Fuse Data Processing Addendum

1. Data Processing Agreement preamble

1.1. This Data Processing Agreement ("**DPA**") is entered into between Fuse Universal Ltd ("**Data Processor**") and the Customer ("**Data Controller**") (together the "**Parties**") and sets out the rights and obligations that apply to the Data Processor's handling of personal data on behalf of the Data Controller. **"Personal Data**" shall mean personal data as defined by the GDPR.

1.2. This DPA is incorporated by reference into the Master Customer Agreement dated between the Parties ("**Agreement**") for the supply of Services by the Data Processor to the Data Controller.

1.3. This DPA has been designed to ensure the Parties' compliance with Applicable Data Protection Laws. "**Applicable Data Protection Laws**" shall mean all applicable federal, state and foreign data protection, privacy and data security laws, regulations, and directives, including, without limitation, the General Data Protection Regulation (Regulation (EU) 2016/679) ("**GDPR**") and the California Consumer Privacy Act of 2018 ("**CCPA**").

1.4. The terms used in this DPA shall have the meanings set forth in this DPA. Capitalised terms not otherwise defined herein shall have the meaning given to them in the Agreement. Except as modified below, the terms of the Agreement shall remain in full force and effect.

1.5. This DPA shall not exempt the Parties from their respective obligations under Applicable Data Protection Laws.

Now therefore, in consideration of the mutual promises herein and other good and valuable consideration, the Parties to this DPA agree as follows:

2. The rights and obligations of the Data Controller and processing of personal data

2.1. The Data Controller appoints the Data Processor to process the personal data described in Appendix A.

2.2. The details on the subject matter, duration, nature and purpose of processing and the Personal Data categories and data subject types in respect of which will be subjected to processing by the Data Processor in the performance of the Services pursuant to the Agreement are specified in Appendix A.

2.3. The Data Controller shall have both the right and obligation to make decisions about the purposes and means of the processing of personal data and shall be responsible for ensuring that the processing that the Data Processor is instructed to perform is authorised in law.

3. Obligations of the Data Processor

3.1. The Data Processor shall solely be permitted to process personal data on documented instructions from the Data Controller to the extent as is necessary to perform its obligations under the Agreement unless processing is required under EU or Member State law to which the Data Processor is subject. In this case, and where possible to do so, the Data Processor shall inform the Data Controller of this legal requirement prior to processing unless that law prohibits such information on important grounds of public interest

3.2. The Data Processor shall inform the Data Controller as soon as reasonably possible if the instructions, in the opinion of the Data Processor, contravene the GDPR or data protection provisions contained in other EU or Member State law.

4. Confidentiality

4.1. The Data Processor shall reasonably ensure that:

a) only those persons who are currently authorised to do so are able to access the personal data being processed on behalf of the Data Controller;

b) only persons who require access to the personal data in order to fulfil the obligations of the Data Processor

to the Data Controller shall be provided with authorisation; and

c) that persons authorised to process personal data on behalf of the Data Controller have undertaken to observe confidentiality or are subject to suitable statutory obligation of confidentiality.

5. Security of processing

5.1. The Data Processor shall implement appropriate technical and organisational measures to protect the personal data (i) from accidental or unlawful destruction, and (ii) loss, alteration, unauthorised disclosure of, or access to the personal data ("**Safeguards**").

5.2. Safeguards shall, taking into account the state of the art and the costs of the implementation and execution of the measures, ensure an adequate level of protection taking into account the risks involved in the processing and the nature of the personal data to be secured.

5.3. The Data Processor shall, in ensuring the above – in all cases –implement the level of security and the measures specified in Appendix C to this DPA.

5.4. Where the Parties agree on the requirement of establishing additional security measures, the terms and cost of implementing such measures shall be dealt with in the Agreement.

6. Use of Sub-Processors

6.1. The Data Processor shall not engage a third party processor ("**Sub-Processor**") for the fulfilment of this DPA without the prior consent of the Data Controller.

