FAQ: International Transfer of Personal Data post-Schrems II and Brexit

At Cisco, fostering relationships with our Customers and Partners based on trust is of utmost importance. We believe that privacy is a fundamental right and our Customers' and Partners' privacy and security are always top priorities.

We understand that the Schrems II judgment of the Court of Justice of the European Union (CJEU) (and the consequent decision of the Switzerland's Federal Data Protection and Information Commissioner) invalidating the Privacy Shield as a transfer mechanism has caused some confusion and might be difficult to navigate. As the European Commission and the US Department of Commerce work through the decision and develop a path forward, we would like to reassure you that we have taken steps to enable the seamless, safe, and legal cross-border transfer of personal data in accordance with EU and Swiss privacy requirements.

Schrems II

1. What is "Schrems II"?

Schrems II is a case before the CJEU brought by the Irish High Court challenging the validity of the Standard Contractual Clauses (SCCs) to provide adequate safeguards in accordance with EU standards.

In its judgment, the CJEU decided on 16 July 2020 that the EU-US Privacy Shield could no longer be used as a personal data transfer mechanism due to concerns over US surveillance law potentially permitting unfettered access to EU personal data by US intelligence agencies. However, in the same ruling, the CJEU reaffirmed the validity of the SCCs as a transfer mechanism, subject to certain conditions. Data exporters (i.e., companies transferring personal data outside of the EU – e.g., Cisco EU Customers), where appropriate with the collaboration of the data importer (e.g., Cisco), will now have the responsibility to verify, on a case-by-case basis, if the law and practices of the non-EU third country provide "essentially equivalent" protection for personal data transferred from the EU. When conducting this analysis, the parties must take into account, among other things, the circumstances of transfer, nature of the data, and the availability of possible additional safeguards (or 'supplementary measures').

On 21 June 2021, the European Data Protection Board (EDPB – a group of national data protection authorities from across the EU) published final guidance on the *Schrems II* decision. The EDPB recommendations outline technical, organizational, and contractual supplementary measures (i.e., in addition to the SCCs or other Article 46 transfer mechanism) which may be combined as appropriate in a particular data processing context to bring the level of protection of data transferred to a 'third country' (outside the EU/EEA) up to the EU standard of essential equivalence.

2. How does the Schrems II decision impact Cisco's Customers and Partners?

Neither Cisco nor our Customers and Partners handle EU personal data that would be of interest to U.S. intelligence agencies (i.e., foreign intelligence important to the national security of the U.S.). We do not engage in data processing or transfers that present the type of risks to privacy and mass surveillance that were of concern to the CJEU in Schrems II (i.e., consumer communications and behaviour). Personal data processed by Cisco does not pose a real risk of overreaching US surveillance and unwarranted intrusion on the "fundamental rights and freedoms" of EU data subjects.

To ensure safe, secure, and legal international data flows, Cisco participates in the APEC Cross Border Privacy Rules system, APEC Privacy Recognition for Processors, Privacy Shield, EU Binding Corporate Rules – Controller (our BCR-Processor application is currently pending), and SCCs. The vast majority of Customers and Partners have executed a Master Data Protection Agreement (MDPA) with Cisco which incorporates SCCs. In response to the Schrems II ruling, we have updated our SCC template to include references to the additional safeguards already put in place by Cisco. Those safeguards are outlined below.

For those who have a MDPA with SCCs in place or will execute new SCCs, i.e. the new set of SCCs published by the European Commission in 2021, there is no further action needed. If you are unsure about whether you have concluded a MDPA with SCCs with us, please reach out to your Cisco representative.

3. What are the SCCs and does Cisco use them?

The European Commission's Standard Contractual Clauses (SCCs) are a contractual terms template that have been pre-approved by the European Commission and serve as a legal transfer mechanism to allow personal data to flow outside of the EU/EEA. SCCs have been used for over a decade to provide contractual safeguards according to EU data protection standards. Cisco has used SCCs for many years for internal intercompany transfers, suppliers, as well as with our Customers and Partners. The SCCs are an integral part of our MDPA, which is required for Cisco suppliers and available to customers, partners, and anyone who does business with Cisco. All Cisco entities (no matter where in the world they are located) that receive, and process EU personal data do so in accordance with EU requirements and standards -- as agreed to in the SCCs and as a matter of mandatory corporate policy (BCR-Controller).

