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

Häufig gestellte Fragen für Kunden:

Einhaltung von europäischen Datenschutzgesetzen

Welche Dienste bietet Meraki an?

Meraki LLC („**Meraki**“ oder das „**Unternehmen**“), eine hundertprozentige Tochtergesellschaft von Cisco Systems, Inc. und Kern der Cloud Networking Group, ist führender Anbieter von cloud-basierten Netzwerkkomponenten. Meraki bietet Netzwerklösungen, mit denen Bereitstellung und Verwaltung von Netzwerken der Unternehmensklasse erheblich vereinfacht werden.

Wie erbringt Meraki seine Dienste?

Meraki verkauft sowohl Netzwerk-Hardwaregeräte wie Wireless Access Points, Switches und Security Appliances als auch Zugriff auf seine Cloud-basierte Software, mit der diese Geräte verwaltet werden. Meraki stellt seinen Kunden diese Managementsoftware über das Internet zur Verfügung. Die Kunden greifen auf diese dann über ihren gewerblich verfügbaren Internetzugang und ihre Webbrowser-Software zu. Die Kunden melden sich von einer Meraki-Website aus beim Meraki-Dienst an und greifen mithilfe ihrer individuellen Benutzernamen und Passwörter auf ihre Konten zu. Für die Konten können zusätzliche Authentifizierungsmethoden festgelegt werden.

Wie hält Meraki die europäischen Datenschutzgesetze ein?

Neben der Implementierung eines soliden Programms für Datenschutz und -sicherheit, ist Meraki bestrebt, die geltenden Datenschutzgesetze einzuhalten und bemüht sich darum, die in den relevanten Texten dargelegten Best Practices zu befolgen. Dazu gehören beispielsweise die *Richtlinie 94/46/EG des Europäischen Parlaments oder des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr* (die „**Datenschutzrichtlinie**“), wie sie in die Gesetze der einzelnen Länder eingebunden wurde, das *schweizerische Bundesgesetz über den Datenschutz vom 19. Juni 1992*, das *deutsche Bundesdatenschutzgesetz* vom 20. Dezember 1990 (zuletzt geändert am 14. September 1994) und die nicht bindende *Stellungnahme 05/2012 zum Cloud Computing* die am 1. Juli 2012 von der Artikel-29-Datenschutzgruppe veröffentlicht wurde.

Wie steht es um das Safe Harbor-Abkommen zwischen den USA und der EU?

Am 6. Oktober 2015 gab der Europäische Gerichtshof eine Entscheidung bekannt, die das Safe Harbor-Abkommen zwischen den USA und der EU („**Safe Harbor**“) für ungültig erklärte und bestimmte, dass das Abkommen keine gültige rechtliche Grundlage für die Übertragung personenbezogener Daten aus Europa in die Vereinigten Staaten darstellt.

In Abwesenheit von Safe Harbor können Unternehmen, die personenbezogene Daten aus der EU versenden und empfangen, ebenfalls die geltenden Datenschutzbestimmungen einhalten, indem sie Standardvertragsklauseln unterzeichnen, die aus einer Reihe von Vertragsbestimmungen bestehen, die von der Europäischen Kommission genehmigt wurden. Wie nachfolgend erläutert bietet Cisco Meraki den Kunden eine Ergänzung zur Datenverarbeitung an, die diese genehmigten Bestimmungen enthält. Wir verpflichten unsere Kunden nicht dazu, diesen Bestimmungen zuzustimmen, bieten aber diese Option an, um unseren Kunden eine zusätzliche Möglichkeit bereitzustellen, den Anforderungen der geltenden Datenschutzgesetze nachzukommen.

Tritt Meraki in Bezug auf Kundendaten als für die Verarbeitung Verantwortlicher oder Auftragsverarbeiter auf?

In Artikel 2 der Datenschutzrichtlinie wird der Auftragsverarbeiter als „natürliche oder juristische Person ..., die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet“ und der für die Verarbeitung Verantwortliche als „natürliche oder juristische Person ..., die allein oder gemeinsam mit anderen über die Zwecke, Bedingungen und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“ definiert.

