PERSONAL DATA PRIVACY AND PROTECTION CLAUSES FOR VENDOR CONTRACTS

PART A – GLOBAL EXCLUDING EUROPE

To the extent Vendor will be provided with or have access to Personal Information (as defined below), the following data privacy clauses of this Part A (referred to in this Part A as the "Clauses") shall be incorporated into and form a part of the Contract by and between Vendor and Company for the purchase of goods and / or services by Company from Vendor.

1. DEFINITIONS.

"Data Privacy Standards" means all relevant and applicable federal, state and provincial data privacy standards, including, but not limited to, Florida Information Protection Act, SB 1524, the Massachusetts Office of Consumer Affairs and Business Regulation Standards for the Protection of Personal Information, 201 CMR 17.00, HIPAA and HITECH.

"Individual" means Company, Company's employees and Company's business partners wherever located, except Europe.

"Personal Information" means the following:
(a) Personally identifiable information (PII) of an Individual, which includes:

- First name and last name or first initial and last name in combination with any one or more of the data elements listed below that relate to such Individual;
- Social Security Number (or country specific equivalent);
- Driver's license number or state-issued identification card number;
- Financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to an Individual's financial account;
- Passport number;
- Medical history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional or health insurance information;
- Username or email address coupled with a password or security question and answer that would permit access to an online account; and/or
- Any information contained in Company's information systems; and/or

(b) Protected health information (PHI), which includes information related to an Individual's health care or payment related to health care that directly or indirectly identifies the Individual.
"Subcontractor" means a third party, agent, other contractor, or subcontractor of Vendor.

2. COMPLIANCE WITH DATA PRIVACY STANDARDS.

To the extent Vendor maintains, acquires, discloses, uses, or has access to any Personal Information, Vendor shall comply with all Data Privacy Standards. Vendor shall notify Company in writing immediately if Vendor is no longer in compliance with Data Privacy Standards with respect to any Personal Information.

3. RETURN OR DESTRUCTION OF PERSONAL INFORMATION.

If at any time during the term of the Contract any part of Personal Information, in any form, that Vendor obtains from Company ceases to be required by Vendor for the performance of its obligations under the Contract, or upon termination of the Contract, whichever occurs first, Vendor shall, within fourteen (14) days thereafter, promptly notify Company and securely return such Personal Information to Company, or, at Company's written request destroy, un-install and/or remove all copies of such Personal Information in Vendor's possession or control, or such part of the Personal Information which relates to the part of the Contract which is terminated, or the part no longer required, as appropriate, and certify to Company that the same has been completed.

4. USE OF SUBCONTRACTORS WITH ACCESS TO PERSONAL INFORMATION.

When Vendor utilizes a Subcontractor in connection with its performance of its obligations under the Contract and Vendor provides such Subcontractor with access to Personal Information, Vendor shall provide Company with prompt notice of the identity of such Subcontractor and the extent of the role that such Subcontractor will play in connection with the sale of goods or performance of services under the Contract. Moreover, all such Subcontractors given access to any Personal Information must agree to: (a) abide by the Clauses set forth herein, including, without limitation, its provisions relating to compliance with Data Privacy Standards for the protection of Personal Information and Notice of Security and/or Privacy Incident; (b) restrict use of Personal Information only for Subcontractor's internal business purposes and only as necessary for the sale of goods or to render services to Vendor in connection with Vendor's performance of its obligations under the Contract, and (iii) certify in writing, upon completion of any sale of goods or performance of services by a Subcontractor, that the Subcontractor has immediately un-installed, removed, and/or destroyed all copies of Personal Information within 30 days of Subcontractor's completion of the sale of goods or performance of services to Vendor.

