dSchulWLAN

Infoblatt Datenschutz

verantwortlich:	Ulf Liermann; UL
Version:	1.0 vom: 03.04.2020
Status:	Gültig
Aktenzeichen:	-/-
Schutzstufe:	keine Schutzstufe
Zielgruppe:	Kunden

Inhaltsverzeichnis

Änderungsverzeichnis

Version	Änderungs-datum	Gliederungs-punkt	Erläuterung der Änderung	Autor/in
1.0	03.04.2020			Ulf Liermann

1 Einleitung

In diesem Dokument werden die Maßnahmen und Leistungen zur Einhaltung der DSGVO-Konformität des Dataport-Produkts dSchul-WLAN erläutert. Dataport greift bei diesem Produkt auf das Herstellerportfolio des Cloud IT-Unternehmen Cisco Meraki zu.

2 Cisco Merakis Verpflichtung zur DSGVO-Bereitschaft

Cisco Meraki unterstützt Kunden und Partner bei der Steuerung der DSGVO durch den Schutz und die Respektierung personenbezogener Daten, unabhängig davon, wo sie erhoben oder verarbeitet werden, und verpflichtet sich zur Einhaltung geltender regulatorischer Rahmenbedingungen in den USA und im Ausland einschließlich der DSGVO. Zusammen mit dem Cisco Privacy Office hat Cisco Meraki ein funktionsübergreifendes Team aus Experten für Produkte, Technik, Recht und Datenschutz eingerichtet, um sicherzustellen, dass Cisco Meraki die DSGVO-Anforderungen erfüllt.

- **Richtlinien und Standards**: Weiterentwicklung von Standards und Prozessen zur Definition des Lebenszyklus personenbezogener Daten sowie Gewährleistung von Datentransparenz, Genauigkeit, Zugänglichkeit, Vollständigkeit, Sicherheit und Konsistenz auf der gesamten Cisco Meraki-Plattform.
- **Data Inventory and Mapping**: Abschluss einer Bewertung der Cisco Meraki-Produktarchitektur, die als Datenschutz-Folgenabschätzung (Data Protection Impact Assessment, DPIA) bekannt ist.
- **Incident Response**: laufende Überprüfung und Aktualisierung des Incident-Response-Prozesses von Cisco Meraki, einschließlich verbesserter Koordination mit funktionsübergreifenden Teams aus den Bereichen Datenschutz, Sicherheit, Recht, Technik und Produkt bei Cisco Meraki und seiner Muttergesellschaft Cisco Systems, Inc.
- **Datenübertragungsmechanismen**: Zertifizierung nach den US-amerikanischen und US-amerikanischen Datenschutzschildrahmen und -grundsätzen, die vom US-Handelsministerium für die Erhebung, Nutzung, Verarbeitung und grenzüberschreitende Übermittlung personenbezogener Daten aus der EU und der Schweiz in die USA festgelegt wurden (Strom); unter der Leitung von Cisco Systems, Inc., Genehmigung von Binding Corporate Rules-C (vollständig); Aktualisierung des Cisco Meraki Data Processing Addendums unter Einbeziehung der Standardvertragsklauseln (SCC) der Europäischen Kommission, um die Übereinstimmung mit den DSGVO-Anforderungen sicherzustellen
- Audits **und Zertifizierungen** von Drittanbietern: Wartung der Cisco Meraki Dashboard Payment Card Industry (PCI) Level 1-Zertifizierung und Datencenter-Zertifizierungen wie SAS70 Typ II / SSAE16 und ISO 27001.
- **Privacy by Design**: kontinuierliche Integration von Datenschutz-, Datenschutz- und Sicherheitsprinzipien in Produktdesign- und Entwicklungsprozesse in allen Phasen des Produktentwicklungszyklus.

- **Datenschutz und Sensibilisierung der Mitarbeiter für den Datenschutz**: Fortlaufende Schulungen und Sensibilisierung der Mitarbeiter in Bezug auf Datenschutz und Datenschutz durch unternehmensweite interaktive Kampagnen, Schulungen, externe Zertifizierungen und Online-Ressourcen für Zusammenarbeit und Kommunikation.
- **Dashboard - Feature - Entwicklung**: Entwicklung von neuen Dashboard -Funktionen von Cisco Meraki helfen Kunden zu ermöglichen, wie die Datenverarbeitung Verantwortliche, um Daten unterliegen Anfragen unter BIPR zu reagieren. Solche Funktionen werden ohne zusätzliche Kosten für Kunden mit gültigen Softwarelizenzen über das Dashboard verfügbar sein.

