Data Processing Agreement (DPA)

This Data Processing Agreement including its Attachments ("***DPA***") is between Perseus Payments Inc. ("***Supplier***") and the entity that receives any Products from Supplier ("***Customer***") pursuant to a written or electronic agreement which governs the provision of those Products ("***Agreement***"), and shall apply to the extent that (i) Supplier Processes Personal Data on behalf of the Customer, and (ii) either the Agreement expressly incorporates this DPA by reference or the parties sign this DPA.

This DPA is supplemental to, and forms an integral part of, the Agreement and is effective upon the earlier of signature or its incorporation into the Agreement ("**Effective Date**"), which incorporation may be specified in the Agreement or an executed amendment to the Agreement. In case of any conflict or inconsistency between the terms of the Agreement and this DPA, this DPA shall take precedence over the terms of the Agreement to the extent of such conflict or inconsistency.

The term of this DPA shall follow the Term of the Agreement. Terms not otherwise defined herein shall have the meaning as set forth in the Agreement.

1. Definitions

"California Personal Information" means Personal Data that is subject to the CCPA.

"Canadian Privacy Laws" means the data protection and privacy laws applicable in Canada and/or its provinces, in each case as hereinafter amended, supersede, or replaced, including:

(i) The Personal Information Protection and Electronic Documents Act of 2000 ("***PIPEDA***");

(ii) In Quebec: the Act to Modernize Legislative Provisions As Regards the Protection of Personal Information, also known as Law 25 (formally known as Bill 64), and the Act Respecting the Protection of Personal Information in the Private Sector, CQLR P-39.1, which is amended thereby (collectively "***Law 25***");

(iii) In Alberta: the Personal Information Protection Act [of Alberta] ("***PIPA Alberta***"); and

(iv) In British Columbia: the Personal Information Protection Act [of British Columbia] ("***PIPA BC***").

"Consumer," "Business," "Sell" and ***"Service Provider"*** shall have the meanings given to them in the CCPA.

"*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.

"*Data Privacy Laws*" means all applicable legislation relating to data protection and privacy which applies to the respective party in the role of Processing Personal Data in question under the Agreement, including without limitation US Privacy Laws, and Canadian Privacy Laws; in each case to the extent applicable and as amended, repealed, consolidated or replaced from time to time.

"*Data Subject*" means the individual to whom Personal Data relates.

"*Instructions*" means the written, documented instructions issued by Customer to Supplier and directing the same to perform a specific or general action with regard to Personal Data.

"*Permitted Affiliates*" means any of Customer's Affiliates (as defined under the Agreement):

(i) That are permitted to use the Products pursuant to the Agreement, but have not signed their own separate agreement with Supplier;

(ii) For whom Supplier Processes Personal Data; and

(iii) That are subject to Data Privacy Laws.

"*Personal Data*" means any information provided by or collected on behalf of Customer relating to an identified or identifiable individual where such information is protected under applicable Data Privacy Laws as personal data, personal information, personally identifiable information, or any equivalent thereof.

"*Personal Data Breach*" means an event that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed by Supplier and/or its Sub-Processors in connection with the provision of the Products, subject to any limitations, exclusions, exceptions, or safe harbors provided for by applicable Data Privacy Laws. "Personal Data Breach" shall not include (a) any such events for which notification is not required pursuant to applicable Data Privacy Laws, or (b) unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems, except to the extent that any such unsuccessful attempts or activities must be disclosed pursuant to applicable Data Privacy Laws.

"*Processing*" means any operation or set of operations which is performed on Personal Data, encompassing the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction or erasure of Personal Data. The terms "Process", "Processes" and "Processed" will be construed accordingly.

"*Processor*" means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

"Products" means the goods and services provided by Supplier to Customer under the Agreement.

"*Sub-Processor*" means any third-party engaged by Supplier to carry out specific Processing activities in accordance with the Instructions and subject to further limitations set forth in this DPA.

