DATA PROCESSING AGREEMENT

This Data Processing Addendum (this "DPA"), forms part of the Software Services Agreement ("Agreement") between you ("Subscriber"), and Entegrata, Inc., a Delaware corporation ("Entegrata" or "Service Provider") (individually a "Party" and collectively as the "Parties"). This DPA shall govern the Processing of Personal Information by Service Provider in connection with Service Provider's provision of the Services to Subscriber pursuant to the Agreement.

1. DEFINITIONS

1.1 "Controller" shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of Personal Information.

1.2 "Data Subject" means an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier, such as name, an identification number, location data, an online identifier, or to one or more factors specific to physical, physiological, genetic, mental, economic, cultural or social identity.

1.3 "Data Protection Law" means all applicable data protection and privacy legislation that applies to the Processing of Personal Information. It shall include, is but not limited to, current and future United States privacy law, including the California Consumer Privacy Act and California Privacy Rights Act ("CCPA"), the Virginia Consumer Data Protection Act ("VCDPA"), the Colorado Privacy Act ("CPA"), the Connecticut Data Privacy Act (CDPA), and the Utah Consumer Privacy Act ("UCPA"); the European Union General Data Protection Regulation ("EU") 2016/679 ("GDPR"); Canada's Personal Information Protection and Electronic Documents Act ("PIPEDA"); and the other data protection laws and regulations of the European Union, the European Economic Area and their member states, and the United Kingdom.

1.4 "Instruction" means the written instruction, issued by Controller to Processor, directing the Processor to perform a specific action with regard to Personal Information (including, but not limited to, depersonalizing, blocking, deletion, making available).

1.5 "Personal Information" means any information relating to an identified or identifiable living individual that is Processed by the Service Provider on behalf of

Subscriber as a result of, or in connection with, the provision of the Services under the Agreement.

1.6 "Information Security Incident" means a breach of security leading to the accidental, unauthorized or unlawful destruction, loss, alteration, disclosure of, or access to, the Personal Information.

1.7 "Processing" or "Process" means commissioned processing of Personal Information, encompassing any operation or set of operations which is performed on Personal Information or on sets of Personal Information, 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.

1.8 "Processor" has the meaning given to such term under applicable Data Protection Laws, and, as used herein, also means "Service Provider" as such term is defined under the CCPA.

1.9 "Service" means the services that Service Provider performs for Subscriber pursuant to the Agreement.

1.10 "Standard Contractual Clauses" or "SCCs" are the standard contractual clauses adopted by the European Commission for the transfer of Personal Information to processors established in third countries.

1.11 "Subscriber Data" has the meaning set forth in the Agreement and may include Subscriber client information that may be subject to attorney/client privilege or a professional obligation to maintain it in confidence, and materials that are disclosed by or on behalf of Subscriber or Users to Entegrata or that are accessed by Entegrata in connection with Subscriber's or its User's use of the Services.

2. Scope, Responsibility, and Term.

2.1 Processing Instructions. Service Provider will Process Personal Information only in accordance with Subscriber's Instructions. Service Provider shall process the Personal Information listed in Attachment A on behalf of Subscriber and for the purposes of fulfilling the Agreement.

2.2 Confidentiality. Service Provider will maintain the confidentiality of the Personal Information and will not disclose the Personal Information to third parties unless Subscriber or this DPA specifically authorizes the disclosure, or as required by domestic law, court or regulator.

2.3 Data Protection Law Obligations. Service Provider will reasonably assist Subscriber with meeting Subscriber's compliance obligations under Data Protection Law, taking into account the nature of Service Provider's processing and the information available to Service Provider. The Parties shall each comply with their respective obligations under all applicable Data Protection Laws.

3. Subscriber Obligations, Representations, and Warranties.

3.1 Compliance with Data Protection Laws. Subscriber agrees to comply with any applicable protection, security or other obligations with respect to Personal Information prescribed by Data Protection Laws. Subscriber has the sole responsibility for the accuracy, quality, and legality of Personal Information provided to the Service Provider and the means by which it was obtained.

