Cisco EU Data Processing Addendum

This EU Data Processing Addendum (“**DPA**”) forms part of the Main Agreement (the “**Agreement**”) between Customer and Cisco, to reflect our agreement about the Processing of Customer Data, including Personal Data, in accordance with the requirements of Data Protection Laws and Regulations. To the extent Cisco, in providing Products and/or Services set forth in the Main Agreement, processes Customer Data or Personal Data on behalf of Customer, the provisions of this DPA apply. References to the Agreement will be construed as including this DPA. Any capitalized terms not defined herein shall have the respective meanings given to them in the Agreement.

This DPA consists of two parts: (i) the main body of this DPA, and (ii) Attachment 1 hereto (with its appendices, the “**Standard Contractual Clauses**”). The Standard Contractual Clauses are the standard contractual clauses for the transfer of Personal Data to processors, in accordance with Article 26(2) of Directive 95/46/EC, pursuant to the European Commission’s decision of February 5, 2010 (the “**Privacy Directive**”). References in the body of this DPA to a particular “**Clause**” refers to clauses in the Standard Contractual Clauses.

How to Execute this DPA:

1. To complete this DPA, you should:

a. Sign the main body of this DPA in the signature box below.

b. Complete any missing information and sign the Standard Contractual Clauses at the end of Attachment 1.

c. Complete any missing information and sign Appendix 1 and Appendix 2 to Attachment 1.

1. Submit the completed and signed DPA to Cisco via email to [dpa@cisco.com](mailto:dpa@cisco.com). Upon receipt of your validly completed DPA, this DPA will be legally binding (provided that you have not overwritten or modified any of the terms beyond completing the missing information).

How this DPA Applies

If the Customer signing this DPA is a party to the Agreement, then this DPA is an addendum to and forms part of the Agreement. If the entity signing this DPA is not a party to the Agreement, then this DPA is not valid and is not legally binding. Such entity should request that the Customer that is a party to the Agreement execute this DPA. Affiliates of Customer that are explicitly covered by the Agreement will also be covered by this DPA.

Data Processing Terms

Customer and Cisco hereby agree to the following provisions with respect to any Personal Data Customer transmits to Cisco by using the Products and/or Services.

1. **DEFINITIONS**

**“Administrative Data”** means data related to employees or representatives of Customer that is collected and used by Cisco in order to administer or manage Cisco’s delivery of the Products and/or Services, or the Customer’s account, for Cisco’s own business purposes. Administrative Data may include Personal Data and information about the contractual commitments between Cisco and Customer, whether collected at the time of the initial registration or thereafter in connection with the delivery, management or administration of Products and/or Services.

**“Affiliate”** means, with respect to any entity, any other entity Controlling, Controlled by or under common Control with such entity, for only so long as such Control exists.

**“Control”** means the direct or indirect ownership of more than 50% of the voting capital or similar right of ownership of an entity, or the legal power to direct or cause the direction of the general management and policies of that entity, whether through the ownership of voting capital, by contract or otherwise. Control and Controlling shall be construed accordingly.

**“Customer Data”** means all data (including text, audio, video or image files) that is provided to Cisco by or on behalf of Customer in connection with Customer’s use of our Products and/or Services., or data developed by Cisco at request of or on behalf of Customer pursuant to a statement of work, contract or other relevant agreement. Customer Data includes log, configuration or firmware files, or core dumps, taken from a Product or Service and provided to Cisco to help us troubleshoot an issue in connection with a support request. Customer Data does **not** include Administrative Data, Support Data, Financing Data or Telemetry Data, as defined herein.

**“Dashboard**” for applicable Products and/or Services, means the user interface features of the hosted Software (as described in the Agreement).

**“Data Controller”** means the entity that determines the purposes and means of the Processing of Personal Data. For purposes of this DPA, Customer is the Data Controller.

**“Data Processor”** means the entity which Processes Personal Data on behalf of the Data Controller. For purposes of this DPA, Cisco, including its Affiliates, is the Data Processor.

**“Data Protection Laws and Regulations”** means all mandatory laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, applicable to the Processing of Personal Data under the Agreement.

**“Data Subject”** means the individual to whom Personal Data relates.

**“Financing Data”** means information related to Customer’s financial health that Customer provides to Cisco in connection with making a purchase or entering into a license agreement for Products and/or Services.

