

## CISCO MERAKI ERGÄNZUNG ZUR DATENVERARBEITUNG NACH EU-VORSCHRIFTEN

Diese Ergänzung zur Datenverarbeitung nach EU-Vorschriften (nachfolgend die „**EZD**“) ist Bestandteil der zusätzlichen Endbenutzer-Lizenzvereinbarung (nachfolgend die „**Vereinbarung**“) zwischen Ihnen (nachfolgend der „**Kunde**“) und Cisco Systems, Inc., dem Mutterkonzern von 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 sind die Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Verarbeiter wie in Abschnitt 9 unten beschrieben. Verweise im Text der EZD auf eine bestimmte „Klausel“ beziehen sich auf Bestimmungen in den Standardvertragsklauseln.

### INKRAFTSETZUNG DIESER EZD:

1. Laden Sie zur Inkraftsetzung die EZD herunter, füllen Sie die Formularfelder aus, unterzeichnen Sie das Dokument, und senden Sie es per E-Mail an [legal@meraki.com](mailto:legal@meraki.com). Der Kunde erkennt an und stimmt zu, dass eine ausgefüllte und unterzeichnete Kopie dieser Vereinbarung per E-Mail an [legal@meraki.com](mailto:legal@meraki.com) gesendet werden muss, damit die Vereinbarung in Kraft tritt.
2. Nach elektronischer Unterzeichnung durch Ihr Unternehmen und Meraki tritt diese EZD (einschließlich der 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 fungieren Meraki und seine Tochtergesellschaften als Datenverarbeiter.

„**Datenschutzgesetze und -richtlinien**“ bezeichnet alle Gesetze und Richtlinien, die auf die Verarbeitung personenbezogener Daten im Rahmen dieser Vereinbarung anwendbar sind, einschließlich Gesetzen und Richtlinien der Europäischen Union, des Europäischen Wirtschaftsraums, der jeweiligen Mitgliedsstaaten und der Schweiz.

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

„**DSGVO**“ bezeichnet die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

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

„**Personenbezogene Daten**“ bezeichnet gemäß Definition in der DSGVO oder einer entsprechenden Nachfolgeregelung Informationen, die als Teil der Kundendaten an Meraki übertragen werden und die Identität einer lebenden Person preisgeben oder bestimmbar machen.

„**Verarbeitung**“ hat die in der DSGVO definierte Bedeutung.

„**Standardvertragsklauseln**“ bezeichnet die zwischen dem Kunden und Meraki geschlossene Vereinbarung gemäß dem Beschluss der Europäischen Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern, die kein angemessenes Datenschutzniveau gewährleisten. Sie ist als Anlage 1 Teil dieser EZD.

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

„**Technische und organisatorische Maßnahmen**“ bezeichnet die unter [https://meraki.cisco.com/lib/pdf/eu\\_technical\\_organizational\\_measures.pdf](https://meraki.cisco.com/lib/pdf/eu_technical_organizational_measures.pdf) beschriebenen Kontrollmaßnahmen, Prozesse und Verfahren in Bezug auf die Maßnahmen von Meraki zur Gewährleistung von Privatsphäre und Datenschutz, einschließlich gelegentlicher Aktualisierungen.

## 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 Korrektheit, Qualität und Rechtmäßigkeit personenbezogener Daten sowie der Mittel zur Beschaffung personenbezogener Daten durch den Kunden, einschließlich der Verantwortung für die Versendung erforderlicher Benachrichtigungen an seine Netzwerkbenutzer und für die Einholung erforderlicher Zustimmungen von seinen Netzwerkbenutzern.

**2.2 Verarbeitung personenbezogener Daten durch Meraki.** Wir werden Kundendaten in Ihrem Namen verarbeiten und verwenden und das ausschließlich im gesetzlich erforderlichen Umfang und ausschließlich entsprechend Ihren Anweisungen (einschließlich per E-Mail übermittelter Anweisungen), sofern diese Anweisungen den Bedingungen dieser Vereinbarung genügen. 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. Meraki wird dem Kunden in angemessenem Umfang und unter Berücksichtigung der Art der Verarbeitung und der Art der Meraki zur Verfügung gestellten Daten alle Informationen und jede Unterstützung zukommen lassen, die der Kunde vernünftigerweise zur Erfüllung seiner aus der DSGVO entstehenden Pflichten zur Durchführung einer Datenschutz-Folgenabschätzung (gemäß DSGVO-Definition) benötigt.

**2.3 Produktkonfiguration.** Der Kunde verpflichtet sich, die Option „EU-Cloud“ in seinem Meraki Dashboard für seine Netzwerke dauerhaft zu aktivieren. Der Konfigurationsleitfaden für die Meraki Option „EU-Cloud“ ist [https://documentation.meraki.com/zGeneral\\_Administration/Privacy\\_and\\_Security/EU\\_Cloud\\_Configuration\\_Guide](https://documentation.meraki.com/zGeneral_Administration/Privacy_and_Security/EU_Cloud_Configuration_Guide) verfügbar unter [https://documentation.meraki.com/zGeneral\\_Administration/Privacy\\_and\\_Security/EU\\_Cloud\\_Configuration\\_Guide](https://documentation.meraki.com/zGeneral_Administration/Privacy_and_Security/EU_Cloud_Configuration_Guide). 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.

**2.4 Details zur Verarbeitung.** Meraki verarbeitet Kundendaten, um Ihnen Produkte gemäß der Vereinbarung bereitstellen zu können. Art und Umfang der Verarbeitung, die Arten von personenbezogenen Daten und die Kategorien von Datensubjekten, die von der Verarbeitung im Rahmen dieser EZD betroffen sind, werden in Anlage 1 dieser EZD aufgeführt.