The EU Commission published an updated version of the SCCs on 4th June 2021 to modernize the SCCs, account for sub-processors, and add additional contractual safeguards in response to the *Schrems II* decision.

Cisco will update our MDPA template to include the new SCCs and roll-out for EU/EEA based Customers, Partners, and Suppliers during the transition period which ends 27 December 2022. From 27 September 2021 Cisco will use the new SCCs for new EU/EEA based Customers

4. What are the EDPB's recommendations on supplementary measures and what measures does Cisco provide?

The supplementary measures identified by the EDPB are designed to enable transfer mechanisms (such as the SCCs) to provide "essentially equivalent" protection. The EDPB's recommendations divide supplementary measures into three groups – technical, contractual, and organizational and provide a non-exhaustive list of examples of each. Which supplementary measures are required to provide essentially equivalent level of protection requires a case-by-case analysis and should be designed to ensure EU data protection standards are met and any law enforcement access is "necessary and proportionate".

Cisco's Privacy Data Sheets and Data Maps illustrate – on a per product basis – what personal data we process, how we process it, why, and where the processing is taking place (including in our European data centres). These Privacy Data Sheets and Maps provide customers, partners, and the general public the information necessary to 'know their transfers' and enable the required case-by-case privacy impact assessment and analysis. We are transparent about what data is involved when using Cisco products and services, whether there is an international transfer, and what risks associated with the type of data or processing concerned. Cisco only processes EU personal data in locations where EU data protection standards can be satisfied, and "essentially equivalent" protection can be provided.

1. **Technical measures:** the EDPB provides the following examples of technical measures that should be considered depending on the particular use case and processing activity: encryption at rest and during transit, bring-your-own-key (BYOK) encryption, and pseudonymisation of data.
   - The Cisco Secure Development Lifecycle (CSDL) supports Privacy by Design with a mandatory Privacy Impact Assessment and Privacy Engineering people, processes, and technologies. Cisco product and service offerings, as well as our enterprise processing activities, are assessed for their compliance with our security and privacy policies, standards, and controls which are based on ISO 27701, SOC2, and other internationally recognized industry standards. Several of our offers (e.g., WebEx) have also obtained independent, external certifications to demonstrate adherence to these standards. Security and Privacy by Design focused controls include verification of no embedded backdoors, encryption and key management, as well as minimization of data collection and use, and alignment to personal data purpose and legal basis. Minimization controls include local identifiers and treating de-identified/psuedonymized data as PII. Personal data is encrypted both at rest and in transit and, in some offers, decryption keys can be held and managed by the Customer. These controls apply to both primary storage as well as backup. Assessments occur prior to product launch, annually, and prior to material changes to functionality, personal data, and/or processing environment.
   - The Privacy Data Sheets and Data Maps provide more information on our privacy and security measures on a per offer basis, including the specific choices on encryption and key management mechanisms. For example:

- WebEx Meetings includes an end-to-end encryption option for communications under which the meeting content (i.e., video, audio, text, and files) cannot be deciphered by Cisco.
- Umbrella provides encryption in transit over the public internet between Umbrella data centers using TLS 1.2. For customer's selecting the EU Umbrella data warehouse, data at rest is also encrypted. In addition, Cisco DNS event logs, proxy event logs, and firewall event logs are segregated and stored in Cisco Umbrella in a de-identified manner separate from the underlying user identity data.

- Through investment in research and development, Cisco constantly updates and improves the security posture of our offers. Cisco works with standards and cryptography groups to develop and adopt new security standards as they mature. For more details, please follow this link.