"US Privacy Laws" means the applicable legislation of the United States of America that are in effect as of the Effective Date relating to data protection and privacy which applies to the respective party in the role of Processing Personal Data in question under the Agreement, in each case as hereinafter amended, superseded, or replaced, including the following:

(i) In **California**: the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act (the "**CCPA**");

(ii) In **Colorado**: the Colorado Privacy Act (the "**CoPA**");

(iii) In **Connecticut**: the Connecticut Personal Data Privacy and Online Monitoring Act (the "**CPDP**");

(iv) In **Delaware**: the Delaware Personal Data Privacy Act (the "**DPDPA**");

(v) In **Iowa**: the Iowa Consumer Data Protection Act (the "**ICDPA**");

(vi) In **Montana**: the Montana Consumer Data Privacy Act (the "**MCDPA**");

(vii) In **Nebraska**: the Nebraska Data Privacy Act (the "**NDPA**");

(viii) In **New Hampshire**: the New Hampshire Data Privacy Act (the "**NHDPA**");

(ix) In **New Jersey**: the New Jersey Data Privacy Act (the "**NJDPA**");

(x) In **Oregon**: the Oregon Consumer Privacy Act (the "**OCPA**");

(xi) In **Texas**: the Texas Data Privacy and Security Act (the "**TDPSA**");

(xii) In **Utah**: the Utah Consumer Privacy Act (the "**UCPA**"); and

(xiii) In **Virginia**: the Virginia Consumer Data Protection Act (the "**VCDPA**").

2. Roles of the Parties

a. Under the CCPA. To the extent that CCPA applies to the Processing activities under the Agreement, the parties acknowledge and agree that Supplier is a Service Provider and Customer is either a (i) Business or (ii) a Service Provider acting on behalf of a Business that is not a party to this DPA. Notwithstanding the foregoing, in the event that Attachment 1, Section A identifies any purposes for which Supplier Processes Personal Data as a 'third party' as that term is defined under the CCPA ("***CCPA Third Party***"), in which case Supplier is a CCPA Third Party.

b. Under US Privacy Laws, except the CCPA. To the extent that US Privacy Laws other than the CCPA apply to the Processing activities under the Agreement, the parties acknowledge and agree that Supplier is a Processor and Customer is either (i) a Controller, or (ii) a Processor acting on behalf of a Controller that is not a party to the Agreement or this DPA.

c. Under Canadian Privacy Laws. To the extent that Canadian Privacy Laws apply to the Processing activities under the Agreement, the parties acknowledge and agree that (i) Supplier Processes Personal Data on behalf of Customer and assumes the obligations under applicable Canadian Privacy Laws that apply to that role, and (ii) Customer, through its Instructions to Supplier, determines the purposes and means of the Processing of Personal Data and assumes the obligations under applicable Canadian Privacy Laws that apply that role.

3. Customer Responsibilities

a. Compliance with Laws. Customer shall be responsible for complying with all its obligations under applicable Data Privacy Laws and shall inform Supplier without undue delay if it is not able to comply with its responsibilities under this sub-section (a) or applicable Data Privacy Laws. In particular but without prejudice to the generality of the foregoing, Customer acknowledges and agrees that it shall be solely responsible for:

(i) the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data;

(ii) complying with all necessary transparency and lawfulness requirements under applicable Data Privacy Laws for the collection and use of the Personal Data, including obtaining any necessary consents and authorizations (particularly for use by Customer for marketing purposes);

(iii) ensuring it has the right to transfer, or provide access to, the Personal Data to Supplier for Processing in accordance with the terms of the Agreement (including this DPA);

(iv) ensuring that its Instructions to Supplier regarding the Processing of Personal Data comply with applicable laws, including Data Privacy Laws; and

(v) complying with all laws (including Data Privacy Laws) applicable to any content created, sent or managed through the Products, including those relating to obtaining consents (where required) to send communications, the content of the communications, and its communication deployment practices.

b. Instructions. The parties agree that the following constitutes Customer's complete and final Instructions to Supplier in relation to the Processing of Personal Data: (i) the terms of the Agreement and this DPA, including the Attachments hereto, (ii) direction from Customer through its use of the Products in accordance with the Agreement, and (iii) this general authorization by Customer which hereby permits Supplier to use Personal Data for any business operations incident to providing the Products to Customer. Additional instructions outside the scope of the Instructions must be agreed to according to the process for amending the Agreement or this DPA, where applicable.

c. Security. Customer is responsible for independently determining whether the data security provided for in the Products adequately meets its obligations under applicable Data Privacy Laws. Customer is also responsible for its secure use of the Products, including protecting account access to the Products and the security of Personal Data in transit to and from the Products (including the secure backup or encryption of any such Personal Data).