**“Main Agreement”** means a Cisco Master Services Agreement, Cloud Services Agreement or similar SaaS terms, Statement of Work, Service Description or Addendum related to the purchase of Products and/or Services.

**“Personal Data”** means data about a living individual transmitted to Cisco as part of the Customer Data from which that person is identified or identifiable, as defined in the Privacy Directive, or any replacement legislation.

**“Processing”** means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

**“Products”** means the Cisco cloud or SaaS products licensed or provided to Customer under the Main Agreement.

**“Security Documentation”** means the information available at Appendix 2 of Attachment 1, as updated from time to time.

**“Services”** means a Cisco service offering described in the applicable Statement of Work or Service Description, provided by Cisco to Customer under the Main Agreement.

**“Standard Contractual Clauses”** means the agreement executed by and between Customer and Cisco attached hereto as Attachment 1 pursuant to the European Commission’s decision of 5 February 2010 on 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.

**“Sub-processor”** means any non-Cisco or Cisco Affiliate Data Processor, engaged by Cisco.

**“Support Data”** means information that Cisco collects when Customer submits a request for support services or other troubleshooting, including information about hardware, software and other details related to the support incident, such as authentication information, information about the condition of the product, system and registry data about software installations and hardware configurations, and error-tracking files.

**“Telemetry Data”** means information generated by instrumentation and logging systems created through the use and operation of the Products and/or Services.

1. **PROCESSING OF PERSONAL DATA**

**2.1** **Customer’s Processing of Personal Data.** Customer shall, in its use of the Products and/or Services, comply with Data Protection Laws and Regulations. For the avoidance of doubt, Customer’s instructions for the Processing of Personal Data must comply with Data Protection Laws and Regulations. In addition, Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data, including providing any required notices to, and obtaining any necessary consent from, its employees, agents or third parties to whom it extends the benefits of the Products and/or Services.

**2.2** **Cisco’s Processing of Personal Data.** We will process and use Customer Data and Personal Data on your behalf and only in accordance with your instructions (including via email) and to the extent required by law. Customer hereby acknowledges that by virtue of using the Products and/or Services it gives Cisco instructions to process and use Customer Data and Personal Data in order to provide the Products and/or Services in accordance with the Agreement. Customer takes full responsibility to keep the amount of Customer Data and Personal Data provided to Cisco to the minimum necessary for the performance of the Products and/or Services.

1. **RIGHTS OF DATA SUBJECTS**

**3.1** **Deletion of Customer Data or and Personal Data.** For applicable Products or Services, the Customer will have the ability, upon termination of this DPA, to request the deletion of Customer Data and Personal Data of an individual Data Subject contained in the Customer Data. Following such deletion request by Customer, Cisco will delete such data from its systems as soon as reasonably practicable.

**3.2** **Data Subject Requests.** Cisco shall, to the extent legally permitted, promptly notify Customer if it receives a request from a Data Subject for access to, correction, amendment or deletion of such Data Subject’s Personal Data. Cisco shall not respond to any such Data Subject request without Customer’s prior written consent except to confirm that the request relates to Customer.

**3.3** **Complaints or Notices related to Personal Data.** In the event Cisco receives any official complaint, notice, or communication that relates to Cisco's processing of Personal Data or either party's compliance with Applicable Laws in connection with Personal Data, to the extent legally permitted, Cisco shall promptly notify Customer and, to the extent applicable, Cisco shall provide Customer with commercially reasonable cooperation and assistance in relation to any such complaint, notice, or communication. Customer shall be responsible for any reasonable costs arising from Cisco’s provision of such assistance.

1. **CISCO PERSONNEL**

**4.1 Confidentiality**. Cisco shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements. Cisco shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

**4.2 Limitation of Access.** Cisco shall ensure that access to Personal Data is limited to those personnel who require such access to perform the Agreement.

**4.3 Data Protection Officer.** Cisco has appointed a data protection officer to the extent this is required by Data Protection Laws and Regulations. Upon request, Cisco will provide the contact details of the appointed person.