3 Netzwerk-Management-Daten und Traffic-Analysen

Die Dashboard-Anwendung für eine Organisation in der Cisco Meraki EU Cloud wird von Rechenzentren in der EU (München, Frankfurt und Dublin) gehostet. **Alle Managementdaten in Bezug auf das Netzwerk, Daten zur Analyse des Endnutzerverkehrs und werden ausschließlich in diesen EU-Datenzentren gespeichert.**

Lediglich die Registrierungsinformationen müssen mit dem Master-Controller synchronisiert werden:

Koordination über den Master Controller

Die Architektur der globalen Cisco Meraki Cloud hängt von der zentralen Orchestrierung durch einen Master-Controller ab, der geografisch in den Rechenzentren von Cisco Meraki in den USA angesiedelt ist.

Dieser Master-Controller speichert mehrere Elemente der Organisationsdefinition, High-Level-Konfigurationsdaten für die in jeder Organisation enthaltenen Meraki-Netzwerke und Anmeldeinformationen für die Dashboard-Administratoren und -Benutzer der Organisation.

In den folgenden Abschnitten wird erläutert, wie eine Organisation erstellt wird, die von der Cisco Meraki EU Cloud gehostet wird, welche Informationselemente mit dem Master-Controller synchronisiert werden, sowie Best Practices, um eine unbeabsichtigte Offenlegung von privaten Daten zu verhindern.

Daten auf dem Master-Controller gespeichert werden:

Registrierungsdaten

Das Dashboard Account Registration-Formular enthält mehrere Datenfelder, die die EU auf dem Master-Controller speichern lassen. Einige dieser Felder sind optional.

Feld	Beschreibung	Anmerkungen
Email	E-Mail-Adresse des primären Administrators	Erforderlich
Unternehmen	Name der Organisation	Erforderlich
Vollständiger Name	Vollständiger Name des primären Administrators	Wahlweise
Adresse	Adresse der Organisation	Wahlweise

Konfigurationsdaten
In den folgenden Abschnitten werden die Datenelemente beschrieben, die auf dem Master-Controller gespeichert sind.

Organisationsdaten

Art	Anmerkungen
Informationen zu Organisationslizenzen	
Organisation EU-Server-ID	
Organisation "Einstellungen" Seite	
Benutzer des Organisationsadministrators	Kann SAML-Benutzer sein
Organisationsadministratoreinstellungen	
Dashboard-Benutzerprofileinstellungen	

Netzwerkdaten

Art	Anmerkungen
Netzwerknamen	Darf beliebige alphanumerische Zeichenfolgen sein
Netzwerkzeitzonen	
Netzwerk-Tags	Darf beliebige alphanumerische Zeichenfolgen sein
"Netzwerkweite" Seiteneinstellungen	
Netzwerkadministrator Benutzer	Kann SAML-Benutzer sein
Netzwerk-Administratoreinstellungen	

Drahtlose Konfigurationsdaten

Art	Anmerkungen
Wireless "Zugriffskontrolle" Seiteneinstellungen	
Wireless "Firewall & Traffic Shaping" Seiteneinstellungen	
Wireless "SSIDs" Seiteneinstellungen	
"Anmelden mit Meraki Authentifizierung" Splash Benutzer	Wahlweise

Siehe hierzu auch:
https://documentation.meraki.com/zGeneral_Administration/Privacy_and_Security/EU_Cloud_Configuration_Guide

Auszug aus FAQ: 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

Ergänzung zur Datenverarbeitung

Cisco 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.

Die EZD liegt bei (Anlage 3)

4 Management-Daten

Nur Daten, die zum Management des WLAN notwendig sind, wie Lokationsdaten, Kennwörter für Nutzer des WLAN-Managements usw. (s a. 3.10.1-(1)). werden im Cloudservice von Cisco Meraki gespeichert und verarbeitet.
Der WLAN-Traffic wird nicht über diesen Dienst verarbeitet.

5 Cisco Meraki EU-Cloud

Der Rechenzentrumsbetreiber der Cisco Meraki-Cloud ist Cisco Meraki selbst.

Unterlagen zu Leistungsfähigkeit finden Sie in der Anlage 1 und Anlage 2, die beide an dieses Dokument angefügt sind.

6 Anlagen

Anlage 1 The Cisco Meraki EU Cloud

The Cisco Meraki EU Cloud

Overview

Cisco Meraki is committed to data protection, privacy, and security and has designed its cloud architecture specifically in a way that enables customers to securely protect their data. European customers can confidently deploy scalable, secure Meraki networks that comply with applicable data protection regulations across the European Economic Area (EEA).