3.2 Representations and Warranties. With respect to the Personal Information disclosed in connection with the Services, Subscriber represents and warrants that:

a) Subscriber has obtained all rights and licenses, and has established all legal bases, necessary consents, and authorizations in order to provide the Service Provider with any Personal Information;
b) Personal Information provided to the Service Provider was collected in a transparent and lawful way in accordance with all applicable laws, including Data Protection Laws;
c) Subscriber will not disclose or otherwise make available, directly or indirectly, to Service Provider, Personal Information of any individual who has exercised an opt-out of any selling, sharing, or Processing of data; and
d) Subscriber provides all necessary notices required by Data Protection Laws in order to Process Personal Information.

4. Service Provider Personnel.

4.1 Confidentiality Obligations. Service Provider will ensure that all of its personnel engaged in the Processing of Personal Information are bound by confidentiality obligations and use restrictions in respect to the Personal Information.

4.2 Limited Access. Service Provider will ensure that access to Personal Information by Service Provider personnel is limited to those personnel who require such access in order for Service Provider to provide the Services under the Agreement.

5. Security.

5.1 Security Measures. Service Provider will implement and maintain technical and organizational measures to protect Personal Information against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Personal Information. Such security measures shall comply with applicable Data Protection Laws.

5.2 Subscriber Security Responsibilities. Subscriber agrees that, without limitation of Service Provider's obligations under this section, Subscriber is solely responsible for its use of the Services, including (a) making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of the Personal Information; (b) securing the account authentication credentials, systems and devices Subscriber uses to access the Services; (c) securing Subscriber's systems and devices that Provider uses to provide the Services; and (d) backing up Personal Information.

5.3 Return of Personal Information. Service Provider agrees to delete or return all Personal Information to the Subscriber upon the termination of the Agreement.

6. Information Security Incident.

6.1 If Service Provider becomes aware of an Information Security Incident, Service Provider will notify Subscriber of the Information Security Incident, take reasonable steps to identify the cause of such Information Security Incident, and take any other steps required under applicable Data Protection Laws. Service Provider's notification of or response to an Information Security Incident will not be construed as an acknowledgement of any fault or liability with respect to the Information Security Incident.

7. Cross-Border Transfers of Personal Information.

7.1 International Transfers. Service Provider must not conduct any international transfer of Personal Information without obtaining Subscriber's prior written consent. Where such consent is granted, Service Provider may only Process Personal Information under the following conditions: (a) Service Provider may process Personal Information in a territory which is subject to adequacy decisions under Data Protection Laws; or (b) Service Provider participates in a valid cross-border transfer mechanism under the applicable Data Protection Laws, so that Service Provider (and, where appropriate, Subscriber) can ensure that appropriate safeguards are in place to ensure an adequate level of protection with respect to the privacy rights of individuals as required by applicable Data Protection Laws.

8. Inquiries by Data Subjects.

8.1 Data Subject Requests. If Service Provider receives any request from a Data Subject in relation to the Data Subject's Personal Information, Service Provider will notify Subscriber of such request.

8.2 Assistance. Service Provider will provide reasonable assistance as necessary for Subscriber to perform its obligations under Data Protection Laws within any deadlines imposed thereunder.

9. Audit.

9.1 Audit Requirements. Subscriber may audit Service Provider's compliance with its obligations under this DPA up to once per year and on such other occasions as may be required by Applicable Data Protection Laws. Service Provider will contribute to such audits by providing Subscriber with the information and assistance reasonably necessary to conduct the audit. If a third party is to conduct the audit, Service Provider may object to the auditor if the auditor is not independent, a competitor of Service Provider, or otherwise manifestly unsuitable. Such objection by Service Provider will require Subscriber to appoint another auditor or conduct the audit itself.

9.2 Audit Requests. To request an audit, Subscriber must submit a proposed audit plan to Service Provider at least thirty (30) days in advance of the proposed audit date and any third-party auditor must sign a customary non-disclosure agreement mutually acceptable to the parties (such acceptance not to be unreasonably withheld) providing for the confidential treatment of all information exchanged in connection with the audit and any reports regarding the results or findings thereof. The proposed audit plan must describe the proposed scope, duration, and start date of the audit. Service Provider will review the proposed audit plan and provide Subscriber with any concerns or questions (for example, any request for information that could compromise Service Provider security, privacy, employment or other relevant policies). Service Provider will work cooperatively with Subscriber to agree on a final audit plan. Nothing in this section shall require Provider to breach any duties of confidentiality. If the controls or measures to be assessed in the requested audit are addressed in an SOC 2 Type 2, ISO, NIST or similar audit report performed by a qualified third-party auditor within twelve (12) months of Subscriber's audit request and Service Provider has confirmed there have been no known material changes in the controls audited since the date of such report, Subscriber agrees to accept such report in lieu of requesting an audit of such controls or measures. The audit must be conducted during regular business hours, subject to the agreed final audit plan and Provider's safety, security or other relevant policies, and may not unreasonably interfere with Provider business activities.