5. NOTICE OF SECURITY AND/OR PRIVACY INCIDENT.

If Vendor, or its Subcontractor, suspect, discover or are notified of a data security incident or potential breach of security and/or privacy relating to Personal Information, Vendor shall immediately, but in no event later than forty-eight (48) hours from suspicion, discovery or notification of the incident or potential breach, notify Company of such incident or potential breach. Vendor shall, upon Company's request, investigate such incident or potential breach, inform Company of the results of any such investigation, and assist Company in maintaining the confidentiality of such information. In addition to the foregoing, Vendor shall provide Company with any assistance necessary to comply with any federal, state and / or provincial laws requiring the provision of notice of any privacy

incident or security breach with respect to any Personal Information to the affected or impacted individuals and / or organizations, in addition to any notification to applicable federal, state and provincial agencies. Vendor shall reimburse Company for all expenses, costs, attorneys' fees, and resulting fines, penalties, and damages associated with such notification if due to Vendor's, or its Subcontractor's, negligence, unauthorized use or disclosure of Personal Information, or breach of its obligations under the Contract.

6. INSURANCE.

Vendor shall purchase and maintain at all times, during the term of the Contract, a professional liability insurance policy and a cyber liability insurance policy with coverage limits of at least $2,000.000. In some instances, Vendor may be required to provide cyber liability insurance policy with higher coverage limits.

7. REMEDIES, DAMAGES AND INDEMNIFICATION.

Vendor shall bear all costs, losses and damages to the extent resulting from Vendor's breach of these Clauses. Vendor agrees to release, defend, indemnify, and hold harmless Company and its Affiliates for claims, losses, penalties and damages and reasonable attorneys' fees and costs to the extent arising out of Vendor's, or its Subcontractor's, negligence, unauthorized use or disclosure of Personal Information and/or Vendor's, or its Subcontractor's, breach of its obligations under these Clauses. Vendor shall inform all of its principals, officers, employees, agents and Subcontractors assigned to consummate the sale of goods or perform services under the Contract of the obligations contained in these Clauses. To the extent necessary and/or required by law, Vendor shall provide training to such employees, agents and Subcontractors to promote compliance with these Clauses. Vendor assumes all liability for any breach of these Clauses by Vendor or any of its principals, officers, employees, agents and Subcontractors.

PART B – EUROPE

To the extent Vendor ("Contracted Processor" "Controller" or "Subprocessor") will be provided with or have access to Personal Data as defined in the EU's General Data Protection Regulation, this Part B shall be incorporated into and form a part of the Contract by and between Vendor and Company for the purchase of goods and / or services by Company from Vendor.

The terms used in this Part B shall have the meanings set forth below. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Principal Agreement. Except as modified below, the terms of the Principal Agreement shall remain in full force and effect.

In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added to the Principal Agreement. Except where the context requires otherwise, references herein to the Principal Agreement are to the Principal Agreement as amended by, and including, this Part B.

1. Definitions

1.1 The following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.1.1 **"*Affiliates*"** means any Person that controls, is controlled by or is under common control with Company, Processor or Subprocessor, respectively. The term "control" means the ownership, directly or indirectly, of fifty percent or more of the voting stock or equity interest of the subject Person. "Person" means any natural person, corporation, unincorporated organization, partnership, association, joint stock buyer, joint venture, trust or government, or any agency or political subdivision of any government, or any other entity. Affiliates are intended third party beneficiaries of this Amendment.

1.1.2 **"*Applicable Laws*"** means (a) European Union or Member State laws with respect to any Company Personal Data in respect of which the Company is subject to EU Data Protection Laws; and (b) any other applicable law with respect to any Company Personal Data in respect of which the Company is subject to any other Data Protection Laws;

1.1.3 **"*Company Personal Data*"** means any Personal Data Processed by a Contracted Processor on behalf of the Company pursuant to or in connection with the Principal Agreement;

1.1.4 **"*Contracted Processor*"** means the natural or legal person, public authority, agency or other body which processes Company Personal Data on behalf of the Controller;

1.1.5 **"*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 Company Personal Data;

where the purposes and means of such processing are determined by Union or Member State law, the Controller or the specific criteria for its nomination may be provided for by Union or Member State law;

1.1.6 **"*Data Protection Laws*"** means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

1.1.7 **"*EEA*"** means the European Economic Area;

1.1.8 **"*EU Data Protection Laws*"** means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including the GDPR and laws implementing or supplementing the GDPR;

1.1.9 **"*GDPR*"** means EU General Data Protection Regulation 2016/679;

1.1.10 **"*Personal Data*"** means any information relating to an identified or identifiable natural person ("**Data Subject**"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

1.1.11 **"*Processing*"** means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

1.1.12 **"*Services*"** means the services and other activities to be supplied to or carried out by or on behalf of Contracted Processor for Company pursuant to the Principal Agreement; and,

1.1.13 **"*Subprocessor*"** means any person (including any third party, but excluding an employee of Contracted Processor or any of its sub-contractors) appointed by or on behalf of Contracted Processor to Process Personal Data on behalf of the Company in connection with the Principal Agreement.