1. **SUB-PROCESSORS**

**5.1 Appointment of Sub-processors.** Customer acknowledges and agrees that (i) Cisco is entitled to retain its affiliates as Sub-processors, and (ii) Cisco or any such affiliate may engage any third parties from time to time to process Customer Data in connection with making the Products and/or the provision of Services. Cisco will only disclose Personal Data to Sub-processors that are parties to written agreements with Cisco including obligations no less protective that the obligations of this DPA. Cisco will, following the Customer's written request, provide to the Customer the names of its Sub-processors processing the Personal Data and the countries outside of the European Union in which such data is or may be processed, provided that such request will not be made more than once in each calendar year.

**5.2 Liability.** Cisco shall be liable for the acts and omissions of its Sub-processors to the same extent Cisco would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

1. **SECURITY; AUDIT RIGHTS**

**6.1** **Controls for the Protection of Personal Data.** Cisco will maintain appropriate technical and organizational safeguards, as described in the Security Documentation against unauthorized or unlawful Processing of the Personal Data, and against accidental loss or destruction of, and damage to the Customer Data, according to the measures set forth on Appendix 2 of Attachment 1. Cisco’s obligations under this Section 6.1 will be satisfied by complying with terms of such Appendix 2 of Attachment 1.

**6.2 Third Party Certifications.** Cisco has obtained the third-party certifications and audits set forth in the Security Documentation. Upon Customer’s written request at reasonable intervals, Cisco shall provide a copy of Cisco’s then most recent third-party audits or certifications (the “**Audit Reports**”), as applicable, or any summaries thereof, that Cisco generally makes available to its customers.

**6.3 Audit Rights.** Cisco will allow Customer to perform an on-site audit of Cisco, at Customer’s sole expense, for compliance with the technical and organizational measures set forth in the Appendix 2 of Attachment 1 if (i) Cisco notifies Customer of a Security Incident, or (ii) if Customer reasonably believes that Cisco is not in compliance with its security commitments under this DPA, or (iii) if such audit legally is required by Customer's Applicable Laws. Such audit must be conducted in accordance with the procedures set forth in Section 6.5 and may not be conducted more than one time per year.

**6.4 Satisfaction of Audit Request.** Upon receipt of a written request to audit, and subject to Customer’s agreement, Cisco may satisfy such audit request by providing Customer with a confidential copy of an Audit Report (described in Section 6.2) in order that Customer may reasonably verify Cisco’s compliance with the technical and organizational measures set forth in Appendix 2 of Attachment 1.

**6.5 Audit Process.** Customer must provide at least 6 weeks’ prior written notice to Cisco of a request to audit. The scope of any audit will be limited to Cisco’s policies, procedures and controls relevant to the protection of Customer Data and defined in Appendix 2 of Attachment 1. All audits will be conducted during normal business hours, at Cisco's principal place of business or other location(s) where Customer’s Customer Data is accessed, processed or administered, and will not unreasonably interfere with Cisco's day-to-day operations. An audit will be conducted at Customer‘s sole cost and by a mutually agreed upon third party contractor who is engaged and paid by Customer, and is under a non-disclosure agreement containing confidentiality provisions substantially similar to those set forth in the Agreement, obligating it to maintain the confidentiality of all Cisco Confidential Information and all audit findings. Before the commencement of any such on-site audit, Cisco and Customer shall mutually agree upon the timing, and duration of the audit and in addition Cisco will provide Cisco’s reimbursement rate for which Customer shall be responsible (Cisco’s then-current professional services rates). Cisco will co-operate with the audit, including providing auditor the right to review but not to copy Cisco security information or materials. Cisco's policy is to share methodology, and executive summary information, not raw data or private information. Customer shall, at no charge, provide to Cisco a full copy of all findings of the audit.

**6.6 Notice of Failure to Comply.** After conducting an audit under Section 6.3 or after receiving a Cisco Report under Section 6.4, Customer must notify Cisco of the specific manner, if any, in which Cisco does not comply with any of the security, confidentiality, or data protection obligations in this DPA, if applicable. Any such information will be deemed Confidential Information of Cisco. Upon such notice, Cisco will use commercially reasonable efforts to make any necessary changes to ensure compliance with such obligations.

