DATA PROCESSOR AGREEMENT

This document was last updated 6 September 2019.

This Data Processor Agreement ("**DPA**") is entered into between:

(1) Center for Innovative OT Solutions, Inc., Address: 4223 South Mason, Suite A Fort Collins, CO 80525 USA hereinafter "**CIOTS**"; and	(2) Name: Address: hereinafter the "**Customer**".

CIOTS and the Customer are jointly referred to as "**Parties**" or individually a "**Party**".

Preamble

WHEREAS CIOTS offers software (the OT Assessment Package, "**OTAP Software**") and corresponding courses for occupational therapists for purposes of training and certifying them in the valid use of a CIOTS assessment tool. The courses are held all over the world. An occupational therapist (the "**Customer**") attending an in-person or online CIOTS training and certification course purchases a software license to use the OTAP Software (as defined below). To complete the training and certification process, the Customer must collect Rater Data (as defined below), enter the Rater Data into the OTAP Software, export a data file with such Rater Data and transfer the data file to CIOTS for Processing. The Processing is necessary to certify the rater in the valid use of a CIOTS assessment tool and continued use of the OTAP Software.

WHEREAS the OTAP Software is locally installed on the Customer's computer or local area network, data stored in the OTAP Software cannot be accessed by CIOTS. Only Rater Data exported and transferred by the Customer to CIOTS is accessible to and processed by CIOTS.

WHEREAS the Customer has purchased a software license to use the OTAP Software, and the Parties have entered into a Software License Agreement (the "**Agreement**"). The following DPA, therefore, is an addition to CIOTS obligations as specified in the Agreement and pertains to the Processing of Rater Data (and other Personal Data, if any) that is transferred by the Customer to CIOTS and CIOTS Processing of that Customer's Rater Data.

NOW, THEREFORE, and in order to ensure an adequate level of protection for all Personal Data resulting from the Agreement and compliance with the Data Protection Law (as defined below), the Parties hereto agree as follows.

1. Definitions

"Agreement" as defined in the Preamble.

“Controller” means the natural or legal person, public authority, agency or other body that, alone or jointly with others, determines the purposes and means of the Processing of Personal Data; where the purposes and means of such Processing are determined by the European Union or EU Member State law, the controller or the specific criteria for its nomination may be provided for by European Union or EU Member State law.

“Controller of the Customer’s Rater Data” means the entity that is the Controller of the Rater Data the Customer transfers to CIOTS during the rater training and certification, i.e. the occupational therapist who owns the OTAP Software license.

“Customer” as defined in the Preamble.

“Data subject” means the natural person to whom Personal Data relates.

“Data Protection Law” means the from time to time applicable laws and regulations with respect to the Processing of Personal Data of European Union citizens, including but not limited to, Regulation (EU) 2016/679 of the European Parliament and of the Council (the “**GDPR**”), Supervisory Authority’s binding decisions, regulations and recommendations and supplementary local adaptions and regulations in respect of data protection.

“OTAP Software” means the software that CIOTS licenses to Customers trained in the *Assessment of Motor and Process* (AMPS), *Evaluation of Social Interaction* (ESI), *School Assessment of Motor and Process Skills* (School AMPS), *Assessment of Compared Qualities — Occupational Performance* (ACQ-OP), or *Assessment of Compared Qualities — Social Interaction* (ACQ-SI).

“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.

“Processing” means any operation or set of operations that 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.

“Processor” means a natural or legal person, public authority, agency or other body that processes Personal Data on behalf of the Controller, e.g. CIOTS when carrying out Rater Data Processing under this DPA.

“Rater Data” the pseudonymized Personal Data that the Customer exports and transfers to CIOTS for rater training and certification, i.e. the Rater Subject’s (i) age, (ii) gender, (iii) general diagnostic category and (iv) test scores; the following are not included in the exported Rater Data transferred to CIOTS: the Rater Subject’s name, hospital- or government-issued identification number or any other identifier code, specific International Classification of Disease diagnostic codes and the final test reports.

“Rater Subject” the person (Data Subject) who agreed to be tested by a Customer in order for the Customer to fulfil the requirements for certification in one of CIOTS assessment tools and from whom the Rater Data in the exported file originates.

“Standard Contract Clauses”, “SCC” or **“the Clauses”** means the European Commission’s Standard Contractual Clauses (Processors) (2010/87/EU), as set out in Appendix 2 herein.

“Subprocessor” means any Processor engaged by CIOTS, or by any other Subprocessor of CIOTS that agrees to receive from CIOTS or from any other Subprocessor of CIOTS, Personal Data exclusively intended for Processing activities to be carried out on behalf of the Customer after the transfer in accordance with the Customer’s instructions, the terms of the Clauses and the terms of the written subcontract.

