DATA PROCESSING ADDENDUM

This Data Processing Addendum (the "DPA") is entered into as of the last date signed below (the "Effective Date") by and between Comodo Security Solutions, Ltd. or a Comodo Affiliate, (hereafter the "Processor" or "Comodo"), and customer identified below, on its behalf and in the name and on behalf of its affiliated companies (the "Controller"). This DPA may refer to Controller and Processor each as a "Party" and collectively as the "Parties." Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement.

1. INTRODUCTION

1.1. Controller has procured certain services provided by Processor pursuant to a written or electronic agreement ("Agreement"). This DPA satisfies Article 28 (3) of the GDPR (defined below) between Controller and Processor),and is incorporated in the Agreement and is intended to reflect the Parties' agreement with regard to the Processing of Personal Data.

1.2. Processor receives and/or is granted access to Personal Data (as defined below) in connection with the provision of the services under the Agreement.

1.3. To comply with applicable European Union Data Protection Legislation (including Regulation (EU) 2016/679 (the "General Data Protection Regulation" or "GDPR") and laws implementing or supplementing the GDPR), Controller requires Processor to agree to this DPA.

1.4. Controller and Processor wish to agree to this DPA on the terms and conditions stated below.

1.5. The obligations and rights of Controller and Controller's affiliates (as applicable) are set out in the Agreement and the DPA.

2. DEFINITIONS

In addition to capitalized terms defined in the Agreement, the following terms shall bear the following meanings:

2.1 "**Applicable Law**" means any applicable (a) statute, regulation, regulatory requirement, by law, ordinance, subordinate legislation, or other law (regardless of its source), mandatory guidance, or code of practice (including in each case any judicial or administrative interpretation of it) in force from time to time in any applicable jurisdiction; or (b) judgment of a relevant court of law or sanction, directive, order, or requirement of any regulatory authority.

2.2 "**Comodo Affiliate**" means an entity which is controlled by, controls or is in common control with Comodo Security Solutions Ltd., including Comodo Security Solutions, Inc.

2.3 "**Data Protection Legislation**" means European Directives 95/46/EC and 2002/58/EC and any legislation and/or regulation implementing or made pursuant to them, or which amends, replaces, re-enacts or consolidates any of them (including the GDPR), and all other applicable laws relating to the processing of Personal Data and privacy that may exist in any relevant jurisdiction.

2.4 "**Personal Data**" means any information relating to an identified or identifiable Data Subject that is collected, transferred, or Processed in connection with the Agreement and this DPA, and that is classified as personal data under Data Protection Legislation (as amended or replaced from time to time), or as specified in the Agreement.

2.5 "**Standard Contractual Clauses**" means the standard contractual clauses annex to the EU Commission Decision 2010/87/EU of 5 February 2010, for the transfer of Personal Data to processors established in Third Countries (and any successor clauses).

2.6 "**Third Countries**" means countries outside of the European Union/European Economic Area which are not recognized as countries providing adequate protection of Personal Data.

2.7 "**Controller**," "**Data Subject**," "**Personal Data Breach**," "**Processing**," "**Processor**," and "**Supervisory Authority**" shall be interpreted in accordance with the GDPR or other applicable Data Protection Legislation in the relevant jurisdiction.

3. INTERPRETATION

3.1 The provisions of the DPA (in particular, the provisions regarding governing law and jurisdiction) apply to this DPA. If there is any conflict or inconsistency between this DPA and the Agreement, the provisions contained in this DPA shall prevail to the extent of the inconsistency, provided always that nothing in this DPA shall permit Processor to Process Personal Data in a manner prohibited by the Agreement, nor shall this DPA narrow or reduce the scope of any Processor obligations under the Agreement (including the definitions in the Agreement applicable to Personal Data or Personal Data Breach). The Parties hereby agree that the Agreement is amended accordingly to give effect to this Section 3.1.

3.2 To the extent that a term of this DPA requires the performance by a Party of an obligation "in accordance with Data Protection Legislation" (or similar), this term requires performance in accordance with such Data Protection Legislation as is in force and applicable at the time of performance and, if the relevant obligation is not then a requirement under applicable Data Protection Legislation, it shall not apply until it is so required.

4. PROCESSING

4.1 **Processing Personal Data.** The Parties agree that the subject matter and details of Processing of Personal Data are set forth in the Agreement and/or this DPA, (including Annex 1). Processor shall Process Personal Data for the duration of the Agreement (unless otherwise agreed in writing) only (a) as necessary to effect Processor's obligations under the Agreement; and/or (b) on documented and customary instructions from Controller, unless otherwise required by Applicable Law(s). Processor shall notify Controller if Processor believes such instruction(s) violate(s) applicable Data Protection Legislation.

