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

FAQ for Customers:

Compliance with European Data Protection Laws

What services does Meraki offer?

Meraki LLC ("**Meraki**" or the "**Company**"), a wholly-owned subsidiary of Cisco Systems, Inc. and the core of Cisco's Cloud Networking Group, is a leading provider of cloud-managed networking equipment. Meraki delivers networking solutions that dramatically simplify the deployment and management of enterprise scale networks.

How does Meraki deliver its services?

Meraki sells both networking hardware devices, such as wireless access points, switches, and security appliances, and access to its cloud-based software that monitors and manages those devices. Meraki makes this management software available to its customers over the Internet, and customers access the management software by means of commercially-available internet access and web browser software. Customers log into the Meraki services from a Meraki website and access their accounts by means of unique usernames and passwords, which can be further configured by the customers to require additional authentication methods.

How does Meraki comply with European data protection laws?

In addition to implementing a robust privacy and data security program, Meraki seeks to comply with applicable privacy laws and endeavors to follow best practices set out in relevant guidance, including the *Directive 94/46 of the European Parliament 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 data* (the "**Privacy Directive**"), as implemented into local laws, Switzerland's *Federal Act on Data Protection of 19 June 1992*, Germany's *Federal Data Protection Act* of December 20, 1990 as amended on 14 September, 1994, and the non-binding *Opinion 05/2012 on Cloud Computing* released by the Article 29 Working Party on July 1, 2012.

What about the US-EU Safe Harbor Framework?

On October 6, 2015, the European Court of Justice issued a decision that invalidated the US-EU Safe Harbor Framework (the "**Safe Harbor**"), ruling that the framework does not provide a valid legal basis for personal data transfers from Europe to the U.S.

In the absence of the Safe Harbor, companies transferring and receiving personal data from the EU can also comply with applicable data protection regulations by signing standard contractual clauses, which consist of a set of contractual terms that have been approved by the European Commission. As described below, Cisco Meraki offers a Data Processing Addendum to customers that incorporates these approved clauses. We do not require our customers to agree to the clauses but offer this option in order to give our customers an additional path to meeting requirements under applicable data protection laws.

Does Meraki act as a data controller or data processor with respect to Customer Data?

Article 2 of the Privacy Directive defines a data processor as "a natural or legal person...which processes personal data on behalf of the data controller" and a data controller as "a natural or legal person...which alone or jointly with others determines the purposes and means of the processing of personal data."

Meraki customers use the hardware devices they purchase from Meraki to provide internet access to their enterprises and guests and to collect and analyze information regarding use of their networks by the devices connecting to the internet via their networks, which includes information about those devices, such as MAC address, device type, etc. (collectively, "**Customer Data**").

Meraki acts as a data processor with respect to Customer Data because its customers, not Meraki, collect information about the use of their own networks and transmit that information to the Meraki servers by means of the hardware. Meraki customers also determine and manage their own network designs, configurations, and deployments, including limiting the extent to which Meraki services process Customer Data. Meraki does not access Customer Data except to provide the services, address technical issues, in response to customer support inquiries, and to the extent required by law. All other use or analysis of Customer Data is conducted by a customer's designated administrative staff with access to Meraki services. A customer can even elect to configure the services to completely eliminate access to Customer Data by Meraki or its employees and limit the functionality of the hardware and services to the minimum extent necessary to provide basic network functionality, such as internet access for terminal devices.

Does Meraki transfer Customer Data outside of the European Economic Area (EEA)?

For customers that have configured their networks to operate using the Meraki EU Cloud, all Customer Data is stored within the EEA, including failover and back-up data. With the EU Cloud enabled, customers may still cause limited and/or deemed transfers of Customer Data to the US, for example by contacting Meraki Support during off-peak hours in the EEA. Instructions to ensure that no Customer Data is transferred out of the EEA are available in Meraki's EU Cloud Configuration Guide.

Does Meraki make contractual commitments regarding compliance with European Privacy laws?

Yes. Meraki offers its customers a Data Processing Addendum ("**DPA**") incorporating the European Commission's standard contractual clauses (commonly known as the "model clauses"), in accordance with the Privacy Directive, pursuant to the European Commission's decision of February 5, 2010. The European Commission has affirmed such contractual commitments to be a valid way that European customers may

transfer personal data outside the EEA. By making these contractual terms available, Meraki ensures that European customers can continue to confidently deploy scalable, secure networks that comply with applicable regulations across the EEA.

How do I execute the Data Processing Addendum?

Customers wishing to execute the DPA should download the document here, complete the missing customer-related information, and email it to legal@meraki.com. Alternatively, customers can click here to complete the missing fields and sign electronically. Further instructions are set forth on the first page of the DPA.

What does the Meraki privacy and data security program entail?

Meraki takes a systematic approach to data protection, privacy, and security. We believe a robust security and privacy program requires active involvement of stakeholders, ongoing education, internal and external assessments, and instilment of best practices within the organization.

The Meraki team has established formal policies and supporting procedures concerning the privacy, security, review, and management of Meraki products and services. The Meraki Chief Information Security Officer and our Privacy Counsel maintain overall responsibility of the program, which is evaluated on a regular basis to ensure it is up to date and follows modern security standards and best practices as well as compliance with applicable privacy regulations.

The Meraki information security and data privacy program includes technical and organizational measures designed to ensure physical security, data integrity and privacy, and transparency. Internally, our program emphasizes controls and processes that affect members of the organization who have a business need to create, modify, upgrade, or support the products and systems that make up the Meraki solution and the products themselves (i.e. Meraki engineers who develop and support Meraki hardware, software, and backend systems).

The Meraki cloud architecture, itself, is designed for top-tier security and data privacy, and follows industry-leading best practices for security and privacy. Meraki datacenters are certified by industry-recognized standards including ISO 9001:2008, ISO 27001, PCI DSS, SSAE16, and ISAE 3402 (SAS-70) including Type II. These datacenters feature state of the art physical and cyber security and highly reliable designs. All Meraki services are replicated across multiple independent datacenters, so that customer-facing services fail over rapidly in the event of a catastrophic datacenter failure.

How does Meraki handle government requests for Customer Data?

Meraki is committed to maintaining the confidentiality, security, and integrity of all Customer Data stored on its servers. And our agreements with customers provide assurances that their data will be protected by our technical, physical, and procedural safeguards and will be kept confidential except in very limited circumstances. One such circumstance is when Meraki has received a lawful, valid subpoena or court order requiring that we deliver Customer Data in a controlled manner as part of an ongoing investigation.

The Meraki and Cisco Legal departments review each subpoena in order to determine its substantive merit and procedural validity. If the subpoena is not confidential, then Meraki will contact the customer regarding the subpoena and allow the customer to engage directly with the law enforcement agency making the request if the customer chooses to do so. If the subpoena is confidential, then Meraki will comply with the order following its determination that the request is in fact a proper one.

What if I have additional questions?

Please contact your Cloud Networking sales representative with more specific questions or concerns. He or she will involve our privacy compliance team as appropriate. Alternatively, you may contact the privacy team directly by emailing privacy@meraki.com.