**DATA PROCESSING ADDENDUM**
**SHOWBIE**

This Data Processing Addendum, dated as of _____ ("**Addendum**"), by _____ and between (the "**Controller**"), and **SHOWBIE Inc. DBA Showbie**, a Canadian corporation (the "**Service Provider**") (collectively referred to as the **"Parties"**), sets forth the terms and conditions relating to the privacy, confidentiality and security of Personal Data (as defined below) associated with services to be rendered by the Service Provider to the Controller pursuant to Showbie's Terms of Use and the order submitted by the Controller for the Services (together, the "**Master Agreement**").

## Introduction

This agreement is made in light of the requirements set out in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (the "**GDPR**") and applicable Data Protection Legislation (as that term is defined below). Definitions used in this agreement shall have the same meaning as set out in the GDPR. This agreement is based on the requirements set out in article 28 of the GDPR.

The purpose of this Agreement is to ensure that Service Provider provides the services under the Master Agreement ("**Services**") to Customer in a manner that complies with the Data Protection Legislation.

Whereas, the Controller or its employees, agents, consultants or contractors (collectively, "**Controller Personnel**") shall provide the Service Provider with access to Personal Data in connection with certain services performed by the Service Provider for or on behalf of the Controller pursuant to the Master Agreement; and

Whereas, the Controller requires that the Service Provider preserve and maintain the privacy, confidentiality, and security of such Personal Data.

Now therefore, in consideration of the mutual covenants and agreements in this Addendum and the Master Agreement and for other good and valuable consideration, the sufficiency of which is hereby acknowledged, the Controller and Service Provider agree as follows:

## I. Definitions

a. **"Applicable Law"** means all applicable European Union ("EU") or national laws and regulations relating to the privacy, confidentiality, security and protection of Personal Data, including, without limitation: the European Union ("EU") General Data Protection Regulation 2016/ 679 ("GDPR"), and EU Member State laws supplementing the GDPR; the EU Directive 2002/ 58/ EC ("e- Privacy Directive"), as replaced from time to time, and EU Member State laws implementing the e-Privacy Directive, including laws regulating the use of cookies and other tracking means as well as unsolicited e-mail communications.

b. "**Data Controller**" has the meaning set out in the Applicable Law.

c. "**Data Processor**" has the meaning set out in the Applicable Law.

d. **"Data Security Measures"** means technical and organizational measures that are

aimed at ensuring a level of security of Personal Data that is appropriate to the risk of the Processing, including protecting Personal Data against accidental or unlawful loss, misuse, unauthorized access, disclosure, alteration, destruction, and all other forms of unlawful Processing, including measures to ensure the confidentiality of Personal Data.

e. **"Data Subject"** means an identified or identifiable natural person to whom the Personal Data pertains.

f. **"Instructions"** means this Addendum and any further written agreement or documentation through which the Data Controller instructs the Data Processor to perform specific Processing of Personal Data.

g. "**Notification Related Costs**" means the Controller's and its affiliates' internal and external costs associated with investigating, addressing and responding to a Personal Data Breach, including but not limited to: (i) preparation and mailing or other transmission of any notifications or other communications to customers, potential customers, clients, employees, agents or others as Controller deems reasonably appropriate; (ii) establishment of a call center or other communications procedures in response to such Personal Data Breach (e.g., customer service FAQs, talking points and training); (iii) public relations and other similar crisis management services; (iv) legal, accounting, consulting and forensic expert fees and expenses associated with the Controller's and its affiliates' investigation of and response to such Personal Data Breach; and (v) costs for commercially reasonable credit monitoring, identity protection services or similar services
    i. that Controller determines are advisable under the circumstances.

h. "**Personal Data**" means any information relating to an identified or identifiable natural person Processed by the Service Provider in accordance with the Controller's Instructions pursuant to this Addendum; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

i. "**Personal Data Breach**" a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.

j. "**Process**", "**Processed**", or "**Processing**" means any operation or set of operations performed upon 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.

k. "**Sub-Processor**" means the entity engaged by the Data Processor or any further Sub- Processor to Process Personal Data on behalf and under the authority of the Data Controller.

