FAQ: International Transfer of Personal Data post-Schrems II

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 Cisco's top priority.

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) might be difficult to navigate for our Customers and Partners. 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, legal cross-border transfer of personal data in accordance with EU and Swiss privacy requirements.

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 valid personal data transfer mechanism due to concerns over US surveillance law. 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 of the third country provides adequate protection of data transferred under EU data protection law, taking into account the circumstances of transfer and possible additional safeguards, if required.

Further guidance from the European Data Protection Board (EDPB) following the Schrems II decision interprets the ruling as applying in the context of BCRs, meaning the circumstances of transfer should also be assessed. The court's ruling took effect immediately, and the US Department of Commerce and European Commission are currently working on a path forward.

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

Cisco is certified under both the EU-US and Swiss-US Privacy Shield Frameworks, which were designed by the U.S. Department of Commerce, and the European Commission and Swiss Administration, respectively, to provide companies with a mechanism to comply with data protection requirements when transferring personal data from the European Union or Switzerland to the United States.

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 under the Privacy Shield Frameworks as the US Department of Commerce continues to administer the Privacy Shield program (including processing submissions for re-certification to the Privacy Shield Frameworks and maintaining the Privacy Shield List). As such, Cisco continues to meet these obligations regardless of whether the mechanisms are still used to transfer data of EU or Swiss customers.

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

The European Commission's Standard Contractual Clauses (SCCs) are contractual terms that have been pre-approved by the European Commission and serve as a legal basis for personal data transfers outside the EU/EEA. SCCs have been available to companies for over 10 years to provide safeguards according to European standards to personal data outside of the EU/EEA and we have been using them as a data transfer mechanism for several years. They have always been an integral part of our Master Data Protection Agreement (MDPA), which is required for Cisco suppliers and available to customers, to enable safe and legal transfers of personal data outside of the EU. Cisco has also executed an inter company personal data transfer agreement incorporating the SCCs. This agreement obligates Cisco entities outside of the EU/EEA, receiving personal data from Cisco entities located inside the EU/EEA, to process such personal data in accordance with the terms of the SCCs.

4. What are Cisco's Binding Corporate Rules?

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.

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 (e.g. customer relationship management). 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 to this, we are delighted to let you know that our Binding Corporate Rules – Processor (BCR-P) have been submitted for approval to the competent data protection authority in the EU. Like Cisco's BCR-C, the 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 in this respect.

5. Does Schrems II affect Cisco's transfer of personal data to the US and other countries?

We would like to reassure you that we can transfer personal data to the US and other countries on the basis of the SCCs when we act as a processor (i.e., when we provide services on behalf of our customers) and on the basis of our BCR-C when acting as controllers (e.g., human resources data, administrative data, billing information, customer relationship management, etc.).

We will also be able to use our BCR-P, once approved, as a valid transfer mechanism when we act as processors. Furthermore, when the new module of the EU Code of Conduct for the transfer of personal data will be completed and approved, Cisco will also be able to use this as an additional valid transfer mechanism when acting as a processor in the context of Cloud Services.

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

The vast majority of Customers and Partners have concluded SCCs with Cisco. . Therefore, while Customers and Partners should assess the law of countries to which data is transferred, the circumstances of transfer and the additional safeguards put in place by Cisco as outlined below, for those who have concluded SCCs there is no need to change terms of the contract.

If you are unsure about whether you have concluded a MDPA with us, please reach out to your Cisco representative.

7. Where is my data located?

We encourage you to consult our Privacy Data Sheets and Data Maps, which illustrate on a per-offer basis what personal data we process, how we process it and where the data is located (including our European Data Centers). They also outline what additional security measures we have put in place for specific offers that potentially handle more sensitive information (e.g. end-to-end encryption for communication with Webex Meetings).

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. Under FISA 702, an independent court may authorize the US government to issue orders requiring US companies to disclose communications data of 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.

In its decision, the CJEU ruled that where transfers of personal data to the US are subject to FISA 702 and EO 12333 the transfer mechanism used does not provide an essentially equivalent protection as EU law.

