Supplier Information Security and Privacy Exhibit
("Security Exhibit")

1. Definitions

In this Exhibit F, any reference to Supplier will be deemed to be a reference to Cisco. In addition the following terms shall have the following meanings:

a. "**Terms**" means the terms and conditions to which this Supplier Security Exhibit is attached and incorporated as well as any applicable Statement of Work, Work Order, Order, or similar commercial document related to the products or services Supplier provides.

b. **"Approved Jurisdiction**" means a member state of the European Economic Area, or other jurisdiction as may be approved as having adequate legal protections for data by the European Commission currently found here: **http://ec.europa.eu/justice/data-protection/data-collection/data-transfer/index_en.htm.**

c. **"Customer Data**" means the Customer data, applications, and other content that Supplier may have, Process or have access to. Customer Data includes any Customer data (including any "downstream" End User data) or applications. For clarity, to the extent Customer Data contains Personal Data, the terms related to Personal Data will also apply.

d. **"Customer"** has the meaning given in clause 2 of these Terms.

e. **"Data Controller**" means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data

f. **"Data Processor**" means a natural or legal person, public authority, agency or any other body, which processes personal data on behalf of the Data Controller.

g. **"EEA"** or "**European Economic Area**" means those countries that are members of European Free Trade Association (EFTA), and the then-current, post-accession member states of the European Union.

h. **"End User"** means any Customer.

i. "**EU Directives**", the Data Protection Directive 95/46/ EC and Directive on Privacy and Electronic Communications 2002/58/EC and (and respective local implementing laws) concerning the processing of personal data and the protection of privacy in the electronic communications sector, and any amendments or replacements to them. For clarity, the EU Directives are a subset of Applicable Law.

j. **"Special Categories of Data"** means Personal Data that contains such information such as Social Security number, national ID number, bank or other

financial account information (including PINs), mother's maiden name, biometric data (e.g. finger print data), or sensitive personal data (as that term is defined by the Data Protection Directive 95/46/EC).

k. "**Information Security Breach**" means an actual or suspected theft, loss, or corruption of Customer Data, or an actual or suspected unauthorized access, receipt, use, or modification of Customer Data.

l. "**Personal Data**" means data that relates to an identified or identifiable natural person on its own or together with other information likely to come into the hands of the data holder.

m. To "**Process**" data means any operation or set of operations that is performed upon Customer Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, access to, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction. "**Processes**" and "**Processing**" shall be construed accordingly.

n. **"Sub-Processor"** means a person who processes Personal Data on behalf of a Data Processor.

o. "**Supplier**" means Cisco and its affiliates, including any contractors, officers, agents, or employees and any Supplier subcontractors (in all cases if subcontracting is allowed by the Terms).

2 **General Standards.**

2.1 **Security Measures**. Supplier will implement and maintain, as a part of its security program a written information security program that is appropriate to the nature and scope of Supplier's activities and services, and as reasonably requested by Customer designed, maintained, and updated, as necessary, to reasonably address known risks to Customer Data. The information security program will contain the security measures provided in this Security Exhibit (including any Attachments and referenced certifications) and any terms contained in the Terms as it relates to Customer Data to protect Customer Data against loss, unauthorized alteration, unauthorized disclosure or access, all other unauthorized or unlawful forms of Processing, and any Information Security Breach. Specifically, Supplier will implement the technical and organizational security measures contained in Attachment 3, Appendix 2 (the "**TOMs"**). The Supplier shall achieve the ISO 27001:2013 certification not later than December 31, 2015.

2.2 **Limitation on Processing**. Supplier will only Process or use Customer Data on its systems or facilities to the extent necessary to perform its obligations under the Terms and only for the purposes provided under the Terms.

2.3 **No Transfer of Rights in Customer Data**. Subject to Clause 3.3(g), Supplier may not lease, sell, distribute, or otherwise encumber Customer Data (including

in aggregated form) unless mutually agreed to by separate signed, written agreement.

2.4 **Limitation on Obligations**. The requirements contained in this Security Exhibit will apply to the extent Supplier Processes Customer Data and has control over such Processing or may access Customer Data.