Subscriber will promptly notify Service Provider of any non-compliance discovered during the course of an audit and provide Service Provider any audit reports generated in connection with any audit under this section, unless prohibited by Applicable Data Protection Laws. Subscriber may use the audit reports only for the purposes of meeting Subscriber's regulatory audit requirements and/or confirming compliance with the requirements of this DPA.

9.3 Audit Expenses. Any audits are at Subscriber's sole expense. Subscriber shall reimburse Service Provider for any time expended by Service Provider and any third parties in connection with any audits or inspections under this section at Service Provider's then-current professional services rates, which shall be made available to Subscriber upon request. Subscriber will be responsible for any fees charged by any auditor appointed by Subscriber to execute any such audit.

10. Subprocessors

10.1 Authorization. Subscriber specifically authorizes the engagement and use of Microsoft to process Personal Information. Subscriber specifically authorizes the engagement of the additional subprocessors to process Personal Information if: (a) Subscriber is provided with an opportunity to object on reasonable grounds to the appointment of each subprocessor within three (3) days after Service Provider supplies Subscriber with details in writing regarding such subprocessor. The Parties agree to work together in good faith to resolve any such objection. If the parties are unable to reach a mutually acceptable resolution with respect to a particular subprocessor within a reasonable timeframe and Service Provider advises that use of such subprocessor is required for continued provision of Services, Subscriber may, as its sole and exclusive remedy, terminate the Agreement and cancel the Service by providing written notice to Service Provider and pay Service Provider for all amounts due and owing under the Agreement as of the date of such termination. Any amounts previously paid shall be nonrefundable.

11. Miscellaneous Provisions.

11.1 Limitation of Liability. This DPA and liability or remedies arising herein are subject to any and all limitations on liability and disclaimers of types of damages in the Agreement to the maximum extent permitted by applicable law.

11.2 Termination. This DPA will remain in full force and effect so long as the Agreement remains in effect or Service Provider retains any of the Personal Information

related to the Agreement in its possession or control. This DPA automatically terminates upon termination or expiration of the Agreement.

11.3 Data Protection Laws. If a change in any Data Protection Laws prevents either party from fulfilling all or part of its Agreement obligations, the Parties may agree to suspend the Processing of the Personal Information until that Processing complies with the new requirements. If the Parties are unable to bring the Personal Information Processing into compliance with the Data Protection Laws within thirty (30) days, either Party may terminate the Agreement with immediate effect on written notice to the other Party, in which event all accrued but unpaid fees of under the Agreement through the date of termination shall become due and payable and all fees previously paid shall be nonrefundable.

11.4 Notice. Notices under this DPA and the Standard Contractual Clauses shall be in accordance with the Agreement.

ATTACHMENT A

B. DESCRIPTION OF DATA TRANSFERRED

Data Subjects

Subscriber may submit Personal Information to Service Provider, the extent of which is determined and controlled by the Subscriber, and which may include, but is not limited to, Personal Information relating to the following categories of Data Subjects:

(i) Current and former personnel of the Subscriber;
(ii) Contractors, suppliers, vendors, prospects, business partners of the Subscriber;
(iii) Employees, directors, managers or contact persons of Subscriber's clients, suppliers, prospects, and business partners;
(iv) Customers or clients of Subscriber;
(v) Internet users; and
(vi) Subscriber's users authorized to use the Services.

Type of Personal Information

Personal Information to be submitted includes any identification number or one or more factors specific to the physical, physiological, mental, economic, cultural or social identity

of a Data Subject included in Subscriber Data and accessed and stored within the Subscriber's instance of the Services by reference to which the Data Subject may be directly or indirectly identified.

Special Categories of Personal Information

Subscriber may submit special categories of data to the Service Provider, the extent of which is determined and controlled by the Subscriber in its sole discretion, and which is, for the sake of clarity, Personal Information with information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, or data concerning health or sex life.