

## **EU GDPR DATA PROCESSING ADDENDUM**

This Data Processing Addendum (“**DPA**”), forms part of the Master Service Agreement, or other written or electronic agreement, by and between Eduspot. (“**the Company**”) (Incorporating Teachers2Parents Ltd, EduSoft Ltd, BehaviourWatch Ltd, Smart Payments Ltd and Schoolswire Ltd) and the undersigned customer of the Company (“**Customer**”) for certain services (collectively, the “**Service**”) provided by the Company (the “**Master Agreement**”). Each of Customer and the Company may be referred to herein as a “**party**” and together as the “**parties**.”

The parties have agreed to enter into this DPA in order to ensure that adequate safeguards are put in place with respect to the protection of such Personal Data as required by EU Data Protection Laws.

### **DOCUMENT OVERVIEW:**

- Main Body of the DPA between the Company and the Customer (Page 2-6, signature required on Page 6)
- Annex 1, Details of the Personal Data and Processing Activities (Page 7)
- Annex 2, EU Model Clauses for the transfer of data (Page 8-13)
- Appendix 1, Definitions for Annex 2 (Page 14-15)
- Appendix 2, Security Measures (Page 16-18 18)

### **HOW TO EXECUTE THIS DPA:**

1. This DPA consists of two parts: the main body of the DPA, and Annexes 1, 2, and 3 (including Appendices 1 and 2).
2. This DPA has been pre-signed on behalf of the Company.
3. To complete this DPA, Customer must complete the information in the signature boxes and sign on Pages 6.
4. Send the completed and signed DPA to the Company by email, indicating the Customer’s Legal Name (as set out on the applicable the Company Order Form or invoice, if applicable), to [compliance@eduspot.co.uk](mailto:compliance@eduspot.co.uk).

Upon receipt of the validly completed DPA by the Company at this email address, this DPA will become legally binding.

### **HOW THIS DPA APPLIES**

This DPA is an addendum to and forms part of the Master Agreement. The Customer entity signing this DPA must be the same as the Customer entity party to the Master Agreement.

### **DATA PROCESSING TERMS**

In the course of providing the Service to Customer pursuant to the Master Agreement, the Company may process Personal Data on behalf of Customer. The Company agrees to comply with the following provisions with respect to any Personal Data submitted by or for Customer to the Company or collected and processed by or for Customer using the Company’s services.

The parties agree that the obligations under this DPA that are specific to the GDPR shall not apply until the GDPR has come into full force and effect.



## 1. DEFINITIONS

- a. The following definitions are used in this DPA:
  - i. **“Adequate Country”** means a country or territory that is recognised under EU Data Protection Laws as providing adequate protection for Personal Data;
  - ii. **“Customer Group”** means Customer and any of its Affiliates established and/or doing business in the EEA, or United Kingdom;
  - iii. **“EU Data Protection Laws”** means all current laws and regulations of the European Union, the European Economic Area, their member states, and the United Kingdom, applicable to the processing of Personal Data under the Master Agreement, including (where applicable) the GDPR and any future changes or modifications to said laws;
  - iv. **“GDPR”** means the General Data Protection Regulation (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);
  - v. **“Personal Data”** means all data which is defined as *‘personal data’* under EU Data Protection Laws and to which EU Data Protection Laws apply and which is provided by the Customer to the Company, and accessed, stored or otherwise;

## 2. STATUS OF THE PARTIES

- a. The type of Personal Data processed pursuant to this DPA and the subject matter, duration, nature, and purpose of the processing, and the categories of data subjects, are as described in Annex 1.
- b. Each party warrants in relation to Personal Data that it will comply (and will warrant that any of its personnel comply and use commercially reasonable efforts to warrant that its sub-processors comply), with EU Data Protection Laws. As between the parties, the Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which the Customer acquired Personal Data.
- c. In respect of the parties' rights and obligations under this DPA regarding the Personal Data, the parties hereby acknowledge and agree that the Customer is the data controller and the Company is the data processor, and accordingly the Company agrees that it shall process all Personal Data in accordance with its obligations pursuant to this DPA.
- d. Where and to the extent that the Company processes data which is defined as *‘personal data’* under EU Data Protection Laws as a data controller as set out in the Company Privacy Policy, the Company will comply with applicable EU Data Protection Laws in respect of that processing.
- e. Each party shall appoint an individual within its organisation authorised to respond from time to time to enquiries regarding the Personal Data and each party shall deal with such enquiries promptly.