“Supervisory Authority” means the supervisory authority/supervisory authorities authorized to conduct supervision of Processing of Personal Data or considered to be a supervisory authority concerned under the Data Protection Law.

1.1 Unless otherwise stated, any other term or concept used in capitalized letters in this DPA (except in some cases as part of a heading) shall have the meaning and conception that is established in the Data Protection Law and otherwise in the Agreement, unless the circumstances obviously require another interpretation.

2. Purpose

2.1 The purpose of this DPA is to ensure that CIOTS Processing is carried out in accordance with the applicable requirements for data Processing and obligations under Data Protection Law. This DPA ensures the adequate protection of personal integrity and fundamental rights of individuals during the transfer of Personal Data by the Customer to CIOTS in relation to the Customer's completing of rater training and certification, and thereafter, during the storage of the Personal Data as necessary to verify that the Customer has completed the rater training and certification process and is using the CIOTS assessment tool in a valid and reliable way.

2.2 Under this DPA, CIOTS will only process pseudonymized Personal Data, i.e. Rater Data, in order to fulfill CIOTS obligations to Customers for rater certification required for their use of the OTAP Software in accordance with the Agreement. Hence, it will not be possible for CIOTS to identify the Data Subject behind the Rater Data without additional information by the Customer or the Controller of the Customer's Rater Data.

3. Responsibilities and instructions

3.1 The Customer is the Controller for the Processing of the Personal Data processed under this DPA. The Customer is therefore responsible for complying with Data Protection Law. If another entity is the Controller for Customer's Rater Data, or if the Customer is joint Controller with another entity for the relevant Personal Data, the Customer shall inform CIOTS accordingly. If so, the Customer, by transferring Rater Data, hereby confirms that he or she is authorized or otherwise has obtained permission to transfer Rater Data to CIOTS.

3.2 The type of Personal Data and categories of those Data Subjects that are processed by CIOTS under this DPA, as well as the purpose, nature, duration and object of the Processing, are described in Appendix 1 (Instructions regarding handling of Personal Data).

3.3 Personal Data under this DPA may also be processed if such Processing is required by Union or Member law to which CIOTS or a Subprocessor is subject. If such Processing is required, CIOTS or the Subprocessor shall inform the Customer of the legal requirement before the Processing, unless such information is prohibited according to a public interest under this law.

3.4 During the term of this DPA and thereafter, CIOTS has the right to store and, in other ways, to process data that originates from the Customer, provided that such data are aggregated and rendered irreversibly anonymous, i.e. does not contain Personal Data and, therefore, does not constitute Personal Data in format or contents that are subject to such Processing. The aggregated and anonymous data may be used for research and development purposes.

4. Applicability of Standard Contractual Clauses

4.1 In order to uphold an adequate level of protection during the transfer of the Personal Data by the Customer to CIOTS, the European Commission's Standard Contractual Clauses (Processors) (2010/87/EU) (the "**SCC**") in Appendix 2 shall apply throughout the term as set out herein. The SCC stipulates the specific obligations of the Parties with regard to the data transfer by the Customer to CIOTS and CIOTS Processing thereof.

4.2 In case of any discrepancy between the wording in this DPA and the SCC, the SCC shall in all cases prevail.

5. Security and confidentiality

5.1 CIOTS shall implement appropriate technical and organizational measures, as required by the Data Protection Rules, to ensure a level of security appropriate to the risk, to protect Personal Data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to such Personal Data. Such measures include measures to protect Personal Data required by article 32 of the GDPR.

5.2 CIOTS undertakes to ensure that persons authorized to process Personal Data have undertaken confidentiality obligations as regards the Processing of Personal Data. CIOTS will not disclose Personal Data or other information concerning the Processing of Personal Data to a third party, with the exception of CIOTS Subprocessors, without explicit instructions from the Customer, and unless such disclosure is required under the Data Protection Rules.

5.3 To fulfil the security requirements provided for in this DPA, CIOTS has implemented the security measures that are laid out in Appendix 1. The Customer confirms that these measures are, according to the Customer's reasonable judgment, sufficient to meet the Controller's needs. If the Customer requests additional security measures, CIOTS shall try to meet such requirements as far as possible, with fair compensation by the Customer requesting additional security measures.

6. Assistance

6.1 In the event CIOTS receives a request for information from a Rater Subject, Supervisory Authority or other third party regarding the Processing of Personal Data, CIOTS shall, without undue delay, forward such request to the Customer if and to the extent allowed under applicable Data Protection Rules.