1.

## II. Roles and Responsibilities of the Parties

a. The Parties acknowledge and agree that the Controller is acting as a Data Controller and has the sole and exclusive authority to determine the purposes and

means of the Processing of Personal Data under this Addendum, and the Service Provider is acting as a Data Processor on behalf and under the Instructions of the Controller.

b. Any Personal Data will at all times be and remain the sole property of the Controller and the Service Provider will not have or obtain any rights therein.

## III. Obligations of the Service Provider

The Service Provider agrees and warrants to:

a. Process Personal Data disclosed to it by the Controller only on behalf of and in accordance with the Instructions of the Controller and Annex 1 of this Addendum, unless the Service Provider is otherwise required by Applicable Law, in which case the Service Provider shall inform the Controller of that legal requirement before Processing the Personal Data, unless informing the Controller is prohibited by law on important grounds of public interest. The Service Provider shall immediately inform the Controller if, in the Service Provider's opinion, an Instruction provided infringes Applicable Law.

b. Hold in strict confidence (i) the existence and terms of the Master Agreement (including this Addendum), and any related agreement, and (ii) any and all Personal Data.

c. Ensure that any person authorized by the Service Provider to process Personal Data in the context of the Services is subject to a duly enforceable contractual or statutory confidentiality obligation, and only processes Personal Data in accordance with the Instructions of the Controller.

d. The Service Provider is based in Canada and avails of the European Commission decision approving data transfers to Canada pursuant to the 2002/2/EC Commission Decision of 20 December 2001. The Service Provider may transfer and process Personal Data received from or on behalf of the Controller to third parties (which shall include without limitation any affiliates of the Service Provider) with the authorization of the Controller. A list of such third parties is included at Annex 1. The Controller hereby authorizes transfers to these third parties. Where a third party is located outside the European Economic Area, the Service Provider shall, in advance of any such transfer, ensure that the transfer is permitted under the GDPR, which may include:

   a) that the third party execute Standard Contractual Clauses for transfers from Data Controllers to Data Processors approved by the Commission pursuant to Decision 2010/87/EU, as amended by Commission Implementing Decision (EU)2016/2297, a copy of which is attached at Appendix III;

   b) the third party to be certified under a framework approved by the European Commission to facilitate such transfers; or

   c) the existence of any other specifically approved safeguard for data transfers (as recognized under the GDPR) and/or a European Commission finding of adequacy.

e. Inform the Controller promptly and without undue delay of any formal requests from Data Subjects exercising their rights of access, correction or erasure of their Personal Data, their right to restrict or to object to the Processing, as well as their right to data portability, and not respond to such requests, unless instructed by the Controller in writing to do so. Taking into account the nature of the Processing of Personal Data, the Service Provider shall assist the Controller, by appropriate technical and organizational measures, insofar as possible, in fulfilling the Controller's obligations to respond to a Data Subject's request to exercise their rights with respect to their Personal Data.

f. Notify the Controller immediately in writing of any subpoena or other judicial or administrative order by a government authority or proceeding seeking access to or disclosure of Personal Data. The Controller shall have the right to defend such action in lieu of and on behalf of the Service Provider. The Controller may, if it so chooses, seek a protective order. The Service Provider shall reasonably cooperate with the Controller in such defense.

g. Provide reasonable assistance to the Controller in complying with the Controller's obligations under Applicable Law.

h. Maintain internal record(s) of Processing activities, copies of which shall be provided by the Service Provider to the Controller or supervisory authorities upon request. Such records must contain at least: (i) the name and contact details of the Service Provider; (ii) the categories of Processing activities carried out under this Addendum; (iii) information on data transfers to a third country or a third party, where applicable; and (iv) a general description of the Data Security Measures implemented to protect Personal Data processed under this Addendum.