4.2 **Processor Personnel.** Processor shall take reasonable steps to ensure that access to Personal Data is limited on a need to know/access basis, and that all Processor personnel (including sub-processors) with such access are competent to handle the Personal Data and subject to confidentiality obligations with respect to Controller's Personal Data.

4.3 **Sub-Processing.** With respect to any sub-processor:

4.3.1 Processor shall ensure that the sub-processor is committed, by written contract, to provide the level of protection for Personal Data required by the Agreement, this DPA, and Applicable Law(s); and

4.3.2 Controller agrees that Comodo may engage either Comodo affiliated companies or third party providers as sub-Processors under this Addendum and hereby provides Comodo with a general written authorization for the engagement of such sub-processors in the provision of services. Comodo will restrict the processing activities performed by sub-Processors to only what is strictly necessary to provide the services to Controller. Comodo shall impose appropriate contractual obligations in writing upon the sub-Processors that are no less protective than this Addendum. Comodo makes available to Controller a list of all sub-Processors used by Comodo in the provision of service, which is available upon written request and subject to confidentiality and security obligations.

5. DATA SUBJECT RIGHTS

5.1 Processor shall (a) assist Controller to fulfill Controller's obligations regarding a Data Subject's request to exercise his or her rights, as applicable, under applicable Data Protection Legislation (*e.g.*, rights of access, rectification, erasure, restriction of processing, data portability, objection, etc.); and (b) immediately notify Controller if it receives a request from a Data Subject to exercise his or her rights, as applicable, under applicable Data Protection Legislation regarding Personal Data.

6. INFORMATION SECURITY

6.1   Information Security. Processor shall implement reasonable and appropriate technical and organizational measures to provide an adequate level of security and protect Personal Data against unauthorized or unlawful Processing or a Personal Data Breach. Without limiting the foregoing, such technical and organizational measures may be set forth in the Agreement and/or this DPA (including Annex 2).

6.2   Personal Data Breach. In the event Processor becomes aware of a Personal Data Breach involving Personal Data, it shall:

6.2.1   Immediately notify Controller of (a) the nature of the Personal Data Breach and any actions taken (or proposed to be taken) to address or mitigate the Personal Data Breach; (b) the number of individuals, the location of the individuals potentially affected (if known) and types of Personal Data concerned; (c) contact information for Processor's data protection officer or other relevant contact who can provide additional information; and

6.2.2   Assist Controller in meeting its obligations under applicable Data Security Legislation.

7.   TRANSFERS OUTSIDE THE EUROPEAN UNION/EUROPEAN ECONOMIC AREA

7.1   Processor shall only transfer Personal Data from the European Union to a country outside the European Economic Area (a) with Controller's prior written approval to such transfer; and (b) pursuant to an approved data transfer mechanism. The Parties shall use an appropriate data transfer mechanism, which may include (c) a determination of "adequacy" for the country in which Processor processes the Personal Data; (d) Standard Contractual Clauses, set out in Annex 3 to this DPA; or (e) other data transfer mechanisms approved under applicable Data Protection Legislation. For this DPA, the Parties will rely on either clause (c), clause (d), or clause (e) above.

7.2   The agreed-upon data transfer mechanism shall apply for any Personal Data that originated in the European Union or relates to Data Subjects based in the European Union. No transfer of Personal Data from inside the European Union to a country outside the European Economic Area shall take place prior to the implementation of the agreed-upon data transfer mechanism.

7.3   In case of any conflict or inconsistency between the provisions of this DPA and the agreed-upon data transfer mechanism, or in the event that the data transfer mechanism imposes more onerous obligations than the provisions of this DPA, the provisions contained in the data transfer mechanism shall prevail to the extent of the inconsistency, provided always that nothing in the data transfer mechanism shall permit Processor to Process Personal Data in a manner prohibited by this DPA or the Agreement.

8.   DATA PROTECTION IMPACT ASSESSMENT AND OTHER OBLIGATIONS

8.1   In relation to Processing of Personal Data by Processor, Processor shall, at the written request of Controller:

8.1.1   Assist Controller with any data protection impact assessments or prior consultations with Supervisory Authorities, as required under applicable Data Protection Legislation;

8.1.2   Make available to Controller all information necessary to demonstrate compliance with Processor's obligations under applicable Data Protection Legislation, this DPA, and the Agreement; and

8.1.3   Contribute to any audits.

9.   DELETION OR RETURN OF PERSONAL DATA

9.1   Upon termination or expiration of the Agreement, at Controller's option, Processor shall delete or return all Personal Data, including any existing copies thereof in Processor's possession, unless Applicable Law(s) require(s) otherwise.