1. **SECURITY BREACH MANAGEMENT AND NOTIFICATION**

Cisco maintains security incident management policies and procedures, including detailed security incident escalation procedures. If Cisco becomes aware of any unauthorized disclosure of Customer Data in breach of Section [6.1](#ControlsProtection61) (a “**Security Incident**”), then Cisco will notify Customer within forty-eight (48) hours and provide Customer with relevant information about the Security Incident, including, to the extent then known, the type of Customer Data involved, the volume of Customer Data disclosed, the circumstances of the incident, mitigation steps taken, and remedial and preventative action taken.

1. **ADDITIONAL TERMS FOR TRANSFER OF PERSONAL DATA FROM THE EEA**

**8.1 Application of Standard Contractual Clauses.** The Standard Contractual Clauses and the terms of this Section 8 will apply to the Processing of Personal Data by Cisco in the course of providing the Products and/or Services:

**8.1.1** The Standard Contractual Clauses apply only to Personal Data that is transferred from the European Economic Area (EEA) to outside the EEA, either directly or via onward transfer, to any country or recipient: (i) not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the Privacy Directive), and (ii) not covered by a suitable framework recognized by the relevant authorities or courts as providing adequate protection for personal data.

**8.1.2** Any enforcement of the Standard Contractual Clauses in accordance with Clause 3 by a “data subject” or an association or other body on a data subject’s behalf, will be subject to the terms of this DPA, with such enforcing party standing in the shoes of Customer.

**8.2 Instructions.** This DPA and the Agreement are the complete and final instructions of Customer (“**Data Exporter**”) to Cisco (“**Data Importer**”) for the Processing of Personal Data. For the purposes of Clause 5(a) of the Standard Contractual Clauses, the Data Exporter hereby instructs the Data Importer to process Personal Data: (a) in accordance with the Agreement; (b) at the request of Customer, including requests made in connection with Support Services; and (c) as initiated by End Users in their use of Customer’s networks.

**8.3 Sub-processors.** Pursuant to Clause 5(h) of the Standard Contractual Clauses, the Data Exporter acknowledges and expressly agrees that Cisco’s affiliates may be retained as Sub-processors, and (b) Cisco and Cisco’s affiliates respectively may engage third-party Sub-processors in the course of providing the Products and/or Services. Data Importer shall make available to Data Exporter a current list of Sub-processors for the respective Services with the identities of those Sub-processors (“**Sub-processor List**”) on an annual basis.

**8.3.1 Objection Right for new Sub-processors.** If Data Exporter is legally prohibited from consenting to Data Importer’s use of a new Sub-processor, then Data Exporter will notify Data Importer of such prohibition in writing within 10 business days after receipt of Data Importer’s notice. Data Importer will use reasonable efforts to make available to Data Exporter a change in the affected Products and/or Services or recommend a commercially reasonable change to Data Exporter’s configuration or use of the affected Products and/or Services to avoid processing of Personal Data by said new Sub-processor. If Data Importer is unable to make available such change within a reasonable period of time, which shall not exceed 60 days, then Data Exporter may terminate any applicable Agreement in respect only to those Products and/or Services that cannot be provided by Data Importer without the use of the objected-to new Sub-processor, by providing written notice to Data Importer. Data Exporter shall receive a pro-rated refund of any prepaid fees for such licenses or Services for the period following the effective date of termination.

**8.4 Certification of Deletion.** The parties agree that Data Importer’s satisfaction of its obligations in Sections [3.1](#DeletionCustomer31), [3.2](#DataSubjectRequests32), and 7 will be deemed to satisfy its obligations in Clause 12(1), and that the certification of deletion of Personal Data described in Clause 12(1) will be provided only upon Data Exporter’s written request.

1. **LEGAL EFFECT; TERMINATION**

This DPA shall only become legally binding between Customer and Cisco when fully executed and will terminate when the Main Agreement terminates, without further action required by either party.

1. **CONFLICT.**

In the event of any conflict or inconsistency between this DPA and the Agreement, this DPA will prevail.

IN WITNESS WHEREOF, the parties have caused this EU Data Processing Addendum to be duly executed. Each party warrants and represents that its respective signatories whose signatures appear below are on the date of signature duly authorized.

|  |  |  |
| --- | --- | --- |
| **CUSTOMER** |  | **CISCO** |
|  | **Cisco Systems, Inc.** |
|  |  |  |
| Authorized Signature |  | Authorized Signature |
| Name |  | Name |
| Title |  | Title |
| Date |  | Date |

Attachment 1

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.:

(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.