## IV Sub-Processing

Where the Data Processor engages another processor (sub-processor) for carrying out specific processing activities on behalf of the Data Controller, the same data protection obligations as set out this processor agreement or other legal act between the Data Controller and the processor as referred to in article 28, paragraph 3, of the GDPR, shall be imposed on that other processor (sub-processor) by way of contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR. Where that other processor (sub-processor) fails to fulfill its data protection obligations, the initial Data Processor shall remain fully liable to the Data Controller for the performance of that other processor's (sub-processor's) obligations. Data Controller agrees that Data Processor is engaging these sub-processors and hereby provides general authorization for Data Processor to engage any sub-processors to provide similar or related services. Data Processor shall provide Data Controller with at least 14 days' prior notice of any new sub-processors. Notification of sub-processors will be sent to Data Controller via email. If, within 7 days of receipt of that notice, Data Controller notifies Data Processor in writing of any objections (on reasonable grounds) to the proposed appointment, Data Processor shall work with Data Controller in good faith to make available a commercially reasonable change in the provision of the Services which avoids the

use of that proposed sub-processor; and where such a change cannot be made within 14 days from Data Processor's receipt of Data Controller 's notice, Data Controller may by written notice to Data Processor with immediate effect terminate the Services Agreement to the extent that it relates to the Services which require the use of the proposed sub-processor.

## V Compliance with Applicable Laws

a. The Service Provider represents and warrants that no Applicable Law, or legal requirement, or privacy or information security enforcement action, investigation, litigation or claim prohibits the Service Provider from fulfilling its obligations under this Addendum.

b. The Service Provider shall in good faith negotiate any further Data Processing Agreement reasonably requested by the Controller for purposes of compliance with the Applicable Law. In case of any conflict between this Addendum and the Master Agreement, this Addendum shall prevail with regard to the Processing of Personal Data covered by it.

c. The Service Provider shall comply with all Applicable Laws.

## VI Data Security

The Service Provider shall develop, maintain, and implement a comprehensive written information security program that complies with Applicable Law including, but not limited to, the Data Security Measures described in Annex 2 of this Addendum. The Service Provider's information security program shall include appropriate administrative, technical, physical, organizational and operational safeguards and other security measures designed to (i) ensure the security and confidentiality of Personal Data; (ii) protect against any anticipated threats or hazards to the security and integrity of Personal Data; and (iii) protect against any Personal Data Breach, including, as appropriate:

a. The pseudonymization and encryption of the Personal Data;

b. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;

c. The ability to restore the availability and access to the Personal Data in a timely manner in the event of a physical or technical incident; and

d. A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures adopted pursuant to this provision for ensuring the security of the Processing.

A) The Service Provider shall supervise Service Provider Personnel to the extent required to maintain appropriate privacy, confidentiality and security of Personal Data. The Service Provider shall provide training, as appropriate, regarding the privacy, confidentiality and information security requirements set forth in this Addendum to all Service Provider Personnel who have access to Personal Data.

B) Promptly upon the expiration or earlier termination of the Master Agreement, or such earlier time as the Controller requests, the Service Provider shall return to the Controller or its designee, or at the Controller's request, securely destroy or render unreadable or indecipherable if return is not reasonably feasible or desirable to the Controller (which decision shall be based solely on the Controller's written statement), each and every original and copy in every media of all Personal Data in the Service Provider's, its affiliates' or their respective subcontractors' possession, custody or control. Promptly following any return or alternate action taken to comply with this Clause VI(C), the Service Provider shall provide to the Controller a completed certificate certifying that such return or alternate action occurred. In the event applicable law does not permit the Service Provider to comply with the delivery or destruction of the Personal Data, the Service Provider warrants that it shall ensure the confidentiality of the Personal Data and that it shall not use or disclose any Personal Data after termination of this Addendum.