## 3. RECHTE VON DATENSUBJEKTEN

- 3.1 Löschung personenbezogener Daten.** Der Kunde hat im Meraki Dashboard die Möglichkeit, gemäß eventuell geltender 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 benachrichtigen, wenn ein Datensubjekt Zugriff auf seine personenbezogenen Daten, die Korrektur, Übertragung oder Löschung seiner personenbezogenen Daten oder eine Einschränkung der Verarbeitung seiner personenbezogenen Daten beantragt. Außer wo gesetzlich vorgeschrieben wird Meraki auf solche Anfragen von Datensubjekten nicht ohne vorherige schriftliche Zustimmung des Kunden reagieren. Ausgenommen hiervon ist eine Reaktion zur Bestätigung, dass sich die Anfrage auf den Kunden bezieht, und zum Verweis des Datensubjekts an den Kunden. Meraki wird den Kunden unter Berücksichtigung der Art der Verarbeitung in vernünftigem und angemessenem Rahmen und im gesetzlich zulässigen Umfang mit technischen und organisatorischen Maßnahmen bei der Beantwortung von Datensubjektanfragen unterstützen, sofern die Beantwortung einer gegebenen Datensubjektanfrage laut Gesetz erforderlich ist. Die Kosten für eine solche Unterstützung durch Meraki obliegen dem Kunden, im gesetzlich zulässigen Umfang und abgesehen von im Rahmen der gewöhnlichen Betriebsabläufe und Betriebsausgaben anfallenden Kosten.

#### **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 erträgliche Schritte unternehmen, um die Zuverlässigkeit aller mit der Verarbeitung personenbezogener Daten betrauten Meraki Mitarbeiter zu gewährleisten. Diese Schritte umfassen unter anderem eine Leumundsprüfung aller neuen Mitarbeiter im gesetzlich zulässigen Rahmen, unter Einhaltung aller geltenden Gesetze und der Richtlinien von Meraki.
- 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 Beauftragter für Datenschutz und Privatsphäre.** Meraki hat einen Beauftragten für Datenschutz und Privatsphäre ernannt. Die Kontaktdaten des ernannten Beauftragten gibt Meraki auf Anfrage an [privacy@cisco.com](mailto:privacy@cisco.com) heraus.

#### **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 oder seine Tochtergesellschaften werden personenbezogene Daten nur an solche Unterauftragsverarbeiter übermitteln, die Vertragspartei einer schriftlichen Vereinbarung mit Meraki oder der jeweiligen Tochtergesellschaft sind, und nur dann, wenn die in der betreffenden Vereinbarung definierten Verpflichtungen hinsichtlich des Schutzes von Kundendaten im Rahmen der durch den Unterauftragsverarbeiter durchgeführten Verarbeitung nicht weniger streng sind als die in dieser EZD definierten Verpflichtungen.
- 5.2 Aktuelle Unterauftragsverarbeiter, Benachrichtigung über neue Unterauftragsverarbeiter.** Meraki wird dem Kunden unter [www.meraki.cisco.com/trust#subprocessors](http://www.meraki.cisco.com/trust#subprocessors) eine Liste der aktuellen Unterauftragsverarbeiter für die Produkte zur Verfügung stellen. Diese Liste wird von Zeit zu Zeit aktualisiert. Meraki wird im Dashboard-Konto des Kunden einen Hinweis (die „**Dashboard-Benachrichtigung**“) veröffentlichen, bevor im Rahmen der Produktbereitstellung neue Unterauftragsverarbeiter autorisiert werden. Wenn der Kunde Einwände gegen den Einsatz eines neuen Unterauftragsverarbeiters durch Meraki hat, kann der Kunde seine Lizenzen für gehostete Software

kündigen. Dies gilt nur für Lizenzen für Produkte, die Meraki nicht ohne Einsatz des neuen Unterauftragsverarbeiters („**Neuer Unterauftragsverarbeiter**“) bereitstellen kann, gegen den der Kunde Einwände hat. Die Kündigung muss schriftlich gegenüber Meraki ausgesprochen werden, innerhalb einer vernünftigen Frist ab Veröffentlichung der Dashboard-Benachrichtigung. Diese Frist darf dreißig (30) Tage nicht überschreiten (die „**Kündigungsfrist**“). Dies gilt, sofern Meraki die Inanspruchnahme des neuen Unterauftragsverarbeiters nicht während oder nach der Kündigungsfrist untersagt wird.

- 5.3 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 die in der vorliegenden Vereinbarung definierten technischen und organisatorischen Maßnahmen implementiert und werden diese beibehalten. Meraki überwacht regelmäßig die Einhaltung dieser Sicherheitsmaßnahmen und wird während der Laufzeit der Vereinbarung angemessene Sicherheitsmaßnahmen vorhalten.
- 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 stellt Meraki unter Beachtung der geltenden Vertraulichkeitspflichten eine Kopie seiner zu diesem Zeitpunkt neuesten Prüfungen oder Zertifizierungen durch Dritte („**Prüfberichte**“) zur Verfügung, sofern verfügbar, oder entsprechende Zusammenfassungen, wie sie Meraki seinen Kunden allgemein zur Verfügung stellt. Zwischen Aufforderungen dieser Art sind vernünftige Zeitabstände einzuhalten.

## **7. MANAGEMENT VON SICHERHEITSLÜCKEN**

Meraki verpflichtet sich, Richtlinien und Verfahren zum Management von Sicherheitsvorfällen vorzuhalten, einschließlich detaillierter Eskalationsverfahren für Sicherheitsvorfälle. Falls Meraki Kenntnis erlangt von einer widerrechtlichen Zerstörung, einem widerrechtlichen Verlust, einer widerrechtlichen Änderung oder einer unbefugten Offenlegung von Kundendaten (einem „**Sicherheitsvorfall**“), 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. Die Verpflichtungen in Abschnitt 7 gelten nicht für Sicherheitsvorfälle, die durch den Kunden oder durch die Netzwerkbenutzer des Kunden verursacht werden.