1.2 Any term not defined herein shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

2. Processing of Company Personal Data

2.1 Contracted Processor shall not Process Company Personal Data other than on the Company's documented written instructions, unless Processing is required by Applicable Laws to which the relevant Contracted Processor is subject, in which case Contracted Processor shall to the extent permitted by Applicable Laws,

inform the Company of that legal requirement before the relevant Processing of that Personal Data.

2.2 Section 13 below sets out certain information regarding the Contracted Processors' Processing of Company Personal Data as required by Article 28(3) of the GDPR (and, possibly, equivalent requirements of other Data Protection Laws). Company may make amendments to Section 13 by written notice to Contracted Processor from time to time as Company reasonably considers necessary to meet those requirements. Nothing in Section 13 (including as amended pursuant to this section 2.2) confers any right or imposes any obligation on any party to this Part B.

3. Personnel Confidentiality

Contracted Processor shall take reasonable steps to ensure the reliability of any of its employees, agents or contractors who may have access to Company Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Company Personal Data, for the purposes of the Principal Agreement, to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, and ensure that all such individuals are subject to a strict duty of confidentiality.

4. Security

4.1 Taking into account the state of the art, the costs of implementation, 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, Contracted Processor shall in relation to Company Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, but not limited to, the measures referred to in Article 32(1) of the GDPR.

4.2 In assessing the appropriate level of security, Contracted Processor shall take into account the risks that are presented by Processing, in relation to a Personal Data Breach.

5. **Subprocessing**

5.1 Company authorises Contracted Processor and Subprocessor to appoint Subprocessors in accordance with this section 5 and any restrictions in the Principal Agreement.

5.2 Contracted Processor shall give Company prior written notice of the proposed appointment of any new Subprocessor, including full details of the Processing to be undertaken by the Subprocessor.

5.3 Contracted Processor shall not appoint (nor disclose any Company Personal Data to) the proposed Subprocessor except with the prior written consent of Company.

5.4 With respect to each Subprocessor, Contracted Processor shall:

5.4.1 Before the Subprocessor first Processes Company Personal Data, carry out adequate due diligence to ensure that the Subprocessor is capable

of providing the level of protection for Company Personal Data required by the Principal Agreement;

5.4.2 Ensure that the arrangements between (a) Contracted Processor and its relevant intermediate Subprocessor or any other Subprocessor; and (b) the intermediate Subprocessor and any other Subprocessor, are governed by a written contract including terms which offer at least the same level of protection for Company Personal Data as those set out in this Part B and meet the requirements of Article 28(3) of the GDPR; and,

5.4.3 Provide to Company for review such copies of the Contracted Processors' agreements with Subprocessors (which may be redacted to remove confidential commercial information not relevant to the requirements of this Part B) as Company may request from time to time.

6. Data Subject Rights

6.1 Contracted Processor shall provide reasonable assistance to Company in the preparation of any data protection impact assessments or consultations with relevant data privacy authorities, which Company considers to be required by Article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law. Such assistance shall be in relation to Contracted Processor's Processing of Company Personal Data, taking into account the nature of the Processing and information available to the Contracted Processor.

6.2 Taking into account the nature of the Processing, Contracted Processor shall assist the Company by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Company's obligations, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.3 Contracted Processor shall:

6.3.1 promptly notify Company if it or any of its Subprocessors receives a request from a Data Subject under any Data Protection Law in respect of Company Personal Data; and,

6.3.2 ensure that the it and any of its Subprocessors does not respond to that request except on the documented instructions of Company or as required by Applicable Laws to which the Contracted Processor is subject, in which case Contracted Processor shall to the extent permitted by Applicable Laws inform Company of that legal requirement before the Contracted Processor responds to the request.