6.2. A list of approved Sub-Processors as at the date of this DPA is listed in Appendix B to this DPA and the Data Processor shall maintain and provide updated copies of this list to the Data Controller when it adds or removes Sub-Processors in accordance with this Agreement.

6.3. Notwithstanding this, the Data Controller consents to the Data Processor engaging Sub-Processors to process the personal data, provided that:

a) the Data Processor shall inform the Data Controller of any planned changes with regard to additions to or replacement of Sub-processors (including details of the processing it performs or will perform) as listed in Appendix B to this DPA; and

b) the Data Processor shall ensure that the Sub-Processor is subject to the same data protection obligations as those specified in this DPA on the basis of a contract or other legal document under EU law or the national law of the Member States.

6.4. If the Sub-Processor does not fulfil his data protection obligations, the Data Processor shall remain liable to the Data Controller as regards the fulfilment of the obligations of the Sub-Processor.

7. Transfer of data to third countries or international organisations

7.1. Without the approval of the Data Controller, the Data Processor cannot – within the framework of this Data Processing Agreement:

a) disclose personal data to a data controller in a third country or in an international organisation;

b) assign the processing of personal data to a sub-processor in a third country; or

c) have the data processed in another of the Data Processor's divisions which is located in a third country,

unless otherwise specified within this DPA.

7.2. The Data Controller's instructions or approval of the transfer of personal data to a third country, if applicable, shall be set out in Appendix C to this Data Processing Agreement.

7.3. The Data Processor may only process, or permit the processing, of personal data outside the European Economic Area ("**EEA**") under the following conditions:

a) the Data Processor is processing personal data in a territory which is subject to a current finding by the European Commission under the Applicable Data Protection Laws that the territory provides adequate

protection for the privacy rights of individuals;

b) the Data Processor participates in a valid cross-border transfer mechanism under the Applicable Data Protection Laws, so that the Data Processor (and, where appropriate, the Data Controller) can ensure that appropriate safeguards are in place to ensure an adequate level of protection with respect to the privacy rights of individuals as required by Article 46 of the GDPR; or

c) processing is required under EU or Member State law to which the Data Processor is subject. In such a case, the Data Processor shall inform the Data Controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

7.4. To the extent any processing of Personal Data by Data Processor and its sub-processors take place in any country outside the EEA (other than exclusively in an Adequate Country), the parties agree that the EC Standard Contractual Clauses approved by the EU authorities under EU Data Protection Laws and set out in Exhibit 1, and as updated from time to time, will apply in respect of that processing and Data Processor will comply with the obligations of the 'data importer' in the EC Standard Contractual Clauses and Data Controller will comply with the obligations of 'data exporter'. By entering into this DPA, the Parties are deemed to be signing the EC Standard Contractual Clauses, as updated from time to time, and its applicable Appendices. The parties agree to enter into any updated EC Standard Contractual Clauses as approved by the EU authorities under EU Data Protection Laws.

7.5. Should the EC Standard Contractual Clauses or other method applied for cross-border processing under Clause 7.3 cease to be a lawful means of transferring the Personal Data, the parties shall comply with any alternative lawful method of transfer required and complete any documentation required for such alternative lawful method of transfer.

7.6. The following terms will apply to the European Union Standard Contractual Clauses set out in Exhibit 1 (whether used pursuant to clause 7.3 or 7.4) and as updated from time to time:

7.6.1 The Customer may exercise its right of audit under clause 5.1(f) of the Standard Contractual Clauses as set out in, and subject to the requirements of, clause 11.1 of this DPA; and

7.6.2 The data importer may appoint sub-processors as set out, and subject to the requirements of this DPA.

8. Assistance to the Data Controller and Data Subject Rights

8.1. The Data Processor shall, as far as reasonably possible, assist the Data Controller in the fulfilment of the Data Controller's obligations to respond to requests for the exercise of the data subjects' rights including with: the right of access by the data subject, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object; and the right to object to the result of automated individual decision-making, including profiling ("**Data Subject Request**").