## **8. RÜCKGABE UND LÖSCHUNG VON KUNDENDATEN**

Bei Beendigung der Vereinbarung wird Meraki auf schriftliche Anfrage des Kunden und innerhalb eines angemessenen Zeitraums: (i) dem Kunden alle personenbezogenen Daten zur Verfügung stellen oder (ii) die Kundendaten einschließlich personenbezogener Daten löschen, ihre Verarbeitung einschränken und/oder sie anonymisieren, auf solche Art und Weise, dass weder der Kunde noch Dritte auf die Daten zugreifen können oder Identitäten aus ihnen herleiten können. Meraki wird auf eine solche Anfrage so schnell wie praktisch durchführbar reagieren, es sei denn, eine solche Rückgabe, Löschung, Verarbeitungseinschränkung oder Anonymisierung ist nicht durchführbar oder eine weitere Aufbewahrung und Verarbeitung ist laut geltendem Gesetz erforderlich oder zulässig.

## **9. ÜBERTRAGUNG PERSONENBEZOGENER DATEN AUSSERHALB DER EU**

- 9.1 Übertragungsmechanismen.** Gemäß den Bedingungen dieser EZD stellt Meraki die nachfolgend aufgeführten Übertragungsmechanismen zur Verfügung. Sie gelten in der nachstehend definierten Reihenfolge und ausschließlich für personenbezogene Daten, die aus der Europäischen Union, dem Europäischen Wirtschaftsraum (EWR) und/oder den jeweiligen Mitgliedstaaten oder aus der Schweiz unmittelbar oder per Weiterübermittlung in Länder übertragen werden, die kein angemessenes Datenschutzniveau gemäß den Datenschutzgesetzen und -richtlinien gewährleisten, und nur insofern die Übermittlung den Datenschutzgesetzen und -richtlinien unterliegt:

- 9.1.1 EU-US-Datenschutzschild und Schweiz-US-Datenschutzschild.** Meraki (als von der Cisco Systems, Inc.

Zertifizierung abgedeckte juristische Person) wird seine Selbstzertifizierung unter dem vom US-amerikanischen Handelsministerium regulierten EU-US-Datenschutzschild und Schweiz-US-Datenschutzschild bzw. etwaigen Nachfolgevereinbarungen aufrechterhalten und seine Konformität mit den darin formulierten Bedingungen für die Übermittlung personenbezogener Daten aus dem Europäischen Wirtschaftsraum und/oder der Schweiz in die Vereinigten Staaten von Amerika gewährleisten.

**9.1.2 Standardvertragsklauseln.** Der Kunde und Meraki haben die Möglichkeit, zusätzlich Standardvertragsklauseln gemäß den Bedingungen in Abschnitt 9.2 zu vereinbaren. 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 Zusätzliche Bedingungen für die Standardvertragsklauseln**

**9.2.1 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. Meraki verarbeitet die personenbezogenen Daten ausschließlich zum Zweck der Bereitstellung der Produkte für den Kunden, des Managements der Kundenbeziehung, der Verbesserung der Produkte und der Einhaltung der geltenden Gesetze.

**9.2.2 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 auf Anfragen im Zusammenhang mit Support-Services und (c) im Rahmen der Nutzung der Netzwerke des Kunden durch die Netzwerkbenutzer des Kunden zu verarbeiten.

**9.2.3 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 gemäß Abschnitt 5.2 dieser EZD im Rahmen der Bereitstellung der Produkte Dritte als Unterauftragsverarbeiter einsetzen können.

**9.2.4 Benachrichtigungen hinsichtlich Unterauftragsverarbeiter.** Meraki stellt dem Kunden nach schriftlicher Aufforderung eine Liste der Unterauftragsverarbeiter gemäß Abschnitt 5.2 dieser EZD zur Verfügung und/oder eine Kopie der Vereinbarung, die mit einem in der Aufforderung des Kunden ausdrücklich genannten Unterauftragsverarbeiter über die Verarbeitung personenbezogener Daten geschlossen wurde. Bei Bedarf kann Meraki vor Aushändigung an den Kunden kaufmännisch sensible oder vertrauliche Informationen aus dieser Vereinbarung entfernen.

**9.2.5 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. Eine weitergehende Prüfung ist nur zulässig, wenn die Unzulänglichkeit der Prüfberichte nachgewiesen werden kann, und darf in keinem Fall mehr als 1-mal jährlich durchgeführt werden. Die Anfrage ist schriftlich zu stellen, mit vernünftiger Vorlaufzeit. Ort, Art und Weise und Umfang werden von den Parteien nach dem Grundsatz von Treu und Glauben vereinbart. Der Umfang beschränkt sich auf die von Meraki eingesetzten Verfahren mit Relevanz für den Schutz personenbezogener Daten. Im Falle einer solchen Prüfung wird der Kunde Meraki im gesetzlich zulässigen Umfang für den entstandenen Zeitaufwand entschädigen, zu den zum jeweiligen Zeitpunkt geltenden Meraki Preisen für Professional Services. Diese werden dem Kunden auf Anfrage zur Verfügung gestellt.

**9.2.6 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 UND BEENDIGUNG**

Um Missverständnisse auszuschließen, wird diese EZD zwischen dem Kunden und Meraki erst rechtsverbindlich, wenn die im vorstehenden Abschnitt „INKRAFTSETZUNG DIESER EZD“ beschriebenen Schritte vollständig durchgeführt wurden. Zur Vermeidung von Zweifeln 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 deutsche Übersetzung dieser EZD wird nur zu Referenzzwecken zur Verfügung gestellt. Im Falle eines Widerspruchs zwischen der deutschen

Übersetzung und der englischen Version der EZD hat die englische Version der EZD Vorrang.

