Meraki LLC
500 Terry Francois Blvd.
San Francisco, CA 94158
T 415.432.1000

CISCO MERAKI
EU DATA PROCESSING ADDENDUM

This EU Data Processing Addendum ("**DPA**") forms part of the Supplemental End User License Agreement (the "**Agreement**") between you ("**Customer**") and Cisco Systems, Inc., the parent company of Meraki LLC, a Delaware limited liability company ("**Meraki**"), to reflect our agreement about the Processing of Customer Data, including Personal Data, in accordance with the requirements of Data Protection Laws and Regulations. References to the Agreement will be construed as including this DPA. Any capitalized terms not defined herein will 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 as described in Section 9 below. References in the body of the DPA to a particular "Clause" refer to clauses in the Standard Contractual Clauses.

HOW TO EXECUTE THIS DPA:

1. To execute this DPA, please do one of the following:
   a. download this DPA, complete the form fields, sign, and email to legal@meraki.com. Customer acknowledges and agrees that a completed and signed copy of this Agreement must be emailed to legal@meraki.com for the Agreement to become effective; or
   b. click here to complete the form fields and sign electronically.

2. Once electronically executed by both your company and Meraki, this DPA (including the Standard Contractual Clauses) will be effective and your signatory will receive a fully-executed copy by email.

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. However, this DPA will immediately and automatically terminate if Customer does not enable the "EU Cloud" configuration in its Meraki Dashboard account.

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 its affiliate or parent that is a party to the Agreement execute this DPA. Affiliates of such Customer entity that are explicitly covered by the Agreement will also be covered by this DPA.

DATA PROCESSING TERMS

Customer and Meraki hereby agree that the following terms govern Customer's transmission of any Personal Data to Meraki by means of the Products.

1. DEFINITIONS

"**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, Meraki, including its affiliates, is the Data Processor.

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

"**Data Subject**" means the individual to whom Personal Data relates.

"**GDPR**" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

"Meraki Dashboard" means Meraki's online software platform, including the "Dashboard" interface.

"**Personal Data**" means data about a living individual transmitted to Meraki as part of the Customer Data from which that person is identified or identifiable, as defined in the GDPR, or any replacement legislation.

"Processing" has the meaning given to it in the GDPR.

"**Standard Contractual Clauses**" means the agreement executed by and between Customer and Meraki 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 Data Processor engaged by Meraki.

"**Technical and Organizational Measures**" means the list of controls, processes, and procedures described at https://meraki.cisco.com/lib/pdf/eu_technical_organizational_measures.pdf, as updated from time to time, regarding Meraki's privacy and data security practices.

2. PROCESSING OF PERSONAL DATA

2.1 **Customer's Responsibilities.** Customer will, in its use of the Products, comply with the requirements of Data Protection Laws and Regulations. In addition, Customer will 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 consents from, its Network Users.

2.2 **Meraki's Processing of Personal Data.** We will process and use Customer Data on your behalf and only in accordance with your instructions (including via email), where such instructions are consistent with the terms of this Agreement, and to the extent required by law. Customer hereby acknowledges that by virtue of using the Products it gives Meraki instructions to process and use Customer Data in order to provide the Products in accordance with the Agreement. Personal Data is Confidential Information pursuant to the Agreement. Taking into account the nature of the processing and the information available to Meraki, Meraki will provide such reasonable information and assistance as Customer reasonably requires in assisting with Customer's obligations under GDPR with respect to data protection impact assessments (as such term is defined under GDPR.)

2.3 **Product Configuration.** Customer has and will continue to have the "EU Cloud" enabled in its Meraki Dashboard for its Networks. The Meraki "EU Cloud" Configuration Guide is available at: https://documentation.meraki.com/zGeneral_Administration/Privacy_and_Security/EU_Cloud_Configuration_Guide. Customer acknowledges that, at no additional cost, it can configure the Products to significantly limit the Customer Data and Personal Data that are transmitted to Meraki.

2.4 **Details of the Processing.** Meraki Processes Customer Data to provide the Products to you in accordance with the Agreement. The nature and scope of the processing, the types of Personal Data and the categories of Data Subjects processed under this DPA are specified in Attachment 1 to this DPA.