8.2. Taking into account the nature of the processing, the Data Processor shall provide reasonable assistance at the Data Controller's expense, to the Data Controller by providing appropriate technical and organizational measures, insofar as this is reasonably possible, for the fulfilment of Data Controller's obligation to address any Data Subject Request.

9. Notification of personal data breach

9.1. On discovery of personal data breach at the Data Processor's facilities or a Sub-Processor's facilities ("**Security Incident**"), the Data Processor shall as soon as reasonably practicable notify the Data Controller.

9.2. The Data Processor's notification to the Data Controller shall, if possible, take place within 48 hours after the Data Processor has discovered the breach to enable the Data Controller to comply with its data breach reporting obligations under (and in accordance with the timescales required by) GDPR.

9.3. The Data Processor shall provide reasonable assistance to the Data Controller in the reporting of the breach to the relevant supervisory authority.

10. Erasure of data

10.1. On termination of the Agreement, the Data Processor shall, at the Data Controller's discretion, return all the personal data to the Data Controller and erase existing copies, except to the extent that EU law or Member State law requires storage of the personal data.

11. Inspection and audit

11.1. The Data Processor shall make available to the Data Controller all information reasonably necessary to allow for and contribute to audits, including inspections performed by the Data Controller or another third party auditor mandated by the Data Controller, at the Data Controller's expense, provided that the Data Controller: (i) gives the Data Processor reasonable prior notice of its intention to audit; (ii) conducts it audit during normal business hours; and (iii) and takes all reasonable measures to prevent unnecessary disruption to the Data Processor's operations.

11.2. The Data Controller will not exercise its audit rights under this clause 11 more than once in any twelve (12) calendar month period, except (i) if and when required by instruction of a competent data protection authority, or (ii) where the Data Controller believes a further audit is necessary due to a Security Incident by the Data Processor.

11.3. The Data Controller's inspection of sub-processors, if applicable, shall be performed through the Data Processor.

12. Applicability of the CCPA

12.1. To the extent that the Data Processor will process any personal data that is subject to the CCPA, the Data Processor shall act as a "service provider," as such term is defined in the CCPA, and shall assist the Data Controller by appropriate technical and organizational measures for the fulfilment of the Data Controller's obligations under the CCPA, including without limitation responding to verified requests by a "consumer," as such term is defined in the CCPA.

12.2. Furthermore, the Data Processor will not engage a Sub-Processor with access to personal data except with the Data Controller's prior written consent in accordance with Clause 6 of this DPA and the Data Processor will only do so for a "business purpose," as such term is defined in the CCPA, pursuant to a written contract by and between the Data Processor and such Sub-Processor. Any such approved Sub-Processor shall agree to terms that are at least as protective of personal data as the terms of this DPA.

12.3. The Data Processor certifies that it understands it will comply with the responsibilities and restrictions imposed by this DPA as a service provider under the CCPA.

13. The Parties' agreement on other terms

13.1. The consequences of the Parties' breach of this DPA, if applicable, shall be specified in the Agreement.

13.2. In the event of a conflict between DPA and the data protection provisions within the Agreement (except where explicitly agreed otherwise in writing between the Parties), the terms and conditions set forth in this DPA shall prevail and govern and control the relationship between the Parties.

14. Commencement and termination

14.1. This DPA shall become effective on the date of both Parties' signature to the Agreement.

14.2. This Data Processing Agreement may be terminated according to the terms specified in the Agreement.

14.3. This DPA shall apply for as long as the processing is performed. Irrespective of the termination of the Agreement and/or this DPA, the DPA shall remain in force until the termination of the processing and the erasure of the data by the Data Processor and any sub-processors.