**VII. Data Breach Notification**

A. The Service Provider shall immediately inform the Controller in writing of any Personal Data Breach of which the Service Provider becomes aware, but in no case longer than seventy two (72) hours after it becomes aware of the Personal Data Breach. The notification to the Controller shall include all available information regarding such Personal Data Breach, including information on:

   a. The nature of the Personal Data Breach including where possible, the categories and approximate number of affected Data Subjects and the categories and approximate number of affected Personal Data records;

   b. The likely consequences of the Personal Data Breach; and

   c. The measures taken or proposed to be taken to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

The Service Provider shall promptly take all necessary and advisable corrective actions, and shall cooperate fully with the Controller in all reasonable and lawful efforts to prevent, mitigate or rectify such Breach. The Service Provider shall provide such assistance as required to enable the Controller to satisfy the Controller's obligation to notify the relevant supervisory authority and Data Subjects of a personal data breach under Articles 33 and 34 of the GDPR. The content of any filings, communications, notices, press releases or reports on any Personal Data Breach must be approved by the Controller prior to any publication or communication thereof. The Service Provider shall be responsible for the costs and expenses associated with the performance of its obligations described in this paragraph, unless the Personal Data Breach is caused by the acts or omissions of the Controller or its affiliates.

B. In the event of a Personal Data Breach involving Personal Data in the Service Provider's possession, custody or controller for which the Service Provider is otherwise responsible, the Service Provider shall reimburse the Controller on demand for all commercially reasonable Notification Related Costs incurred by the Controller arising out of or in connection with any such Personal Data Breach.

## VIII. Audit

Service Provider shall on written request (but not more than once per year, other than in the event of a breach) make available to the Controller all information necessary to demonstrate compliance with the obligations set forth in this Addendum and, at the Controller's expense, allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller. Upon prior written request by the Controller (provided that it shall be not more than once per year other than in the event of a breach), the Service Provider agrees to cooperate and, within reasonable time, provide the Controller with:

(a) audit reports and all information necessary to demonstrate Service Provider's compliance with the obligations laid down in this Addendum; and

(b) confirmation that the audit has not revealed any material vulnerability in the Service Provider's systems, or to the extent that any such vulnerability was detected, that the Service Provider has fully remedied such vulnerability. The Service Provider's failure to comply with this obligation shall entitle the Controller to suspend the Processing of Personal Data Processed by the Service Provider, and to terminate any further Processing of Personal Data, this Addendum and/or the Master Agreement, if doing so is required to comply with Applicable Law.

## IX. Injunctive Relief

The Service Provider agrees that any Processing of Personal Data in violation of this Addendum, the Controller's Instructions or any Applicable Law, or the occurrence of any Personal Data Breach, will cause immediate and irreparable harm to the Controller for which money damages will not constitute an adequate remedy. Therefore, the Service Provider agrees that the Controller may seek and be granted specific performance and injunctive or other equitable relief for any such violation or incident, in addition to its remedies at law, without proof of actual damages.

## X. Liability

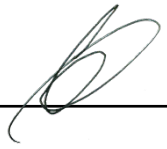
The Service Provider agrees to indemnify and hold the Controller harmless from and against any direct damages, fines, costs or expenses that it may incur or that arise out of or in connection with a third party claim relating to any violation of this Addendum.

## IX. Governing Law

To the extent required by Applicable Law, this Addendum shall be governed by the law of **Ireland.** In all other cases, this Addendum shall be governed by the laws of the jurisdiction specified in the Agreement.

**IN WITNESS WHEREOF**, the parties acknowledge their agreement to the foregoing by due execution of the Addendum by their respective authorized representatives.

**Showbie**

Signature: 

Name: ColinBramm

Title: CEO and Cofounder

Address: #1400, 10117 Jasper Avenue, Edmonton, AB Canada T5J 1W8

Phone: 1.866. 925. 3904

Date: May 1, 2018

**School/district**

Signature: _____

Name: _____

Title: _____

Address: _____

Phone: _____

Date _____

## ANNEX 1: SCOPE OF THE DATA PROCESSING

This Annex forms part of the Data Processing Addendum between the Controller and the Service Provider.