## 3. COMPANY OBLIGATIONS

- a. With respect to all Personal Data, the Company warrants that it shall:
  - i. only process Personal Data in order to provide the Service, and shall act only in accordance with: (i) this DPA, (ii) the Customer's written instructions as represented by the Master Agreement and this DPA, and (iii) as required by applicable laws;
  - ii. as soon as reasonably practicable upon becoming aware, inform the Customer if, in the Company's opinion, any instructions provided by the Customer under clause 3.a(i) violate the GDPR;
  - iii. implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks that are presented by the processing of Personal Data, in particular protection against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or



access to Personal Data. Such measures include, without limitation, the security measures set out in Appendix 2;

- iv. take reasonable steps to ensure that only authorised personnel have access to such Personal Data and that any persons whom it authorises to have access to the Personal Data are under obligations of confidentiality;
  - v. as soon as reasonably practicable upon becoming aware, notify the Customer of any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed by the Company, its sub-processors, or any other identified or unidentified third party (a “**Security Breach**”);
  - vi. promptly provide the Customer with reasonable cooperation and assistance in respect of a Security Breach and all reasonable information in the Company’s possession concerning such Security Breach insofar as it affects the Customer, including the following to the extent then known:
    1. the possible cause and consequences for the data subjects of the Security Breach;
    2. the categories of Personal Data involved;
    3. a summary of the possible consequences for the relevant data subjects;
    4. a summary of the unauthorised recipients of the Personal Data; and
    5. the measures taken by the Company to mitigate any damage;
  - vii. not make any public announcement about a Security Breach (a “**Breach Notice**”) without the prior written consent of the Customer, unless required by applicable law;
  - viii. promptly notify the Customer if it receives a request from a data subject to access, rectify or erase that individual’s Personal Data, or if a data subject objects to the processing of, or makes a data portability request in respect of, such Personal Data (each a “**Data Subject Request**”). The Company shall not respond to a Data Subject Request without the Customer’s prior written consent except to confirm that such request relates to the Customer, to which the Customer hereby agrees. To the extent that the Customer does not have the ability to address a Data Subject Request, then upon Customer’s request the Company shall provide reasonable assistance to the Customer to facilitate such Data Subject Request to the extent able and in line with applicable law. Customer shall cover all costs incurred by the Company in connection with its provision of such assistance;
  - ix. other than to the extent required to comply with applicable law, as soon as reasonably practicable following termination or expiry of the Master Agreement or completion of the Service, the Company will delete all Personal Data (including copies thereof) processed pursuant to this DPA.
- b. Taking into account the nature of processing and the information available to the Company, provide reasonable assistance to the Customer as the Customer reasonably requests in relation to the Company’s obligations under EU Data Protection Laws in connection with its provision of such assistance with respect to:
- i. data protection impact assessments (as such term is defined in the GDPR);
  - ii. notification to the supervisory authority under EU Data Protection Laws and/or communications to data subjects by the Customer in response to any Security Breach; and



- iii. the Customer's compliance with its obligations under the GDPR with respect to the security of processing.

