**DATA PROCESSOR AGREEMENT**

**BETWEEN:**

(1) [INSERT CUSTOMER COMPANY NAME AND REGISTERED ADDRESS] (the "**Data Controller**"); and

(2) TDS (TIME DATA SECURITY) LIMITED having its registered office at Unit 9/10, 2050 Orchard Avenue, Citywest Business Campus, Dublin 24, Ireland (the "**Data Processor**").

**BACKGROUND**

1. The Data Processor and the Data Controller have one or more written Master Subscription Agreement, Maintenance Agreements, purchase orders or other means of ordering (the “Agreement”) pursuant to which Data Processor provides software applications and any professional, implementation, maintenance or other support services to the Data Controller. The provision of such services may entail the Processing of Personal Data.
2. The parties have agreed to enter into this DPA to ensure the protection and security of data passed from the Data Controller to the Data Processor for processing or accessing by the Data Processor on the authority of the Data Controller for processingor otherwise received by the Data Processor for processing on the Data Controller's behalf complies with obligations in the Data Protection Laws.

**IT IS AGREED**

1. **DEFINITIONS AND INTERPRETATION**
   1. In this DPA:

"***Data***" means any information of whatever nature that, by whatever means, is provided to the Data Processor by the Data Controller, is accessed by the Data Processor on the authority of the Data Controller or is otherwise received by the Data Processor on the Data Controller's behalf,for the purposes of the Processing specified in clause 3.1(a), and shall include, without limitation, any Personal Data;

“***Data Protection Laws***” means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, applicable to the Processing of Personal Data under the Agreement. These include, but are not limited to the Data Protection Acts 1988-2003, European Union Directive 95/46/EC and European Union Regulation 2016/679 and any amending legislation;

"***Data Subject***", “***Data Processor***”, “***Data Controller***”, "***Personal Data***" and "***Processing***" shall have the same meanings as are assigned to those terms in the Data Protection Laws;

“***Standard Contractual Clauses***” means (where applicable) the agreement executed by and between the Data Controller and the Data Processor and attached as Schedule 2 pursuant to the European Commission’s decision of 5 February 2010 on Standard Contractual Clauses (European Commission Decision C (2010)593) for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection;

“***Schedule***” means the schedule annexed to and forming part of this DPA;

"***Services***" meansthe services provided by the Data Processor to the Data Controller under the Agreement;

* 1. In this DPA any reference, express or implied, to an enactment (which includes any legislation in any jurisdiction) includes references to:
  2. that enactment as re-enacted, amended, extended or applied by or under any other enactment (before, on or after the date of this DPA);
  3. any enactment which that enactment re-enacts (with or without modification); and
  4. any subordinate legislation made (before, on or after the date of this DPA) under that enactment, as re-enacted, amended, extended or applied as described in clause 1.2(a), or under any enactment referred to in clause 1.2(b).
  5. In this DPA:

1. references to a person include an individual, a body corporate and an unincorporated association of persons;
2. references to a party to this DPA include references to the successors or assignees of that party.
   1. Clauses 1.1 to 1.3 apply unless the contrary intention appears.
3. **APPLICATION OF THIS DPA**
   1. This DPA shall apply to:
4. all Data sent from the date of this DPA by the Data Controller to the Data Processor for Processing;
5. all Data accessed by the Data Processor on the authority of the Data Controller for Processing from the date of this DPA; and
6. all Data otherwise received by the Data Processor for Processing on the Data Controller's behalf;

in relation to the Services.

