JacksonLewis

Data Protection Commissioner v. Facebook Ireland and Schrems (Schrems II) FAQs

The following FAQs summarize the implications of *Schrems II*.

1. IN *SCHREMS II*, THE COURT OF JUSTICE FOR THE EUROPEAN UNION (CJEU) INVALIDATED THE EU-U.S. PRIVACY SHIELD PROGRAM. IS THE PROGRAM CLOSED?

No. Although the CJEU invalidated the EU-U.S. Privacy Shield as an adequate mechanism for transferring personal data from the EEA to the U.S., the U.S. Department of Commerce will continue operating the program, including accepting company self-certifications and applications for certification, while it works with the EU to address the CJEU decision. While U.S. companies can no longer rely on their EU-U.S. Privacy Shield certification as the lawful basis to transfer or receive EEA personal data, they may wish to keep the certification current in the event it can be leveraged for any future agreement negotiated to replace the EU-U.S. Privacy Shield.

2. HOW SHOULD COMPANIES HANDLE EUROPEAN ECONOMIC AREA (EEA) PERSONAL DATA CURRENTLY IN THE U.S. AS A RESULT OF A TRANSFER UNDER THE EU-U.S. PRIVACY SHIELD?

This EEA personal data is still entitled to the protections of the EU-U.S. Privacy Shield and U.S. companies must continue to comply with their obligations under the program. Notwithstanding, the CJEU opinion states that U.S. companies must destroy or return this personal data to the EEA as a result of the Court's decision. Based on the actions it takes in response to *Schrems II*, a U.S. importer should review and update its privacy policies and statements regarding the collection and transfer of personal data.

3. DOES *SCHREMS II* APPLY TO THE SWISS-U.S. PRIVACY SHIELD?

No. The CJEU decision does not apply to the Swiss-U.S. Privacy Shield. The Swiss data protection authority, the FDPIC, states it "has taken note of the CJEU ruling. This ruling is not directly applicable to Switzerland. The FDPIC will examine the judgement in detail and comment on it in due course."

4. ARE THE CONTROLLER-PROCESSOR STANDARD CONTRACTUAL CLAUSES (SCCS) STILL VALID?

Yes. The controller-processor SCCs are still valid. However, the CJEU noted that a data exporter may need to supplement the SCCs to provide an appropriate level of data protection, particularly where a country's surveillance laws and activities violate applicable EU data privacy laws. The European Commission is expected to publish updated SCCs.

5. WHAT ARE THE DATA EXPORTER'S OBLIGATIONS WHEN USING SCCS?

The data exporter must:

- Conduct due diligence to ensure the data importer can provide an adequate level of protection for EEA personal data;
- Immediately suspend or terminate the transfer upon notification from the data importer that it cannot comply with the terms of the SCCs; and
- Notify the applicable supervisory authority if it does not plan to suspend or terminate the transfer or contract upon notice from the data importer of its inability to comply with the SCCs.

The data exporter should document and retain its determinations and actions.

6. WHAT SHOULD THE DATA EXPORTER'S DUE DILIGENCE INCLUDE?

The data exporter should review and document:

- The type and sensitivity of the personal data being transferred from the EEA;
- The purpose for transferring;
- The processing to occur in the U.S.;
- Existing safeguards, including whether the data is encrypted in transit or at rest; and
- Whether the importer or its sub-contractors and service providers are required to disclose the personal data to U.S. law enforcement under applicable U.S. law.

Based on this review, and other relevant factors, the data exporter may choose to incorporate supplemental provisions into the SCCs to provide an adequate level of data protection or may determine the data importer is unable to provide an adequate level of data protection to enter into the SCCs.

7. SHOULD THE DATA EXPORTER REVIEW ITS EXISTING SCCS?

Yes. The data exporter's duty to verify the importer's ability to provide adequate data protection, and the supervisory authorities' obligation to suspend or terminate transfers to third countries without adequacy determinations where the transfer fails to provide an adequate level of protection, existed prior to the CJEU's decision. Data exporters should review their existing agreements to ascertain whether they provide the appropriate level of data protection.

8. WHEN IS A U.S. ORGANIZATION A DATA IMPORTER?

A U.S. organization that receives personal data from the EEA for processing based on the data controller's instructions — whether from a third party, affiliate, or member of its corporate group — is a data importer for purposes of the EU General Data Protection Regulation (GDPR). This applies regardless of whether the personal data is consumer data, employee data, business related, or other (*e.g.*, a company's U.S. headquarters receives EEA employee personal data for HR administration or a U.S. marketing company receives an EEA merchant's customer personal data to provide marketing services).