#### 4. SUB PROCESSING

- a. The Customer grants a general authorisation: (a) to the Company to appoint other affiliates as sub-processors, and (b) the Company and its affiliates to engage third-party sub-processors for performance of Service provided that:
  - i. The Company maintains an up-to-date list of its sub-processors on the Company website and will add the names of new and replacement sub-processors to the list prior to them starting sub-processing of Personal Data. If the Customer has a reasonable objection to any new or replacement sub-processor, it shall notify the Company of such objections in writing within ten (10) days of the notification and the parties will seek to resolve the matter in good faith. If the Company is reasonably able to provide the Service to the Customer in accordance with the Master Agreement without using the sub-processor and decides in its discretion to do so, then the Customer will have no further rights under this clause 4.a.i in respect of the proposed use of the sub-processor. If the Company requires use of the sub-processor in its discretion and is unable to satisfy the Customer as to the suitability of the sub-processor or the documentation and protections in place between the Company and the sub-processor within ninety (90) days from the Customer's notification of objections, the Customer may within thirty (30) days following the end of the ninety (90) day period referred to above, terminate the applicable Service with at least thirty (30) days written notice, solely with respect to the service(s) to which the proposed new sub-processor's processing of Personal Data relates. If the Customer does not provide a timely objection to any new or replacement sub-processor in accordance with this clause 4.a.i, the Customer will be deemed to have consented to the sub-processor and waived its right to object. The Company may use a new or replacement sub-processor whilst the objection procedure in this clause 4.a.i is in process. The customer agrees that this addresses required sub-processor notification requirements within Annex 2 11.a.
  - ii. The Company will ensure that any sub-processor it engages to provide an aspect of the Service on its behalf in connection with this DPA does so only on the basis of a written contract which imposes on such sub-processor terms substantially no less protective of Personal Data than those imposed on the Company in the DPA (the "**Relevant Terms**"). The Company shall procure the performance by such sub-processor of the Relevant Terms and shall remain liable for any breach of this DPA that is caused by an act, error, or omission of its sub-processor.

#### 5. AUDIT AND RECORDS

- a. The Company shall, in accordance with EU Data Protection Laws, make available to the Customer such information in the Company's possession or control as the Customer may reasonably request with a view to demonstrating the Company's compliance with the obligations of data processors under EU Data Protection Law in relation to its processing of Personal Data.
- b. The Customer may exercise its right of audit under EU Data Protection Laws in relation to Personal Data, through the Company providing:
  - i. An audit report not older than eighteen (18) months, prepared by an independent external auditor demonstrating that the Company's technical and organisational measures are sufficient and in accordance with an accepted industry audit standard; and
  - ii. Additional information in the Company possession or control to an EU supervisory authority when it requests or requires additional information in relation to the processing of Personal Data carried out by the Company under this DPA.



## 6. DATA TRANSFER

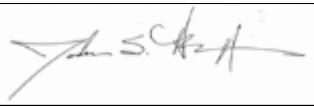
- a. To the extent any processing of Personal Data by the Company takes place in any country outside the EEA (except if in an Adequate Country), the parties agree that the standard contractual clauses approved by the EU authorities under EU Data Protection Laws and set out in Annex 2 will apply in respect of that processing, and the Company will comply with the obligations of the 'data importer' in the standard contractual clauses and the Customer will comply with the obligations of the 'data exporter'.
- b. The Customer acknowledges and accepts that the provision of the Service under the Master Agreement may require the processing of Personal Data by sub-processors in countries outside the EEA.
- c. If, in the performance of this DPA, the Company transfers any Personal Data to a sub-processor located outside of the EEA (without prejudice to clause 4), the Company shall in advance of any such transfer ensure that a legal mechanism to achieve adequacy in respect of that processing is in place, such as:
  - i. the requirement for the Company to execute or warrant that the sub-processor execute to the benefit of the Customer standard contractual clauses approved by the EU authorities under EU Data Protection Laws and set out in Annex 2;
  - ii. the requirement for the sub-processor to be certified under the EU-U.S. Privacy Shield Framework; or
  - iii. the existence of any other specifically approved safeguard for data transfers (as recognised under EU Data Protection Laws) and/or a European Commission finding of adequacy.

