DATA PROCESSING AGREEMENT
SOCRATIVE

[CUSTOMER] ("**Customer**"), on behalf of itself, and for the benefit of its Affiliates, has contracted with Showbie, Inc. ("**Vendor**") (maker of Socrative), to perform certain processing functions on behalf of the Customer pursuant to an agreement entered into between them dated [insert date] ("**Services Agreement**"), including the processing of Personal Data (as defined in the Definitions section below).

1. 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 Vendor provides the services under the Services Agreement ("**Services**") to Customer in a manner that complies with the Data Protection Legislation.

2. General

In respect of the parties' rights and obligations under this Agreement regarding the Personal Data, the parties hereby acknowledge and agree that Customer is the "**Data Controller**" and Vendor is the "**Data Processor**" and accordingly Vendor agrees that it shall process all Personal Data in accordance with its obligations pursuant to this Agreement.

The Data Processor guarantees that it has appropriate technical and organizational measures in place to meet the requirements of the GDPR and ensure protection of the rights of the data subject.

3. Engagement of Sub-Processors

The Data Processor shall not engage another processor without prior specific or general written authorization of the Data Controller. In case of general written authorization, the Data Processor shall inform the Data Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

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.

For a list of sub-processors used by Socrative, see Annex 2.

4. Subject Matter

The parties have entered into a Services Agreement under which Vendor is providing quizzing software services to Customer and its end users.

5. Nature and Purpose of Processing

(a) The categories of data to be processed are first name, last name, email address, user ID, school name, location, activity within the service, and IP address.

The performance of the Service will involve processing of Personal Data as follows:

(b) The duration of the processing will be until the earlier of: (i) expiry/termination of the Services Agreement or (ii) the date upon which processing is no longer necessary for the purposes of either party performing its obligations under the Services Agreement (to the extent applicable);

(c) The nature of the processing will be collection, analysis, storage of Personal Data to allow Vendor to provide the Services;

(d) The processing is necessary for the provision of the Services under the Services Agreement;

(e) The categories of data subjects are teachers and students.

6. Compliance with Controller's Instructions and International Transfers

The Data Processor shall process the Personal Data only on documented instructions from the Data Controller, including any transfer of data to a third countries or international organizations.

The Data Processor 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 Data Processor may transfer and process Personal Data received from or on behalf of the Data Controller to third parties (which shall include without limitation any affiliates of Data Processor) with the authorization of the Data Controller. A list of such third parties is included at Annex 2. The Data Controller hereby authorises transfers to these third parties. Where such third party is located outside the European Economic Area, Data Processor shall, in advance of any such transfer, ensure that the transfer is permitted under the GDPR , which may include:

(a) The requirement for Data Processor to execute or procure 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 and attached hereto at Annex 3.

The Data Controller hereby authorizes the Data Processor to enter into the Standard Contractual Clauses contained in Annex 1 with the subcontractor in the Customer's name and on its behalf. The Data Processor will make the executed Standard Contractual Clauses available to the Data Controller on request.

(b) The requirement for 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.

7. Confidentiality

The Data Processor shall ensure that persons authorized to process the Personal Data have committed themselves to confidentiality by way of a written agreement or are under an appropriate statutory obligation of confidentiality.

8. Security of Processing

The Data Processor shall implement appropriate technical and organizational measures in accordance with article 32 of the GDPR to ensure a level of security appropriate to the risk, including as appropriate, as more particularly set out in Annex 1:

(a) The pseudonymization and encryption of 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 Personal Data in a timely manner in the event of a physical or technical incident; and

(d) A process for regularly testing, accessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

9. Requests by Data Subjects

As further set out in Chapter III of the GDPR, data subject has certain rights (e.g. information and access to Personal Data, rectification and erasure, restriction of processing, data portability, right to object and automated individual decision-making). The Data Controller is obliged to facilitate the exercise of these data subject rights under articles 15 to 22 of the GDPR. The Data Processor shall assist the Data Controller by appropriate technical and organizational measures for the fulfillment of the Data Controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR.

10. Security of Processing, Personal Data Breach, Impact Assessment and Prior Consultation

As further set out in articles 32 to 36 of the GDPR, Data Controller has certain obligations (e.g. notification of data breach to the supervisory authority, communication of data breach to the data subject, making a data protection impact assessment and prior consultation with the supervisory authority in certain cases).