\*\*\*\*\*

**DEUTSCHE ÜBERSETZUNG DER ENGLISCHSPRACHIGEN VERSION DES "CISCO MERAKI EU DATA PROCESSING ADDENDUM (DPA)" AUSSCHLIESSLICH FÜR REFERENZZWECKE, DAHER BITTE NUR DIE ENGLISCHSPRACHIGE VERSION [HIER](#) ZEICHNEN.**

## ANLAGE 1

### Standardvertragsklauseln (Auftragsverarbeiter)

zum Zweck von Artikel 26(2) der Richtlinie 95/46/EG für die Übermittlung personenbezogener Daten in Drittländer, die kein angemessenes Datenschutzniveau gewährleisten

Name des Daten exportierenden Unternehmens: .....

Adresse: .....

Telefon: ..... ; Telefax: ..... ; E-Mail: .....

Weitere Informationen zur Bestimmung des Unternehmens:

.....  
(Datenexporteur)

und

Name des Daten importierenden Unternehmens: Meraki LLC  
Adresse: 500 Terry Francois Blvd., San Francisco, CA 94158, USA  
Telefon: +1 415 432-1000; E-Mail: legal@meraki.com

(Datenimporteur)

jeweils eine „Partei“; zusammen „die Parteien“,

VEREINBAREN die folgenden Vertragsklauseln (die Klauseln) zur Bestimmung angemessener Sicherheitsmaßnahmen in Bezug auf den Schutz der Privatsphäre, der Grundrechte und der Freiheiten von Einzelpersonen für die Übertragung der in Anhang 1 benannten personenbezogenen Daten durch den Datenexporteur an den Datenimporteur.

### § 1

#### Definitionen

Für die Zwecke der Klauseln gelten folgende Begriffsbestimmungen:

- (a) „*Personenbezogene Daten*“, „*besondere Kategorien personenbezogener Daten*“, „*Verarbeitung*“, „*für die Verarbeitung Verantwortlicher*“, „*Auftragsverarbeiter*“, „*Datensubjekt*“ (betroffene Person) und „*Kontrollstelle*“ haben die gleiche Bedeutung wie in der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.
- (b) „*Datenexporteur*“ bezeichnet den für die Verarbeitung Verantwortlichen, der die personenbezogenen Daten überträgt.
- (c) „*Datenimporteur*“ bezeichnet den Auftragsverarbeiter, der dem Erhalt der personenbezogenen Daten vom Datenexporteur zur Verarbeitung in dessen Auftrag nach der Übertragung gemäß dessen Anweisungen und den Bestimmungen der Klauseln zustimmt und nicht dem System eines Drittlandes zur Gewährleistung eines angemessenen Schutzniveaus im Sinne von Artikel 25(1) der Richtlinie 95/46/EG unterliegt.
- (d) „*Unterauftragsverarbeiter*“ bezeichnet jeden vom Datenimporteur oder von einem anderen Unterauftragsverarbeiter des Datenimporteurs beauftragten Auftragsverarbeiter, der dem Erhalt der personenbezogenen Daten vom Datenimporteur oder jedem anderen Unterauftragsverarbeiter des Datenimporteurs ausschließlich zu Verarbeitungszwecken im Auftrag des Datenexporteurs nach der Übertragung gemäß dessen Anweisungen sowie den Bestimmungen der Klauseln und des schriftlichen Nebenvertrags zustimmt.

- (e) „Geltendes Datenschutzgesetz“ bezeichnet das Gesetz, das die Grundrechte und die Grundfreiheiten von natürlichen Personen und insbesondere deren Recht auf Privatsphäre in Bezug auf die Verarbeitung personenbezogener Daten schützt und auf einen für die Datenverarbeitung Verantwortlichen in dem Mitgliedsstaat anwendbar ist, in dem der Datenexporteur seinen Sitz hat.
- (f) „Technische und organisatorische Sicherheitsmaßnahmen“ bezeichnen Maßnahmen zum Schutz personenbezogener Daten vor versehentlicher oder rechtswidriger Vernichtung oder versehentlichem Verlust, versehentlicher Änderung, unbefugter Offenlegung oder unbefugtem Zugriff, insbesondere bei der Übertragung von Daten über ein Netzwerk zum Zwecke der Verarbeitung, sowie vor allen anderen rechtswidrigen Formen der Verarbeitung.

## § 2

### **Details der Übertragung**

Die Details der Übertragung und insbesondere die besonderen Kategorien personenbezogener Daten, soweit zutreffend, werden in Anhang 1 als wesentlichem Bestandteil der Klauseln benannt.

## § 3

### **Drittbegünstigtenklausel**

1. Das Datensubjekt kann gegenüber dem Datenexporteur diese Klausel sowie § 4(b) bis (i), § 5(a) bis (e) und (g) bis (j), § 6(1) und (2), § 7, § 8(2) und §§ 9 bis 12 als Drittbegünstigter durchsetzen.
2. Das Datensubjekt kann gegenüber dem Datenimporteur diese Klausel sowie § 5(a) bis (e) und (g), § 6, § 7, § 8(2) und §§ 9 bis 12 in solchen Fällen durchsetzen, in denen der Datenexporteur faktisch oder rechtlich nicht mehr besteht, es sei denn, eine Nachfolgekörperschaft hat kraft Vertrags oder kraft Gesetzes die gesamten Rechtspflichten des Datenexporteurs und damit die Rechte und Pflichten des Datenexporteurs übernommen. In diesem Fall kann das Datensubjekt die oben genannten Klauseln gegenüber der Nachfolgekörperschaft durchsetzen.
3. Das Datensubjekt kann gegenüber dem Unterauftragsverarbeiter diese Klausel sowie § 5(a) bis (e) und (g), § 6, § 7, § 8(2) und §§ 9 bis 12 in solchen Fällen durchsetzen, in denen sowohl der Datenexporteur als auch der Datenimporteur faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sind, es sei denn, eine Nachfolgekörperschaft hat kraft Vertrags oder kraft Gesetzes die gesamten Rechtspflichten des Datenexporteurs und damit die Rechte und Pflichten des Datenexporteurs übernommen. In diesem Fall kann das Datensubjekt die oben genannten Klauseln gegenüber der Nachfolgekörperschaft durchsetzen. Diese Haftpflicht des Unterauftragsverarbeiters ist auf dessen eigene Verarbeitungsvorgänge gemäß den Klauseln beschränkt.
4. Die Parteien widersprechen nicht einer Vertretung eines Datensubjekts durch eine Organisation oder andere Körperschaft auf dessen ausdrücklichen Wunsch und in Übereinstimmung mit nationalem Recht.