## 7. GENERAL

- a. This DPA is without prejudice to the rights and obligations of the parties under the Master Agreement which shall continue to have full force and effect. In the event of any conflict between the terms of this DPA and the terms of the Master Agreement, the terms of this DPA shall prevail so far as the subject matter concerns the processing of Personal Data.
- b. The Company's liability under or in connection with this DPA (including under the standard contractual clauses set out in Annex 2) is subject to the limitations on liability contained in the Master Agreement.
- c. This DPA does not confer any third-party beneficiary rights, it is intended for the benefit of the parties hereto and their respective permitted successors and assigns only, and is not for the benefit of, nor may any provision hereof be enforced by, any other person.
- d. The choice of law and jurisdiction concerning this DPA and any action related thereto shall be consistent with and pursuant to the Master Agreement. In the absence of choice of law and jurisdiction selection, the parties shall mutually agree upon choice of law and jurisdiction.
- e. This DPA is the final, complete and exclusive agreement of the parties with respect to the subject matter hereof and supersedes and merges all prior discussions and agreements between the parties with respect to such subject matter. No modification of, amendment to, or waiver of any rights under the DPA will be effective unless in writing and signed by an authorised signatory of each party. This DPA may be executed in counterparts, each of which shall be deemed to be an original, but all of which, taken together, shall constitute one and the same agreement. Each person signing below represents and warrants that he or she is duly authorised and has legal capacity to execute and deliver this DPA. Each party represents and warrants to the other that the execution and delivery of this DPA, and the performance of such party's obligations hereunder, have been duly authorised and that this DPA is a valid and legally binding agreement on each such party, enforceable in accordance with its terms.



**IN WITNESS WHEREOF**, the parties have each caused this DPA to be signed and delivered by its duly authorised representative

<b>CUSTOMER:</b>		<b>COMPANY: Eduspot</b>	
<b>BY</b>		<b>BY</b>	
<b>NAME</b>		<b>NAME</b>	Joshua Hiller
<b>TITLE</b>		<b>TITLE</b>	Principal Information Security Officer
<b>ADDRESS</b>		<b>ADDRESS</b>	2 Darker Street, Leicester, LE1 4SL
<b>DATE</b>		<b>DATE</b>	May 7, 2018



## Annex 1

### Details of the Personal Data and Processing Activities

1. Personal data means all data which is defined as '*personal data*' under EU Data Protection Laws and to which EU Data Protection Laws apply and which is provided by the Customer to the Company, and accessed, stored or otherwise for delivery of contracted Services under the Master Agreement.
2. The duration of the processing will be: until the earliest of (i) expiry/termination of the Master Agreement, or (ii) the date upon which processing is no longer necessary for the purpose of either party performing its obligations under the Master Agreement (to the extent possible).
3. The processing will comprise: processing necessary to provide the Service to Customer, pursuant to the Master Agreement.
4. The purpose(s) of the processing is/are: necessary of the provision of the Service;
5. Personal Data may concern the following data subjects:
  - Prospective customer, customers, vendors of the Customer (who are natural persons), suppliers, authorised agents, and subscribers;
  - Employees or contact persons of the Customer's prospective customers and Customer's current customers, subcontractors, business partners, and vendors (who are natural persons); and/or
  - Natural persons authorised by the Customer to operate on their behalf.



## Annex 2

2010 EU Model clauses extracted from 2010/87/EU Annex EU Standard Contractual Clauses for the transfer of personal data. In order to be enforceable, these model clauses shall not be revised.

### INTRODUCTION

Both parties have agreed on the following Contractual Clauses (the “**Clauses**”) in order to adduce adequate safeguards with respect to 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 PURPOSE 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 are specified in Appendix 1 which forms an integral part of the Clauses.

#### 3. THIRD PARTY BENEFICIARY

- a. The data subject can enforce against the data exporter this Clause, Clause 4.a(ii) to (ix), Clause 5.a(i) to (v), and (vii) to (ix), Clause 6.a and 6.b, Clause 7, Clause 8.b, and Clauses 9 to 12 as third-party beneficiary.