14.4. The DPA and the Agreement shall be interdependent and cannot be terminated separately. The DPA may however – without termination of the Agreement – be replaced by an alternative valid data processing agreement.

15. Governing Law and Jurisdiction

15.1. The Parties to this DPA shall submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity or

termination or the consequences of its nullity.

15.2. The DPA and all non-contractual or other obligations arising of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Agreement.

16. Severance

16.1. Should any of the provisions of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, preserving the Parties intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part has never been contained therein.

17. Data Processor and Data Controller contacts

17.1. In the event your designated account manager at Cornerstone cannot assist with a data privacy enquiry, you may contact Cornerstone's data protection officer at john.taylor@fuseuniversal.com.

17.2. The Parties shall be under obligation continuously to inform each other of changes to contacts/contact

Please sign and return the enclosed copy of this Addendum as instructed to acknowledge the supplementation of these terms to the Agreement.

[Signatures follow on the next page]

CUSTOMER

Customer name (Required): _____

Signature (Required): _____

Name (Required) : _____

Title (Optional) : _____

Date (Required): _____

EU Representative (Required only where applicable): _____

Contact details: _____

Data Protection Officer (Required only where applicable): _____

Contact details: _____

FUSE

Notwithstanding the signatures below of any other Fuse Entity, a Fuse Entity is not a party to this Addendum unless they are a party to the Agreement for the provision of the Software and/or Services to you.

Data Protection Point of Contact John Taylor
Contact Details: john.taylor@fuseuniversal.com

Fuse Universal Limited:	Signature:	_____
	Name:	_____
	Title:	_____
	Date:	_____
Fuse Universal LLC:	Signature:	_____
	Name:	_____
	Title:	_____
	Date:	_____
Fuse Universal Pty Limited:	Signature:	_____
	Name:	_____
	Title:	_____
	Date:	_____

Appendix A Information about the processing

The purpose of the Data Processor's processing of personal data on behalf of the Data Controller is:

- The purpose of data processing is to provide learning and training functionality for the data controller's users.

The Data Processor's processing of personal data on behalf of the Data Controller shall mainly pertain to (the nature of the processing):

- The data processor maintains and runs the Fuse service that stores and processes user and learning data.

Processing includes the following categories of data subject:

- Data Controller's employees, contractors.

The Processing concerns the following categories of data:

- Data Controller's employees' data.

The processing includes the following types of personal data about data subjects:

The only mandatory user data requirement for Fuse is a unique username for each user on the customer's instance. All other data is optional and defined by the Data Controller. This is typically generic business personal data. For example:

- Personal data such as:
    - first name/last name
    - username (unique)
    - email address (unique)
    - custom fields such as: location, department, role, hire date, line manager etc.

In addition, the Data Controller collects the following personal data:

Technical data such as:

- IP address
- browser language
- browser type and version
- geolocation
- operating system
- third-party cookie information (where we use third-party services to provide Fuse functionality)

- Fuse activity:
    - login history and transactional activity information (views, likes, shares etc.)
    - training history and learning completions
    - error logs
    - metadata for user-generated content such document uploads and video recordings

The Data Processor's processing of personal data on behalf of the Data Controller may be performed when this DPA commences. Processing has the following duration:

- Processing and storage of user data for the term of the license agreement and for the period of 60 days thereafter at which point the personal data is destroyed in line with Data Processor's service termination process.

Appendix B Terms of the Data Processor's use of sub-processors and list of approved sub-processors

B.1 Approved sub-processors

1. Supplier may engage other processors ("**Subprocessors**") for the Processing of Personal Data under this Data Processing Agreement, provided Supplier ensures such Subprocessors' compliance with the terms of this Agreement. As of the effective date of the Agreement, the Supplier relies on the Subprocessors listed in the Order as well as below to provide the Services.