## § 4

### **Pflichten des Datenexporteurs**

Der Datenexporteur stimmt zu und gewährleistet,

- (a) dass die Verarbeitung, einschließlich der Übertragung, der personenbezogenen Daten gemäß den entsprechenden Bestimmungen des geltenden Datenschutzgesetzes erfolgt ist und weiterhin erfolgen wird (und sofern zutreffend den zuständigen Behörden des Mitgliedsstaats des Datenexporteurs gemeldet wurde) und nicht gegen die entsprechenden Bestimmungen dieses Staates verstößt.
- (b) dass er den Datenimporteur angewiesen hat und während der Dauer der Verarbeitung der personenbezogenen Daten weiterhin anweisen wird, die übertragenen personenbezogenen Daten ausschließlich im Auftrag des Datenexporteurs und gemäß geltenden Datenschutzgesetzen und den Klauseln zu verarbeiten.
- (c) dass der Datenimporteur hinreichende Garantien hinsichtlich der in Anhang 2 dieses Vertrags benannten technischen und organisatorischen Sicherheitsmaßnahmen leisten wird.



- (d) dass nach Bewertung der Anforderungen des geltenden Datenschutzgesetzes die Sicherheitsmaßnahmen zum Schutz personenbezogener Daten vor versehentlicher oder rechtswidriger Vernichtung oder versehentlichem Verlust, versehentlicher Änderung, unbefugter Offenlegung oder unbefugtem Zugriff, insbesondere bei der Übertragung von Daten über ein Netzwerk zum Zwecke der Verarbeitung, sowie vor allen anderen rechtswidrigen Formen der Verarbeitung angemessen sind, und dass diese Maßnahmen in Bezug auf den Stand der Technik und die Kosten ihrer Implementierung ein angemessenes Sicherheitsniveau gegenüber den von der Verarbeitung und der Art der zu schützenden Daten ausgehenden Risiken gewährleisten.
- (e) dass er die Einhaltung der Sicherheitsmaßnahmen gewährleistet.
- (f) dass bei einer Übertragung von Daten besonderer Kategorien das Datensubjekt darüber informiert wurde oder vor oder sobald möglich nach der Übertragung darüber informiert wird, dass die Daten möglicherweise in ein Drittland übertragen werden, das kein angemessenes Schutzniveau im Sinne der Richtlinie 95/46/EG gewährleistet.
- (g) dass er jegliche vom Datenimporteur oder von einem Unterauftragsverarbeiter gemäß § 5(b) und § 8(3) erhaltene Benachrichtigung an die Datenschutzkontrollstelle weiterleitet, wenn der Datenexporteur die Übertragung fortsetzt oder die Aussetzung aufhebt.
- (h) dass er den Datensubjekten auf Anfrage eine Kopie der Klauseln mit Ausnahme von Anhang 2 zur Verfügung stellt sowie eine zusammenfassende Beschreibung der Sicherheitsmaßnahmen und eine Kopie jedes Vertrags zur Unterauftragsverarbeitung, der gemäß den Klauseln erstellt werden muss, es sei denn, die Klauseln oder der Vertrag enthalten kaufmännische Informationen. Diese können entfernt werden.
- (i) dass bei einer Unterauftragsverarbeitung die Verarbeitung gemäß § 11 durch einen Unterauftragsverarbeiter erfolgt, der mindestens dasselbe Datenschutzniveau für die personenbezogenen Daten und die Rechte des Datensubjekts gewährleistet wie der Datenimporteur gemäß den Klauseln.
- (e) dass er die Einhaltung von § 4(a) bis (i) gewährleistet.

## § 5

### ***Pflichten des Datenimporteurs***

Der Datenimporteur stimmt zu und gewährleistet,

- (a) dass er die Daten ausschließlich im Auftrag des Datenexporteurs und gemäß dessen Anweisungen und den Klauseln verarbeitet und dass er sich bei Nichteinhaltung der Anweisungen oder der Klauseln ungeachtet des Grundes verpflichtet, den Datenexporteur unverzüglich darüber zu informieren. In einem solchen Fall ist der Datenexporteur zur Aussetzung der Datenübertragung und/oder zur Auflösung des Vertrags berechtigt.
- (b) dass er keinen Grund zu der Annahme hat, dass das auf ihn anwendbare Gesetz der Befolgung der vom Datenexporteur erhaltenen Anweisungen und der Erfüllung seiner Pflichten gemäß dem Vertrag entgegensteht und dass er im Falle einer Änderung dieses Gesetzes, die sich mit hoher Wahrscheinlichkeit nachteilig auf die in den Klauseln benannten Garantien und Pflichten auswirkt, den Datenexporteur nach Kenntniserlangung unverzüglich über diese Änderung benachrichtigt. In einem solchen Fall ist der Datenexporteur zur Aussetzung der Datenübertragung und/oder zur Auflösung des Vertrags berechtigt.
- (c) dass er vor der Verarbeitung der übertragenen personenbezogenen Daten die in Anhang 2 benannten technischen und organisatorischen Sicherheitsmaßnahmen implementiert hat.
- (d) dass er den Datenexporteur unverzüglich benachrichtigen wird über:
  - (i) jede rechtsverbindliche Aufforderung zur Offenlegung der personenbezogenen Daten durch eine Vollzugsbehörde, sofern nicht anderweitig untersagt, etwa durch ein strafrechtliches Verbot zum Schutz der Vertraulichkeit einer Vollzugsuntersuchung
  - (ii) jeden versehentlichen oder unbefugten Zugriff
  - (iii) jede direkt von Datensubjekten erhaltene Anfrage (ohne auf diese Anfrage zu reagieren, sofern nicht anderweitig dazu autorisiert)
- (e) dass er alle Anfragen des Datenexporteurs in Bezug auf die Verarbeitung der übertragenen personenbezogenen Daten unverzüglich und ordnungsgemäß beantwortet und die Hinweise der Kontrollstelle in Bezug auf die Verarbeitung der übertragenen Daten befolgt.
- (f) dass er auf Aufforderung des Datenexporteurs seine Einrichtungen zur Datenverarbeitung einer Prüfung der Verarbeitungsvorgänge gemäß den Klauseln durch den Datenexporteur oder eine Prüfstelle unterzieht, deren