Die Kunden von Meraki verwenden die Hardwaregeräte, die sie von Meraki erwerben, zur Bereitstellung des Internetzugangs für ihre Unternehmen und Gäste sowie zur Erfassung und Analyse von Informationen bezüglich der Nutzung ihrer Netzwerke durch die Geräte, die sich über ihre Netzwerke mit dem Internet verbinden; darunter fallen beispielsweise Informationen zu diesen Geräten wie die MAC-Adresse, der Gerätetyp usw. (zusammen die „**Kundendaten**“).

Meraki tritt in Bezug auf Kundendaten als Auftragsverarbeiter auf, da seine Kunden, und nicht das Unternehmen Meraki, Informationen über die Nutzung ihrer eigenen Netzwerke erfassen und diese Informationen an die Server von Meraki mittels der Hardware übermitteln. Darüber hinaus bestimmen und verwalten die Kunden von Meraki ihre Netzwerkdesigns, Konfigurationen und Bereitstellungen selbst und sie selbst bestimmen ebenfalls, in welchem Umfang durch die Services von Meraki Kundendaten verarbeitet werden. Meraki greift nur auf Kundendaten zu, um die Dienste bereitzustellen, technische Probleme zu behandeln, auf Support-Anfragen des Kunden zu reagieren und gesetzlichen Anforderungen nachzukommen. Jede andere Nutzung oder Analyse von Kundendaten wird von den Verwaltungsmitarbeitern des Kunden durchgeführt, die Zugriff auf Services von Meraki haben. Kunden können die Dienste sogar so einstellen, dass der Zugriff auf Kundendaten durch Meraki oder seine Mitarbeiter vollständig verwährt wird und dass die Funktionen der Hardware und der Dienste auf das Ausmaß beschränkt werden, das nötig ist, um die grundlegenden Netzwerkfunktionen wie den Internetzugang für Endgeräte bereitzustellen.

Übermittelt Meraki Kundendaten in Länder außerhalb des Europäischen Wirtschaftsraums (EWR)?

Für Kunden, die ihre Netzwerke für den Betrieb unter Verwendung der Meraki EU-Cloud konfiguriert haben, werden sämtliche Kundendaten einschließlich Failover und Backup innerhalb des EWR gespeichert. Wenn die EU-Cloud aktiviert ist, können Kunden dennoch begrenzte und/oder für erforderlich gehaltene Übertragungen von Kundendaten in die Vereinigten Staaten verursachen, wenn sie beispielsweise außerhalb der üblichen Bürozeiten im EWR Kontakt zum Support von Meraki aufnehmen. Anweisungen dazu, wie sichergestellt wird, dass keine Kundendaten aus dem EWR übertragen werden, befinden sich im EU Cloud Configuration Guide von Meraki.

Geht Meraki vertragliche Verpflichtungen in Hinblick auf die Einhaltung der europäischen Datenschutzgesetze ein?

Ja. Meraki bietet seinen Kunden eine Ergänzung zur Datenverarbeitung (nachfolgend die „**EZD**“) an, die die Standardvertragsklauseln der Europäischen Kommission (allgemein als „Musterklauseln“ bezeichnet) in Übereinstimmung mit der Datenschutzrichtlinie entsprechend der Entscheidung der Europäischen Kommission vom 5. Februar 2010 beinhaltet. Die Europäische Kommission hat bestätigt, dass diese vertraglichen Bestimmungen eine zulässiges Verfahren sind, um personenbezogene Daten nach außerhalb des EWR übertragen zu können. Durch die Bereitstellung dieser Vertragsbedingungen stellt Meraki sicher, dass europäische Kunden weiterhin sicher skalierbare, sichere Netzwerke bereitstellen können, die den geltenden Richtlinien im EWR entsprechen.

Wie setze ich die Ergänzung zur Datenverarbeitung in Kraft?

Kunden, die die EZD in Kraft setzen wollen, müssen hier das entsprechende Dokument herunterladen, die fehlenden kundenbezogenen Daten eintragen und das Dokument per E-Mail an legal@meraki.com senden. Alternativ können Kunden hier klicken, um die fehlenden Felder elektronisch auszufüllen und zu unterzeichnen. Weitere Anweisungen hierzu befinden sich auf der ersten Seite der EZD.

Wofür steht das Datenschutz- und -sicherheitsprogramm von Meraki?