2. Prior to the engagement of another Subprocessor, the Supplier shall inform your administrator and your contact of the intended subprocessing at least 30 days prior thereto, thereby giving you the opportunity to object to such change on reasonable grounds, as set forth in Article 28 GDPR.

3. You authorize the Supplier to transfer Personal Data to the Supplier's Affiliates and/or other Subprocessors located in locations outside the European Economic Area, as is reasonably required to provide support, perform technical projects or perform other types of services under the Fuse Master Customer Agreement, provided that, to the extent applicable, either: (i) such locations are recognized by the European Commission as providing adequate data protection; (ii) the Supplier has executed on your behalf the EU Standard Contractual Clauses with such Affiliates and/or other Subprocessors (you hereby grant such proxy to the Supplier); or (iii) upon your request, you execute the EU Standard Contractual Clauses directly with such Affiliates and/or other Subprocessors.

4. The Supplier shall remain fully liable to you for the performance of its Subprocessors' obligations hereunder.

Name	Address	Description of processing
Airbrake USA	228 Hamilton Ave, 3rd Floor Palo Alto, CA 94301	Application exception logging and tracking - Processes in EU & US
Amazon Web Services	One Burlington Plaza, Burlington Rd, Dublin 4	Hosting Services - processed in EU West (Dublin, Ireland)
Atlassisian	Level 6 341 George Street Sydney, NSW 2000 Australia	Hosted Support and Delivery platform-processed in EU West (Dublin, Ireland)
Auth0	Auth0, Inc. 10900 NE 8th Street, Suite 700 Bellevue, Washington 98004	Identity Management, authentication and authorisation - processed globally to support global login.
DataDog	New York Times Bldg, 620 8th Ave 45th Floor New York USA	Logging and Application Performance Monitoring - anonymised data processed in EU & US
Dell Boomi	US East Coast Office 1400 Liberty Ridge Drive Chesterbrook PA19087 USA	HR Integrations (if enabled) – processes in EU West (Dublin, Ireland)
Fastly	475 Brannan St. #300	Content Delivery Network - Processes

	San Francisco, CA 94107	worldwide (Closest POP to connecting users)
Fuse Universal LLC	303 Wyman St, Suite 325, Waltham, Massachusetts, 02451	Fuse Subsidiary - processes in US
Fuse Universal PTY Limited	Level 5, 1 Chifley Square, Sydney, New South Wales, NSW2000, Australia	Fuse Subsidiary - processes in Australia
Fuse Universal SA (Pty) Ltd	12 Pinewood Rd, Newlands, Cape Town, 7700	Fuse Subsidiary providing support services – processes in South Africa
Good Data	San Francisco 1 Post Street, Suite 400. San Francisco, CA 94104 USA	System Analytics – processed in Rackspace, London
Google	1600 Amphitheatre Parkway in Mountain View, California, United States	Gsuite + Google cloud. Corporate productivity and language translations. Processes in EU and US
Hub Spot	25 First Street, 2nd Floor Cambridge, MA 02141 United States	CRM and communication trend tracking. Processes EU
NeosAlpha Technologies Limited	Maidenhead Concorde Park Concorde Road Building 3, 1st Floor, Maidenhead SL6 4FJ	Consultancy and support for Boomi iPaaS used to support customer integrations. Processes in UK
Ping Identity	1001 17th Street Suite 100 Denver, CO 80202	Identity Management, authentication and authorisation - Processes in EU
Pink Elephant	Pink Elephant Corporate Head Office 5575 North Service Road, Suite 200 Burlington, ON L7L 6M1 Canada	ITIL and process improvement consultancy - Processes in EU
Productboard	612 Howard Street, 4th Floor, San Francisco CA 94105, USA	Product vision, features and Roadmap - Processes in US
Salesforce	Salesforce Tower 415 Mission Street, 3rd Floor San Francisco, CA 94105	CRM Software - Processes in EU (DE / FRA)
Telestream	848 Gold Flat Road Nevada City, CA 95959, USA	Video Transcoding - processed in EU West (Dublin, Ireland)
Twilio (Sendgrid)	375 Beale St suite 300 San,	SMTP Relay email notifications - processed