unabhängige Mitglieder mit erforderlichen Berufsqualifikationen und Verschwiegenheitsverpflichtung sofern zutreffend in Absprache mit der Kontrollstelle durch den Datenexporteur zu benennen sind.

- (g) dass er dem Datensubjekt auf Anfrage eine Kopie der Klauseln oder eines Vertrags für die Unterauftragsverarbeitung zur Verfügung stellt, es sei denn, die Klauseln oder der Vertrag enthalten kaufmännische Informationen (die in diesem Fall entfernt werden können), mit Ausnahme von Anhang 2, der durch eine zusammenfassende Beschreibung der Sicherheitsmaßnahmen zu ersetzen ist, sofern dem Datensubjekt vom Datenexporteur keine Kopie zur Verfügung gestellt werden kann.
- (h) dass er vor einer Unterauftragsverarbeitung den Datenexporteur informiert und dessen schriftliche Genehmigung einholt.
- (i) dass die Verarbeitung durch den Unterauftragsverarbeiter gemäß § 11 erfolgt.
- (j) dass er dem Datenexporteur unverzüglich eine Kopie jeder mit einem Unterauftragsverarbeiter abgeschlossenen Vereinbarung zur Verfügung stellt.

## § 6

### **Haftung**

1. Die Parteien vereinbaren, dass ein Datensubjekt, das aufgrund einer Verletzung der in § 3 oder § 11 benannten Pflichten durch eine Partei oder einen Unterauftragsverarbeiter einen Schaden erlitten hat, zum Erhalt einer Entschädigung vom Datenexporteur berechtigt ist.
2. Kann ein Datensubjekt eine Entschädigung gemäß Abs. 1 aufgrund einer Verletzung einer in § 3 oder § 11 benannten Pflicht durch den Datenimporteur oder dessen Unterauftragsverarbeiter vom Datenexporteur nicht einfordern, weil der Datenexporteur faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist, so stimmt der Datenimporteur zu, dass das Datensubjekt eine Forderung gegen den Datenimporteur anstelle des Datenexporteurs richten kann, es sei denn, eine Nachfolgekörperschaft hat kraft Vertrags oder kraft Gesetzes die gesamten Rechtspflichten des Datenexporteurs übernommen. In diesem Fall kann das Datensubjekt seine Rechte gegenüber der Nachfolgekörperschaft durchsetzen.

Der Datenimporteur darf sich nicht auf eine Pflichtverletzung durch einen Unterauftragsverarbeiter verlassen, um seiner eigenen Haftung zu entgehen.

3. Kann ein Datensubjekt eine Entschädigung gemäß Abs. 1 und 2 aufgrund einer Verletzung einer in § 3 oder § 11 benannten Pflicht durch den Unterauftragsverarbeiter vom Datenexporteur oder Datenimporteur nicht einfordern, weil sowohl der Datenexporteur als auch der Datenimporteur faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sind, so stimmt der Unterauftragsverarbeiter zu, dass das Datensubjekt eine Forderung gegen den Unterauftragsverarbeiter in Bezug auf dessen eigene Verarbeitungsvorgänge gemäß den Klauseln anstelle des Datenexporteurs oder des Datenimporteurs richten kann, es sei denn, eine Nachfolgekörperschaft hat kraft Vertrags oder kraft Gesetzes die gesamten Rechtspflichten des Datenexporteurs oder des Datenimporteurs übernommen. In diesem Fall kann das Datensubjekt seine Rechte gegenüber der Nachfolgekörperschaft durchsetzen. Die Haftung des Unterauftragsverarbeiters ist auf dessen eigene Verarbeitungsvorgänge gemäß den Klauseln beschränkt.

## § 7

### **Schlichtung und Gerichtsstand**

1. Der Datenimporteur stimmt zu, dass er bei Geltendmachung von Drittbegünstigtenrechten und/oder Einforderung einer Entschädigung gemäß den Klauseln gegen ihn durch ein Datensubjekt die Entscheidung des Datensubjekts akzeptiert,
  - (a) den Rechtsstreit durch eine unabhängige Person oder sofern zutreffend durch die Kontrollstelle schlichten zu lassen.
  - (b) den Rechtsstreit durch die Gerichte im Mitgliedsstaat des Datenexporteurs schlichten zu lassen.
2. Die Parteien vereinbaren, dass die Entscheidung des Datensubjekts nicht dessen verfahrensrechtliche oder materielle Rechte zur Einholung eines Rechtsbehelfs gemäß anderen Bestimmungen nationaler oder internationaler Gesetze beeinträchtigt.

## § 8

### **Zusammenarbeit mit Kontrollstellen**

1. Der Datenexporteur stimmt zu, auf Aufforderung oder sofern nach geltendem Datenschutzgesetz erforderlich eine Kopie dieses Vertrags an die Kontrollstelle zu übermitteln.
2. Die Parteien vereinbaren, dass die Kontrollstelle zur Durchführung einer Prüfung des Datenimporteurs und jedes Unterauftragsverarbeiters mit identischem Umfang und unter identischen Bedingungen wie eine Prüfung des Datenexporteurs gemäß geltendem Datenschutzgesetz berechtigt ist.
3. Der Datenimporteur wird den Datenexporteur umgehend über das Vorhandensein eines auf ihn oder einen Unterauftragsverarbeiter anwendbaren Gesetzes informieren, das der Durchführung einer Prüfung des Datenimporteurs oder eines Unterauftragsverarbeiters gemäß Abs. 2 entgegensteht. In einem solchen Fall ist der Datenexporteur zur Ergreifung der in § 5(b) vorgesehenen Maßnahmen berechtigt.