1. **DATA PROCESSING**
   1. In consideration of the undertakings provided by the Data Controller in clause 4, the Data Processor agrees to Process the Data to which this DPA applies in accordance with the terms and conditions set out in this DPA, and in particular the Data Processor agrees that it shall:
2. process the Data at all times in accordance with the Data Protection Laws and solely for the purposes (connected with provision by the Data Processor of the Services) and in the mannerspecified from time to timeby the Data Controller in writing and for no other purpose or in any mannerexcept with the express priorwritten consent of the Data Controller;
3. in a manner consistent with the Data Protection Laws and with any guidance issued by the Data Protection Commissioner, implement appropriate technical and organisational measures (as documented by the Data Processor in Appendix 2 to safeguard the Data from unauthorised or unlawful Processing or accidental loss, destruction or damage, and that having regard to the state of technological development and the cost of implementing any measures, such measures shall ensure a level of security appropriate to the harm that might result from unauthorised or unlawful processing or accidental loss, destruction or damage and to the nature of the Data to be protected;
4. implement the appropriate organisational and technological solutions in order to assist the Data Controller promptly with any and all issues which may arise in relation to the processing of the personal data, including the resolution of any complaints, the detection and reporting of any breach and the timely response to subject access requests which may be received from Data Subjects to whom the Personal Data refers;
5. ensure that only such of its employees who may be required by it to assist it in meeting its obligations under the Agreement shall have access to the Personal Data and that all such employees shall have undergone training in the law of data protection, their duty of confidentiality under contract and in the care and handling of the Personal Data;
6. ensure that each of its agents and subcontractors (as listed by the Data Processor in Schedule 1) are made aware of its obligations under this DPA with regard to the security and protection of the Data and shall require that they enter into binding obligations with the Data Processor in order to maintain the levels of security and protection provided for in this DPA;
7. not divulge the Data whether directly or indirectly to any person, firm or company or otherwisewithout the express prior writtenconsent of the Data Controller except to those of its employees, agents and subcontractors who are engaged in the Processing of the Data and are subject to the binding obligations referred to in clause 3.1(c) or except as may be required by any law or regulation;
8. in the event of the exercise by Data Subjects of any of their rights under the Data Protection Laws in relation to the Data, inform the Data Controller as soon as possible, and the Data Processor further agrees to assist the Data Controller with all data subject information requests which may be received from any Data Subject in relation to any Data;
9. not Process or transfer the Data outside of the European Union except with the express prior written authority of the Data Controller, where such authority constitutes correct signing of the Standard Contractual Clauses as provided in Schedule 2; and
10. allow its data processing facilities, procedures and documentation to be submitted for scrutiny by the Data Controller or its representatives in order to ascertain compliance with the terms of this DPA.
11. **OBLIGATIONS OF THE DATA CONTROLLER**
    1. In consideration of the obligations undertaken by the Data Processor in clause 3, the Data Controller agrees that it shall ensure that it complies at all times with the Data Protection Laws, and, in particular, the Data Controller shall ensure that any disclosure of Personal Data made by it to the Data Processor is made with the data subject's consent or is otherwise lawful.
12. **TERMINATION**
    1. This DPA shall terminate automatically upon termination or expiry of the Data Processor's obligations in relation to the Services, and on termination of this DPA the Data Processor shall forthwith deliver to the Data Controller or destroy, at the Data Controller's sole option, all the Data Controller's Data in its possession or under its control.
    2. Either party shall be entitled to terminate this DPA forthwith by notice in writing to the other if:
       1. Either party is in material breach of this DPA which, in the case of a breach capable of remedy, shall not have been remedied within thirty (30) days from the date of notice from the terminating party identifying the breach and requiring its remedy; or
       2. Either party becomes insolvent, has a receiver or liquidator appointed over the whole or any part of its assets, enters into any agreement with its creditors, or has an order made or resolution passed for it to be wound up (otherwise than in furtherance of a scheme for solvent amalgamation or reconstruction).
13. **GOVERNING LAW**
    1. This DPA will be governed by the laws of Ireland, and the parties submit to the exclusive jurisdiction of the Irish courts for all purposes connected with this DPA, including the enforcement of any judgement made under or in connection with it.
14. **WAIVER**
    1. Failure by either party to exercise or enforce any rights available to that party or the giving of any forbearance, delay or indulgence shall not be construed as a waiver of that party's rights under this DPA.
15. **INVALIDITY**
    1. If any term or provision of this DPA shall be held to be illegal or unenforceable in whole or in part under any enactment or rule of law such term or provision or part shall to that extent be deemed not to form part of this DPA but the enforceability of the remainder of this DPA shall not be affected provided however that if any term or provision or part of this DPA is severed as illegal or unenforceable, the parties shall seek to agree to modify this DPA to the extent necessary to render it lawful and enforceable and as nearly as possible to reflect the intentions of the parties embodied in this DPA including without limitation the illegal or unenforceable term or provision or part.
16. **ENTIRE AGREEMENT**
    1. This DPA and the documents attached to or referred to in this DPA shall constitute the entire understanding between the parties relating to this subject matter and shall supersede all prior agreements, negotiations and discussions between the parties. In particular the parties warrant and represent to each other that in entering into this DPA they have not relied upon any statement of fact or opinion made by the other, its officers, servants or agents which has not been included expressly in this DPA.
17. **NOTICES**
    1. Notices shall be in writing and shall be sent to the other party marked for the attention of the person at the address set out at the beginning of this DPA. Notices may be sent by recorded delivery or by email. Correctly addressed notices sent by recorded delivery shall be deemed to have been delivered two business days after posting and correctly directed emails shall be deemed to have been delivered instantaneously on transmission.
18. **INDEMNITIES**
    1. Each party shall indemnify the other against all demands, actions, penalties, fines and proceedings costs, expense including legal and professional expenses, damages, loss, including loss of business or loss of profits, liabilities, demands, claims, actions or proceedings which a party may incur arising out of any breach of this DPA howsoever arising for which the other party may be liable.
19. **DATA SUBJECT RIGHTS**
    1. The Data Subject is hereby entitled to enforce the terms and conditions of this DPA as a third-party beneficiary.