3. **Data Protection and Privacy.** If Supplier Processes Personal Data in the course of providing the products or services under the Terms, the following additional terms will apply:

3.1 Data Controller, Data Processor and Data Sub-processor.

a) Subject to clause 3.1(c), Supplier will Process the Personal Data solely on behalf of Customer.

b) Where Supplier is Processing the Personal Data of End Users, Supplier will act as a Sub-processor of Customer.

c) Where Supplier processes Personal Data relating to Customer's employees or Customers' employees in order to administer the provision of the services (such as the use of an administrator's contact details) the Supplier will do so as a Data Controller.

3.2 Compliance with Applicable Law. The parties shall comply with all Applicable Laws (including without limitation, the EU Directives, the FTC Act, the Gramm-Leech-Bliley Act, and the Personal Information Protection and Electronic Documents Act) in the provision of the Services, as set out in and in accordance with Section 17 of the Terms. Supplier expressly disclaims any responsibility or obligation to comply with the Health Insurance Portability and Accountability Act (HIPAA), including any obligations of a Business Associate under HIPAA.

3.3 Supplier Practices. Supplier will ensure that it will:

a) Only Process the Personal Data in accordance with Customer instructions, the Terms, and this Security Exhibit, but only to the extent that such instructions are consistent with Applicable Law. If Supplier reasonably believes that Customer's instructions are inconsistent with Applicable Law will promptly notify Customer of such;

b) Implement and maintain commercially reasonable and appropriate physical, technical and organizational security measures described in this Security Exhibit (including any Attachments or referenced certifications) to protect Personal Data against accidental or unlawful destruction; accidental loss, alteration, unauthorized disclosure or access; all other unlawful forms of Processing, and any Information Security Breach;

c) Maintain accurate records consistent with Supplier's provision of the Services

and role as a Data Processor or Sub-processor, with respect to any Personal Data received from Customer under the Terms**;**

d) Take reasonable steps to ensure the reliability of its staff and any other person acting under its supervision who may come into contact with, or otherwise have access to and Process, Personal Data; and ensure that such personnel are aware of their responsibilities under this Security Exhibit and any Applicable Law (or Supplier's own written binding policies are at least as restrictive as this Security Exhibit);

e) To the extent that in providing the Services to Customer Supplier Processes End User Personal Data which is subject to the EU Directives:

   1. Supplier shall not disclose, transfer to, access, or Process the Personal Data in a different jurisdiction to the jurisdiction to which the End User uploaded it unless instructed or authorized to do so by that End User, in which case the Standard Contractual Clauses described in Clause 5 shall apply to the extent the second jurisdiction is other than an Approved jurisdiction;

   2. notwithstanding clause 3.3(e)(i), Customer acknowledges that as part of the Services Supplier may provide support from jurisdictions which are not Approved Jurisdictions, which may involve Supplier manipulating or remotely operating the infrastructure and software on which Personal Data resides but which shall not involve Supplier accessing Personal Data unless expressly authorized to do so by Customer. In any event, Supplier shall provider the support described in this paragraph (ii) in compliance with the Standard Contractual Clauses described in Clause 5.

f) To the extent that in providing the Services to Customer Supplier Processes End User Personal Data which is not subject to the EU Directives:

   1. Supplier shall not disclose, transfer to, access, or Process the Personal Data in a different jurisdiction to the jurisdiction to which the End User uploaded it unless authorized to do so by that End User and Supplier complies with the TOMs in carrying out such disclosure, transfer, access or Processing;

   2. notwithstanding clause 3.3(f)(i), Customer acknowledges that as part of the Services Supplier may provide support from remote jurisdictions, which may involve Supplier manipulating or remotely operating the infrastructure and software on which Personal Data resides but which shall not involve Supplier accessing Personal Data unless expressly authorized to do so by Customer, and Supplier complies with the TOMs in providing such support.

g) Notify Customer promptly and provide Customer an opportunity to intervene in any judicial or administrative process when Supplier is required by law, court order, warrant, subpoena, or other legal or judicial process to disclose any

Personal Data to any person other than Customer, or an Customer sub-contractor expressly approved by Customer or the relevant Customer to receive such information, provided such notification is not prohibited by law. Subject to the foregoing conditions, Customer acknowledges that Supplier's compliance with such a legal obligation is permitted under the Terms and under its agreements with its Resellers.