4. Supplier Obligations

a. Compliance with Instructions. Supplier shall only Process Personal Data for the purposes described in this DPA, including Attachment 1, or as otherwise agreed within the scope of Customer's lawful Instructions, except where and to the extent otherwise permitted by applicable law. Supplier is not responsible for compliance with any Data Privacy Laws applicable to Customer or Customer's industry that are not generally applicable to Supplier.

b. Conflict of Laws. If Supplier becomes aware that it can no longer meet its obligations under the applicable Data Privacy Laws or Process Personal Data in accordance with Customer's Instructions due to a legal requirement under any applicable law, Supplier will:

(i) promptly notify Customer of that legal requirement to the extent permitted by the applicable law; and

(ii) where necessary, cease all Processing (other than merely storing and maintaining the security of the affected Personal Data) until such time as Customer issues new Instructions with which Supplier is able to comply. If this provision is invoked, Supplier will not be liable to Customer under the Agreement for any failure to provide the applicable Products until such time as Customer issues new lawful Instructions with regard to the Processing.

c. Technical and Organizational Measures. Supplier shall implement and maintain appropriate technical and organizational measures to protect Personal Data from Personal Data Breaches, as described under Attachment 2 (*Technical and Organizational Measures*) of this DPA. Notwithstanding any provision to the contrary, Supplier may modify or update the contents of Attachment 2 at its discretion provided that such modification or update does not result in a material degradation in the technical and organizational measures set forth therein.

d. Confidentiality. Supplier shall ensure that any personnel whom Supplier authorizes to Process Personal Data on its behalf is subject to appropriate confidentiality obligations (whether a contractual or statutory duty) with respect to that Personal Data.

e. Personal Data Breaches. In the event that Supplier becomes aware of any Personal Data Breach, Supplier will notify Customer without undue delay, and in any case within any time period set forth in applicable Data Privacy Laws. Customer hereby agrees that Supplier may, in its discretion, provide any legally required notices of Personal Data Breaches to applicable authorities and/or affected Data Subjects, provided that Customer shall have the right to propose commercially reasonable edits to any such notices; otherwise, if Supplier defers to Customer to provide any such notices then Supplier shall provide Customer with such reasonable assistance as necessary to enable Customer to provide any such notices. Customer may, at its own effort and expense, send any notices that are not required by applicable law.

f. Deletion or Return of Personal Data. Supplier will Process Personal Data for the duration of the Agreement only, unless otherwise agreed in writing. Supplier will delete or return all Personal Data (including copies thereof) Processed pursuant to this DPA on termination or expiration of the Products in accordance with the procedures and timeframes set out in the Agreement. Notwithstanding the foregoing and subject to applicable Data Privacy Laws, Supplier may continue to retain Customer's Personal Data for as long as necessary to comply with Supplier's legal and regulatory obligations; to enable fraud monitoring, detection and loss prevention activities; to comply with Supplier's tax, accounting, and financial reporting obligations; and where required by Supplier's contractual commitments to third-parties. Any such processing that extends beyond the term of the Agreement shall be done in accordance with the terms of this DPA and any applicable Data Privacy Laws.

g. Demonstration of Compliance. Supplier shall make available to Customer all information reasonably necessary to demonstrate compliance with this DPA and applicable Data Privacy Laws and shall allow for and contribute to audits,

including inspections by Customer, in order to assess compliance with this DPA and applicable Data Privacy Laws. Customer acknowledges and agrees that it shall exercise its audit and inspection rights under this DPA by instructing Supplier to supply, on a confidential basis, (i) a summary copy of an independently validated report of its security programs (e.g. SOC 2, Type II Report), along with copies of any related policies and other documentation, or its hosting provider's security programs and related policies and documentation if Supplier does not host the Personal Data itself, or (ii) if Supplier does not have such a report, written responses to all reasonable requests for information made by Customer necessary to confirm Supplier's compliance with this DPA, along with copies of any related policies and other documentation. Customer shall not exercise this right to audit and inspect more than once per calendar year.

h. Supplier Assistance to Customer. To the extent required by applicable Data Privacy Laws, Supplier shall assist Customer with Customer's obligations under those applicable Data Privacy Laws. Such assistance may be provided through Product functionality, in which case Customer agrees to utilize such functionality before asking Supplier for further assistance.