3. RIGHTS OF DATA SUBJECTS

3.1 **Deletion of Personal Data.** The Meraki Dashboard gives Customer the ability to delete Personal Data of an individual Data Subject, as may be required by Data Protection Laws and Regulations, in such a way as to render the data inaccessible and unidentifiable to Customer or any third party. Following such deletion by Customer, Meraki will fully remove such data from its systems as soon as reasonably practicable and within a maximum period of 14 months.

3.2 **Data Subject Requests.** Meraki will, to the extent legally permitted, promptly notify Customer if it receives a request from a Data Subject for access to, correction, restriction, portability, or deletion of such Data Subject's Personal Data. Except as required by law, Meraki will not respond to any such Data Subject request without Customer's prior written consent except to confirm that the request relates to Customer and to direct the Data Subject to the Customer as appropriate. Taking into consideration the nature of the Processing, Meraki will assist Customer through reasonable and appropriate technical and organizational

measures in responding to any Data Subject request to the extent Meraki is legally permitted to do so and the response to such Data Subject request is legally required. To the extent legally permitted and outside the ordinary course and cost of business, Customer is responsible for the costs associated with any such assistance provided by Meraki.

4. MERAKI PERSONNEL

4.1 **Confidentiality.** Meraki will 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. Meraki will ensure that such confidentiality obligations survive the termination of the personnel engagement.

4.2 **Reliability.** Meraki will take commercially reasonable steps to ensure the reliability of any Meraki personnel engaged in the Processing of Personal Data, including by conducting background checks on all new employees to the extent permitted and in compliance with applicable law and Meraki's policies.

4.3 **Limitation of Access.** Meraki will ensure that access to Personal Data is limited to those personnel who require such access to perform the Agreement.

4.4 **Data Protection & Privacy Lead.** Meraki has appointed a data protection and privacy lead. Upon request to privacy@cisco.com, Meraki will provide the contact details of the appointed person.

5. SUB-PROCESSORS

5.1 **Appointment of Sub-processors.** Customer acknowledges and agrees that (i) Meraki is entitled to retain its affiliates as Sub-processors, and (ii) Meraki or any such affiliate may engage any third parties from time to time to process Customer Data in connection with making the Products available to Customer. Meraki or its affiliates will only disclose Personal Data to Sub-processors that are parties to written agreements with Meraki or its affiliates, as applicable, that include obligations no less protective that the obligations of this DPA with respect to the protection of Customer Data to the extent applicable to the nature of the processing provided by such Sub-processor.

5.2 **Current Sub-processors; Notification of New Sub-processors**. Meraki will make available to Customer a list of current Sub-processors for the Products at https://meraki.cisco.com/trust#subprocessors as updated from time to time. Meraki will provide notice in Customer's Dashboard account before authorizing any new Sub-processor(s) in connection with providing the Products (the "**Dashboard Notice**"). If Customer objects to Meraki's use of a new Sub-processor, Customer may terminate any Hosted Software Licenses in respect of only those Products that cannot be provided by Meraki without the use of the objected-to new Sub-processor (the "**New Sub-processor**"), by providing written notice to Meraki within a reasonable period of time following the Dashboard Notice, such period not to exceed thirty (30) days (the "**Notice Period**"); provided, that Meraki will not be prohibited from engaging the New Sub-processor during or after the Notice Period.

5.3 **Liability.** Meraki will be liable for the acts and omissions of its Sub-processors to the same extent Meraki 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.

6. SECURITY

6.1 **Technical and Organizational Measures.** We have implemented and will maintain Technical and Organizational Measures as set forth herein. Meraki regularly monitors compliance with these safeguards and will continue to maintain appropriate safeguards during the term of the Agreement.

6.2 **Certifications and Audits.** Meraki has obtained the third-party certifications and audits listed in the Technical and Organizational Measures. Upon Customer's written request at reasonable intervals, and subject to confidentiality obligations, Meraki will provide a copy of Meraki's then most recent third-party audits or certifications (the "**Audit Reports**"), as applicable, or summaries thereof, that Meraki generally makes available to its customers.

7. SECURITY BREACH MANAGEMENT

Meraki maintains security incident management policies and procedures, including detailed security incident escalation procedures. If Meraki becomes aware of any unlawful destruction, loss, alteration or unauthorized disclosure of Customer Data (a "**Security Incident**"), then Meraki will notify Customer without undue delay and provide Customer with relevant information about the Security Incident, including 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. The obligations in this Section 7 do not apply to Security Incidents caused by Customer or Customer's Network Users.