- b. The data subject can enforce against the data importer this Clause, Clause 5.a(i) to (v) and (vii), Clause 6, Clause 7, clause 8.b, 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.
- c. The data subject can enforce against the sub-processor this Clause, Clause 5.a(i) to (v) and (vii), Clause 6, Clause 7, Clause 8.a, 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.
- d. 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**

- a. The data exporter agrees and warrants:
  - i. 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;
  - ii. 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;
  - iii. that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
  - iv. 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;
  - v. that it will ensure compliance with the security measures;
  - vi. 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;
  - vii. to forward any notification received from the data importer or any sub-processor pursuant to Clause 5.a(ii) and Clause 8.c to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
  - viii. 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;

- ix. 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
- x. that it will ensure compliance with Clause 4.a(i) to (ix).

## 5. OBLIGATIONS OF THE DATA IMPORTER

a. The data importer agrees and warrants:

- i. 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;
- ii. 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;
- iii. that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
- iv. that it will promptly notify the data exporter about:
  - 1. 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;
  - 2. any accidental or unauthorised access; and
  - 3. any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
- v. 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;
- vi. 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;
- vii. 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;

- viii. that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;
- ix. that the processing services by the sub-processor will be carried out in accordance with Clause 11;
- x. to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

## **6. LIABILITY**

- a. 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.
- b. If a data subject is not able to bring a claim for compensation in accordance with paragraph “6.a” 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.
- c. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs “6.a” and “6.b”, 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**

- a. 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:
  - i. to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
  - ii. to refer the dispute to the courts in the Member State in which the data exporter is established.
- b. 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 or national or international law.

## **8. CO-OPERATION WITH SUPERVISORY AUTHORITY**

- a. 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.



- b. 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.
- c. 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 8.b. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5.a(ii).

## **9. GOVERNING LAW**

The Clauses shall be governed by the laws of the Member State in which the data exporter is established.

## **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**

- a. 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.
- b. 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 6.a 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.
- c. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 11.a shall be governed by the law of the Member State in which the data exporter is established.
- d. 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.a(x), 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**

- a. 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. 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 12.a.



# **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 (i) the legal entity that has entered into a contract with the Company for provision of Services and executed the Clauses as a data exporter and (ii) all affiliates of such entity established within the EEA, which have purchased services from the Company.

### **Data Importer:**

The data importer is the Company, which processes Personal Data upon the instruction of the data exporter in accordance with the terms of the agreement between the data exporter and the Company.

### **Data Subjects:**

The personal data transferred concern the following categories of data subjects:

The data exporter may submit Personal Data to the Company, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Prospective customers, customers, suppliers, authorised agents, minors, subscribers, and vendors of the data exporter (who are natural persons);
- Employees or contact persons of the data exporter's prospective customers, customers, subcontractors, business partners, and vendors (who are natural persons);
- Natural persons authorised by the data exporter to use the services provided by the Company to the data exporter.

### **Categories of Data:**

The personal data transferred concern the following categories of data:

The data exporter may submit Personal Data to the Company, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to, the following categories of Personal Data:

- Names, titles, position, employer, contact information (email, phone, fax, physical address etc.), identification data, professional life data, personal life data, connection data, or localisation data (including IP addresses).

### **Special Categories of Data (if appropriate)**

The personal data transferred concern the following special categories of data:

The data exporter may submit special categories of data to the Company, the extent of which is determined and controlled by the data exporter in its sole discretion. Such special categories of data include, but may not be limited



to, Personal Data with information revealing racial or ethnic origins, political opinions, and religious or philosophical beliefs.

### **Processing Operations**

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

The objective of the processing of Personal Data by the Company is to provide the Service, pursuant to the Master Agreement.