7. **Personal Data Breach**

7.1 Contracted Processor shall notify Company without undue delay, and in any event, at least 24 hours prior to providing notice to any governmental authorities under subsection 7.2 below, upon Contracted Processor or any Subprocessor becoming aware of a Personal Data Breach affecting Company Personal Data, and provide Company with sufficient information to allow Company to meet any obligations to

report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2 Contracted Processor and its Subprocessors shall provide notice to the appropriate authorities pursuant to the timeliness requirements under EU Data Protection Laws and GDPR.

7.3 Contracted Processor shall cooperate with Company and take such reasonable commercial steps as are directed by Company to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. Deletion of Company Personal Data

8.1 Subject to section 8.2, Contracted Processor shall promptly and in any event within 30 days of the date of cessation of any Services involving the Processing of Company Personal Data (the "***Cessation Date***"), delete, so as not to be recovered or reconstructed, and procure the deletion of all copies of Company Personal Data. Contracted Processor shall provide written certification to Company that it has fully complied with the deletion requirements of this section within thirty (30) days of the Cessation Date.

8.2 Each Contracted Processor may retain Company Personal Data only to the extent and for such period as required by Applicable Laws and always provided that Contracted Processor shall ensure the confidentiality of all such Company Personal Data and shall ensure that such Company Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose.

8.3 Any Contracted Processor retaining Company Personal Data pursuant to section 8.2 shall inform the Company of said retention of Company Personal Data within 15 days of the Cessation Date.

9. Audit rights

9.1 Contracted Processor shall make available to Company on request all information necessary to demonstrate compliance with this Part B, and shall allow for and contribute to audits, including inspections, by Company or an auditor mandated by Company in relation to the Processing of Company Personal Data by the Contracted Processors or any of its Subprocessors.

10. Additional Responsibilities

10.1 Contracted Processor shall take all necessary actions, and provide Company with all information needed, to ensure that both Company and Contracted Processor are in compliance with Data Protection Laws, including Article 28 of the GDPR.

10.2 Contracted Processor shall immediately notify Company if it, or any Contracted Processor, is asked to take any action which may infringe on Data Protection Laws.

10.3 Contracted Processor shall purchase and maintain at all times, during the term of the Principal Agreement, a professional liability insurance policy and a cyber

liability insurance policy with coverage limits of at least $2,000,000 per breach or incident.

11. Remedies, Damages and Indemnification

11.1 Contracted Processor shall bear all costs, losses and damages to the extent resulting from Contracted Processor's breach of this Part B. Contracted Processor shall reimburse Company for all expenses, costs, attorneys' fees, and resulting fines, penalties, and damages associated with any Personal Data Breach, if due to Contracted Processor's or its Subprocessor's negligence, unauthorized use or disclosure of Personal Data, or beach of its obligations under the Principal Agreement. Contracted Processor agrees to release, defend, indemnify, and hold harmless Company and its officers, directors, and Affiliates for claims, losses, penalties and damages and reasonable attorneys' fees and costs to the extent arising out of Contracted Processor's, or its Subprocessor's, negligence, unauthorized use or disclosure of Personal Data and/or Contracted Processor's, or its Subprocessor's, breach of its obligations under this Part B. Contracted Processor shall inform all of its principals, officers, employees, agents and Subprocessors assigned to consummate the sale of goods or perform services under the Principal Agreement of the obligations contained in this Part B. To the extent necessary and/or required by law, Contracted Processor shall provide training to employees, agents and Subprocessors to promote compliance with this Part B. Contracted Processor assumes all liability for any breach of this Part B by Contracted Processor or any of its principals, officers, employees, agents and Subprocessors.

12. General Terms

12.1 Nothing in this Part B relieves the Contracted Processors of their own direct responsibilities and liabilities under Applicable Laws, including the GDPR.

13. Personal Data Processing Details

13.1 Principal Agreement between Vendor and Company must set forth certain details of the Processing of Company Personal Data as required by Article 28(3) GDPR;

13.2 The subject matter and duration of the Processing of the Company Personal Data are set out in the Principal Agreement and this Addendum;

13.3 The nature and purpose of the Processing of Company Data;

13.4 The types of Company Personal Data to be Processed;

13.5 The categories of Data Subject to whom the Company Personal Data relates; and

13.6 The obligations and rights of Company.