5. Data Subject Requests

As part of Supplier's obligation under Section 4(f) above, where required by applicable Data Privacy Laws, Supplier will assist Customer with Customer's obligation to respond to requests from data protection authorities and Data Subjects that seek to exercise their rights under applicable Data Privacy Laws ("***Data Subject Requests***"). All Data Subject Requests must provide sufficient information for Supplier to verify the identity of the Data Subject. Customer shall reimburse Supplier for any commercially reasonable costs that arise from any such assistance that is in addition to that which Supplier normally provides to its customers.

If a Data Subject Request or other communication regarding the Processing of Personal Data under the Agreement is made directly to Supplier, Supplier will, to the extent that Supplier can identify Customer as the source of the Personal Data in question through its standard due diligence processes, promptly inform Customer of such Data Subject Request and will advise the Data Subject to submit their request to Customer. Customer shall otherwise be solely responsible for responding to any Data Subject Requests.

6. Data Protection Assessments

To the extent required by applicable law, Supplier will provide reasonable assistance to Customer to enable Customer to conduct and document data protection assessments, provided that the required information is reasonably available to Supplier, and Customer does not otherwise have access to the required information.

7. Sub-Processors

Customer agrees that Supplier may engage Sub-Processors to Process Personal Data on Customer's behalf.

Where Supplier engages Sub-Processors, Supplier will execute a written agreement with any Sub-Processor that imposes data protection and privacy terms on the Sub-Processors that provide at least the same level of protection for Personal Data as those in this DPA and that requires the Sub-Processor to meet the obligations of the Supplier with respect to the Personal Data, to the extent applicable to the nature of the services provided by such Sub-Processors. Supplier will remain responsible for each Sub-Processor's compliance with the obligations of this DPA and for any acts or omissions of such Sub-Processor that cause Supplier to breach any of its obligations under this DPA.

For those Customers that provide Personal Data of Data Subjects who are subject to CoPA, Customer has the right to object to the use of any particular Sub-Processor, in which case Customer may request a list of Supplier's Sub-Processors.

8. International Processing

Customer acknowledges and agrees that Supplier may Process Personal Data on a global basis as necessary to provide the Products in accordance with the Agreement. Supplier shall ensure such transfers are made in compliance with the requirements of applicable Data Privacy Laws.

9. Additional Provisions for California Personal Information

a. Scope. This Section 9 (Additional Provisions for California Personal Information) shall apply only with respect to California Personal Information. In the event that the terms and conditions in this Section 9 conflict with those in the other sections of this DPA, the terms and conditions in this Section 9 shall take precedence.

b. Responsibilities as a Service Provider. The parties agree that when Supplier is acting as a Service Provider (see Section 2(a)) Supplier will process California Personal Information strictly for the limited purposes set forth in Attachment 1 of this DPA and as otherwise permitted by the CCPA, including the permitted purposes set forth in the 'business purpose' definition in Section 1798.140(e) (the "***Business Purposes***").

(i) As Service Provider, Supplier shall not:

(A) combine the California Personal Information that the Supplier receives from, or on behalf of, the Customer with California Personal Information that it receives from, or on behalf of, another person or persons, or collects from its own interaction with a consumer, provided that the Supplier may combine California Personal Information to perform any Business Purposes permitted under the CCPA, and may also aggregate, deidentify, or anonymize California Personal Information so it no longer meets the California Personal Information definition, and may use such aggregated, deidentified, or anonymized data for its own research and development purposes or for any other purpose that is not prohibited under the CCPA;

(B) sell or share (as those terms are defined in the CCPA) California Personal Information;

(C) retain, use, or disclose California Personal Information for any purpose, including any commercial purpose, other than for the Business Purposes or as otherwise permitted by the CCPA; or

(D) retain, use, or disclose California Personal Information outside of the direct business relationship between Customer and Supplier, unless otherwise permitted by the CCPA.

(ii) As a Service Provider, Supplier shall:

(A) comply with all applicable obligations imposed by the CCPA;

(B) provide the same level of privacy protection as is required by the Customer under the CCPA;

(C) implement reasonable security procedures and practices appropriate to the nature of the California Personal Information received to protect the California Personal Information from unauthorized or illegal access, destruction, use, modification, or disclosure;

(D) promptly comply with any Customer request or instruction requiring the Supplier to provide, amend, transfer, or delete California Personal Information, or to stop, mitigate, or remedy any unauthorized processing;

(E) provide the Customer with reasonable and appropriate steps to (1) stop and remediate unauthorized use of California Personal Information and (2) ensure that Supplier uses the California Personal Information in a manner consistent with the Customer's obligations under the CCPA; and