The Meraki EU Cloud

The Meraki cloud architecture leverages a globally distributed public cloud architecture that provides built–in reliability, security, and redundancy. Specifically to meet the needs of European customers, Meraki created the EU Cloud, a separate part of the Meraki cloud architecture designed to meet the needs of European customers and regulations. Hosted on data centers located exclusively in the EEA, the Meraki EU Cloud provides reliability and business redundancy offered by a distributed architecture while ensuring that no personal data leaves the EEA.

Additionally, the EU Cloud's out–of–band architecture ensures only management information, and not network traffic, passes through EU Cloud datacenters. The EU Cloud architecture enables customers to satisfy their legal obligations and simultaneously realize all the advantages cloud management offers, including centralized visibility and control, unified management of wireless and wired networks, and reduced operational expense.

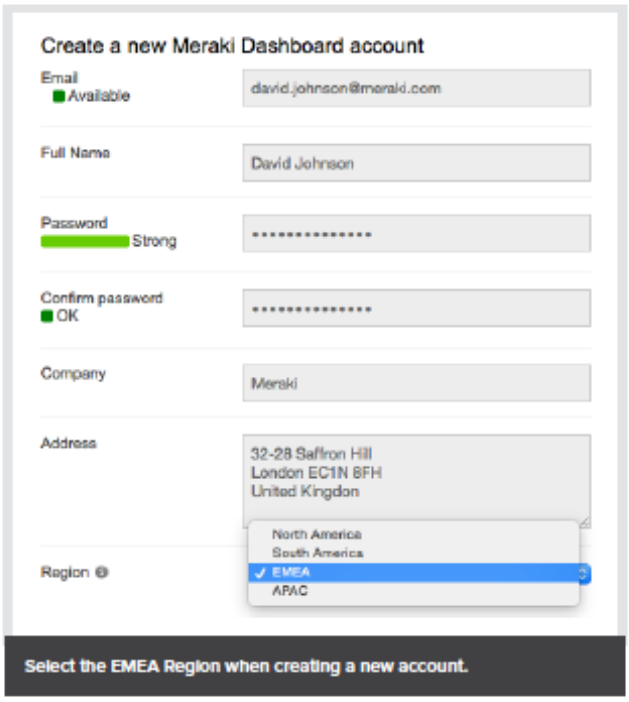
Reliable, Secure, Certified

The Meraki EU Cloud is built on a PCI DSS Level 1 certified system architecture and operates with a 99.99% Service Level Agreement. Additionally, Meraki EU Cloud data centers are certified with one or more of the following:

- ISO 9001:2008
- ISO 27001:2008
- PCI DSS

Meraki and the EU Cloud are compliant with the following applicable European data protection regulatory frameworks and local laws:

- EU Directive 95/46/EC
- German Federal Data Protection Act
- Article 29 Working Party Opinion of July 1, 2012



Select the EMEA Region when creating a new account.

Security Made Simple

Creating a secure deployment hosted in the EU Cloud is as simple as selecting the EMEA Region when creating a Meraki account. Meraki ensures that accounts created by selecting the EMEA Region are hosted by the Meraki EU Cloud and that those accounts comply with the above.

Reference Documentation

Additional documentation and detail about data privacy and security are available, including the following:

- EU Privacy Compliance FAQ
- EU Cloud Configuration Guide
- More information about the Meraki architecture, security policies, and procedures is available online

For more information please send an email to privacy@meraki.com

Anlage 2 Cisco Meraki Data Center Design

Cisco Meraki Datacenter Design

Der Cisco Meraki-Service ist in Tier-1-SAS70-Typ-II-zertifizierten Datencentern zusammengefasst. Diese Rechenzentren verfügen über hochmoderne physische und Cyber-Sicherheit sowie hoch zuverlässige Designs. Alle Cisco Meraki-Dienste werden über mehrere unabhängige Datencenter hinweg repliziert, so dass bei Ausfall eines katastrophalen Datencenters die kundenseitigen Dienste schnell fehlschlagen.