2. **Contractual measures:** the EDPB guidance also called out the need for contractual commitments to provide transparency about processing location, applicable laws, and government demands for data.
   - The new version of the EU Standard Contractual Clauses for transferring personal data to third countries (published on 4 June 2021) contain contractual provisions on notification and handling government data demands in accordance with the expectations of the EDPB. These additions are in line with Cisco's existing practices and we will add the new SCCs to our MDPA .
   - Cisco believes that law enforcement and national security agencies should go directly to our business and government customers to obtain information or data regarding those entities, their employees, and users.
   - Cisco will notify the customer that its data has been requested (so that the customer may attempt to limit or prevent disclosure), unless applicable law prohibits notification. Where appropriate and in order to protect our customer's legitimate interests, Cisco will, through appropriate legal process or other means, challenge requests that prohibit notification to the customer (see our Principled Approach for Government Requests for Data).
   - Cisco has always had a "no backdoor policy". Our product development practices (CSDL) specifically prohibit any intentionally developed capabilities or product features that are designed to allow undisclosed and/or undocumented device or network access, or undisclosed and/or undocumented access to device information and/or services.
   - Cisco does not purposefully create or change its business processes in a manner that facilitates access to personal data or systems without necessary permissions.
3. **Organizational measures:** the EDPB also outlines recommendations for accountability and governance for handling access demands, documenting demands, publishing transparency reports, data minimization measures, and adoption of data privacy and security standards and certifications.
   - Cisco has received very few law enforcement requests for data over the years. Our transparency reports detail numbers of accepted and rejected government demands for data twice a year. The reports further split out US National Security demands – such as FISA orders – into a separate category.

- Our privacy and security certifications demonstrate that we have implemented appropriate controls, including data minimisation and organisational measures designed to limit the personal data processed and protect against unauthorised access.
- Cisco products and program regularly undergoes self-assessments and independent, external testing and certification. Cisco's IT security certifications include ISO 27001, ISO 27017, ISO 27018, SOC 2 and SOC 3, as well as BSI C5 (Cloud Computing Compliance Controls Catalog).

5. Are these safeguards applicable to transfers to other countries than the US?

The CJEU's ruling upheld the validity of EU personal data transfers using SCCs to third countries in general, not just to the US. The Court did not opine on the "essential equivalence" of any other third country laws, rather the data exporter is required to assess whether "essential equivalent" protection can be provided when EU personal data is being imported and processed in any non-EU/EEA country.

While most transfers of personal data out of the EEA will be to the US, some Cisco services, such as Technical Assistance (TAC) Service Delivery, may involve transfers to other third countries. As such, please be assured that the legal, technical, and organizational safeguards as well as transparency measures mentioned above are globally applicable. Cisco complies with all applicable privacy and data protection laws regardless of jurisdiction in which it operates. Further, Cisco secures any data transfers by means of the appropriate transfer mechanism in combination with technical, organizational and contractual measures. Cisco only processes personal data in locations where our policies, standards, and controls for protection can be met.

6. Does Cisco use transfer tools other than the SCCs for EU/EEA Personal Data?

Cisco transfers EU/EEA personal data on the basis of Binding Corporate Rules (BCR-C) when acting as a controller (e.g., human resources data, administrative data, billing information, and customer relationship management).

Binding corporate rules (BCRs) are data protection policies adhered to by companies established in the EU for transfers of personal data outside the EU within a group of undertakings or enterprises. Such rules must include all general data protection principles and enforceable rights to ensure appropriate safeguards for data transfers. They are legally binding and enforced by every member concerned within the group. BCRs require approval by the competent data protection authority in the EU.

BCRs remain a valid transfer mechanism after the *Schrems II* ruling. While they were not explicitly mentioned in the judgement, subsequent guidance from the EDPB suggested that transfers based on any of the Article 46 transfer tools (including BCRs) should be subject to the case-by-case assessment to demonstrate essential equivalence of protection and may require the adoption of supplementary measures as discussed above.

Our Binding Corporate Rules – Controller (BCR-C) have been approved by the European data protection supervisory authorities. This approval demonstrates that Cisco's Data Protection & Privacy Program is aligned with EU requirements, including the GDPR. Cisco's BCR-C set forth the mandatory, minimum standards for handling EU personal data by Cisco, as a data controller. Our approved BCR-C

serve as a legally valid transfer mechanism and commits Cisco to processing EU personal data in accordance with EU data protection standards anywhere that Cisco operates in the world.