6.2 By technical and organizational measures that are appropriate, taking into account the nature of the Processing, CIOTS shall assist the Customer, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests from the Rater Subject when a Rater Subject exercises its rights in accordance with the Data Protection Law.

6.3 CIOTS shall also, to a reasonable extent, and taking into account the nature of Processing and the information available to CIOTS, support the Customer in assisting Rater Subjects in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR.

6.4 CIOTS shall, without delay, inform the Customer of any suspicion of or established data breach as regards the Personal Data that are processed by CIOTS hereunder and will, with fair compensation, assist the Customer in distributing information and reports as required under Data Protection Rules.

6.5 CIOTS shall assist the Customer in fulfilling potential duties to enable data portability regarding Rater Data being processed by CIOTS.

6.6 Due to the nature of the Processing, CIOTS requires, as a precondition for CIOTS to be able to fulfil requests according to this section 6, that the Customer provides CIOTS with the necessary additional information in order to de-pseudonymize the Rater Data, if necessary.

7. Contact with Supervisory Authority

7.1 CIOTS shall inform the Customer of any contacts from the Supervisory Authority concerning the Processing of Personal Data under this DPA. CIOTS is not entitled to represent the Customer or act on behalf of the Customer in relation to the Supervisory Authority if not required by Data Protection Law.

8. Subprocessors

8.1 The Customer hereby gives CIOTS prior general authorization to engage Subprocessors in the Processing of Personal Data, provided that CIOTS enters into a written agreement that imposes corresponding Data Protection obligations on the Subprocessor as set out in this DPA and the SCC.

8.2 CIOTS shall inform the Customer of any intended changes concerning the addition or replacement of a Subprocessor by e-mail or through the CIOTS website www.innovativesolutions.com, thereby giving the Customer the opportunity to object to such changes. If the Customer objects to CIOTS using a certain Subprocessor, the Customer shall compensate CIOTS as set out in Section 12.

8.3 If CIOTS uses Subprocessors according to article 8.1 above, CIOTS is responsible for the Subprocessor fulfilling all the obligations and respecting all the limits set out in this DPA towards CIOTS.

9. Transfers of Personal Data outside the EU/EEA

9.1 CIOTS is an American corporation established in Colorado, USA. In other words, when performing the rater training and certification, the Rater Data will be transferred by the Customer to CIOTS, i.e. transferred outside the EU/EEA. The provisions in this DPA, with appendices, governs such transfer and thus the SCC in Appendix 2 will ensure the adequate level of protection for the transferred Personal Data.

9.2 CIOTS or a Subprocessor may transfer Rater Data to a place outside the EU/EEA provided that CIOTS ensures that there is a lawful basis for the transfer under the Data Protection Law, e.g. through the application of the SCC for the transfer of Personal Data to a third country, or provisions that replace these.

10. Audits

10.1 CIOTS shall provide the Customer with all information required to comply with the obligations according to this DPA and Data Protection Law within reasonable time after such request has been made by the Customer to CIOTS.

10.2 CIOTS shall enable and contribute to audits, including inspections carried out by the Customer or by another independent auditor selected by the Customer, and that CIOTS may reasonably accept. The auditor is required to sign sufficient confidentiality agreements provided by CIOTS prior to audits. The Customer has the right to perform one audit per year without cost, including audits performed on the Customer's behalf. If the Customer would like to carry out additional audits the Customer must compensate CIOTS for all costs associated with the audit/audits.

10.3 CIOTS shall, regarding the obligations stated in section 8 of this DPA, immediately inform the Customer if CIOTS considers an instruction to be in violation of Data Protection Law.

11. Confidentiality

11.1 CIOTS shall, where applicable, comply with national legislation applicable to classified or confidential information. CIOTS undertakes to ensure that personnel authorized to process Personal Data under this DPA have undertaken to observe confidentiality for the Processing or are subject to applicable statutory duty of confidentiality.

11.2 Section 10.1 above does not apply to information requested by a Supervisory Authority in accordance with Data Protection Law or other statutory obligation.

11.3 The confidentiality obligation also applies after the Agreement and/or the DPA has ceased to apply.

12. Compensation

12.1 CIOTS shall be entitled to fair compensation for all work, costs and expenditures stemming from or related to:

(i) instructions for Processing from the Customer that exceed the functionalities and the level of security that CIOTS normally offers its clients, or that require CIOTS to make special adjustments for the Customer in the OTAP Software or otherwise;

(ii) CIOTS performance of any of its undertakings under sections 5, 6 and 10; or

(iii) the Customer's objection to a new Subprocessor pursuant to section 8.