Verfügbarkeitsüberwachung

- 99,99% Uptime Service Level Agreement (das ist weniger als eine Stunde pro Jahr)
- 24x7 automatische Fehlererkennung - alle Server werden alle fünf Minuten von mehreren Standorten aus getestet
- Schnelle Eskalationsverfahren für mehrere Operationsteams
- Unabhängiges Ausfallalarmsystem mit 3x Redundanz

Redundanz

- Fünf geografisch verteilte Rechenzentren
- Die Daten jedes Kunden (Netzwerkkonfiguration und Nutzungsmetriken) werden über drei unabhängige Rechenzentren hinweg repliziert
- Echtzeit-Replikation von Daten zwischen Datencentern (innerhalb von 60 Sekunden)
- Nächtliche archivarische Backups

Katastrophale Erholung

- Schnelles Failover auf Hotspare bei Hardwareausfall oder Naturkatastrophen
- Die Out-of-Band-Architektur bewahrt die Netzwerkfunktionalität des Endbenutzers, selbst wenn die Verbindung zu den Cloud-Diensten von Cisco Meraki unterbrochen ist
- Failover-Verfahren werden wöchentlich durchgeführt

Cloud-Servicesicherheit

- 24x7 automatische Einbruchserkennung
- Geschützt über IP- und Port-basierte Firewalls
- Remote-Zugriff durch IP-Adresse eingeschränkt und durch öffentlichen Schlüssel (RSA) verifiziert
- Systeme sind nicht über einen Passwort-Zugang zugänglich
- Administratoren werden bei Konfigurationsänderungen automatisch benachrichtigt

Out-of-Band-Architektur

- In der Cloud werden nur Netzwerkkonfigurations- und Nutzungsstatistiken gespeichert
- Endbenutzerdaten durchlaufen nicht das Datencenter
- Alle sensiblen Daten (zB Passwörter) werden verschlüsselt gespeichert

Physische Sicherheit

- Ein hochsicheres Kartenschlüsselsystem und biometrische Leser werden verwendet, um den Zugang zu Einrichtungen zu steuern
- Alle Eingänge, Ausgänge und Schränke werden videoüberwacht
- Sicherheitsbeauftragte überwachen den gesamten Datenverkehr rund um die Uhr in und aus den Rechenzentren und stellen sicher, dass die Eingabevorgänge eingehalten werden

Katastrophenvorbereitung

- Rechenzentren verfügen über ausgeklügelte Sprinkleranlagen mit Verriegelungen, um ein unbeabsichtigtes Austreten von Wasser zu verhindern
- Dieselgeneratoren bieten Backup-Power bei Stromausfall
- USV-Systeme versorgen den Strom mit Strom und sorgen für eine ordnungsgemäße Abschaltung im Falle eines vollständigen Stromausfalls
- Jedes Datencenter verfügt über Dienste von mindestens zwei Top-Tier-Carriern
- Seismische Verstrebungen sind für den Doppelboden, die Schränke und die Trägersysteme vorgesehen
- Im Falle eines katastrophalen Datencenterausfalls werden Dienste in ein anderes geografisch getrenntes Datencenter umgeschaltet

Umweltkontrollen

- Überproportionierte HVAC-Systeme bieten Kühlung und Feuchtigkeitskontrolle
- Bodenbelagsysteme sind für die Luftverteilung bestimmt

Regelmäßige Penetrationstests

- Alle Cisco Meraki-Rechenzentren werden täglich von einem unabhängigen Drittanbieter getestet

Datacenter-Zertifizierung

- Cisco Meraki-Rechenzentren sind nach SAS70 Typ II zertifiziert

Anlage 3 Ergänzung zur Datenverarbeitung

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

CISCO MERAKI
ERGÄNZUNG ZUR DATENVERARBEITUNG NACH EU-VORSCHRIFTEN

Diese Ergänzung zur Datenverarbeitung nach EU-Vorschriften (nachfolgend die „**EZD**") ist Bestandteil der Endkundenvereinbarung (nachfolgend die „**Vereinbarung**") zwischen Ihnen (nachfolgend der „**Kunde**") und Meraki LLC, einer Gesellschaft mit beschränkter Haftung nach Recht des US-Staates Delaware (nachfolgend „**Meraki**"). Sie stellt unser Übereinkommen hinsichtlich der Verarbeitung personenbezogener Daten und anderer Kundendaten unter Einhaltung der Datenschutzgesetze und -richtlinien dar. Verweise auf die Vereinbarung sind im Sinne der EZD auszulegen. Alle hierin nicht definierten Begriffe haben die Bedeutung, die ihnen in der Vereinbarung zugeschrieben wurde.