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

Webex Teams, Meetings, Meraki and other Cisco SaaS offers are considered electronic communication services or remote computing services. Therefore,transferred customer data in that context may theoretically be within the scope of FISA 702. It is very important to note, however, that communications data (usually targeted by FISA 702) for Webex Teams, Meetings and Meraki are generally stored in the customer's region and not subject to transfer to the US. 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. We are not directly subject to surveillance requirements under EO 12333 nor voluntarily cooperating with any program authorized by the EO. In accordance with the ruling of the Schrems II decision, supplementary measures should be put in place when data is transferred to third countries where essentially equivalent protection is not legally available in order to ensure appropriate safeguards are in place. Please refer to the next answer for details on the additional safeguards being taken by Cisco.

10. Does Cisco provide additional safeguards for transfers to the US that are potentially subject to FISA 702 Orders or EO 12333 authorised programs?

We are currently awaiting guidance from the EDPB on what kind of legal, organisational and technical supplementary measures could be provided post-Schrems II. In the meantime, on top of our holistic approach to privacy and security, we can demonstrate measures we are already taking that limit disproportionate access by government authorities to our Customers' and Partners' data.

Legal measures

On top of complying with the SCCs, we commit to a principle-based review to examine government demands for data and appropriately narrow and challenge requests which are not necessary and proportionate. We will notify our customer (unless such notification is prohibited by law) to give them the opportunity to limit or prevent disclosure. We also challenge requests that prohibit notification to the customer. Please be aware that we will only provide the data to an agency with appropriate authority under applicable law to demand this data from us and we will only provide the specifically requested information or data in certain limited circumstances.

Transparency measures

We publish a Transparency report detailing numbers of government demands detailing numbers of accepted and rejected government demands for data twice a year. This gives every customer the opportunity to see for themselves how many inquiries are received and that no EU personal data has been handed over to authorities in the USA so far.

We also make use of verifications mechanisms such as privacy and data security certifications (including but not limited to ISO 27001, ISO 27017, ISO 27018, SOC 2 Type II and SOC 3). These demonstrate data minimization and organizational security measures that limit the pool of data available for access and protect against unauthorized access.

Technical and organizational measures

In addition to this, our Privacy Data Sheets and Data Privacy Maps outline how, where and by whom personal data is processed across our portfolio of solutions. Our Privacy Data Sheets provide also details on our offer-specific security and organisational measures, including where we encrypt data during transit (safeguarding against access under EO 12333 during transfers to the US) and at rest.

A key priority for Cisco is the secure processing of personal data through appropriate technical and organizational measures. Only a technically secure environment ensures confidentiality, integrity and availability. Cisco ensures uniform implementation throughout the company with appropriate data protection and data security policies (e.g.: Security Vulnerability Policy, BCRs etc.), with an industry-leading security design and leading-edge encryption. Cisco Webex Meetings customers, for example, can opt for true end-to-end encryption (E2EE) of video, audio, text, and meeting content. With E2EE enabled by the administrator, Cisco Webex does not have access to the encryption keys used by meeting hosts and participants and cannot decrypt the data nor media streams. With E2EE, the meeting encryption key is generated by the meeting host and securely distributed to only the meeting participants. This makes interception and reading impossible, also by Cisco itself.

Moreover, Cisco regularly undergoes independent 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). Last but not least, through research and development, Cisco ensures that the technical measures are constantly improved to the highest level (e.g. post-quantum encryption).

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

The Court's ruling upholds the validity of transfers using SCCs to third countries in general, not just to the US. While the Court did not reach conclusions on the essential equivalence of any other third country laws, the same assessments and thresholds for transfer will also apply.

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

12. How will Brexit affect data flows to and from the UK?

The Withdrawal Agreement agreed between the UK and the EU allows for a transition period until the end of 2020. There is no change regarding data flows to and from the UK during this transition period. As of 1st January 2021, the UK will be deemed a third country. The UK government is seeking an adequacy finding from the EU during the transition period.

If the UK and EU do not come to an agreement on data protection during the transition period, the UK will become a third country in the eyes of the EU Commission. In that case, lawful transfer of personal data from the EU to the UK will have to be subject to an approved transfer mechanism that provides appropriate safeguards. The UK government and the UK data protection authority (ICO) have stated they will recognize all 27 EU member states as providing adequate protection for personal data of UK individuals. Therefore, the transfer of personal data of UK individuals to EU member states will be unaffected until the UK Government states otherwise.

If there is no agreement on data protection by the end of the transition period Cisco will enter into the SCCs with EU based customers where the service involves a transfer of their personal data to the UK. This means EU based customers can continue to use a Cisco service where personal data is processed in the UK.

13. 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.