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

Clause 7

***Mediation and jurisdiction***

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

(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.

1. 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, namely [*data exporter to insert relevant Member State].*

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, namely *[data exporter to insert relevant Member State].*
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

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

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

**On behalf of the data exporter:**

Name (written out in full):

Position:

Address:

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

Signature……………………………………….

(stamp of organisation)

**On behalf of the data importer:**

Name (written out in full):

Position:

Address:

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

Signature……………………………………….

(stamp of organisation)

APPENDIX 1 to 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 exporter is the undersigned entity signing as the “Data Exporter”.*

**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):

*Individual users of any local area network (LAN) created in whole or part using Cisco Products and/or Services purchased by the data exporter.*

**Categories of data**

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

* *Account usernames (commonly, the user’s e-mail address)*
* *Each of the following (which may, depending on names selected by the data controller, contain personal data):*
* *Organization Name*
* *Network Name*
* *Network Tags*
* *SSID name, and*
* *Address from Create Organization page (not required)*

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

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

*N/A*

**Processing operations**

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

*The personal data is transmitted by a terminal device to the hardware endpoints with which the device connects, and the hardware endpoint transmits the personal data by means of an encrypted connection to Cisco’s servers in order to display the personal data to the customer by means of the SAAS interface the customer uses to manage and configure the hardware endpoints.*

DATA EXPORTER DATA IMPORTER

Name: ……………………………………….. Name: …………………………………………

Authorised Signature ………………………. Authorised Signature …………………………

APPENDIX 2 to the Standard Contractual Clauses

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

**Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):**

1. **Data Protection Executives; Notices.** Each of the parties will designate and notify the other party of its respective Data Protection Executive(s) responsible for the obligations set forth on this Appendix 2.

Any notices under this Appendix or the underlying Agreement should be communicated as follows:

a. communications regarding the day-to-day obligations should be communicated in writing via email or other written notice to each of the Data Protection Executives (or their designees), and

b. communications regarding any proposed changes to the terms of this Appendix or the terms of a party’s Customer Data obligations under the Agreement should be directed as required under the notice provisions of the Agreement with copies provided to the Data Protection Executives (or their designees). No such changes will modify this Appendix or the Agreement unless agreed by the parties pursuant to the appropriate change management procedure under the Agreement.

1. **General Security Practices**

2.1. Processor has implemented and shall maintain appropriate technical and organisational measures to protect Customer Data against accidental loss, destruction or alteration, unauthorized disclosure or access, or unlawful destruction, including the policies, and procedures and internal controls set forth in this Appendix 2 for its personnel, equipment, and facilities at the Processor locations providing the any services to Cisco and/or Customers (“Services”). The Services are set forth in one or more agreements between Cisco and Customers, but may include (a) customer service activities, such as processing orders, providing technical support and improving offerings, (b) sales and marketing activities as permissible under applicable law, (c) consulting, professional, security, storage, hosting and other services delivered to Customers, including services offered by means of the products and solutions described at <http://www.cisco.com>, and (d) internal business processes and management, fraud detection and prevention, and compliance with governmental, legislative and regulatory bodies.

1. **Technical and Organizational Security Measures**

**3.1. Organization of Information Security**

a. **Security Ownership.** Processor has appointed one or more security officers responsible for coordinating and monitoring the security rules and procedures.

b. **Security Roles and Responsibilities.** Processor personnel with access to Customer Data are subject to confidentiality obligations.

c. **Risk Management.** Processor performed a risk assessment before processing the Customer Data or offering the Services.

**3.2. Human Resources Security**

a. **General**. Processor informs its personnel about relevant security procedures and their respective roles. Processor also informs its personnel of possible consequences of breaching its security policies and procedures. Employees who violate Processor security policies may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of his or her contract or assignment with Processor.

b. **Training.** Processor personnel with access to Customer Data receive:

i. annual security education and training regarding privacy and security procedures for the Services to aid in the prevention of unauthorized use (or inadvertent disclosure) of Customer Data;

ii. training regarding effectively responding to security events; and

iii. training is regularly reinforced through refresher training courses, emails, posters, notice boards and other training materials.

c. **Background Checks.** Processor personnel are subject to criminal background checks.