h) To the extent the relevant Service requires the Supplier to be responsible for the accuracy of any Personal Data, make all reasonable efforts to ensure that Personal Data are accurate and up to date at all times while in its custody or under its control, to the extent Supplier has the ability to do so;

i) Provide full, reasonable cooperation and assistance to Customer in allowing the persons to whom Personal Data relate to have access to those data and to delete or correct such Personal Data if they are demonstrably incorrect (or, if Customer does not agree that they are incorrect, to have recorded the fact that the relevant person considers the data to be incorrect);

j) Provide Customer with such information as Customer may reasonably require from time to time to demonstrate Supplier's or the sub-contractor's compliance with this Security Exhibit including Cisco Applicable Law as set out in and in accordance with Section 17 of the Terms;

k) Provide such assistance as Customer reasonably requests and Supplier or a sub-contractor is reasonably able to provide with a view to meeting any applicable filing, approval or similar requirements in relation to Clause 5 arising under Applicable Law.

l) Assist Customer if Customer needs to provide information (including details of the services provided by Supplier) to a competent supervisory authority, whether directly or indirectly via a Customer, to the extent that such information is solely in the possession of Supplier or its subcontractors.

m) To the extent not prohibited by any of Supplier's confidentiality obligations, promptly notify Customer in writing if and to the extent that any investigation, litigation or other dispute (excluding any arbitration proceedings) finds that Supplier has materially not complied with the TOMs, and such non-compliance is relevant to the Services Supplier provides to Customer under the Terms.

n) On termination of the Terms and the Customer Service for whatever reason, or upon written request at any time during the Term, Supplier will cease to Process any Personal Data received from Customer, and within a reasonable period will at the request of Customer: 1) return the Personal Data; 2) destroy all the Personal Data in its control; and/or 3) securely and completely erase all Personal Data (using a policy aligned with standards such as US Department of Defence 5220.22 M or British HMG Infosec Standard 5, Enhanced Standard) in its possession or control. At Customer's request, Supplier will give Customer a certificate signed by one of its senior managers, confirming that it has fully

complied with this Clause.

3.4 Special Categories of Data. To the extent that Supplier Processes Special Categories of Data, the security measures referred to in this Security Exhibit shall also include, at a minimum (a) routine risk assessments to Supplier's (or its subcontractor's) information security program, and (b) regular testing and monitoring to measure and confirm the effectiveness of the information security program's key controls, systems, and procedures. Further, Supplier shall protect all Special Categories of Data stored on electronic databases, servers, or other forms of non-mobile devices against all reasonably anticipated forms of compromise by use of the safeguards contained in Attachment 3, Appendix 2.

4. <u>Certifications.</u>

Supplier will provide Customer with (i) the executive summary of the results of any data privacy or data security audits and (ii) all certifications it currently maintains that apply to the systems, policies, and procedures that govern the Processing of Customer Data.

4.1 Customer agrees to keep the contents of and reports related to Supplier's certifications confidential consistent with the confidentiality terms contained in the Terms between the parties. This does not prevent Customer from disclosing a certification, subject to the imposition of substantially similar confidentiality undertakings on the recipient of such disclosure:

a) to respond to a claim that Customer does not maintain adequate security which relates to the Services or products provided by Supplier, provided that Customer first notifies Supplier of the claim and provides Supplier with the opportunity to intervene in such claim; or

b) subject to obtaining Supplier's prior written consent (not to be unreasonably withheld or delayed), to provide Customers with certification information related to the Services.

5. <u>Standard Contractual Clauses for the Processing of Personal Data</u>. If in accordance with clause 3.3(e) Supplier Processes Personal Data in a jurisdiction that is not an Approved Jurisdiction, the following additional terms will apply to Supplier and Supplier's subcontractors and/or affiliates (where subcontracting or performance is allowed by the Terms):

5.1 The Standard Contractual Clauses for the Transfer of Personal Data ("**Model Clauses**") are incorporated into this Exhibit as Attachment 3 and will apply where Supplier will be Processing Personal Data received from an End User whose Personal Data is subject to the EU Directives in a jurisdiction that is not an Approved Jurisdiction. If such Model Clauses are superseded by new or modified Model Clauses, and Supplier decides in its sole discretion to use such new or modified Model Clauses for End Users and Resellers, the new or modified Model Clauses shall be deemed to be incorporated into this Exhibit replacing the then-current Attachment 3, and Supplier will promptly begin

complying with such Model Clauses to the extent they apply. Customer, its Reseller and the Supplier will abide by the obligations set forth under Model Clauses for data importer and/or subprocessor as the case may be.