## **Appendix 2**

### Security Measures

The Company has implemented and shall maintain a security program in accordance with industry standards. More specifically, The Company's security program shall include:

#### **Access Control of Processing Areas**

The Company implements suitable measures in order to prevent unauthorised persons from gaining access to the data processing equipment (namely telephones, database and application servers and related (hardware) where the personal data are processed or used, including:

- Establishing security areas;
- Protection and restriction of access paths;
- Establishing access authorisations for employees and third parties;
- The data centre and/or operation centre where personal data are hosted is secured by a security alarm system, and other appropriate security measures.

#### **Access Control to Data Processing Systems**

The Company implements suitable measures to prevent their data processing systems from being used by unauthorised persons, including:

- Use of adequate encryption technologies;
- Identification of the terminal and/or the terminal user to the company and processing systems;
- Automatic temporary lock-out of user terminal if left idle, identification and password required to reopen;
- Automatic temporary lock-out of the user ID when several erroneous passwords are entered;
- Monitoring of break-in attempts (alerts).

#### **Access Control to Use Specific Areas of Data Processing Systems**

The Company commits that the persons entitled to use their data processing system are only able to access the data within the scope and to the extent covered by their respective access permission (authorisation) and that personal data cannot be read, copied or modified or removed without authorisation. This shall be accomplished by various measures including:

- Employee policies and training in respect of each employee's access rights to the personal data;
- Allocation of individual terminals and /or terminal user, and identification characteristics exclusive to specific functions;
- Release of data only to authorised persons, including allocation of differentiated access rights and roles;
- Use of adequate encryption technologies; and
- Control of files, controlled and documented destruction of data.

#### **Availability Control**

The Company implements suitable measures to ensure that personal data are protected from accidental destruction or loss, including:

- Infrastructure redundancy; and
- Backup is stored at an alternative site and available for restore in case of failure of the primary system.



## Transmission Control

The Company implements suitable measures to prevent the personal data from being read, copied, altered or deleted by unauthorised parties during the transmission thereof or during the transport of the data media. This is accomplished by various measures including:

- Use of adequate firewall, VPN and encryption technologies to protect the gateways and pipelines through which the data travels;
- Certain highly confidential Personal data (e.g., personally identifiable information such as National ID numbers, credit or debit card numbers) is also encrypted within the system; and
- Providing user alert upon incomplete transfer of data (end to end check); and
- As far as possible, all data transmissions are logged, monitored and tracked.

## Input Control

The Company implements suitable input control measures, including:

- Authentication of the authorised personnel;
- Protective measures for the data input into memory, as well as for the reading, alteration and deletion of stored data;
- Utilisation of unique authentication credentials or codes (passwords);
- Providing that entries to data processing facilities (the rooms housing the computer hardware and related equipment) are kept locked;
- Automatic log-off of user ID's that have not been used for a substantial period of time; and
- Electronic recording of entries.

## Separation of Processing for Different Purposes

The Company implements suitable measures to ensure that data collected for different purposes can be processed separately, including:

- Access to data is separated through application security for the appropriate users;
- Modules within the company's database separate which data is used for which purpose, i.e. by functionality and function
- At the database level, data is stored in different normalised tables, separated per module, per Controller Customer or function they support; and
- Interfaces, batch processes and reports are designed for only specific purposes and functions, so data collected for specific purposes is processed separately.

## Documentation

The Company will keep documentation of technical and organisational measures in case of audits and for the conservation of evidence. The Company shall take reasonable steps to ensure that persons employed by it, and other persons at the place of work concerned, are aware of and comply with the technical and organisational measures set forth in this Appendix 2.

## Monitoring

The Company shall implement suitable measures to monitor access restrictions to the company's system administrators and to ensure that they act in accordance with instructions received. This is accomplished by various measures including:



- Individual appointment of system administrators;
- Adoption of suitable measures to register system administrators' access logs to the infrastructure and keep them secure, accurate and unmodified for at least six months;
- Yearly audits of system administrators' activity to assess compliance with assigned tasks, the instructions received by the Company and applicable laws;
- Keeping an updated list with system administrators' identification details (e.g. name, surname, function or organisational area) and tasks assigned and providing it promptly to the customer upon request.