**3.3. Asset Management**

a. **Asset Inventory.** Assets associated with information and information-processing facilities are identified and an inventory of assets is maintained.

b. **Information Classification.** Processor classifies Customer Data to help identify it and to allow for access to it to be appropriately restricted.

c. **Media Handling**

Processor personnel:

i. Use trusted devices that are configured with security software and automatic patching;

ii. Follow Cisco’s Trusted Device Standard

(at <http://wwwin.cisco.com/infosec/policies/standards/trusteddevice.shtml>) when accessing Customer Data or when having Customer Data in his/her control;

iii. Avoid accepting or storing Customer Data on a non-trusted device (meaning one that does not comply to Cisco’s Trusted Device Standard). This includes smartphones, tablets, USB drives and CDs that do not meet Cisco’s Trusted Device Standard;

iv. Encrypt Customer Data stored on a mobile device, including laptops, smartphones, tables, USB drives and CDs; and

v. Take measures to prevent accidental exposure of customer data, including using privacy filters on laptops when in areas where over-the-shoulder viewing of Customer Data is possible.

**3.4. Personnel Access Controls**

a. **Access Policy.** An access control policy is established, documented, and reviewed based on business and information security requirements.

b. **Access Recordkeeping.** Processor maintains a record of security privileges of its personnel that have access to Customer Data, networks and network services.

c. **Access Authorization.**

i. Processor has user account creation and deletion procedures, with appropriate approvals, for granting and revoking access to Cisco’s and Customers’ systems and networks at regular intervals based on the principle of “least privilege” and need-to-know criteria based on job role.

ii. Processor maintains and updates a record of personnel authorized to access systems that contain Customer Data.

iii. For systems that process Customer Data, Processor revalidates access of users who change reporting structure and deactivates authentication credentials that have not been used for a period of time not to exceed six months.

iv. Processor identifies those personnel who may grant, alter or cancel authorized access to data, systems and networks.

v. Processor ensures that, each personnel having access to its systems have a single unique identifier/log-in.

vi. Processor maintains strict policies against any shared “generic” user identification access.

d. **Network Design.** For systems that process Customer Data, Processor has controls to avoid personnel assuming access rights they have not been assigned to gain unauthorized access to Customer Data.

e. **Least Privilege.** Processor limits access to Customer Data to those Processor personnel performing the Services and, to the extent technical support is needed, its personnel performing such technical support.

f. **Integrity and Confidentiality**

i. Processor instructs its personnel to automatically lock screens and/or disable administrative sessions when leaving premises that are controlled by Processor or when computers are otherwise left unattended.

ii. Processor computers and trusted devices automatically lock after ten (10) minutes of inactivity.

iii. Processor stores passwords in a secured and restricted way that makes them unintelligible while they are in force.

g. **Authentication**

i. Processor uses industry standard practices to identify and authenticate users who attempt to access information systems. Where authentication mechanisms are based on passwords, Processor requires that the passwords be renewed regularly, no less often than every 6 months.

ii. Where authentication mechanisms are based on passwords, Processor requires the password to be at least eight characters long and conform to very strong password control parameters including length, character complexity, and non-repeatability.

iii. Processor ensures that de-activated or expired identifiers are not granted to other individuals.

iv. Processor monitors repeated attempts to gain access to the information system using an invalid password.

v. Processor maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed.

vi. Processor limits access to file stores and/or systems in which passwords are stored.

**3.5. Cryptography**

a. **Cryptographic controls policy**

i. Processor has a policy on the use of cryptographic controls based on assessed risks

ii. Processor assesses and manages the lifecycle of cryptographic algorithms, hashing algorithms, etc. and deprecates and disallows usage of weak cypher suites, and mathematically insufficient block lengths and bit lengths.

iii. Processor’s cryptographic controls/policy addresses appropriate algorithm selections, key management and other core features of cryptographic implementations.

b. **Key management.** Processor has procedures for distributing, storing, archiving and changing/updating keys; recovering, revoking/destroying and dealing with compromised keys; and logging all transactions associated with keys.

**3.6. Physical and Environmental Security**

a. **Physical Access to Facilities**

i. Processor limits access to facilities where systems that process Customer Data are located to authorized individuals.

ii. Access is controlled through key card and/or appropriate sign-in procedures for facilities with systems processing Customer Data. Personnel must be registered and are required to carry appropriate identification badges.

b. **Physical Access to Equipment.** Processor equipment that is located off premises is protected using industry standard process to limit access to authorized individuals.

c. **Protection from Disruptions.** Processor uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference.

d. **Clear Desk.** Processor has policies requiring a “clean desk/clear screen” at the end of the workday.