(F) notify Customer immediately if it receives any complaint, notice, or communication that directly or indirectly relates either party's compliance with the CCPA; specifically, the Supplier must notify the Customer within seven (7) business days if it receives a verifiable consumer request under the CCPA.

c. Responsibilities as a CCPA Third Party. The parties agree that when Supplier is acting as a CCPA Third Party (see Section 2(a)) Supplier will process California Personal Information strictly for the limited purposes set forth in Attachment

1 of this DPA, including any Business Purposes and any CCPA Third Party purposes as identified therein, and as otherwise permitted by the CCPA (the "***CCPA Third Party Purposes***").

(i) As a CCPA Third Party, Supplier shall:

(A) Only use the California Personal Information for the CCPA Third Party Purposes;

(B) Comply with all applicable obligations imposed by the CCPA;

(C) Provide the same level of privacy protection as is required by the Customer under the CCPA;

(D) Implement reasonable security procedures and practices appropriate to the nature of the California Personal Information received to protect the California Personal Information from unauthorized or illegal access, destruction, use, modification, or disclosure;

(E) Permit the Customer to take reasonable and appropriate steps to (1) stop and remediate unauthorized use of California Personal Information and (2) ensure that the Supplier uses the California Personal Information in a manner consistent with the Customer's obligations under the CCPA; and

(F) Notify Customer immediately if it receives any complaint, notice, or communication that directly or indirectly relates either party's compliance with the CCPA, including any request to opt out of the sale or sharing of Personal Data; specifically, the Supplier must notify the Customer within seven (7) business days if it receives a verifiable consumer request under the CCPA.

d. Certification. Supplier certifies that it understands and will comply with the restrictions set out in Section 9(b) (*Responsibilities as a Service Provider*) and Section 9(c) (*Responsibilities as a CCPA Third Party*).

10. General Provisions

a. Amendments. Notwithstanding anything else to the contrary in the Agreement and without prejudice to Section 4(a) (*Compliance with Instructions*), or Section 4(c) (*Technical and Organizational Measures*), Supplier reserves the right to make any updates and changes to this DPA or list of Sub-Processors. Any such modifications become effective thirty (30) days after the date that Supplier either (1) notifies Customer that the updated DPA or list of Sub-Processors has been posted to a particular URL, or (2) where applicable pursuant to CoPA, distributes the updated DPA or list of Sub-Processors to any known point-of-contact for Customer. Customer is responsible for reviewing and becoming familiar with the updated DPA or list of Sub-Processors. If, prior to the effective date of the updated DPA or list of Sub-Processors, Customer notifies Supplier of its objection to any modification of the DPA or list of Sub-Processors, then Supplier shall either (i) negotiate with Customer in good faith to resolve any such objection, or (ii) upon thirty (30) days' notice to Customer, terminate the DPA and any portion of the Agreement that governs Products which are dependent upon its execution. If Supplier exercises its right to terminate pursuant to the terms of this Section, Customer shall be entitled to a pro-rata refund of any Fees already paid by Customer for the affected Products, calculated from the effective date of any such termination.

b. Severability. If any individual provisions of this DPA are determined to be invalid or unenforceable, the validity and enforceability of the other provisions of this DPA shall not be affected.

c. Limitation of Liability. Each party's liability, and where applicable, each of Customer's Affiliates' liability, taken in aggregate, arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, shall be subject to the limitations and exclusions of liability set out in the Agreement. In no event shall either party's liability be limited with respect to any individual Data Subject's data protection and privacy rights under this DPA or otherwise.

d. Governing Law. This DPA shall be governed by and construed in accordance with the governing law and jurisdiction provisions in the Agreement, unless required otherwise by Data Privacy Laws.

e. Aggregate, Deidentified, and Anonymized Data. Supplier may aggregate, deidentify, or anonymize Personal Data so it no longer meets the Personal Data definition under applicable Data Privacy Laws, and may use such aggregated, deidentified, or anonymized data for its own research and development purposes or for any other purpose that is not prohibited under applicable Data Privacy Laws. Supplier shall take reasonable measures to ensure that the data cannot be associated with a Data Subject and shall not attempt to re-identify the data. Supplier shall contractually obligate any recipients of the data to comply with the requirements of this Section 10(e).