	Francisco CA 94105 USA	EU & US SMS notification relay - processed EU & US
Voicebase	44 Montgomery St, San Francisco, CA 94104 USA	Audio Transcribing – processes in EU
Zoom	55 Almaden Boulevard, Suite 400, 500, 600, San Jose, CA 95113	Video Conferencing - Processes in EU & US

Appendix C Instruction pertaining to the use of personal data

C.1 The subject of/instruction for the processing

The Data Processor's processing of personal data on behalf of the Data Controller shall be carried out by the Data Processor performing the following:

The purpose of data processing is to provide learning and training functionality for the Data Controller's users as describe in the Agreement.

C.2 Security of processing

The level of security shall reflect the following:

The Data Processor shall implement the following measures that have been agreed with the Data Controller (on the basis of the risk assessment that the Data Controller has performed):

- Provide mechanisms for the Data Controller to manage and pseudonymise its user data.
- Control unauthorised access to personal data and content in line with Data Processor's access control and privacy policies.
- Ensure availability of the platform in line with Data Processor's SLA.
- Provide the level of service, security, auditing and disaster recovery as outlined in Data Processor's ISO27001 policies.

C.3 Storage period/erasure procedures

In line with Data Processor's service termination process the Data Processor will destroy all data and content belonging to the Data Controller within the agreed mutually grace period.

C.4 Processing location

Processing of the personal data under this DPA cannot be performed at other locations than the following without the Data Controller's prior written consent:

- The Data Controller user data is held, stored and processed in ***the locations stated in the Appendix B***

C.5 Instruction for or approval of the transfer of personal data to third countries

- The Data Controller provides instructions and consent pertaining to the transfer of personal data to a third country, the Data Processor shall be entitled within the framework of this DPA to perform such transfer.

Appendix D EU Standard Contractual Clauses for the transfer of personal data to data processors established in third countries which do not ensure an adequate level of data protection

---

INTRODUCTION

Both 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.

AGREED TERMS

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 EU Data Protection Laws 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 entity 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 EU Data Protection Laws 95/46/EC;

(d) the "**sub-processor**" means any processor engaged by the data importer or by any other sub- processor of the data importer who agrees to receive from the data importer or from any other sub-processor 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; and

(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.

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.

3. Third-party beneficiary clause

3.1 The data subject can enforce against the data exporter this Clause, Clause 4.1(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.

3.2 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.

3.3 The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub- processor shall be limited to its own processing operations under the Clauses.

3.4 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.

4. Obligations of the data exporter

4.1 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 EU Data Protection Laws 95/46/EC;

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

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

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

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

5. Obligations of the data importer

5.1 The data importer agrees and warrants:

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

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

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

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

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

(ii) any accidental or unauthorised access; and

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

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

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

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

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

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

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

6. Liability

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

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

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

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

7. Mediation and jurisdiction

7.1 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.

7.2 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.

8. Co-operation with supervisory authorities

8.1 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.

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

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

9. Governing law

The Clauses shall be governed by the governing law of the member state in which the data exporter is established, namely ...

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.

11. Sub-processing

11.1 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 fulfill 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.

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

11.3 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 England and Wales.

11.4 The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5.1(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

12. Obligation after the termination of personal data-processing services

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

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

Appendix 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):

An entity that has executed the EU Standard Contractual Clauses as a data exporter and that uses to the data importer's Services.

Data importer

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

An entity which provides the Services to the data exporter.

Data subjects

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

See Exhibit 1 of the DPA

Categories of data

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

See Exhibit 1 of the DPA

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please

specify): none

Processing operations

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

Use of contact details and related data for the purposes of the Services.

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):

Data importer's security policies, practices and processes are hereby incorporated by reference.