The Data Processor shall assist the Data Controller in ensuring compliance with the obligations pursuant to articles 32-36 GDPR. In particular, the Data Processor shall notify the Data Controller, without undue delay, of any actual or suspected data breaches and in all other aspects assist the Data Controller in ensuring compliance with articles 32 to 36 of the GDPR. In particular, the Data Processor shall provide the Data Controller with full cooperation and assistance in respect of the data breach and all information in Data Processor's possession concerning the data breach, without undue delay, including the following:

(a) The probable cause and consequences of the breach;

(b) The categories of Personal Data involved;

(c) A summary of the probable consequences for the relevant data subjects;

(d) A summary of the unauthorized recipients of the Personal Data; and

(e) The measures taken by Data Processor to mitigate any damage.

11. Return and Deletion of Personal Data

The Data Processor shall, at the choice of Data Controller, delete or return all the personal data to the Data Controller at the end of the provision of services relating to processing, and delete any existing copies unless Union or Member State law requires storage of the personal data.

12. Audit, Compliance and Duty to Inform

The Data Processor shall maintain written records of all categories of processing activities carried out on behalf of the Data Controller.

The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with the obligations laid down in article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller. Data Processor shall immediately inform the Data Controller if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions.

If Data Controller believes that an on-site audit is necessary, Data Processor agrees to give Data Controller access to Data Processor's premises (subject to any reasonable confidentiality and security measures at a mutually acceptable time), and to any stored Personal Data and data processing programs it has on-site. Data Controller is entitled to have the audit carried out by a third party

13. No Additional Compensation

The Data Processor's compensation is being included in the services charges set out in the Services Agreement referred above, and the Data Processor shall thus not be entitled to any additional compensation for carrying out its obligations under this Addendum.

14. Governing Law and Dispute Resolution

The governing law and dispute resolution clause set out in the Services Agreement referred to above shall also be applicable to this Data Processing Agreement, provided that to the extent required by Applicable Law, this Addendum shall be governed by the laws of Ireland.

15. Definitions

"**Data Controller**" has the meaning set out in the Data Protection Legislation;

"**Data Processor**" has the meaning set out in the Data Protection Legislation;

"**Data Protection Legislation**" means all privacy laws applicable to any Personal Data processed under or in connection with this Agreement, including, without limitation, in particular Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing the Directive 95/46/EC (General Data Protection Regulation)("GDPR", the Privacy and Electronic Communications Directive 2002/58/EC and all national legislation implementing or supplementing the foregoing and all associated codes of practice and other guidance issued by any applicable data protection authority, all as amended, re- enacted and/or replaced and in force from time to time;

"**Personal Data**" has the meaning set out in the Data Protection Legislation and relates only to personal data of which Customer is the Data Controller and in relation to which the Vendor is providing the Services under the Services Agreement;

"**Process**" and other derivations such as "processed" and "processing" means any use of or processing applied to any Personal Data and includes "processing" as defined in the Data Protection Legislation;

SCC Agreement: the standard contractual clauses for the transfer of personal data from the European Union to processors established in third countries (controller-to-processor transfers), as set out in the Annex to Commission Decision 2010/87/EU.

***

Acknowledgement

Acknowledged by:

_____

[School/company name]

_____

[First name, last name]

_____

[Title]

_____

[Signature]

_____

[Date]

Showbie, Inc.

Colin Bramm

CEO and Cofounder

ANNEX 1: 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.

ANNEX 2: 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

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 and grades
4) IP address
5) Country
6) School name and type

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)
Fuel Education (USA)
Google/G-Suite (USA)
Intercom (USA)
PersistIQ (USA)
Productboard (USA)
Pubnub (USA)
Sentry (USA)
Slack (USA)
Stripe (USA)
Typeform (Spain)
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 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 organization: .....

Address:.....

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

Other information needed to identify the organization:

……
(the data exporter)

And
Name of the data importing organization:……..

Address:.....

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

Other information needed to identify the organization:

……
(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 subprocessor 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 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 sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely ……
……
……

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

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the 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 attached):