13. Liability

13.1 If CIOTS, any person acting under the authority of CIOTS or a Subprocessor, processes Personal Data in violation of this DPA or contrary to the documented lawful instructions that the Customer has provided CIOTS, CIOTS shall, in consideration of the limitation of liability arising from the Agreement, compensate the Customer for direct damages due to the wrongful Processing.

13.2 During the term of this DPA and thereafter, the Customer shall indemnify and hold CIOTS harmless from any direct and indirect damage, including claims from Data Subjects and third parties, that CIOTS has suffered due to unclear, inadequate or unlawful instructions from the Customer, or otherwise, depending on the circumstances deriving from the Customer.

13.3 CIOTS obligation to pay damages, laid down in section 13.1 above, only applies, provided that i) the Customer without undue delay informs CIOTS in writing of any claims against the Customer; and ii) the Customer allows CIOTS to control the defense of the claim and make independent decisions regarding settlement.

13.4 This section 13 shall not be considered as limiting any of the Parties' liability towards Data Subjects set out in Clause 6 of the SCC.

14. Term and Termination

14.1 This DPA enters into force when duly signed by both Parties either separately as an amendment to the Agreement or as a part of the Agreement and remains in force as long as CIOTS is Processing Personal Data on behalf of the Customer.

14.2 Upon termination of the Agreement or this DPA (depending on which occurs first), CIOTS shall, in accordance with the Customer's instructions, delete or return the Personal Data that CIOTS is Processing to the Customer and make sure that all Subprocessors do the same.

14.3 If the Customer has not requested that the Personal Data should be deleted, CIOTS shall delete the Personal Data not later than one-hundred-and-eighty (180) days after the termination of the DPA or the Agreement (whichever occurs first). CIOTS shall delete any existing copies unless the storage of Personal Data is required by Union law or the national law of the Member State.

14.4 When deleting Personal Data, CIOTS may, in accordance with section 3.4 of this DPA, aggregate and render Rater Data irreversibly anonymous for research and development purposes.

15. Transfer of the DPA

15.1 The Customer has the right to transfer the rights and/or obligations under this DPA (including but not limited to the rights and/or obligations as set forth in the SCC), at any time, to its employer or principal if the Agreement is transferred to such party. If so, the Customer shall notify CIOTS about the transfer in writing.

16. Amendments

16.1 If any applicable Data Protection Laws are changed during the term of this DPA, or if the Supervisory Authority issues guidelines, decisions or regulations concerning the application of the Data Protection Law that result in this DPA no longer meeting the requirements for a DPA, the Parties shall make the necessary changes to this DPA in order to meet such new or additional requirements. Such changes shall enter into force no later than thirty (30) days after a Party sends a notice of change to the other Party or otherwise no later than prescribed by the Data Protection Law, guidelines, decisions or regulations of the Supervisory Authority.

16.2 Other amendments to this DPA, in order to be binding, must be made in writing and duly signed by both Parties.

17. Miscellaneous

17.1 This DPA supersedes and replaces all prior DPAs between the Parties and supersedes any deviating provisions of the Agreement concerning the subject matter of this DPA, regardless if otherwise stated in the Agreement.

17.2 In addition, the terms of the Agreement shall also apply to CIOTS Processing of Personal Data and the obligations under this DPA. However, in the event of contradictions between the provisions of the Agreement and this DPA, the provisions of the DPA will supersede regarding all Processing of Personal Data. The provisions of the Agreement may not restrict or modify any of the obligations of this DPA.

17.3 This DPA, including appendices, shall be governed by the law and subject to the forum(s) set out in the SCC in Appendix 2.

* * * *

This DPA has been drawn up in duplicates whereof each Party has taken one each.

Place:	Place:
Date:	Date:
Center for Innovative OT Solutions, Inc.	Customer
_________________________________	_________________________________
Signature (CIOTS representative)	Signature (occupational therapist)
_________________________________	_________________________________
Name (printed)	Name (printed)

Appendix 1 – Data Processing and IT security measures

In the following data Processing and IT security measures, all capitalized words shall have the same meaning as defined in the DPA, unless otherwise expressly stated.