## § 9

### **Anwendbares Recht**

Die Klauseln unterliegen den Gesetzen des Mitgliedsstaats des Datenexporteurs, nämlich

---

## § 10

### **Veränderungen am Vertrag**

Die Parteien verpflichten sich, die Klauseln nicht abzuwandeln oder zu verändern. Dadurch wird nicht ausgeschlossen, dass die Parteien Klauseln zu geschäftsbezogenen Punkten ergänzen, sofern erforderlich und sofern diese nicht der Klausel widersprechen.

## § 11

### **Unterauftragsverarbeitung**

1. Der Datenimporteur darf keine Verarbeitungsvorgänge im Auftrag des Datenexporteurs gemäß den Klauseln ohne vorherige schriftliche Genehmigung des Datenexporteurs durch Unterauftragsverarbeiter durchführen lassen. Überträgt der Datenimporteur seine Pflichten gemäß den Klauseln mit Genehmigung des Datenexporteurs auf einen Unterauftragsverarbeiter, so hat er hierfür eine schriftliche Vereinbarung mit dem Unterauftragsverarbeiter zu schließen, die dem Unterauftragsverarbeiter die identischen Pflichten wie dem Datenimporteur gemäß den Klauseln auferlegt. Kommt der Unterauftragsverarbeiter der Einhaltung seiner Datenschutzverpflichtungen gemäß dieser schriftlichen Vereinbarung nicht nach, so ist der Datenimporteur für die Einhaltung der Verpflichtungen des Unterauftragsverarbeiters gemäß dieser Vereinbarung gegenüber dem Datenexporteur vollständig haftbar.
  2. Die schriftliche Vereinbarung zwischen dem Datenimporteur und dem Unterauftragsverarbeiter hat außerdem eine Drittbegünstigtenklausel gemäß § 3 für solche Fälle zu enthalten, in denen das Datensubjekt eine Entschädigung gemäß § 6 Abs. 1 vom Datenexporteur oder Datenimporteur nicht einfordern kann, weil diese faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sind und keine Nachfolgekörperschaft kraft Vertrags oder kraft Gesetzes die gesamten Rechtspflichten des Datenexporteurs oder des Datenimporteurs übernommen hat. Diese Haftpflicht des Unterauftragsverarbeiters ist auf dessen eigene Verarbeitungsvorgänge gemäß den Klauseln beschränkt.
  3. Die Bestimmungen bezüglich Datenschutzaspekte für die in Abs. 1 benannte Unterauftragsverarbeitung des Vertrags unterliegen den Gesetzen des Mitgliedsstaats des Datenexporteurs, nämlich
- 
4. Der Datenexporteur hat eine Liste der gemäß den Klauseln geschlossenen und vom Datenimporteur gemäß § 5(j) gemeldeten Vereinbarungen für die Unterauftragsverarbeitung zu führen und mindestens einmal jährlich zu aktualisieren. Diese Liste ist der Datenschutzkontrollstelle des Datenexporteurs zur Verfügung zu stellen.

***Pflichten nach Beendigung der Verarbeitung personenbezogener Daten***

1. Die Parteien vereinbaren, dass nach Beendigung der Datenverarbeitung der Datenimporteur und der Unterauftragsverarbeiter nach Wahl des Datenexporteurs alle übertragenen personenbezogenen Daten sowie Kopien davon an den Datenexporteur zurückgeben sowie alle personenbezogenen Daten zerstören und dies gegenüber dem Datenexporteur bestätigen, es sei denn, auf den Datenimporteur anwendbare Gesetze stehen der vollständigen oder teilweisen Rückgabe oder Zerstörung der übertragenen personenbezogenen Daten entgegen. In diesem Fall gewährleistet der Datenimporteur, dass er die Vertraulichkeit der übertragenen personenbezogenen Daten garantiert und die übertragenen personenbezogenen Daten nicht weiter aktiv verarbeiten wird.
2. Der Datenimporteur und der Unterauftragsverarbeiter gewährleisten, dass sie auf Aufforderung des Datenexporteurs und/oder der Kontrollstelle ihre Einrichtungen zur Datenverarbeitung einer Prüfung der in Abs. 1 benannten Maßnahmen unterziehen.

## ANHANG 1 ZU DEN STANDARDVERTRAGSKLAUSELN

Dieser Anhang ist Teil der Klauseln und von den Parteien zu vervollständigen und zu unterzeichnen.

Die Mitgliedsstaaten können gemäß ihren nationalen Verfahren weitere erforderliche Informationen bestimmen, die in diesem Anhang aufzunehmen sind.

### Datenexporteur

Datenexporteur ist (bitte kurz die für die Übertragung relevanten Aktivitäten angeben):

### Datenimporteur

Datenimporteur ist (bitte kurz die für die Übertragung relevanten Aktivitäten angeben):

*Meraki LLC, eine Gesellschaft mit beschränkter Haftung nach Recht des US-Staates Delaware. Meraki bietet seinen Kunden Software-as-a-Service (SaaS) zur Verwaltung ihrer Netzwerkhardware, die sie an ihren Standorten bereitstellen. Im Rahmen der Bereitstellung der SaaS-Oberfläche verarbeitet Meraki Netzwerkprotokollinformationen, einschließlich einer begrenzten Anzahl personenbezogener Daten.*

### Datensubjekte

Die übertragenen personenbezogenen Daten betreffen die folgenden Kategorien von Datensubjekten (bitte angeben):