Diese EZD besteht aus zwei Teilen: (i) dem Hauptteil dieser EZD und (ii) Anlage 1 hierzu (den „**Standardvertragsklauseln**" einschließlich Anhängen). Die Standardvertragsklauseln regeln die Übertragung personenbezogener Daten an Auftragsverarbeiter gemäß Artikel 26(2) der EU-Richtlinie 95/46/EG („**Datenschutzrichtlinie**") entsprechend der Entscheidung der Europäischen Kommission vom 5. Februar 2010. Verweise im Text der EZD auf eine bestimmte „Klausel" beziehen sich auf Bestimmungen in den Standardvertragsklauseln.

INKRAFTSETZUNG DIESER EZD:

1. Führen Sie einen der folgenden Schritte durch, um diese EZD in Kraft zu setzen:
   a. Laden Sie diese EZD herunter, füllen Sie die Formularfelder aus, unterschreiben Sie das Dokument, und senden Sie es zur Gegenzeichnung per E-Mail an legal@meraki.com; oder
   b. Klicken Sie hier, um die Formularfelder auszufüllen und das Dokument elektronisch zu unterzeichnen.
2. Nach Unterzeichnung durch Ihr Unternehmen und Meraki tritt diese EZD (einschließlich Standardvertragsklauseln) in Kraft, und Ihr Unterzeichner erhält per E-Mail eine rechtsverbindliche Kopie.

GÜLTIGKEIT DIESER EZD

Ist der Kunde, der diese EZD unterzeichnet, eine Vertragspartei, so ist diese EZD eine Ergänzung und ein Teil der Vereinbarung. Diese EZD verliert jedoch sofort und automatisch ihre Gültigkeit, wenn der Kunde in seinem Meraki Dashboard nicht die Konfiguration „EU-Cloud" aktiviert.

Ist die juristische Person, die diese EZD unterzeichnet, keine Vertragspartei, so ist diese EZD nichtig und nicht rechtsverbindlich. Eine solche juristische Person muss diese EZD von einer Tochtergesellschaft oder der Muttergesellschaft in Kraft setzen lassen, die eine Vertragspartei ist. Tochtergesellschaften einer solchen juristischen Kundenperson, die ausdrücklich durch die Vereinbarung abgedeckt sind, werden auch durch diese EZD abgedeckt.

DATENVERARBEITUNGSBEDINGUNGEN

Der Kunde und Meraki vereinbaren hiermit, dass die Übertragung personenbezogener Daten des Kunden an Meraki mittels der Produkte den folgenden Bedingungen unterliegt.

1. DEFINITIONEN

„**Für die Verarbeitung Verantwortlicher**" bezeichnet die juristische Person, die Zwecke und Mittel zur Verarbeitung personenbezogener Daten bestimmt. Im Rahmen dieser EZD ist der Kunde der für die Verarbeitung Verantwortliche.

„**Datenverarbeiter**" bezeichnet die juristische Person, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet. Im Rahmen dieser EZD ist Meraki, einschließlich Tochtergesellschaften, der Datenverarbeiter.

„**Datenschutzgesetze und -richtlinien**" bezeichnen alle Gesetze und Richtlinien, einschließlich Gesetze und Richtlinien der Europäischen Union, des Europäischen Wirtschaftsraums und ihrer Mitgliedsstaaten, die auf die Verarbeitung personenbezogener Daten gemäß der Vereinbarung anwendbar sind.

„**Datensubjekt**" bezeichnet die Person, auf die sich die personenbezogenen Daten beziehen.

„**Meraki Dashboard**" bezeichnet die Online-Softwareplattform von Meraki, einschließlich der „Dashboard"-Oberfläche.

„**Personenbezogene Daten**" bezeichnen gemäß Definition in der Datenschutzrichtlinie oder einer entsprechenden Nachfolgeregelung als Teil der Kundendaten an Meraki übertragene Informationen, die eine lebende Person bestimmen oder bestimmbar machen.

„**Verarbeitung**" hat die in der Datenschutzrichtlinie zugewiesene Bedeutung.

„**Standardvertragsklauseln**" bezeichnen die Vereinbarung, die durch und zwischen Kunde und Meraki in Kraft gesetzt wird und gemäß der Entscheidung der Europäischen Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer, die kein angemessenes Datenschutzniveau gewährleisten, als Anlage 1 Teil dieser EZD sind.

„**Unterauftragsverarbeiter**" bezeichnet einen von Meraki beauftragten Datenverarbeiter.

„**Technische und organisatorische Maßnahmen**" bezeichnen die unter https://meraki.cisco.com/lib/pdf/eu_technical_organizational_measures.pdf beschriebenen Kontrollmaßnahmen, Prozesse und Verfahren einschließlich gelegentlicher Aktualisierungen in Bezug auf Verfahren von Meraki hinsichtlich Privatsphäre und Datenschutz.

