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. The term "Company", as used herein, shall also mean "Buyer".

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, California Consumer Protection Act, Illinois Biometric Information Privacy Act, 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 from Vendor. The term "Company", as used herein, shall also mean "Buyer".

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 "***Standard Contractual Clauses***" means the contractual clauses adopted by the European Commission pursuant to Commission Decision 2010/87/EUand set out in Annex 2 of this Part B.

1.1.14 **"*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 Annex 1 to this Addendum 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 Annex 1 by written notice to Contracted Processor from time to time as Company reasonably considers necessary to meet those requirements. Nothing in Annex 1 (including as amended pursuant to this section 2.2) confers any right or imposes any obligation on any party to this Addendum.

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. International Data Transfers

9.1 If Company Personal Data is transferred from the EEA, United Kingdom or Switzerland by the Contract Processor to a jurisdiction with respect to which the European Commission has not made a full finding of adequacy or, where the European Commission has made a partial finding of adequacy and the Personal Data being transferred is not covered by such partial adequacy finding, the Standard Contractual Clauses shall apply.

9.2 The parties hereby agree that if a new version of the Standard Contractual Clauses is officially and formally adopted by the EU Commission pursuant to Article 28(7) of the GDPR, such new version shall automatically, without further action of the parties, replace the current version of the Standard Contractual Clauses in Annex 2.

9.3 The Parties hereby agree that if the United Kingdom, as a result of, or in connection with, the United Kingdom leaving the EU, officially and formally adopts its own

version of the Standard Contractual Clauses ("*UK Standard Contractual Clauses*"), the UK Standard Contractual Clauses shall be incorporated herein and shall apply to all transfers of Company Personal Data from the UK to any jurisdiction that is not covered by a UK adequacy finding or relevant partial adequacy finding. For the avoidance of doubt, the Standard Contractual Clauses shall continue to apply with respect to transfers of Company Personal Data from the EEA and Switzerland in accordance with clause 9.1.

10. Audit rights

10.1 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.

11. Additional Responsibilities

11.1 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.

11.2 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.

11.3 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.

12. Remedies, Damages and Indemnification

12.1 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.

13. General Terms

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

ANNEX 1

DETAILS OF PROCESSING OF COMPANY PERSONAL DATA

This Annex 1 includes certain details of the Processing of Company Personal Data as required by Article 28(3) GDPR.

1. Subject matter and duration of the Processing of Company Personal Data

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

2. The nature and purpose of the Processing of Company Personal Data

[Include description here (for example, for business purpose, to comply with legal obligation, etc.)]

3. The types of Company Personal Data to be Processed

[Include list of data types here (for example, Date of Birth, Social Service Number, any information that can be used to identify an EU Resident)]

4. The categories of Data Subject to whom the Company Personal Data relates

[Include categories of data subjects here, (for example, Employee, Former Employee, Beneficiary, Customer, etc.)]

5. The obligations and rights of Company

The obligations and rights of Company are set out in the Principal Agreement and this Addendum.

ANNEX 2

STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

Company (also referred to herein as "**data exporter**") and **Contracted Processor** (also referred to herein as "**data importer**") (each a "**party**", together the "**parties**") have entered into the Principal Agreement pursuant to the terms of which the Contracted Processor may process or store certain Company Personal Data, together with a Data Protection Addendum ("**DPA**") which incorporates the following Standard Contractual Clauses (also referred to herein as the "**Clauses**") in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by data exporter to the data importer of the personal data specified in Appendix I.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the 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 Member State in which the data exporter is established;

(f) *'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.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of

the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect 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, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely […].

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its

obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely […].

4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

Appendix I to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties

Data exporter

The data exporter is: […please specify briefly your activities relevant to the transfer]

Data importer

The data importer is: […please specify briefly your activities relevant to the transfer]

Data subjects

The personal data transferred concern the following categories of data subjects: […]

Categories of data

The personal data transferred concern the following categories of data: […]

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data: […]

Processing operations

The personal data transferred will be subject to the following basic processing activities: […]

Signed for and on behalf of the data importer: _____

Name: _____

Date: _____

Signed for and on behalf of the data exporter: _____

Name: _____

Date: _____

Appendix II to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

[…]