*Einzelbenutzer eines lokalen Netzwerks (LAN), das ganz oder teilweise durch die Verwendung der vom Datenexporteur erworbenen Meraki Produkte erstellt wurde*

### Datenkategorien

Die übertragenen personenbezogenen Daten betreffen die folgenden Kategorien von Daten (bitte angeben):

- *MAC-Adresse (alle Produkte)*
- *MAC-Adresse mit Benutzernamen (Dashboard, MR-Produkte, MX-Produkte, SM-Produkt)*
- *MAC-Adresse mit IP-Adresse (MR-Produkte, MX-Produkte)*
- *MAC-Adresse mit RSSI (Received Signal Strength Indicator) (MR-Produkte)*
- *MAC-Adresse mit URL (MX-Produkte)*
- *MAC-Adresse mit Durchwahlnummer (DID) (MR-Produkte)*
- *IP-Adresse (alle Produkte)*
- *E-Mail-Adresse mit IP-Adresse (Dashboard)*
- *E-Mail-Adresse (Dashboard)*
- *Video (MV-Produkte)*
- *Audio (MV-Produkte)*
- *Audio, DID (MC-Produkte)*
- *DID (MC-Produkte)*
- *DID und Benutzername (MC-Produkte)*
- *Daten-Backups (alle Produkte)*
- *UUID (Universally Unique Identifier) (MR-Produkte, MX-Wireless-Produkte)*
- *Client-Hostname (alle Produkte, Name vom Geräteeigentümer festgelegt)*
- *Active Directory Server-Benutzername, -Passwort und -Gruppen (MC-Produkte und SM-Produkt, Name vom Eigentümer festgelegt)*
- *Azure Active Directory Server-Benutzername und -Passwort (MC-Produkte, Name vom Eigentümer festgelegt)*
- *Verzeichnisinformationen (d. h.: Benutzername) (SM-Produkt, wenn vom Administrator eingegeben)*
- *Benutzerkonteninformationen (d. h.: Benutzername) (SM-Produkt, wenn vom Benutzer eingegeben)*
- *LDAP-Benutzernamen (MI-Produkt)*
- *alle personenbezogenen Daten, auf die der technische Support von Meraki bei der Bereitstellung technischer Support-Services von Standorten außerhalb des EWR aus zugreift*
- *Anmeldeinformationen zur Authentifizierung bei der Anmeldung bei Verwendung bestimmter Benutzerauthentifizierungsmethoden, darunter:*
  - *Authentifizierung über Facebook, SMS oder Google*
  - *von Meraki gehostete Authentifizierung*

- *Im Dashboard kann der Datenexporteur zudem direkt in seinem Dashboard-Konto die Dashboard-Felder konfigurieren, einschließlich der Felder für Unternehmensnamen, Netzwerknamen, Netzwerk-Tags, SSID-Namen, Benutzerauthentifizierungsmethoden und Unternehmensadresse (optional). Datenexporteure, die ein versehentliches Senden personenbezogener Daten an den Datenimporteur vermeiden möchten, sollten bei der Konfiguration ihres Dashboard-Kontos keine personenbezogenen Daten in diese Felder eingeben.*

*Durch Aktivieren der Funktion „EU-Cloud“ auf der Meraki SaaS-Oberfläche können Datenexporteure die Übertragung aller anderen Kategorien personenbezogener Daten an Empfänger außerhalb der EU verhindern.*

### **Besondere Datenkategorien (sofern erforderlich)**

Die übertragenen personenbezogenen Daten betreffen die folgenden besonderen Kategorien von Daten (bitte angeben):

–

### **Verarbeitungsvorgänge**

Die übertragenen personenbezogenen Daten werden den folgenden grundlegenden Verarbeitungsvorgängen unterzogen (bitte angeben):

*Die übermittelten personenbezogenen Daten können die folgenden grundlegenden Verarbeitungsprozesse durchlaufen, gegebenenfalls weitergehend geregelt in vertraglichen Vereinbarungen zwischen Meraki und dem Datenexporteur: (a) Prozesse im Kundenservice, z. B. Bestellabwicklung, Leistung von technischem Support und Verbesserung von Produkten, (b) Prozesse im Vertrieb oder im Marketing im jeweils gesetzlich zulässigen Rahmen, (c) Prozesse im Rahmen der Bereitstellung der Meraki Produkte, einschließlich der als Dashboard bekannten SaaS-Oberfläche, über die der Kunde seine Meraki Netzwerkhardware verwaltet und konfiguriert und (d) interne Geschäftsprozesse und Verwaltungsprozesse, Prozesse zur Betrugsaufdeckung und Betrugsprävention sowie Prozesse zur Einhaltung von behördlichen, gesetzlichen und ordnungspolitischen Vorgaben.*

[Unterschriftenseite folgt]

## ANHANG 2 ZU DEN STANDARDVERTRAGSKLAUSELN

Dieser Anhang ist Teil der Klauseln und von den Parteien zu vervollständigen und zu unterzeichnen.

**Beschreibung der vom Datenimporteur gemäß §§ 4(d) und 5(c) bzw. dem beigefügten Dokument/Gesetzestext implementierten technischen und organisatorischen Sicherheitsmaßnahmen:**

*Der Datenimporteur verpflichtet sich, unter Berücksichtigung sowohl des Standes der Technik als auch der Kosten der Umsetzung, angemessene technische und organisatorische Sicherheitsmaßnahmen zu ergreifen gegen eine unbefugte oder rechtswidrige Verarbeitung der Kundendaten, einschließlich personenbezogener Daten, sowie gegen versehentlichen Verlust oder versehentliche Zerstörung oder Beschädigung der Kundendaten, einschließlich der unter [https://meraki.cisco.com/lib/pdf/eu technical organizational measures.pdf](https://meraki.cisco.com/lib/pdf/eu_technical_organizational_measures.pdf) beschriebenen Maßnahmen sowie deren gelegentlicher Aktualisierungen.*