Signed........................................................................ Date....................................

on behalf of [INSERT CUSTOMER NAME]- the “**Data Controller**”

Signed......................................................................... Date....................................

on behalf of TDS (TIME DATA SECURITY) LIMITED - the “**Data Processor**”

**SCHEDULE 1**

**Subcontractors**

In order to undertake the Processing that has been commissioned by the Data Controller, the Data Processor shall avail itself of the services of third parties who will process data by its mandate (“**Subcontractors**”).

* + - Amazon Web Services, Inc (**AWS**): AWS provide a hosting service on the cloud which TDS use to store data collected by the Data Controller.
    - Amazon Web Services, Inc. P.O. Box 81226, Seattle, WA 98108-1226

# SCHEDULE 2

# Commission Decision C (2010)593

# Standard Contractual Clauses (processors)

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

Name of the data exporting organisation:

Address:

Tel.: ; fax: ; e-mail:

Other information needed to identify the organisation:

……………………………………………………………  
(the data **exporter**)

**And**

Name of the data importing organisation:

Address:

Tel.: ; fax: ; e-mail:

Other information needed to identify the organisation:

…………………………………………………………………  
(the data **importer**)

each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

**Definitions**

For the purposes of the Clauses:

1. *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[[1]](#footnote-1);
2. '*the data exporter'* means the controller who transfers the personal data;
3. *'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;
4. *'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;
5. '*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;
6. *'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:

1. 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;
2. 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;
3. that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
4. 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;
5. that it will ensure compliance with the security measures;
6. 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;
7. 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;
8. 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;
9. 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
10. that it will ensure compliance with Clause 4(a) to (i).

Clause 5

**Obligations of the data importer[[2]](#footnote-2)**

The data importer agrees and warrants:

1. 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;
2. 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;
3. that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
4. 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;
5. 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;
6. 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;
7. 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;
8. that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;
9. that the processing services by the subprocessor will be carried out in accordance with Clause 11;
10. 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.

1. 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:
  2. to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
  3. to refer the dispute to the courts in the Member State in which the data exporter is established.
  4. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

**Cooperation with supervisory authorities**

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

**Governing Law**

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

Clause 10

**Variation of the contract**

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

**Subprocessing**

* + 1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses[[3]](#footnote-3). Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
    2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
    3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
    4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

**Obligation after the termination of personal data processing services**

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

**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 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):

This section is deemed to be populated with the name of the Data Controller.

**Data importer**

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

This section is deemed to be populated with the name of the Data Processor.

**Data subjects**

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

To be completed

**Categories of data**

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

To be completed

**Special categories of data (if appropriate)**

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

To be completed

**Processing operations**

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

The subject matter of the processing is the provision of the service and the performance of the data importer’s other obligations under the MSA.

**DATA EXPORTER**

[Populated with details of, and deemed to be signed on behalf of, the data exporter:]

Name:………………………………

Authorised Signature ……………………

**DATA IMPORTER**

[Populated with details of, and deemed to be signed on behalf of, the 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):

**Technical and Organisational Measures of the Data Processor**

The organisational, operational and technological processes and procedures adopted must comply with the principles of ISO/IEC 27001:2013 as appropriate to the Services being provided to the Data Controller. The Data Controller will use ISO/IEC 27002:2013 as the basis for auditing compliance with the guarantees which the Data Processor provides in relation to this obligation. The Data Processor shall provide details of those measures here.

The Data Processor is compliant with ISO/IEC 27001:2013 which provides assurance that the Data Processor is effectively managing its information security risks in accordance with Data Protection Laws.

In addition, the following measures are implemented in the processing of the Data:

* data minimisation & pseudonymisation;
* data encryption at rest and in transit;
* Firewall and endpoint protection monitored at all times;
* Back-ups are performed regularly;
* Data Processor uses a third-party provider (Edgescan) to run vulnerability scans on the network on at least a monthly basis, as well as utilising other tools;
* Access to components and services is strictly controlled by the Data Processor’s security team;
* Wireless networks are secured using WPA2 encryption;

The following is implemented across the organisation to safeguard the Data:

* Employees are trained on information security and privacy procedures;
* Access to confidential information is restricted to authorized personnel only;
* Secure document destruction policies for all sensitive information;
* Account and password configuration requirements for all employees;
* Policies and procedures are reviewed periodically to ensure compliance with relevant legislation and industry best practice.

1. Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone. [↑](#footnote-ref-1)
2. Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter* *alia,* internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements. [↑](#footnote-ref-2)
3. This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision. [↑](#footnote-ref-3)