2. VERARBEITUNG PERSONENBEZOGENER DATEN

2.1 **Pflichten des Kunden.** Der Kunde verpflichtet sich, bei seiner Anwendung der Produkte die Bestimmungen der Datenschutzgesetze und -richtlinien einzuhalten. Darüber hinaus übernimmt der Kunde die alleinige Verantwortung für die Genauigkeit, Qualität und Rechtmäßigkeit personenbezogener Daten sowie der Mittel zur Beschaffung personenbezogener Daten durch den Kunden, einschließlich Versendung erforderlicher Benachrichtigungen an und Einholung erforderlicher Zustimmungen von Netzwerkbenutzern.

2.2 **Verarbeitung personenbezogener Daten durch Meraki.** Wir verarbeiten und verwenden Kundendaten in Ihrem Namen und handeln dabei ausschließlich entsprechend Ihren Anweisungen (einschließlich per E-Mail) sowie gemäß den gesetzlichen Vorgaben. Der Kunde bestätigt hiermit, dass sich aus seiner Anwendung der Produkte ein Auftrag an Meraki zur Verarbeitung und Verwendung von Kundendaten ergibt, der es ermöglicht, die Produkte gemäß dieser Vereinbarung bereitzustellen. Personenbezogene Daten sind vertrauliche Informationen entsprechend der Vereinbarung.

2.3 **Produktkonfiguration.** Der Kunde verpflichtet sich, die Option „EU-Cloud" in seinem Meraki Dashboard für seine Netzwerke dauerhaft zu aktivieren. Der Kunde bestätigt, dass er ohne zusätzliche Kosten die Produkte so konfigurieren kann, dass die an Meraki übertragenen Kundendaten und personenbezogenen Daten erheblich begrenzt werden.

3. RECHTE VON DATENSUBJEKTEN

3.1 **Löschung personenbezogener Daten.** Der Kunde hat im Meraki Dashboard die Möglichkeit, gemäß möglichen Vorgaben durch Datenschutzgesetze und -richtlinien personenbezogene Daten eines bestimmten Datensubjekts so zu löschen, dass die Daten weder für den Kunden noch für Dritte zugänglich oder identifizierbar sind. Meraki wird nach einer solchen Löschung durch den Kunden sobald nach vernünftigem Ermessen möglich, jedoch maximal innerhalb von 14 Monaten, diese Daten vollständig aus seinen Systemen entfernen.

3.2 **Anfragen von Datensubjekten.** Meraki wird den Kunden im gesetzlich zulässigen Umfang umgehend über den Erhalt einer Anfrage eines Datensubjekts wegen des Zugriffs auf oder der Korrektur, Änderung oder Löschung von personenbezogenen Daten dieses Datensubjekts benachrichtigen. Meraki wird auf solche Anfragen von Datensubjekten ohne vorherige schriftliche Genehmigung des Kunden nicht reagieren, außer zur Bestätigung, dass sich die Anfrage auf den Kunden bezieht. Dem Kunden obliegt die Verantwortung für die Reaktion auf solche Anfragen durch die Löschung von Daten gemäß Abschnitt 3.1.

4. MITARBEITER VON MERAKI

4.1 **Vertraulichkeit.** Meraki wird seine an der Verarbeitung personenbezogener Daten beteiligten Mitarbeiter über die Vertraulichkeit personenbezogener Daten informieren und diese Mitarbeiter in ihren Pflichten schulen sowie schriftliche Vertraulichkeitsvereinbarungen unterzeichnen lassen. Meraki wird dafür Sorge tragen, dass diese Vertraulichkeitspflichten auch nach Beendigung der Arbeitsverhältnisse dieser Mitarbeiter in Kraft bleiben.

4.2 **Zuverlässigkeit.** Meraki wird wirtschaftlich angemessene Schritte unternehmen, um die Zuverlässigkeit seiner an der Verarbeitung personenbezogener Daten beteiligten Mitarbeiter sicherzustellen, etwa durch die Durchführung von Hintergrundprüfungen für neue Mitarbeiter.

4.3 **Zugriffsbeschränkung.** Meraki wird dafür Sorge tragen, dass der Zugriff auf personenbezogene Daten auf Mitarbeiter beschränkt wird, die diesen Zugriff zur Durchführung der Vereinbarung benötigen.