5.2 If Supplier subcontracts any Processing of such Personal Data (if expressly allowed by the Terms and Applicable Law), it will:

a) Notify Customer in advance of such processing and obtain Customer's written permission before proceeding**.**

b) Ensure that Supplier's Subcontractor(s) abide by Clause 5 with respect to such Personal Data.

6. **Limited retention of Customer Data**. Subject to Applicable Law, Supplier shall not retain any Customer Data for longer than is necessary for the performance of the Services or as requested by Customer.

7. **Information Security Breach**. Where Supplier knows or reasonably suspects that an Information Security Breach has affected Customer Data, Supplier shall promptly notify Customer (in any case within the later of 24 hours or one (1) business day following such discovery in the case of a known breach, or 48 hours in the case of a suspected breach) and cooperate with Customer in any post-breach investigation, remediation, and communication efforts. In addition, Supplier will conduct a forensic and security review and audit in connection with such Information Security Breach and make any reasonably required or reasonably requested updates to its security and privacy measures to prevent recurrence.

8. **Remedies**.

Supplier agrees that, in the event of a breach of this Security Exhibit, Customer will have an adequate remedy in damages and therefore Customer shall be entitled to seek injunctive or equitable relief to immediately cease or prevent the use or disclosure of Personal Data not contemplated by the Terms and to enforce the terms of this Security Exhibit or ensure compliance with any Applicable Law.

Attachment 1
Reserved

Attachment 2- Reserved

Attachment 3

Standard Contractual Clauses

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: [Insert Name of Customer Entity Sending Data to Supplier]

Address:[Provide corporate address of the above Entity]

Tel.:[Insert Phone Number of Customer employee responsible for managing Supplier]; e-mail:[Insert email Customer employee responsible for managing Supplier OR group alias email]

("**Data Exporter" or "Customer"**)

And

Name of the data importing organisation:[Insert name of Supplier]

Address: [Provide corporate address of the above Entity]

Tel.:[Telephone number of key Supplier Contact]; e-mail:[email of key supplier contact or a specific alias (e.g. NOT questions@supplier.com)

Other information needed to identify the organisation:

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

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

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

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 organizational 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 Sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

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

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a Sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and 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 organizational security measures specified in Appendix 2 before processing the personal data transferred;

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

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

(ii) any accidental or unauthorised access, and

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

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

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

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

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

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

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

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 Sub-processor 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 Sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become

insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract 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 Sub-processor 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 Sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the Sub-processor agrees that the data subject may issue a claim against the data Sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the Sub-processor shall be limited to its own processing operations under the Clauses.

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 Sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

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

Clause 9

Governing Law

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

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

Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the Sub-processor which imposes the same obligations on the Sub-processor as are imposed on the data importer under the Clauses[1]. Where the Sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the Sub-processor's obligations under such agreement.

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

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely ……
……..

4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (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 Sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless

legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

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

Liability

The parties agree that if one party is held liable for a violation of the clauses committed by the other party, the latter will, to the extent to which it is liable, indemnify the first party for any cost, charge, damages, expenses or loss it has incurred.

Indemnification is contingent upon:

(a) the data exporter promptly notifying the data importer of a claim; and

(b) the data importer being given the possibility to cooperate with the data exporter in the defence and settlement of the claim.

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 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):

[Describe what Customer is doing as it relates to the Customer or Supplier]

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):

[To the extent you know, describe who the Personal Information relates to (e.g. The customers of Virgin Mobile)]

Categories of data

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

[To the extent you know, describe what sort of personal information may be processed]

Special categories of data (if appropriate)

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

[List if there is any highly sensitive data that will be processed- e.g. social security number, credit or banking transactions, information about race, religion or other sensitive HR data]

Processing operations

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

[To the extent you know, identify what Supplier/data importer will be doing with the Personal Data- e.g. storage only, transmission, maintaining directories of phone numbers, etc.]

DATA EXPORTER

Name:……

Authorised Signature ……

DATA IMPORTER

Name:……

Authorised Signature ……