriate to increase availability.
- Monetate ensures routine backups are taken of Transferred Data.

c. **Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.** Monetate has taken the following measures designed to ensure the possibility to quickly restore Monetate system or Transferred Data in the event of a physical or technical incident:

- Monetate maintains an Incident Response Plan (IRP) that it updates from time to time as needed. The IRP includes procedures for handling and reporting incidents including detection and reaction to possible Security Incidents.
- Capacity management measures are taken to monitor resource consumption of systems as well as plan future resource requirements.

d. **Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing.** Monetate has taken the following measures designed to ensure the regular review and assessment of security measures:

- Monetate conducts regular penetration testing and vulnerability scanning of the Services.
- Monetate must maintain a channel to allow security researchers to report identified security vulnerabilities in the Services.

e. **Measures for user identification and authorization**. Monetate has taken the following measures designed to validate and authenticate users:

- Monetate maintains administrative controls which govern access under the principle of least privilege.
- Access to non-public data or functionality requires authentication prior to access.
- Two-factor or two-step authentication is required.

f. **Measures for the protection of data during transmission**. Monetate has taken the following measures designed to ensure transmission control to ensure that Transferred Data cannot be read, copied, changed, or deleted without authorization during its transfer and that Transferred Data can be monitored and determined to which recipients a transfer of Transferred Data is intended:

- Transferred Data is encrypted in transit as described above.

g. **Measures for the protection of data during storage**. Monetate has taken the following control measures designed to ensure that Transferred Data cannot be read, copied, changed, or deleted without authorization while stored on data media:
    - Transferred Data is encrypted at rest as described above.
    - Two-factor or two-step authentication is required.

h. **Measures for ensuring physical security of locations at which personal data are processed**. Monetate has taken the measures identified above regarding the physical security of Transferred Data.
    - Physical access within data processing facilities is controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means.

i. **Measures for ensuring events logging**. Monetate has taken the following measures designed to ensure the verifiability of event log files:
    - Monetate records application and system logs to collect information, exception errors, information security events, and privileged access events.
    - Monetate maintains administrative controls which govern access under the principle of least privilege.

j. **Measures for ensuring system configuration, including default configuration**. Monetate has taken the following measures designed to ensure that all in-scope systems and devices are compliant with baseline configuration settings:
    - Monetate ensures that access to information and application system functions is restricted to authorized personnel only.

k. **Measures for internal IT and IT security governance and management**. Monetate has a dedicated and identified person to oversee its information security and compliance program. Monetate is annually audited by an independent third-party against an industry standard (e.g., PCI, SOC 2 Type II, ISO 27001, etc.).

l. **Measures for certification/assurance of processes and products**. Monetate is annually audited by an independent third-party against an industry standard (e.g., PCI, SOC 2 Type II, ISO 27001, etc.).

m. **Measures for ensuring data minimization**. Monetate has taken the following measures designed to reduce the amount of data collected by the Service:
    - Monetate will implement capabilities for the Controller to customize which data is collected by the Service, where practical.

n. **Measures for ensuring data quality**. Monetate has taken the following measures designed to ensure that the data flow creates and sustains good data quality:
    - Monetate has established processes for data subjects to exercise their data protection rights (right to amend and update information).
    - Monetate's documentation clearly states the types of data Controller are prohibited from transferring to Monetate.

o. **Measures for ensuring limited data retention**. Monetate has established processes designed to ensure that Transferred Data is deleted in accordance with the terms of the Agreement following the termination of the Agreement.

p. **Measures for ensuring accountability**. Monetate has an appointed Data Protection Officer (DPO) or another similar role who is responsible for overseeing Monetate's compliance with its legal and contractual privacy-related obligations throughout the data lifecycle.

q. **Measures for allowing data portability and ensuring erasure**. Monetate has established processes in relation to the exercise by users of their privacy rights (including without limitation, rights of data portability and erasure).