Meraki verfolgt in Sachen Datenschutz, Privatsphäre und Sicherheit einen systematischen Ansatz. Wir sind davon überzeugt, dass ein solides Sicherheits- und Datenschutzprogramm eine aktive Beteiligung der Interessenvertreter, kontinuierliche Schulungen, interne und externe Bewertungen sowie die Verankerung von Best Practices innerhalb des Unternehmens voraussetzt.

Das Meraki-Team hat formale Richtlinien und unterstützende Verfahren bezüglich Datenschutz, Sicherheit, Prüfung und Verwaltung der Meraki-Produkte und -Dienste eingeführt. Der Chief Information Security Officer und der Datenschutzberater von Meraki tragen die Gesamtverantwortung für das Programm. Dieses wird regelmäßig dahingehend bewertet, ob es aktuell ist, den modernen Sicherheitsstandards und Best Practices entspricht, und ob die geltenden Datenschutzbestimmungen eingehalten werden.

Das Informationssicherheits- und Datenschutzprogramm von Meraki umfasst technische und organisatorische Maßnahmen zur Sicherstellung von physischer Sicherheit, Datenintegrität und -schutz sowie Transparenz. Intern wird mit unserem Programm ein Schwerpunkt auf Kontrollen und Verfahren gelegt, die sowohl solche Mitglieder des Unternehmens, die die Produkte und Systeme der Lösung von Meraki erstellen, modifizieren, aktualisieren oder unterstützen, als auch die Produkte selbst betreffen (z. B. Meraki Techniker, die an der Entwicklung und am Support der Meraki Hardware, Software und Back-End-Systeme beteiligt sind).

Bereits die Cloud-Architektur von Meraki ist auf Sicherheit und Datenschutz der Spitzenklasse ausgelegt und erfüllt die diesbezüglichen Best Practices der Branche. Rechenzentren von Meraki sind nach Branchenstandards wie z. B. ISO 9001:2008, ISO 27001, PCI DSS, SSAE16 und ISAE 3402 (SAS-70) einschließlich Typ II zertifiziert. Diese Rechenzentren verfügen über topmodernen physischen und virtuellen Schutz und höchst zuverlässige Designs. Alle Dienste von Meraki werden in mehreren unabhängigen Rechenzentren repliziert, sodass bei Kundendiensten im Falle eines katastrophalen Störfalls des Rechenzentrums ein schnelles Failover möglich ist.

Wie geht Meraki mit staatlichen Anfragen nach Kundendaten um?

Meraki ist bestrebt, die Vertraulichkeit, Sicherheit und Integrität aller auf seinen Servern gespeicherten Kundendaten zu bewahren. Unsere Vereinbarungen mit Kunden enthalten zudem Zusicherungen, dass die Vertraulichkeit ihrer Daten durch unsere technischen, physischen und verfahrensmäßigen Schutzmaßnahmen gewahrt wird. Hierbei gibt es in seltenen Fällen Ausnahmen. Eine dieser Ausnahmen besteht dann, wenn Meraki eine gerichtliche, gültige Vorladung oder Anordnung erhält, durch die wir dazu aufgefordert werden, Kundendaten im Rahmen einer laufenden Untersuchung kontrolliert offenzulegen.

Die Rechtsabteilungen von Meraki und Cisco prüfen jede Vorladung in Hinblick auf ihre Stichhaltigkeit und verfahrensrechtliche Gültigkeit. Ist die Vorladung nicht vertraulich zu behandeln, wendet sich Meraki diesbezüglich an den Kunden und gibt diesem Gelegenheit, sich direkt mit der betroffenen Strafverfolgungsbehörde in Verbindung zu setzen, falls er dies wünscht. Ist die Vorladung vertraulich zu behandeln, kommt Meraki der Anordnung nach, sobald die Gültigkeit der Anfrage bestätigt wurde.

Was, wenn ich weitere Fragen habe?

Bitte wenden Sie sich an Ihren Cloud Networking-Vertriebsmitarbeiter, wenn Sie spezifischere Fragen oder Bedenken haben. Er oder sie wird dann bei Bedarf auch das Datenschutz-Compliance-Team hinzuziehen. Alternativ können Sie sich unter privacy@meraki.com auch direkt an das Datenschutz-Compliance-Team wenden.