Data Processing measures

Purposes Please specify all purposes for which the Personal Data will be processed by CIOTS as the Customer's data Processor	CIOTS processes Personal Data for the purpose of certifying the occupational therapist Customer in the use of one of CIOTS assessment tools, fulfilling the service under the Agreement and to enable the Customer to use the OTAP Software in professional activities.
Categories of data Please specify the Personal Data that will be processed by CIOTS as data Processor	CIOTS processes data regarding Rater Subjects transferred by the Customer to CIOTS when using CIOTS services, i.e. Rater Data: i. age, ii. gender, iii. general diagnostic category, and iv. test scores. CIOTS does not process any Personal Data other than the Rater Data. CIOTS does not process sensitive Personal Data, e.g. race, ethnic origin, religious or philosophical views, sexual orientation, political opinions, or membership in professional unions. The Customer is responsible for ensuring that sensitive Personal Data are not transferred to CIOTS.
Categories of Data Subjects Please specify the categories of Data Subjects whose Personal Data will be processed by CIOTS as data Processor	CIOTS processes the following categories of Data Subjects: • Rater Subjects that appear in such material, i.e. exported data files, that the Customer transfers to CIOTS during rater training and certification.
Retention requirements Please specify the retention time of Personal Data stored by CIOTS	The Personal Data must be deleted at the Customer's request and according to the Customer's instructions. CIOTS has a retention period of one-hundred-and-eighty (180) days after the termination of the Agreement or DPA in accordance with the obligations set forth in the DPA.

IT security measures

Access control	Access to data is limited to CIOTS staff via account permissions.
Back-up	CIOTS runs backups daily and monthly. Daily backups are retained for twenty-one (21) days; monthly backups are retained for one-hundred-and-eighty (180) days before they are permanently deleted.
Logging of access to personal data	None.

Authorization and authorities	Specified CIOTS staff web application administrators are given role-based access via username/password-protected accounts.
Encryption of data communication	Data are encrypted in communication via Secure Socket Layer (SSL); they are not encrypted at rest.
Deletion	Upon request from the Customer or a Data Subject, and otherwise one-hundred-and-eighty (180) days after the termination of the DPA or the Agreement, whichever comes first.
Service and repairs of units where personal data are stored	Handled by Subprocessor, DreamHost, LLC.
Firewalls, separation of environments and anti-virus protection	Site secured by our Subprocessor, Dreamhost, LCC, through their DreamShield malware remover and mod_security web application firewall for apache. More information can be found at https://www.dreamhost.com/security. DreamHost, LLC, access is only granted for support as needed.

APPENDIX 2 – STANDARD CONTRACTUAL CLAUSES FOR THE TRANSFER OF PERSONAL DATA

EUROPEAN COMMISSION
DIRECTORATE-GENERAL JUSTICE

Directorate C: Fundamental rights and Union citizenship
Unit C.3: Data protection

Commission Decision C(2010)593
Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

(1) **The Customer**, as defined in the DPA to which these Clauses are attached as an Appendix 2, (the "**data exporter**");

and

(2) **CIOTS,** as defined in the DPA to which these Clauses are attached as Appendix 2 (the "**data importer**");

(each a "**Party**"; and together the "**Parties**"),

HAVE AGREED on the following Contractual Clauses (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 the data exporter to the data importer of the personal data specified in Appendix 1.

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[1];

(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

[1] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

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 subprocessor 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 subprocessor 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 subprocessor 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 subprocessing 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 subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor 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 subprocessing, 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 subprocessing, it has previously informed the data exporter and obtained its prior written consent;

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

(j) to send promptly a copy of any subprocessor 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 subprocessor 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 subprocessor 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 subprocessor 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 subprocessor 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 subprocessor agrees that the data subject may issue a claim against the data subprocessor 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 subprocessor 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 subprocessor, 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 subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, 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.

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

Subprocessing

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 subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses[2]. Where the subprocessor 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 subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor 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 subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing 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.
4. The data exporter shall keep a list of subprocessing 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 subprocessor 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 subprocessor 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 1 – Description of the Transfer

Data exporter

The data exporter has contracted the data importer for certain activities including the processing of personal data on its behalf as further described and set out in the DPA to which these Standard Contractual Clauses makes an integral part. As part of the processing, personal data needs to be transferred outside EU.

Data importer

[2] This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

The data importer has been contracted by the data exporter to process personal data on the data exporters behalf as further described and set out in the DPA to which these Standard Contractual Clauses makes an integral part. As part of the processing, personal data needs to be transferred outside EU.

Data subjects

The personal data transferred concern the categories of data subjects as set out in the DPA and Appendix 1 to the DPA that the Parties have entered into.

Categories of data

The personal data transferred concern the categories of data as set out in the Appendix 1 to the DPA.

Processing operations

The personal data transferred will be subject to the processing activities set out in Appendix 1 to the DPA.

Appendix 2 – Security Measures

The technical and organizational security measures implemented by the data importer is further described and set out in Appendix 1 to the DPA.