4.4 **Datenschutzbeauftragter.** Soweit gemäß Datenschutzgesetzen und -richtlinien vorgeschrieben, hat Meraki einen Datenschutzbeauftragten ernannt. Meraki wird die Kontaktdaten des ernannten Beauftragten auf Verlangen herausgeben.

5. UNTERAUFTRAGSVERARBEITER

5.1 **Ernennung von Unterauftragsverarbeitern.** Der Kunde bestätigt und erkennt an, dass (i) Meraki berechtigt ist, seine Tochtergesellschaften als Unterauftragsverarbeiter einzusetzen, und (ii) dass Meraki oder eine Tochtergesellschaft zu gegebener Zeit Dritte mit der Verarbeitung von Kundendaten im Zusammenhang mit der Bereitstellung der Produkte an den Kunden beauftragen dürfen. Meraki wird personenbezogene Daten nur gegenüber Unterauftragsverarbeitern offenlegen, die Vertragsparteien schriftlicher Vereinbarungen mit Meraki sind, in denen Pflichten von mindestens dem Umfang der in dieser EZD geregelten Pflichten geregelt sind.

5.2 **Haftung.** Meraki ist für die Handlungen und Unterlassungen seiner Unterauftragsverarbeiter im selben Umfang haftbar wie bei einer Durchführung der Services jedes Unterauftragsverarbeiters direkt gemäß dieser EZD, sofern nichts anderes in der Vereinbarung festgelegt ist.

6. SICHERHEIT

6.1 **Technische und organisatorische Maßnahmen.** Wir haben technische und organisatorische Maßnahmen implementiert und werden diese vorhalten. Meraki überwacht regelmäßig die Einhaltung dieser Sicherheitsmaßnahmen und wird während der Laufzeit der Vereinbarung angemessene Sicherheitsmaßnahmen vorhalten. Der Kunde erkennt an, dass die in diesem Abschnitt 6.1 beschriebenen Maßnahmen die Anforderungen von § 9 des *Bundesdatenschutzgesetzes* erfüllen, sofern auf den Kunden anwendbar.

6.2 **Zertifizierungen und Prüfungen** Meraki hat die unter den technischen und organisatorischen Maßnahmen aufgeführten Zertifizierungen und Prüfungen durch Dritte erlangt. Auf schriftliche Aufforderung des Kunden in angemessenen Abständen stellt Meraki eine Kopie seiner zu diesem Zeitpunkt neuesten Prüfungen oder Zertifizierungen durch Dritte („**Prüfberichte**"), sofern zutreffend, oder Zusammenfassungen dieser Berichte zur Verfügung, die Meraki seinen Kunden allgemein zur Verfügung stellt.

7. MANAGEMENT VON SICHERHEITSLÜCKEN

Meraki verpflichtet sich, Richtlinien und Verfahren zum Management von Sicherheitsvorfällen vorzuhalten, einschließlich detaillierter Eskalationsverfahren für Sicherheitsvorfälle. Falls Meraki eine unbefugte Offenlegung von Kundendaten (ein „Sicherheitsvorfall") zur Kenntnis gelangt, wird Meraki den Kunden unverzüglich darüber informieren und dem Kunden die relevanten Informationen über den Sicherheitsvorfall zur Verfügung stellen, einschließlich der Art der betroffenen Kundendaten, des Umfangs der offengelegten Kundendaten, der Umstände des Vorfalls, der ergriffenen Maßnahmen zur Minimierung der Folgen sowie ergriffener Abhilfemaßnahmen und Vorbeugemaßnahmen.

8. RÜCKGABE UND LÖSCHUNG VON KUNDENDATEN

Nach Beendigung der Vereinbarung hat der Kunde die Möglichkeit, alle Kundendaten, einschließlich personenbezogener Daten, so zu löschen, dass diese Daten weder für den Kunden noch für Dritte zugänglich oder identifizierbar sind. Meraki wird nach einer solchen Löschung durch den Kunden sobald nach vernünftigem Ermessen möglich, jedoch maximal innerhalb von 14 Monaten, diese Daten vollständig aus seinen Systemen entfernen.

