# Data Processing Addendum

This Data Processing Addendum ("**Addendum**") dated _____ ("**Addendum Effective Date**") forms part of the Terms of Service ("**Agreement**") between Pronto Holdings LTD (d/b/a Simplesat) ("**Simplesat**") acting on its own behalf and as agent for each Simplesat Affiliate (as defined below); and _____ ("**Customer**") acting on its own behalf and as agent for each Customer Affiliate.

The terms used in this Addendum shall have the meanings set forth in this Addendum. Capitalized 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.

The parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Agreement. The following obligations shall only apply to the extent required by Data Protection Laws (as defined below) with regard to the relevant Customer Personal Data (as defined below), if applicable.

**1.** Definitions.

1.1. "Affiliate" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with either Customer or Simplesat respectively, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.

1.2. "Controller," "Processor," "Data Subject," "Processing," "Supervisory Authority," "Personal Data Breach," and "Special Categories of Personal Data" shall have the same meaning as in the applicable Data Protection Law.

1.3. "Customer Personal Data" means Personal Data received from or on behalf of Customer that is covered by a Data Protection Law.

1.4. "Data Protection Laws" means: (i) the California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 *et seq.* ("CCPA"); and (ii) the EU General Data Protection Regulation 2016/679 ("GDPR"), as well as any other applicable national rule and legislation on the protection of personal data in the European Union that is already in force or that will come into force during the term of this Addendum, and any data protection laws substantially amending, replacing or superseding the GDPR following any exit by the United Kingdom from the European Union, or, and to the extent applicable, the data protection or privacy laws of any other Member State of the European Economic Area.

1.5. "EEA" means the European Economic Area as well as any country for which the European Commission has published an adequacy decision as published at https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en.

1.6. "Personal Data" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household.

1.7. "Restricted Transfer" means the onward transfer of Customer Personal Data that is located in the European Economic Area to Simplesat in a country that is not in the EEA, where such transfer would be prohibited by Data Protection Laws in the absence of the Standard Contractual Clauses or another adequate transfer mechanism as approved by the European Commission.

1.8. "Standard Contractual Clauses" means the standard contractual clauses for the transfer of Personal Data to Processors established in third countries which do not ensure an adequate level of data protection pursuant to the European Commission's decision (C(2010)593) of 5 February 2010 attached to this Addendum as Exhibit 2.

1.9. "Subprocessor" means any Processor (including any third party and any Simplesat Affiliate) appointed by Simplesat to Process Customer Personal Data on behalf of Customer or any Customer Affiliate.

2. Data Processing Terms. While providing the Services to Customer and Customer Affiliates pursuant to the Agreement, Simplesat and Simplesat Affiliates may Process Customer Personal Data on behalf of Customer or any Customer Affiliate as per the terms of this Addendum. Simplesat agrees to comply with the following provisions with respect to any Customer Personal Data submitted by or for Customer or any Customer Affiliate to the Services or otherwise collected and Processed by or for Customer or any Customer Affiliate by Simplesat or any Simplesat Affiliate. Simplesat shall only retain, use, or disclose Customer Personal Data as necessary for Simplesat's performance of its obligations under the Agreement and only in accordance with Customer's instructions. Simplesat shall not sell any Customer Personal Data as the term "selling" is defined in the CCPA. Simplesat shall not take any action that would cause any transfers of Customer Personal Data to or from Simplesat to qualify as "selling personal information" under the CCPA.

**3.** Processing of Customer Personal Data. Simplesat shall not Process Customer Personal Data other than on Customer's documented instructions unless Processing is required by Data Protection Laws to which Simplesat is subject, in which case Simplesat shall to the extent permitted by Data Protection Laws inform Customer of that legal requirement before Processing Customer Personal Data. For the avoidance of doubt, the Agreement, including any Processing reasonably necessary and proportionate to achieve the business purpose outlined in the Agreement, and any related SOW entered into by Customer shall constitute documented instructions for the purposes of this Addendum. Customer shall be responsible for: (1) giving adequate notice and making all appropriate disclosures to Data Subjects regarding Customer's use and disclosure and Simplesat's Processing of Customer Personal Data; and (2) obtaining all necessary rights, and, where applicable, all appropriate and valid consents to disclose such Customer Personal Data to Simplesat to permit the Processing of such Customer Personal Data by Simplesat for the purposes of performing Simplesat's obligations under the Agreement or as may be required by Data Protection Laws. Customer shall notify Simplesat of any changes in, or revocation of, the permission to use, disclose, or otherwise process Customer Personal Data that would impact Simplesat's ability to comply with the Agreement, or Data Protection Laws.