8. RETURN AND DELETION OF CUSTOMER DATA

At the termination of the Agreement, upon Customer's written request and within a reasonable period, Meraki will: (i) make available to Customer all Personal Data, or (ii) delete, restrict processing, and/or de-identify Customer Data, including Personal Data, in such a way as to render such data inaccessible and unidentifiable to Customer or any third party. Unless such return, deletion, restriction of processing, or de-identification is not feasible or continued retention and processing is required or permitted by applicable law, Meraki will respond to such request as soon as reasonably practicable.

9. TRANSFERS OF PERSONAL DATA OUTSIDE EU

9.1 Transfer Mechanisms. Subject to the terms of this DPA, Meraki makes available the following transfer mechanisms which will apply, in the order of precedence set out below, only to Personal Data transferred from the European Union, European Economic Area (EEA) and/or their member states, and Switzerland, either directly or via onward transfer, to countries that do not ensure an adequate level of data protection within the meaning of Data Protection Laws and Regulations, to the extent such transfers are subject to Data Protection Laws and Regulations:

9.1.1 EU-U.S. and Swiss-U.S. Privacy Shield Frameworks. Meraki (as a covered entity under Cisco Systems, Inc.'s certification) will maintain its self-certification to, and compliance with, the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks as administered by the U.S. Department of Commerce, or successor frameworks, with respect to the transfer of Personal Data from the European Economic Area and/or Switzerland to the United States.

9.1.2 Standard Contractual Clauses. Customer and Meraki may also enter into Standard Contractual Clauses subject to the terms of Section 9.2. 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.

9.2 Additional Terms for the Standard Contractual Clauses.

9.2.1 Limitation on Scope of Processing. Meraki's sole objective in Processing the Personal Data is to provide the Products pursuant to the Agreement, and Meraki will Process the Personal Data exclusively for the purposes of providing the Products to Customer, administering the customer relationship, improving Products, and complying with applicable laws.

9.2.2 Instructions. This DPA and the Agreement are the complete and final instructions of Customer to Meraki for the Processing of Personal Data. Any additional or alternate instructions must be agreed upon separately in writing. For the purposes of Clause 5(a), 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 Network Users in their use of Customer's Networks.

9.2.3 Sub-processors. Pursuant to Clause 5(h), the Data Exporter acknowledges and expressly agrees that (a) Meraki's affiliates may be retained as Sub-processors, and (b) Meraki and Meraki's affiliates respectively may engage third-party Sub-processors in the course of providing the Products in accordance with Section 5.2 of this DPA.

9.2.4 Notifications regarding Sub-processors. Meraki will, upon Customer's written request, make available to Customer a list of Sub-Processors in accordance with Section 5.2 of this DPA and/or a copy of any agreement it has in place with any Sub-Processor as specifically identified by Customer's request which relates to the processing of Personal Data. Meraki may remove any commercially sensitive or confidential

information from such agreement as required, before providing it to Customer.

9.2.5 Audits and Certifications. The obligations of Meraki set forth in Section 6, including the obligation to provide the Audit Reports, will be deemed to fully satisfy the audit rights granted under Clauses 5(f) and 12(2) with respect to Customer. Any further audit shall be permitted only upon demonstration that the Audit Reports are insufficient, and in any event not more than once annually, upon written request with reasonable time, place, manner, and scope (which shall be limited to Meraki's procedures relevant to the protection of Personal Data) to be determined by the parties in good faith. In the event of any such audit and to the extent legally permissible, Customer will reimburse Meraki for any time expended at Meraki's then-current professional services rates, which will be made available to Customer upon request.

9.2.6 Certification of Deletion. The parties agree that Data Importer's satisfaction of its obligations in Sections 3.1, 3.2, and 8 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.

10. LEGAL EFFECT; TERMINATION

For avoidance of doubt, this DPA shall only become legally binding between Customer and Meraki when the steps set out in the Section "HOW TO EXECUTE THIS DPA" above have been fully completed. For avoidance of doubt, this DPA will immediately and automatically terminate in the event that any Network of Customer does not have the "EU Cloud" enabled in Meraki Dashboard.