9. ÜBERTRAGUNG PERSONENBEZOGENER DATEN AUSSERHALB DER EU

9.1 Anwendung der Standardvertragsklauseln. Die Standardvertragsklauseln und die Bestimmungen dieses Abschnitts 9 gelten nur für personenbezogene Daten, die aus dem Europäischen Wirtschaftsraum (EWR) entweder direkt oder durch Weiterübermittlung in ein Land oder an einen Empfänger außerhalb des EWR übertragen werden, das bzw. der (i) kein von der Europäischen Kommission anerkanntes angemessenes Datenschutzniveau (gemäß Datenschutzrichtlinie) gewährleistet und (ii) durch keine von den zuständigen Behörden oder Gerichten anerkannte geeignete Rahmenvereinbarung zur Gewährleistung eines angemessenen Schutzes für personenbezogene Daten abgedeckt ist. Jegliche Durchsetzung der Standardvertragsklauseln gemäß § 3 durch ein Datensubjekt, eine Organisation oder eine andere Körperschaft im Auftrag eines Datensubjekts unterliegt den Bestimmungen dieser EZD, wobei die durchsetzende Partei den Standpunkt des Kunden einnimmt.

9.2 Beschränkung des Umfangs der Verarbeitung. Das alleinige Ziel von Meraki bei der Verarbeitung der personenbezogenen Daten besteht in der Bereitstellung der Produkte entsprechend der Vereinbarung, und Meraki verarbeitet die personenbezogenen Daten ausschließlich zum Zweck der Bereitstellung der Produkte für den Kunden.

9.3 Anweisungen. Diese EZD und die Vereinbarung sind vollständige und endgültige Anweisungen des Kunden an Meraki zur Verarbeitung personenbezogener Daten. Alle weiteren oder alternativen Anweisungen bedürfen der separaten schriftlichen Zustimmung. Zum Zweck von § 5(a) weist der Datenexporteur den Datenimporteur hiermit an, personenbezogene Daten (a) gemäß der Vereinbarung; (b) auf Anfrage des Kunden, einschließlich Anfragen im Zusammenhang mit Support-Services; und (c) gemäß Initiierung durch Endbenutzer bei deren Nutzung der Kundennetzwerke zu verarbeiten.

9.4 Unterauftragsverarbeiter. Gemäß § 5(h) bestätigt der Datenexporteur und stimmt ausdrücklich zu, dass (a) Tochtergesellschaften von Meraki als Unterauftragsverarbeiter eingesetzt werden können und (b) Meraki bzw. seine Tochtergesellschaften im Rahmen der Bereitstellung der Produkte Dritte als Unterauftragsverarbeiter einsetzen können.

9.4.1 Benachrichtigungen hinsichtlich Unterauftragsverarbeiter. Meraki stellt dem Kunden nach schriftlicher Aufforderung eine Liste der Unterauftragsverarbeiter und/oder eine Kopie der Vereinbarung zur Verfügung, die mit einem in der Aufforderung des Kunden ausdrücklich genannten Unterauftragsverarbeiter im Zusammenhang mit der Verarbeitung personenbezogener Daten geschlossen wurde. Bei Bedarf kann Meraki vor Aushändigung an den Kunden kaufmännisch sensible oder vertrauliche Informationen aus dieser Vereinbarung entfernen.

9.5 Prüfungen und Zertifizierungen. Durch die Pflichten von Meraki gemäß Abschnitt 6, einschließlich der Pflicht zur Bereitstellung der Prüfberichte, gelten die unter §§ 5(f) und 12(2) in Bezug auf den Kunden zugesicherten Auditierungsrechte als vollständig erfüllt.

9.6 **Zertifizierung der Löschung.** Die Parteien vereinbaren, dass durch die Erfüllung der in den Abschnitten 3.1, 3.2 und 8 geregelten Pflichten des Datenimporteurs dessen Pflichten gemäß § 12(1) als erfüllt gelten und dass die in § 12(1) beschriebene Zertifizierung der Löschung personenbezogener Daten nur auf schriftliche Aufforderung des Datenexporteurs erfolgt.

10. RECHTSWIRKUNG; BEENDIGUNG; SPRACHE

Zur Ausräumung jedes Zweifels wird diese EZD zwischen dem Kunden und Meraki nur rechtsverbindlich, wenn die im vorstehenden Abschnitt „INKRAFTSETZUNG DIESER EZD" beschriebenen formellen Schritte vollständig durchgeführt wurden. Zur Ausräumung jedes Zweifels verliert diese EZD sofort und automatisch ihre Gültigkeit, wenn in einem Netzwerk des Kunden im Meraki Dashboard nicht die Option „EU-Cloud" aktiviert ist.

Die Sprache dieser EZD ist Englisch; Übersetzungen werden nur zu Verständniszwecken zur Verfügung gestellt; im Zweifel hat die englischsprachige Version Vorrang.

[*Unterschriftenseite folgt*]