9. WHAT ARE THE OBLIGATIONS OF THE DATA IMPORTER?

A data importer must determine whether it can provide an adequate level of data protection to the personal data received from the EEA. To do so, the data importer must assess:

- The type and sensitivity of data;
- The processing activities to be performed on that data;
- Whether the data will be subject to an onward transfer to another country;
- Available data protection measures, including encryption in transit or at rest; and
- Whether the importer or its sub-contractor and service providers are subject to U.S. surveillance laws that violate applicable EU privacy laws.

If the importer is unable to do so, it must notify the exporter.

The importer must notify the data exporter immediately if, after the transfer, it determines it is cannot comply with the SCCs.

10. WILL USE OF ENCRYPTION IN TRANSIT OR AT REST SATISFY THE REQUIREMENT FOR AN ADEQUATE LEVEL OF PROTECTION?

Maybe. With respect to U.S. surveillance laws that permit monitoring of personal data flowing through the transatlantic cables from the EEA, certain levels of encryption may serve as appropriate safeguard. It is unclear whether this also will serve as appropriate safeguard in light of U.S. law enforcement requests for data pursuant to FISA 702.

11. WHAT IF AN ORGANIZATION RECEIVES PERSONAL DATA FROM THE EEA PURSUANT TO A CONTROLLER-CONTROLLER TRANSFER?

Schrems II addresses controller-processor SCCs, but not controller-controller transfers. However, it is reasonable to expect the same requirements for an adequate level of protection will apply to controller-controller transfers. As member state supervisory authorities, the European Data Protection Board, and the U.S. address the implications of *Schrems II*, we can anticipate further information relating to controller-controller transfers.

12. DOES *SCHREMS II* AFFECT BINDING CORPORATE RULES (BCRS)?

The CJEU's decision addresses controller-processor SCCs, but not BCRs. However, it is reasonable to expect the same requirements for an adequate level of protection will apply to BCRs. As member state supervisory authorities, the European Data Protection Board, and the U.S. address the implications of *Schrems II*, we can anticipate further information relating to BCRs.

13. WHAT IS THE RISK OF PERFORMING AN UNLAWFUL TRANSFER?

Under the GDPR, a supervisory authority can suspend or terminate the transfer. An impermissible transfer can result in assessment of fines of up to €20,000,000, or in the case of an undertaking, up to four percent of the total worldwide annual turnover of the preceding financial year, whichever is higher. In addition, EEA data subjects may bring a private cause of action against the data exporter for an illegal transfer, either individually or as part of a class action.

14. WHEN CAN A SUPERVISORY AUTHORITY SUSPEND OR TERMINATE A TRANSFER MADE PURSUANT TO SCCS?

A supervisory authority must suspend or terminate a transfer to third country without an adequacy determination if, in light of all the circumstances of the transfer, the SCCs are not or cannot be complied with.

15. DOES THE CJEU DECISION ON SCCS APPLY ONLY TO U.S. DATA IMPORTERS?

No. The decision applies to SCCs used to transfer personal data from the EEA to any country that does not have an adequacy determination.

16. DOES THE CJEU DECISION ON SCCS APPLY WHEN A U.S. DATA IMPORTER TRANSFERS EEA PERSONAL DATA TO A SUB-PROCESSOR IN ANOTHER THIRD COUNTRY?

Schrems II applies to the onward transfer of EEA personal data by the data importer to a sub-processor in a third country that does not have an adequacy determination.

17. HOW ARE EU MEMBER STATES RESPONDING TO THE CJEU DECISION?

EU member states are reviewing the CJEU decision and working with the European Data Protection Bureau to develop guidance.

Data protection authorities in Germany have issued preliminary guidance. The Berlin data protection authority has published specific requirements applicable to the transfer of personal data to the U.S. These include:

- Berlin-based data controllers storing personal data in the U.S. in reliance on the EU-U.S. Privacy Shield must transfer the data back to Europe;
- European data exporters and third country data importers must determine whether the recipient third country allows state access to the data beyond what is permitted by European law. If access is permitted, the transfer is prohibited; and
- Data controllers transferring data to the U.S., especially when using cloud service providers, must use service providers based in the EU or in a country with an adequate level of protection.

In addition, the Rhineland-Palatinate data protection authority has proposed a five-step assessment process for organizations to conduct when assessing the adequacy of protection in the U.S.

18. WHAT RESOURCES ARE AVAILABLE TO HELP IMPORTERS ASSESS WHETHER THEY CAN PROVIDE AN ADEQUATE LEVEL OF PROTECTION?

In addition to the Rhineland-Palatinate five-step assessment, NOYB – European Center for Digital Rights has published a template designed to assist U.S. importers to assess their ability to provide an adequate level of protection.

The EDPB and member state data protection authorities are expected to issue future guidance and the EDPB will be publishing an updated version of SCCs.