4. **Confidentiality.** Simplesat shall take reasonable steps to ensure that individuals that process Customer Personal Data are subject to obligations of confidentiality or are under an appropriate statutory obligation of confidentiality.

5. **Security.** Taking into account the state of the art, the costs of implementation and the nature, scope, context, and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Simplesat shall in relation to Customer Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

6. **Subprocessing.** Simplesat may engage Subprocessors in connection with the provision of the Services, provided that: (1) Simplesat has entered into a written agreement with each Subprocessor containing data protection obligations not less protective than those in this Addendum with respect to the protection of Customer Personal Data to the extent applicable to the nature of the Services provided by such

Subprocessor; and (2) Simplesat shall be liable for the acts and omissions of its Subprocessors to the same extent Simplesat would be liable if performing the Services of each Subprocessor directly under the terms of this Addendum. Simplesat's current list of Subprocessors for the Services is available at www.simplesat.io/subprocessors ("**Subprocessor List**"), which Customer hereby approves and authorizes. Simplesat may engage additional Subprocessors as Simplesat considers reasonably appropriate for the processing of Customer Personal Data in accordance with this Addendum, provided that Simplesat shall notify Customer of the addition or replacement of Subprocessors by making modifications to the Subprocessor List. Customer shall be responsible for periodically checking the Subprocessor List to remain informed of Simplesat's current list of Subprocessors. Customer may, on reasonable grounds, object to a new Subprocessor by notifying Simplesat in writing within 10 days of Simplesat updating the Subprocessor List, giving reasons for Customer's objection. Customer's failure to object within such 10 day period shall be deemed Customer's waiver of its right to object to Simplesat's use of a new Subprocessor added to the Subprocessor List. In the event Customer objects to a new Subprocessor, Simplesat will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Customer Personal Data by the objected to new Subprocessor without unreasonably burdening Customer. If Simplesat is unable to make available such change within a reasonable period of time, which shall not exceed 30 days, Customer may terminate, as Customer's sole and exclusive remedy, the portion of the Agreement with respect only to those Services which cannot be provided by Simplesat without the use of the objected to new Subprocessor by providing written notice to Simplesat.

7. **Data Subject Rights.** Simplesat shall promptly notify Customer if it receives a request from a Data Subject under any Data Protection Laws in respect to Customer Personal Data. In the event that any Data Subject exercises any of its rights under the Data Protection Laws in relation to Customer Personal Data, Simplesat will shall use reasonable commercial efforts to assist Customer in fulfilling its obligations as Controller following written request from Customer, provided that Simplesat may charge Customer on a time and materials basis in the event that Simplesat considers, in its reasonable discretion, that such assistance is onerous, complex, frequent, or time consuming.

8. **Personal Data Breach.** In the event of a Personal Data Breach, Simplesat will notify Customer without undue delay after becoming aware of the Personal Data Breach. Such notification may be delivered to an email address provided by Customer or by direct communication (for example, by phone call or an in-person meeting). Customer is solely responsible for ensuring that the appropriate notification contact details are current and valid. Simplesat will take reasonable steps to provide Customer with information available to Simplesat that Customer may reasonably require to comply with its obligations as Controller to notify impacted Data Subjects or Supervisory Authorities.

9. **Data Protection Impact Assessment and Prior Consultation.** In the event that Customer considers that the Processing of Customer Personal Data requires a privacy impact assessment to be undertaken or requires assistance with any prior consultations to any Supervisory Authority of Customer, following written request from Customer, Simplesat shall use reasonable commercial efforts to provide relevant information and assistance to Customer to fulfil such request, provided that Simplesat may charge Customer on a time and materials basis in the event that Simplesat considers, in its reasonable discretion, that such assistance is onerous, complex, frequent, or time consuming.

10. **Deletion or Return of Customer Personal Data**. Unless otherwise required by applicable Data Protection Laws, following termination or expiration of the Agreement Simplesat shall, at Customer's option, delete or return all Customer Personal Data and all copies to Customer.

11. **Relevant Records and Audit Rights.** Simplesat shall make available to Customer on request all information reasonably necessary to demonstrate compliance with this Addendum and allow for and contribute to audits, including inspections by Customer or an auditor mandated by Customer, not being competitors of Simplesat ("**Mandated Auditor**") of any premises where the Processing of Customer Personal Data takes place in order to assess compliance with this Addendum. Simplesat shall provide

reasonable cooperation to Customer in respect of any such audit and shall at the request of Customer, provide Customer with relevant records of compliance with its obligations under this Addendum. Simplesat shall promptly inform Customer if, in its opinion, a request infringes the Data Protection Laws or any other confidentially obligations with Simplesat's other customers. Customer agrees that: (1) audits may only occur during normal business hours, and where possible only after reasonable notice to Simplesat (not less than 20 days' advance written notice); (2) audits will be conducted in a manner that does not have any adverse impact on Simplesat's normal business operations; (3) Customer and any Mandated Auditor will comply with Simplesat's standard safety, confidentiality, and security procedures in conducting any such audits; and (4) any records, data, or information accessed by Customer or any Mandated Auditor in the performance of any such audit will be deemed to be the Confidential Information of Simplesat. To the extent any such audit incurs in excess of 20 hours of Simplesat personnel time, Simplesat may charge Customer on a time and materials basis for any such excess hours.