11. Parties to this DPA

a. Permitted Affiliates. Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Privacy Laws, in the name and on behalf of its Permitted Affiliates, thereby establishing a separate DPA between Supplier and each such Permitted Affiliate. Each Permitted Affiliate agrees to be bound by the obligations under this DPA. For each separate DPA that is established, the Permitted Affiliate shall be the "Customer."

b. Authorization. The legal entity entering into this DPA as Customer represents that it is authorized to agree to and enter into this DPA for and on behalf of itself and, as applicable, each of its Permitted Affiliates.

c. Remedies. Except where applicable Data Privacy Laws require a Permitted Affiliate to exercise a right or seek any remedy under this DPA against Supplier directly by itself, the parties agree that: (i) solely the Customer entity that is the contracting party to the Agreement shall exercise any right or seek any remedy any Permitted Affiliate may have under this DPA on behalf of its Affiliates, and (ii) the Customer entity that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Permitted Affiliate individually but in a combined manner for itself and all of its Permitted Affiliates together. The Customer entity that is the contracting entity is responsible for coordinating all communication with Supplier under the DPA and shall be entitled to make and receive any communication related to this DPA on behalf of its Permitted Affiliates.

Attachment 1 - Details of Processing

A. Nature and Purpose of Processing

Supplier will Process Personal Data for the limited and specific purposes identified in the Agreement, including as necessary to provide the Products pursuant to the Agreement, as further specified in an Order Form or SOW, and as further instructed by Customer in its use of the Products. Without limiting the generality of the foregoing, Personal Data may be subject to the following Processing activities: (a) storage and other Processing as necessary to provide, maintain and improve the Products provided to Customer; and/or (b) disclosure to third-parties in accordance with the Agreement, this DPA, or as compelled by applicable laws, which may include sending Personal Data to Customer's partners and service providers on Customer's behalf and at their direction.

B. Duration of Processing

Subject to Section 4(f) (*Deletion or Return of Personal Data*) of this DPA, Supplier will Process Personal Data for the duration of the Agreement only, unless otherwise agreed in writing.

C. Categories of Personal Data

Customer may provide the following categories of Personal Data to Supplier in the course of using the Products, or incident to the use thereof, the extent of which is determined and controlled by Customer in its sole discretion:

- Contact Information, including name, mailing address, email address, online user name(s), telephone number, user agent, and similar information.
- Commercial Information, including records of products or services purchased.
- Social Security Number
- IP Address
- Financial information, including payment account information.
- Professional or employment-related information, including job title and place of employment.
- Any other Personal Data submitted by, sent to, or received by Customer, or Customer's end users, via the Products.

D. Special categories of data (if appropriate)

The parties do not anticipate processing special categories of Personal Data or sensitive personal information, as those terms are defined under applicable Data Privacy Laws.

Attachment 2 - Technical and Organizational Measures

Supplier shall comply with its obligations as a Processor under the Data Privacy Laws to keep all Personal Data secure. Without limiting the foregoing, Supplier shall: (a) taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to applicable Data Privacy Laws; and (b) in assessing the appropriate level of security, taking into account in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise processed. Such measures include (as applicable), without limitation:

a) Access Control

Outsourced Processing: Supplier Processes Customer's Personal Data, including Personal Data that is used in conjunction with its hosted Software and Cloud Services, using industry-leading, reputable cloud infrastructure vendors. Supplier maintains contractual relationships with these infrastructure vendors which obligates them to provide their infrastructure services in accordance with standards which conform to the requirements of applicable Data Privacy Laws and that are no less restrictive than this Data Processing Agreement.

Physical and environmental security: Supplier hosts its Cloud Services in multi-tenant environments and deploys industry best practices with respect to isolating each tenant from one another. Supplier hosts its hosted Software in separate virtual environments for each Customer, each controlled in accordance with industry best practices. All of Customer's Personal Data that is not Processed in the hosted Software or Cloud Services is Processed in a virtual environment inaccessible to Customers controlled in accordance with industry best practices.

Authentication: Supplier has implemented strong password policies for all systems that Process Customer's Personal Data. Customers who interact with the Products via the user interface must authenticate before accessing non-public Personal Data.

Authorization: For Cloud Services, Personal Data is stored in multi-tenant storage systems accessible to Customers via only application user interfaces and application programming interfaces, and Customers are not allowed direct access to the underlying application infrastructure. For all systems that Process Customer's Personal Data, the authorization model in each of Supplier's products is designed to ensure that only the appropriately assigned individuals can access relevant features, views, and customization options. Authorization to data sets is performed through validating the user's permissions against the attributes associated with each data set.