**The Processing of Personal Data concerns the following categories of Data Subjects:**

1) Teachers and Administrators
2) Students
3) Parents

**The Processing concerns the following categories of Personal Data:**

1) User's login information and usage within the Service
2) User profile information
3) Student assignments, grades, interactions and messaging
4) IP address
5) Location
6) School name

**The Processing concerns the following categories of Sensitive Data:**

Status as a student at a religious school, if applicable.

**The Processing concerns the following categories of data Processing activities (i.e., purposes of Processing):**

1) Purpose of processing Customer user login and platform information solely to provide the Services.
2) Purpose of managing Student assignments, grades, and progress.

**The duration of data processing is the duration of the contract.**

**The Service Provider uses the following Sub-Processors and such use is hereby authorized by the Data Controller:**

Amazon Web Services (USA)
Amplitude (USA)
Apple (USA)
Chartio (USA)
ChurnZero (USA)
Close.io (USA)
Cloudfront (USA)
ConvertAPI (Lithuania)
Customer.io (USA)
Fuel Education (USA)
Google (USA)
Intercom (USA)
PersistIQ (USA)
Productboard (USA)
Recurly (USA)
Segment.io (USA)
Sentry (USA)
Slack (USA)
Stripe (USA)
Typeform (Spain)

Whereby (Norway)
Xero (New Zealand)
Zapier (USA)

**The Service Provider is based in Canada and avails of the European Commission approving data transfers to organizations where the data processing is covered by PIPEDA. However, it may transfer and process personal information to and in the following jurisdictions outside of the EU:**

United States
South America
Asia
Australia

## ANNEX 2: DATA SECURITY MEASURES

This Annex forms part of the Data Processing Addendum between the Controller and the Service Provider. Taking into account the state of the art, the costs of implementation and the nature, scope, content and purpose of the Processing, the Service Provider agrees to implement the following Data Security Measures:

### 1. Physical access control

Physical access controls to restrict access to sensitive information, including:

- Devices are password protected;
- Devices are locked when left unattended;
- Physical devices and documents are stored in locked locations;
- All devices have tracking software enabled;

### 2. Logical access control

Technical and organizational measures to prevent data Processing systems from being used by unauthorized persons, including:

- User identification and authentication procedures;
- ID/password security procedures (special characters, minimum length, change of password);
- Automatic blocking (e.g., password or timeout);
- Monitoring of break-in-attempts and temporary turn-off of the user ID upon ten erroneous passwords attempts;
- Creation of one master record per user, user master data procedures, per data Processing environment;
- Encryption and pseudonymization:
  - Transmission of data between Showbie devices, thin clients, and servers are encrypted using TLS protocol. This ensures the privacy of the transmitted information and prevents unauthorized users from viewing data.
  - All files are encrypted at rest. We use Amazon's Server Side Encryption to manage the encryption of our files.
  - All databases are encrypted at rest. We use Amazon's KMS to manage the encryption of our database.
  - Our encryption uses 256-bit keys on a symmetric algorithm AES.
  - Data transmissions are encrypted using TLSv1.X protocols. We implement SSL certificates with RSA algorithm and key sizes of 256 bit.

### 3. Data access control

Technical and organizational measures to ensure that persons entitled to use a Data Processing system gain access only to such Personal Data in accordance with their access rights, and that Personal Data cannot be read, copied, modified or deleted without authorization, including:

- Control authorization schemes;
- Differentiated access rights on an as-needed basis (profiles, roles, transactions, and objects);

- Monitoring and logging of accesses;
- Disciplinary action against employees who access personal data without authorization;
- Reports of access;
- Access procedure;
- Change procedure;
- Deletion procedure;
- Encryption and pseudonymization;
- Login protections as described in Section 2 above.

## 4. Disclosure control

Technical and organizational measures to ensure that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media (manual or electronic), and that it can be verified to which companies or other legal entities Personal Data are disclosed, including:

- Logging;
- Transport security;
- Encryption and pseudonymization; and
- Login protections as described in Section 2 above.