10.   GENERAL

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

10.3   Equitable Relief. Processor acknowledges that any breach of its covenants or obligations set forth in this DPA may cause Controller irreparable harm for which monetary damages would not be adequate compensation and agrees that, in the event of such breach or threatened breach, Controller may be entitled to seek equitable relief, including a restraining order, injunctive relief, specific performance, and any other relief that may be available from any court, in addition to any other remedy to which Controller may be entitled at law or in equity. Such remedies shall not be deemed to be exclusive, but shall be in addition to all other remedies available at law or in equity, subject to any express exclusions or limitations in this DPA to the contrary.

10.5   Signature. By signing below, each Party acknowledges that it has carefully read and fully understands this DPA, and each agrees to be bound by the terms of this DPA. This DPA may be signed in counterparts, using an electronic or handwritten signature, which constitute one copy and are of equal effect, whether on original or electronic copies.

IN WITNESS WHEREOF, the undersigned Parties agree to be bound by this DPA as of the Effective Date.

Controller Signature

Controller Name:
Signature:
Name (printed) and Title:
Date Signed:

Comodo Signature

Controller Name: Comodo Security Solutions Ltd. 3rd Floor, 26 Office Village, Exchange Quay Trafford Road, Salford, Manchester, M53EQ UK
Signature:
Name (printed) and Title:
Date Signed:

ANNEX 1:
Subject Matter and Details of Processing

Data Controller / Exporter: The data export is (please specify briefly your activities relevant to the transfer):

The data exporters are the EU affiliates of

_____ as listed in Annex 4

Data Processor / Importer: The data importer is:

The data importer(s) is Comodo Security Solutions, Inc., a global group of companies providing internet security and cybersecurity providing services to Controller that involve Controller's data

Data Subjects: The personal data transferred may concern the following categories of data subjects, as further specified in the Agreement

     __X__ Customer's employees, representatives, customers, vendors, and/or any other business contacts including senders and recipients of emails, as applicable.

     _____ Other [to be identified by Controller]

Categories of Data: The Personal Data transferred concern (but are not limited to) data described in the product or services Agreement.

- Other data reasonably required to implement the services and performance requested by Controller under the Agreement.

Special Categories of Data: The Personal Data transferred will not include sensitive personal data including data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union memberships, genetic data, biometric data, data concerning health, or data concerning a natural person's sex life or sexual orientation.

Processing Operations: The Personal Data transferred will be subject to the following basic processing activities:

- Processing activities in the performance of the services as set forth in the Agreement.

ANNEX 2:
Technical and Organizational Security Measures

Comodo maintains policies and procedures in support of its privacy and security program, including: Information Security Policy, Risk Assessment Policy & Procedures, Business Continuity Plan, Remote Access & Bring Your Own Device (BYOD) Policy, Access Control & Password Policy, Clear Desk & Screen Policy, Third Party/Outsourcing Policy & Procedure, Supplier Due Diligence Policy & Questionnaire, Data Retention & Erasure Policy, Data Protection Policy & Procedure, and Asset Management Policy.

Information and physical security is the protection of the information and data that the Comodo creates, handles and processes in terms of its confidentiality, integrity and availability from threats, internally and externally. Information security is an enabling mechanism for information sharing between parties.

Comodo is committed to preserving information security of all physical, electronic and intangible information assets across the business, including, but not limited to all operations and activities. We aim to provide information and physical security to: protect customer, 3rd party and client data; preserve the integrity of the Comodo and our reputation; comply with legal, statutory, regulatory and contractual compliance; ensure business continuity and minimum disruption; minimize and mitigate against business risk.

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:

Affiliates listed in Annex 4

Other information needed to identify the organisation:

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

And

Name of the data importing organisation: Comodo Security Solutions, Inc.

Address: 1255 Broad Street , Clifton, New Jersey 07013

Tel.:+1 (973) 859-4000

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[1];

(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

---

[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.

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[2]

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

---

[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.

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[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:

---

[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.

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature…………………………………….

(stamp of organisation)

On behalf of the data importer:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature…………………………………….

(stamp of organisation)

Appendix 1 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

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

……

Data importer

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

……

Data subjects

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

……

Categories of data

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

……
………………………………………………………

Special categories of data (if appropriate)

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

……

Processing operations

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

……

DATA EXPORTER

Name:………………………………

Authorised Signature ……………………

DATA IMPORTER

Name:………………………………

Authorised Signature ……………………

<u>**Appendix 2 to the Standard Contractual Clauses**</u>

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):

The technical and organizational security measures for this Appendix are specified in Annex 2 of the Data Processing Addendum.

ANNEX 4:
Controller Affiliates

NAME	ADDRESS