**3.7. Operations Security**

a. **Operational Policy.** Processor maintains policies describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Customer Data and to its systems and networks.

b. **Workstations.** Processor uses the following controls on its workstations that process Customer Data:

i. anti-malware software and firewalls,

ii. password and screensaver controls with automatic lock of workstation upon idleness,

iii. periodic scans to query the hardware and the presence of software, patches, corporate applications, and security components; and

iv. full disk encryption on laptop devices.

c. **Mobile Devices.** Mobile phones and tablets are protected via a mandatory PIN, restrictions on amount of email that can be stored on the device, and a remote wipe capability.

d. **Data Recovery.** Processor maintains multiple copies of Customer Data from which Customer Data can be recovered. Cisco stores copies of Customer Data and data recovery procedures in a different place from where the primary equipment processing the Customer Data is located. Processor has specific procedures in place governing access to these copies of Customer Data.

e. **Logging and Monitoring.** Processor maintains logs of and monitors access to administrator and operator activity and data recovery events.

**3.8. Communications Security and Data Transfer**

a. **Networks.** Processor uses the following controls to secure its networks that access Customer servers which store Customer Data:

i. Network traffic passes through firewalls, which are monitored. Processor has implemented intrusion prevention systems that allow traffic flowing through the firewalls and LAN to be logged and protected 24x7.

ii. Anti-spoofing filters are enabled on routers;

iii. Network, application and server authentication passwords are required to meet minimum complexity guidelines (at least 7 characters with at least 3 of the following four classes: upper case, lower case, numeral, special character) and be changed at least every 180 days.

iv. Initial user passwords are required to be changed during the first logon. Processor policy prohibits the sharing of user IDs and passwords.

v. Firewalls are deployed to protect the perimeter Cisco network.

b. **Virtual Private Networks (“VPN”).** When remote connectivity to the Cisco network is required for processing of Customer Data, Processor uses VPN servers for the remote access with the following or similar capabilities:

i. Supports strong encryption, including AES-256 and 3DES-168 (so long as Customer's security gateway device has a strong-crypto license enabled).

ii. Connections from Customers to Processor locations are only established using the Cisco VPN servers.

iii. The use of two-factor authentication is required.

**3.9. System Acquisition, Development and Maintenance**

a. **Security Requirements.** Processor has adopted security requirements for the purchase or development of information systems, including for application services delivered through public networks.

b. **Development Requirements.** Processor has policies for secure development, system engineering and support. Processor conducts appropriate tests for system security as part of acceptance testing processes.

**3.10. Supplier Relationships**

a. **Policies.** Processor has information security policies or procedures for its use of suppliers. Processor has agreements with suppliers in which they agree to comply with Cisco’s and/or Processor’s security requirements.

b. **Management.** Processor performs periodic audits on key suppliers and manages service delivery by its suppliers and reviews security against the agreements with suppliers.

**3.11. Information Security Incident Management**

a. **Response Process.** Processor maintains a record of information security breaches with a description of the breach, the consequences of the breach, the name of the reporter and to whom the breach was reported, and the procedure for recovering data.

b. **Reporting.** Processor will report within 48 hours to a Customer-designated response center any security incident that has resulted in a loss, misuse or unauthorized acquisition of any Customer Data.

**3.12. Information Security Aspects of Business Continuity Management**

a. **Planning.** Processor maintains emergency and contingency plans for the facilities in which Processor information systems that process Customer Data are located.

b. **Data Recovery.** Processor’s redundant storage and its procedures for recovering data are designed to attempt to reconstruct Customer Data in its original state from before the time it was lost or destroyed.

1. The security measures described in this Appendix 2 are in addition to any confidentiality obligations contained in any other agreement related to the Services between Processor and Customer with respect to Customer Data. In the event a conflict between the terms of such other agreement and this Appendix 2, the terms of this Appendix 2 shall control.

**DATA EXPORTER**

Name:

Authorised Signature…………………………………………..

**DATA IMPORTER**

Name:

Authorised Signature……………………………………………