12. **International Data Transfer.** In the event that any Customer transfers any Customer Personal Data to Simplesat in a country outside the EEA, Customer on behalf of itself and each Customer Affiliate as data exporter and Simplesat on behalf of itself and each Simplesat Affiliate as data importer shall enter into the Standard Contractual Clauses, as set forth in **Exhibit 2**, which terms shall take precedence over those in this Addendum. In the event that the Standard Contractual Clauses cease to be recognized as a legitimate basis for the transfer of Personal Data to an entity located outside the EEA, Customer shall cooperate with Simplesat to identify and implement an alternative legitimate basis to the extent that one is required by the Data Protection Laws. The Standard Contractual Clauses shall come into effect on the later of: (1) the data exporter becoming a party to them; (2) the data importer becoming a party to them; and (3) commencement of the relevant Restricted Transfer.

13. **General Terms.** Any obligation imposed on Simplesat under this Addendum in relation to the Processing of Personal Data shall survive any termination or expiration of this Addendum. Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either: (1) amended as necessary to ensure its validity and enforceability, while preserving the intent of the provision as closely as possible or, if this is not possible, (2) construed in a manner as if the invalid or unenforceable part had never been contained therein. With regard to the subject matter of this Addendum, the provisions of this Addendum shall prevail over the Agreement with regard to data protection obligations for Personal Data of a Data Subject under Data Protection Laws. Notwithstanding anything to the contrary in this Addendum or in the Agreement (including, without limitation, either party's indemnification obligations), neither party will be responsible for any GDPR fines issued or levied under Article 83 of the GDPR against the other party by a regulatory authority or governmental body in connection with such other party's violation of the GDPR.

IN WITNESS WHEREOF, this Addendum is entered into and becomes a binding part of the Agreement with effect from the Addendum Effective Date first set out above.

| **CUSTOMER**: | **SIMPLESAT**: |
|---|---|
| Signature: | Signature: |
| Name: | Name: |
| Title: | Title: |

Date Signed:

Date Signed:

# EXHIBIT 1: DATA SECURITY

Simplesat shall implement and maintain the following data security measures in addition to the measures stated in the Agreement and in accordance with Data Protection Laws.

**Access Control**

Unauthorized persons shall be prevented from gaining physical access to premises, buildings or rooms, where data processing systems are located which process Personal Data. Exceptions may be granted for the purpose of auditing the facilities to third party auditors as long as they are supervised by the Simplesat and do not get access to the personal data themselves.

Simplesat has (without limitation) implemented the following controls:

| **Access Control** |
|---|
| a. Controls to specify authorized individuals permitted to access personal data |
| b. Implemented an access control process to avoid unauthorized access to company's premises |
| c. Implemented an access control process to restrict access to data centers / rooms were data servers are located |
| d. Utilizes video surveillance and alarm devices with reference to access areas |
| e. Ensured that personnel without access authorization (e.g. technicians, cleaning personnel) are accompanied all times when access data processing areas |

**System Access Control**

Data processing systems must be prevented from being used without authorization.

Simplesat has (without limitation) implemented the following controls:

| **System Access Control** |
|---|
| a. Ensured that all systems processing personal data (this includes remote access) are password protected during startup to prevent unauthorized persons from accessing any personal data<br>b. Provides dedicated user IDs for authentication against systems user management for every individual |
| c. Assigns individual user passwords for authentication |
| d. Controls to grant access only to authorized personnel and to assign only the minimum permissions necessary for those personal to access personal data in the performance of their function |
| e. Implemented a password policy that prohibits the sharing of passwords, outlines processes after a disclosure of a password and requires the regular change of passwords |
| f. Ensured that passwords are always stored in encrypted form |
| g. Implemented a proper procedure to deactivate user account when a user leaves the company or function |

| |
|---|
| h. Implemented a proper process to adjust administrator permissions when an administrator leaves company or function |
| i. Implemented a process to log all access to systems |

**Data Access Control**

Persons entitled to use a data processing system shall gain access only to the data to which they have a right of access, and personal data must not be read, copied, modified or removed without authorization in the course of processing.

