PERSONAL DATA PRIVACY AND PROTECTION CLAUSES FOR VENDOR CONTRACTS
(Effective November 18, 2015)

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 Buyer for the purchase of goods and / or services by Buyer 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 Buyer, Buyer's employees and Buyer'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 Buyer'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 Buyer 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 Buyer 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 Buyer and securely return such Personal Information to Buyer, or, at Buyer'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 Buyer 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 Buyer 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 (c) 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 Buyer of such incident or potential breach. Vendor shall, upon Buyer's request, investigate such incident or potential breach, inform Buyer of the results of any such investigation, and assist Buyer in maintaining the confidentiality of such information. In addition to the foregoing, Vendor shall provide Buyer 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 Buyer 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 Buyer 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 will be provided with or have access to Personal Data (as defined below), the following data protection clauses of this Part B (referred to in this Part B as the "Clauses") shall be incorporated into and form a part of the Contract by and between Vendor and Purchaser for the purchase of goods and/or services by Purchaser from Vendor.

1. DEFINITIONS.
Applicable Data Protection Law means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the Processing of Personal Data applicable to a Data Controller in the EU Member State in which the data exporter is established.
Data Controller means 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 Data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by EU national or EU Community law.
Data Processor means a natural or legal person, public authority, agency or any other body which processes Personal Data on behalf of the Data Controller.
Data Subject means a natural person located or residing in Europe and that can be identified or is identifiable by Personal Data.
Member means any person or entity that controls, is controlled by or is under common control with T&L Sugars Limited. Members are intended third party beneficiaries of these Clauses.
Personal Data means any information that identifies a Data Subject, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.
Processing means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.
Subprocessor means any third-party subcontractor engaged by the Data Processor or by any other subcontractor of the Data Processor who agrees to receive from the Data Processor or from any other subcontractor of the Data Processor Personal Data exclusively intended for processing activities to be carried out on behalf of the Data Controller after the transfer in accordance with his instructions, the terms of these Clauses and the terms of the written subcontract.
Technical and Organisational Security Measures means those measures aimed at protecting Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the Processing involves the transmission of data over a network, and against all other unlawful forms of Processing.

2. OBLIGATIONS OF THE DATA PROCESSOR.
Purchaser and Vendor acknowledge that, for the purposes of the Applicable Data Protection Law, Purchaser is the Data Controller and Vendor is the Data Processor of any Personal Data. The Data Processor shall (a) process Personal Data only to the extent, and in such a manner, as is necessary for the purposes of fulfilling its obligations under the Contract and in accordance with Purchaser's instructions from time to time and shall not process Personal Data for any other purpose; (b) keep a record of any processing of Personal Data it carries out on behalf of Purchaser; (c) promptly comply with any request from Purchaser requiring the Data Processor to amend, transfer or delete Personal Data; (d), if the Data Processor receives any complaint, notice or communication which relates directly or indirectly to the processing of Personal Data or to either party's compliance with the Applicable Data Protection Law, immediately notify Purchaser and provide Purchaser with full cooperation and assistance in relation to any such complaint, notice or communication; (e), at Purchaser's request, provide to Purchaser a copy of all Personal Data held by it in the format and on the media reasonably specified by Purchaser; (f) not transfer Personal Data outside the European Economic Area without the prior written consent of Purchaser; and (g) promptly inform Purchaser if any Personal Data is lost or destroyed or becomes damaged, corrupted, or unusable, and restore such Personal Data at its own expense.

3. DATA PROCESSOR'S EMPLOYEES.
3.1. The Data Processor shall ensure that access to Personal Data is limited to (a) those employees who need access to Personal Data to meet the Data Processor's obligations under the Contract; and (b) in the case of any access by any employee, such part or parts of Personal Data as is strictly necessary for performance of that employee's duties.
3.2. The Data Processor shall ensure that all employees (a) are informed of the confidential nature of Personal Data; (b) have undertaken training in the laws relating to handling Personal Data; and (c) are aware both of the Data Processor's duties and their personal duties and obligations under such laws and these Clauses.
3.3. The Data Processor shall take reasonable steps to ensure the reliability of any of the Data Processor's employees who have access to Personal Data.

4. RIGHTS OF THE DATA SUBJECT.
The Data Processor shall notify Purchaser within two (2) working days if it receives a request from a Data Subject for access to that person's Personal Data. The Data Processor shall provide Purchaser with full co-operation and assistance in relation to any request made by a Data Subject to have access to that person's Personal Data. The Data Processor shall not

disclose Personal Data to any Data Subject or to a third party other than at the request of Purchaser or as provided for in these Clauses.

5. RIGHTS OF THE PURCHASER.

Purchaser is entitled, on giving at least (two (2) days' notice to the Data Processor, to inspect or appoint representatives to inspect all facilities, equipment, documents and electronic data relating to the processing of Personal Data by the Data Processor; however, the foregoing requirement to give notice will not apply if Purchaser believes that the Data Processor is in breach of any of its obligations under theses Clauses.

6. WARRANTIES.

The Data Processor warrants that (a) it will process Personal Data in compliance with all applicable laws, enactments, regulations, orders, standards and other similar instruments; and (b) it will take appropriate technical and organisational measures against the unauthorised or unlawful processing of Personal Data and against the accidental loss or destruction of, or damage to, Personal Data to ensure Purchaser's compliance with the Applicable Data Protection Law including, but not limited to, the Technical and Organisational Security Measures. The Data Processor shall notify Purchaser immediately if it becomes aware of any unauthorised or unlawful processing, loss of, damage to or destruction of Personal Data.

7. INDEMNITY.

The Data Processor agrees to indemnify and keep indemnified and defend at its own expense Purchaser against all costs, claims, damages or expenses incurred by Purchaser or for which Purchaser may become liable due to any failure by the Data Processor or its employees, agents, subcontractors or Subprocessors to comply with any of its obligations under these Clauses.

8. APPOINTMENT OF SUBPROCESSORS.

The Data Processor may only authorise Subprocessors to process Personal Data (a) subject to Purchaser's prior written consent where the Data Processor has supplied Purchaser with full details of the Subprocessor; (b) provided that the Subprocessor’s contract with respect to Personal Data contains terms which are substantially the same as those set out in these Clauses; and (c) provided that the Subprocessor’s contract with respect to Personal Data terminates automatically upon the termination of the Agreement for any reason.