[*Signature page follows*]

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	MERAKI
	Meraki LLC
Customer Company Name	
Authorized Signature	Authorized Signature
Name	Todd Nightingale Name
Title	Senior Vice President & General Manager Title
Date	6/28/18 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: Meraki LLC
Address: 500 Terry Francois Blvd., San Francisco, CA 94158, USA
Tel.: +1-415-432-1000; e-mail: legal@meraki.com

(the data **importer**)

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

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

Clause 1

Definitions

For the purposes of the Clauses:

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

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

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

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

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

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

Clause 2

Details of the transfer

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

Clause 3

Third-party beneficiary clause

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

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

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

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

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

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

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

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

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

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

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

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

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

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

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

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

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

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

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

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

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

  (ii) any accidental or unauthorised access, and

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

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

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

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

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

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

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

Clause 6

Liability

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

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

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

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

Clause 7

Mediation and jurisdiction

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

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

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

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

Clause 8

Cooperation with supervisory authorities

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

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

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

Clause 9

Governing Law

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

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 _____.

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): Todd Nightingale
Position: Senior Vice President and General Manager
Address: 500 Terry Francois Blvd., San Francisco, CA 94158, USA
Other information necessary in order for the contract to be binding (if any):

Signature.....

(stamp of organisation)

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

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

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

Data exporter

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

Data importer

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

Meraki LLC, a Delaware limited liability company. Meraki provides software-as-a-serve (SaaS) to its customers to manage Meraki's networking hardware products that customers deploy at customers' sites. Meraki processes networking protocol information, including a limited amount of personal data, as part of providing the SaaS interface.

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 Meraki products purchased by the data exporter.

Categories of data

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

- *MAC Address (All products)*
- *MAC Address with Username (Dashboard, MR products, MX products, SM product)*
- *MAC Address with IP Address (MR products, MX products)*
- *MAC Address with Relative Signal Strength Indicator (RSSI) (MR products)*
- *MAC Address with URL (MX products)*
- *MAC Address with Direct Inward Dialing Number (DID) (MR products)*
- *IP Address (All products)*
- *Email Address with IP Address (Dashboard)*
- *Email Address (Dashboard)*
- *Video (MV products)*
- *Audio (MV products*
- *Audio, DID (MC products)*
- *DID (MC products)*
- *DID and User Name (MC products)*
- *Data Backups (All products)*
- *Unique Universal Identifier (MR products, MX wireless products)*
- *Client Hostname (All products depending on name selected by device owner)*
- *Active Directory Server Username, Password and Groups (MC products and SM product depending on name selected by owner)*
- *Azure Active Directory Server Username and Password (MC products depending on name selected by owner)*
- *Directory Information (ie: username) (SM Product if entered by administrator)*
- *User Account Information (ie: username) (SM Product if entered by user)*
- *LDAP Username (MI Product)*
- *Any personal data accessed by Meraki Technical Support during the course of providing technical support services from locations outside the EEA.*
- *Sign–on authentication credentials when using certain user authentication methods, including:*
    - *Facebook, SMS, or Google authentication*
    - *Meraki–hosted authentication*

- *Dashboard also allows the data exporter to configure Dashboard fields, including organization names, network names, network tags, SSID names, user authentication methods and organization address (optional) directly in their Dashboard account. Data exporters that wish to avoid inadvertently sending personal data to data importer should not include personal data in these fields when configuring their Dashboard account.*

By enabling the "EU Cloud" feature in the Meraki SaaS interface, data exporters can prevent the transfer of all other categories of personal data outside the EU.

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 transferred may be subject to the following basic processing activities, as may be further set forth in contractual agreements entered into from time to time between Meraki and data exporter: (a) customer service activities, such as processing orders, providing technical support and improving products, (b) sales and marketing activities as permissible under applicable law, (c) delivery of the Meraki products including the SaaS interface known as the Dashboard through which customer manages and configures Meraki networking hardware devices, and (d) internal business processes and management, fraud detection and prevention, and compliance with governmental, legislative, and regulatory requirements.

[*Signature page follows*]

Signature Page to Appendix 1

DATA EXPORTER

Name: .....

Authorised Signature .....

DATA IMPORTER

Name: *Meraki LLC*

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):

Data importer will maintain appropriate technical and organizational safeguards, taking into account both the state of technologies and the costs of implementation, against unauthorized or unlawful processing of customer data, including personal data, and against accidental loss or destruction of, and damage to the customer data, including as described at https://meraki.cisco.com/lib/pdf/eu_technical_organizational_measures.pdf, as updated from time to time.

DATA EXPORTER

Name: .....

Authorised Signature .....

DATA IMPORTER

Name: *Meraki LLC*

Authorised Signature .....