Für Cisco sind die Sicherheit und das Vertrauen unserer Kunden und Partner von zentraler Bedeutung.

Schutz und Sicherheit der Daten unserer Kunden haben oberste Priorität.

Die Entscheidung des Europäischen Gerichtshofs vom 16. Juli 2020, mit der das EU-US-Datenschutzschild („Privacy Shield“) für ungültig erklärt wurde (sog. Schrems-II-Entscheidung), wirft bei vielen Fragen auf. Auf die Nutzug von Cisco Produkten und Leistungen hat diese aus den folgenden Gründen jedoch geringe Auswirkungen.

Das Privacy Shield war nur einer von mehreren Mechanismen zur rechtskonformen Übermittlung personenbezogener Daten. In der Schrems-II-Entscheidung bestätigt der Europäische Gerichtshof, dass die EU-Standarddatenschutzklauseln weiterhin geeignet für den internationalen Datentransfer sind. Nötig ist ein angemessenes Schutzniveau, das unter anderem auch durch verbindliche interne Datenschutzvorschriften („Binding Corporate Rules - BCRs“) nachgewiesen werden kann.

Schon vor der Schrems-II-Entscheidung beinhaltete die Cisco Datenschutz-Rahmenvereinbarung („Master Data Protection Agreement - MDPA“) die EU-Standarddatenschutzklauseln. Außerdem verfügt Cisco über Binding Corporate Rules als „Verantwortlicher“ (Controller) und hat die Freigabe der Cisco BCRs als „Auftragsverarbeiter“ (Processor) für Fälle, in denen Cisco künftig weitere Dienstleistungen im Auftrag unserer Kunden erbringen, durch die zuständigen europäischen Datenschutzbehörden beantragt.

Das in den EU-Standarddatenschutzklauseln vorgesehene und somit angemessene Schutzniveau gewährleistet Cisco folgendermaßen:

- **Daten in der Region halten**:
  Regionale Datenhaltung innerhalb europäischer Datenzentren ist ein Kernprinzip von Cisco. Für Kunden aus Deutschland werden zum Beispiel bei Cisco Webex Teams kundengenerierte Daten in Amsterdam, London und Frankfurt gehostet. Angesichts des bevorstehenden Austritts des Vereinigten Königreichs aus der EU (BREXIT) ist ein Ausbau der Cisco Rechenzentrumsstandorte in Europa in der Planung.

- **Rechtssichere Verarbeitung:**
  Personenbezogene Daten werden ausschließlich im Einklang mit den anwendbaren gesetzlichen Vorschriften, insbesondere der Datenschutzgrundverordnung (DSGVO), verarbeitet. Um der aktuellen Datenschutzpraxis Rechnung zu tragen, wird gegenwärtig das Cisco MDPA überarbeitet. Hierbei werden auch aktuelle behördliche Hinweise berücksichtigt.

- **Datensicherheit als Voraussetzung für effektiven Datenschutz und als Mittel gegen unzulässigen Zugriff:**
  Ein Schlüsselprinzip der DSGVO ist die sichere Verarbeitung personenbezogener Daten durch geeignete technische und organisatorische Maßnahmen. Nur eine technisch sichere Umgebung garantiert Vertraulichkeit, Integrität und Verfügbarkeit. Die unternehmensweit einheitliche Umsetzung gewährleistet Cisco mit entsprechenden Datenschutz- und Datensicherheits-Richtlinien (z.B.: Security Vulnerability Policy, BCRs etc.), mit einem branchenführenden Sicherheitsdesign und leading-edge Verschlüsselung. Bei Cisco WebEx Meetings beispielsweise durch die vollständige Übertragung des Schlüsselmanagements auf den Kunden und Ende-zu-Ende-Verschlüsselung. So wird Abfangen und Mitlesen unmöglich. Drittens lässt sich Cisco regelmäßig unabhängig prüfen und zertifizieren. Zu den IT-Sicherheitszertifizierungen gehören ISO 27001, ISO 27017, ISO 27018, SOC 2 und SOC 3, sowie BSI C5 (Cloud Computing Compliance Controls Catalog). Cisco stellt durch Forschung und Entwicklung sicher, dass die technischen Maßnahmen ständig auf höchstem Niveau weiterentwickelt werden (z.B.: Post-Quantum Verschlüsselung).

- **Schutz unserer Kunden bei behördlichen Anfragen und unangemessenen Zugriffgesuchen:**
  Cisco hat ein mehrstufiges Schutzsystem etabliert (sog. Principled Approach to Government Requests for Data). Erster Schutzwall: Das Prinzip der regionalen Datenspeicherung in der Kundenregion . Zweiter Schutzwall: Cisco prüft jede einzelne Behördenanfrage genauestens auf Rechtmäßigkeit und Angemessenheit. Cisco kämpft für seine Kunden mit allen zur Verfügung stehenden Rechtsmitteln. Dazu gehört auch, dass Cisco – wo immer möglich und rechtlich zulässig – behördliche Anfragen eingrenzt und seine Kunden über behördliche Anfragen informiert sowie bei deren Beantwortung einbindet. Dritter Schutzwall: In halbjährlichen Transparenz-Berichten veröffentlicht Cisco sämtliche behördlichen Anfragen. So hat jeder Kunde die Möglichkeit, sich selber ein Bild davon zu machen, wie viele Anfragen eingehen und dass keine personenbezogene Daten aus Deutschland an Behörden in den USA ausgehändigt wurden.

Vertrauen wächst durch Transparenz. Daher stellt Cisco alle erforderlichen Informationen zum Nachweis der Einhaltung der DSGVO Pflichten über das Cisco Trust-Portal (trustportal.cisco.com) sowie über das Cisco Trust-Center trust.cisco.com zur Verfügung.

Weitere aktuelle Informationen hierzu finden Sie auf unserer Webseite oder erfahren Sie über Ihren Cisco Ansprechpartner sowie über das Security & Trust Office Deutschland sto-cisco-germany@external.cisco.com.

Julia O'Shea
DIRECTOR,MGMT-FINANCE

02 October 2020

APPROVED BY LEGAL

Cisco International Limited
9-11 New Square Park
Bedfont Lakes, Feltham
Middlesex, TW14 8HA
United Kingdom