Simplesat has (without limitation) implemented the following controls:

| **Data Access Control** |
|---|
| a. Restricted access to files and programs based on a "need-to-know-basis" |
| b. Stored physical media containing personal data in secured areas |
| c. Controls to grant access only to authorized personnel and to assign only the minimum permissions necessary for those personal to access personal data in the performance of their function |

**Data Transmission Control**

Personal Data must not be read, copied, modified, or removed without authorization during transfer or storage and it shall be possible to establish to whom Personal Data was transferred.

Simplesat has (without limitation) implemented the following controls:

| **Data Transmission Control** |
|---|
| a. Transport physical media containing personal data in sealed containers |
| b. Have shipping and delivery notes |

**Data Entry Control**

Simplesat shall be able retrospectively to examine and establish whether and by whom Personal Data have been entered into data processing systems, modified, or removed.

Simplesat has (without limitation) implemented the following controls:

| **Data Entry Control** |
|---|
| a. Controls to log administrators' and users' activities |
| b. Controls to permit only authorized personnel to modify any Personal Data within the scope of their function |

**Job Control**

Personal Data being processed in the performance of a Services shall be processed solely in accordance with the Agreement and in accordance with appropriate instructions.

Simplesat has (without limitation) implemented the following controls:

| **Job Control** |
|---|
| a. Established controls to ensure processing of Personal Data only for contractual performance |
| b. Controls to ensure staff members and contractors comply with written instructions or contracts |
| c. Ensured that data is always physically or logically separated so that, in each step of the processing, the customer from whom Personal Data originates can be identified. |

**Availability Control**

Personal Data shall be protected against disclosure, accidental or unauthorized destruction or loss.

Simplesat has (without limitation) implemented the following controls:

| **Availability Control** |
|---|
| a. Controls to ensure that Personal Data is not used for any purpose other than for the purposes it has been contracted to perform |
| b. Controls to prevent removal of personal data from Simplesat's business computers or premises for any reason (unless company has specifically authorized such removal for business purposes). |
| c. Implemented network firewalls to prevent unauthorized access to systems and services |

**Organizational Requirements**

The internal organization of Simplesat shall meet the specific requirements of data protection. In particular, Simplesat shall take technical and organizational measures to avoid the accidental mixing of Personal Data.

Simplesat has (without limitation) implemented the following controls:

| **Organizational Requirements** |
|---|
| a. Designated a person responsible for data protection |
| b. Obtained the written commitment of the employees to maintain confidentiality |

EXHIBIT 2: STANDARD CONTRACTUAL CLAUSES

**Commission Decision C(2010)593**
**Standard Contractual Clauses (processors)**

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

**Name of the data exporting organisation:** ……

Address:

Tel.: ; fax: ; e-mail:

Other information needed to identify the organisation:

……
(the data **exporter**)

And

**Name of the data importing organisation:** ……

Address:

Tel.: ; fax: ; e-mail:

Other information needed to identify the organisation:

……
(the data **importer**)

each a "party"; together "the parties",

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

Clause 1

**Definitions**

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) 'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

**Details of the transfer**

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

**Third-party beneficiary clause**

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

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

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

**Obligations of the data exporter**

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

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

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

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

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

Clause 5

**Obligations of the data importer**

The data importer agrees and warrants:

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

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

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

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

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

  (ii) any accidental or unauthorised access, and

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

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

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

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

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

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

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

Clause 6

**Liability**

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

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

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

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

Clause 7

**Mediation and jurisdiction**

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

**Cooperation with supervisory authorities**

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

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

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

Clause 9

**Governing Law**

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

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. 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…….

**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…….

**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):*

The data exporter's activates relevant to the transfer shall be as is described in any Statement of Work or Order Form that makes reference to, is incorporated under, or is subject to the Agreement agreed to between data importer and data exporter.

**Data importer**

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

The data importer's activates relevant to the transfer shall be as is described in any Statement of Work or Order Form that makes reference to, is incorporated under, or is subject to the Agreement agreed to between data importer and data exporter.

**Data subjects**

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

☑ Customers
☑ Prospective Customers
☑ Employees
☐ Prospective Employees
☐ Service Providers
☐ Other …….

**Categories of data**

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

☑ Name
☑ Username or Login Information
☑ Email Address
☐ Phone Number
☐ Contact Details
☐ Account and Financial Information
☐ Credit Card Information
☐ SSN or National ID
☐ Passport Information
☑ IP Address
☐ Other …….

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

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

NOT APPLICABLE

**Processing operations**

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

The nature and purposes of Processing shall be as is described in any Statement of Work or Order Form that makes reference to, is incorporated under, or is subject to the Agreement agreed to between data importer and data exporter.

**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)

Those data security measures listed in Exhibit 1 of the Addendum.