In addition, in September 2020, we submitted our application for Binding Corporate Rules – Processor approval. BCR-P sets forth the mandatory and minimum standards for handling EU personal data by Cisco, when Cisco acts as a data processor (e.g., when we provide services on behalf of our customers) and will also serve as an additional legally valid transfer mechanism when approved.

7. Why is Cisco still certified under the Privacy Shield Frameworks and why are they still mentioned in the Cisco Online Privacy Statement?

The US Department of Commerce issued guidance stating the decisions of the CJEU and the consequent opinion of Switzerland's Federal Data Protection and Information Commissioner (FDPIC) do not relieve participants in the EU-US and Swiss-US Privacy Shields of their obligations to adhere to the principles and requirements of the Privacy Shield Frameworks. The US Department of Commerce continues to administer and enforce the Privacy Shield program. While the Privacy Shield is no longer a valid transfer mechanism, continued participation demonstrates Cisco's continued commitment to adhere to the Privacy Shield principles and EU/Swiss standard of care.

8. What is meant by FISA 702 and EO 12333? How do they relate to Schrems II?

Section 702 of the Foreign Intelligence Surveillance Act (FISA 702) is a US statute establishing a judicial process authorizing a specific type of data acquisition (i.e., foreign intelligence for US national security purposes). Under FISA 702, an independent court may authorize the US government to issue orders requiring US companies to disclose communications data relating to specific non-US persons located outside of the US to obtain specific types of foreign intelligence information.

Executive Order 12333 (EO 12333) is a general directive organizing US intelligence activities. Unlike FISA 702, EO 12333 does not authorize the US government to require any company to disclose data, though it may be used to authorize clandestine intelligence activities involving overseas access to data without the involvement of the company in question.

The CJEU ruled that where transfers of personal data to the US are subject to FISA 702 and EO 12333, the Privacy Shield does not provide an essentially equivalent protection, because these provisions allow for government access beyond what is "necessary and proportionate" for legitimate law enforcement purposes.

9. Are the transfers of personal data by Cisco subject to FISA 702 or EO 12333?

Cisco is not directly subject to surveillance requirements under EO 12333 nor voluntarily cooperating with any program authorized by the EO.

Most Cisco offers are also not subject to FISA 702. However, Webex Teams, Meetings, Meraki and other Cisco SaaS offers are considered electronic communication services or remote computing services. Therefore, customer data transferred and processed in connection with these select offers

may, theoretically, be within the scope for a FISA 702 demand – if such data is related to foreign intelligence necessary for national security purposes. Moreover, the numbers of US National Security Demands, including FISA Orders, are included in our transparency report on government demands for data, which we publish twice a year. Please refer to the section 4 for details on the additional safeguards being taken by Cisco.

Brexit

11. How does Brexit affect data flows to and from the UK?

On 24 December 2020, the EU and UK agreed a post-Brexit trade deal, which included an interim provision for EU to UK transfers of personal data. This meant the UK was not deemed a 'third country' and the f**ree flow of personal data between the UK and EU could continue** as it did during the Brexit transition period for a maximum of six months (up to the end of June 2021). The initial 'bridge' was for 4 months, with a further 2 months extension if both parties agreed additional time was required. That temporary arrangement allowed the EU more time to make an adequacy assessment in relation to the UK.

On 28 June 2021 the EU Commission completed its adequacy assessment and adopted the UK adequacy decision which means transfers of personal data can continue without additional measures being in place. Furthermore, in June 2021, we submitted our application to the ICO for UK Binding Corporate Rules – Controller approval.

12. Where do I get more general information on the processing and transfer of Personal Data by Cisco?

We invite you to consult our Trust Center for all our efforts to keep customer data, including personal data secured with privacy properly respected and for all updates in this regard. For specific information, we invite you to contact your Cisco representative.