## 5. Entry control

Technical and organizational measures to monitor whether data have been entered, changed or removed (deleted), and by whom, from data Processing systems, including:

- Logging and reporting systems;
- Audit trails and documentation.

## 6. Control of instructions

Technical and organizational measures to ensure that Personal Data are Processed solely in accordance with the Instructions of the Controller, including:

- Unambiguous wording of the contract;
- Formal commissioning (request form);
- Criteria for selecting the Processor;
- Process for making changes, including deleting, user data upon request from an authorized administrator or teacher at a school or district using this form: https://showbie.typeform.com/to/y1bMQz;
- Request from parents or students will be forwarded to the Controller;
- Data deletions are permanent and data cannot be recovered.

## 7. Availability control

Technical and organizational measures to ensure that Personal Data are protected against accidental destruction or loss (physical/logical), including:

- Redundancies;
- Backup procedures;
- Cloud-based infrastructure;
- Mirroring of hard disks;
- Uninterrupted power supply;
- Remote storage;
- Strong firewall systems;
- Continual security updates;
- Regular testing;
- Automated third-party audit tools to assess web applications;
- Security training for Showbie employees;
- Disaster recovery plan.

Showbie's cloud-based service utilizes Amazon's AWS. Redundancies are built alongside scaling allowing Socrative to have an up time of 99.9999%. Internal monitoring infrastructure provides visibility into our systems and provides notifications of any anomalies allowing problems to be remedied before they escalate into serious issues.

Regular testing is conducted to ensure regressions do not surface and also to improve reliability and quality of our applications. We use automated third-party audit tools to assess our web applications.

## 8. Separation control

Technical and organizational measures to ensure that Personal Data collected for different purposes can be Processed separately, including:

- Separation of databases;
- "Internal client" concept / limitation of use;
- Segregation of functions (production/testing);
- Procedures for storage, amendment, deletion, transmission of data for different purposes

## 9. Encryption of data

Transmission of data between Showbie devices, thin clients, and servers are encrypted using TLS protocol. This ensures the privacy of the transmitted information and prevents unauthorized users from viewing data.

- All files are encrypted at rest using Amazon's Server Side Encryption.
- All databases are encrypted at rest using Amazon's KMS.
- Encryption uses 256 bit keys on a symmetric algorithm AES.
- Data transmissions are encrypted using TLSv1.X protocols. We implement SSL certificates with RSA algorithm and key sizes of 256 bit.

## ANNEX 3: STANDARD CONTRACTUAL CLAUSES

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

Name of the data exporting organisation:.....

Address:.....

Tel.:..... ; fax:..... ; e-mail:.....

Other information needed to identify the organisation:

……
(the data exporter)

And
Name of the data importing organisation:.....
Address:.....

Tel.:..... ; fax: ..... ; e-mail: .....

Other information needed to identify the organisation:

……
(the data importer)
each a "party"; 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;

(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 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, 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 subprocessor 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 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.

On behalf of the data exporter:
Name (written out in full):
Position:
Address:
Other information necessary in order for the contract to be binding (if any):

Signature…….

(stamp of organisation)

On behalf of the data importer:
Name (written out in full):
Position:
Address:
Other information necessary in order for the contract to be binding (if any):

Signature…….

(stamp of organisation)

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.
The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.
Data exporter
The data exporter is (please specify briefly your activities relevant to the transfer):

Data importer
The data importer is (please specify briefly activities relevant to the transfer):

Data subjects
The personal data transferred concern the following categories of data subjects (please specify):

Categories of data
The personal data transferred concern the following categories of data (please specify):

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data (please specify):

Processing operations
The personal data transferred will be subject to the following basic processing activities (please specify):

DATA EXPORTER

Name:……

Authorised Signature ……

DATA IMPORTER

Name:……

Authorised Signature ……

APPENDIX 2 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 attatched