Application Programming Interface (API) access: Public product APIs may be accessed using an API key or through Oauth authorization.

Access controls: Supplier implements industry standard access controls for all systems that Process Customer's Personal Data. Network access control mechanisms are designed to prevent network traffic using unauthorized protocols from reaching the product infrastructure. The technical measures implemented differ between infrastructure providers and include Virtual Private Cloud (VPC) implementations, security group assignment, and traditional firewall rules.

Intrusion detection and prevention: Supplier implements industry standard intruder detection capabilities for all systems that Process Customer's Personal Data. Supplier has implemented a Web Application Firewall (WAF) solution to protect all internet-accessible systems that Process Customer's Personal Data. The WAF is designed to identify and prevent attacks against publicly available network services.

Static code analysis: Security reviews of code stored in Supplier's source code repositories are regularly performed, checking for logical errors, security flaws, and performance flaws.

Vulnerability testing: Supplier conducts regular vulnerability testing of systems that Process Customer's Personal Data. These vulnerability tests are intended to identify and resolve foreseeable attack vectors and potential abuse scenarios.

Product access: A subset of Supplier's employees have access to the Products and other systems that Process Customer's Personal Data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective customer

support, to troubleshoot potential problems, to detect and respond to security incidents, and implement data security measures. Access is enabled through "just in time" requests for access, and all such requests are logged. Employees are granted access by role, and reviews of high-risk privilege grants and roles are conducted regularly.

External access to Supplier systems that Process Customer's Personal Data is restricted, following the same least privilege model, and requires two-factor authorization and authentication. External access controls are configured and monitored by Supplier IT and Security personnel.

Background checks: All Supplier employees who access systems that Process Customer's Personal Data undergo a background check prior to being extended an employment offer, in accordance with and as permitted by the applicable laws. All employees are required to conduct themselves in a manner consistent with company guidelines, non-disclosure requirements, and ethical standards.

b) Transmission Control

In-transit: For Supplier Products that are accessible via the Internet, Supplier makes HTTPS encryption (also referred to as SSL or TLS) available on every one of its login interfaces. Supplier's HTTPS implementation uses industry standard algorithms and certificates.

At-rest: Supplier stores user passwords following policies that follow industry standard practices for security. Supplier has implemented technologies to ensure that stored data is encrypted at rest.

c) Input Control

Detection: Supplier designed its infrastructure to log extensive information about the system behavior, traffic received, system authentication, and other application requests. Internal systems aggregate log data and alert appropriate employees of malicious, unintended, or anomalous activities. Supplier personnel, including security, operations, and support personnel, are responsive to known incidents.

Response and tracking: Supplier maintains a record of known security incidents that includes description, dates and times of relevant activities, and incident disposition. Suspected and confirmed security incidents are investigated by security, legal, operations, or support personnel, and appropriate resolution steps are identified and documented. For any confirmed incidents, Supplier will take appropriate steps to respond and notify Customer in accordance with the terms of this DPA.

d) Availability Control

Infrastructure availability: The infrastructure providers use commercially reasonable efforts to ensure a minimum of 99% uptime.

Fault tolerance: Backup and replication strategies are designed to ensure redundancy and fail-over protections during a significant processing failure. Customer's Personal Data is backed up to multiple durable data stores.

Online replicas and backups: Where feasible, production databases are designed to replicate data between no less than 1 primary and 1 secondary database. All databases are backed up and maintained using at least industry standard methods. Supplier's systems that Process Customer's Personal Data are designed to ensure redundancy and seamless failover. The server instances that support the Products are also architected with a goal to prevent single points of failure. This design assists Supplier operations in maintaining and updating the Product applications and backend while limiting downtime.

Measures to ensure that personal data are protected from accidental destruction or loss: Supplier has business continuity, incident response, data backup, and disaster recovery procedures designed to maintain business operations and redundancy of systems that Process Customer's Personal Data. Supplier performs regular testing to ensure that availability supporting systems function properly.

e) Certifications

Upon request of Customer, Supplier will provide either (i) a copy of any available independently validated report of its security programs (i.e. SOC 2, Type II, ISO 27001, etc.), or (ii) written responses to all reasonable requests for information, along with copies of any related policies and other documentation.