Special Report

EU-U.S. Privacy Shield Program for Transfer of Personal Data to U.S. Found Invalid

By Joseph J. Lazzarotti & Mary T. Costigan

July 22, 2020

Meet the Authors

Joseph J. Lazzarotti

Principal
908-795-5205
Joseph.Lazzarotti@jacksonlewis.com

Mary T. Costigan

Principal
908-795-5135
Mary.Costigan@jacksonlewis.com

Related Services

International Employment
Privacy, Data and Cybersecurity

The EU-U.S. Privacy Shield program is invalid, the Court of Justice of the European Union (CJEU) declared on July 16, 2020, in the matter of *Data Protection Commissioner v. Facebook Ireland and Schrems* (C-311/18) (*Schrems II*).

In addition, the CJEU affirmed the validity of standard contractual clauses (SCCs) as an adequate mechanism for transferring personal data from the European Economic Area (EEA), subject to heightened scrutiny.

Background

The matter arose from the transfer of Max Schrems' personal data by Facebook Ireland to Facebook Inc. in the United States. The presented questions related to the transfer of personal data from the EEA to a third country for commercial purposes.

Transferring Personal Data Out of EEA

Under the EU General Data Protection Regulation (GDPR), personal data transferred from the EEA to a third country for processing must receive a level of protection essentially equivalent to that guaranteed in the EU. This applies to a transfer from a data exporter to an importer in a third country, as well as an onward transfer by the data importer to another third country. Such data transfers would include, for example, a global Vice President sitting in the U.S. accessing human resources-related data of EEA-based employees on the organization's information systems.

A transfer may occur where the EU Commission has determined the third country ensures an adequate level of data protection. Absent such an "adequacy determination," the transfer of EEA personal data generally may occur only where the data exporter provides "appropriate safeguards" and the EEA data subject has enforceable rights and effective legal remedies. For this purpose, appropriate safeguards may include:

- Adopting binding corporate rules;
- Using approved standard data protection clauses;
- Executing standard contractual clauses;
- Adhering to a code of conduct adopted by the relevant member state Supervisory Authority; or
- Adhering to an approved certification mechanism.

The EU-U.S. Privacy Shield program (and its predecessor, the EU-U.S. Safe Harbor) was a means to provide an adequate level of data protection.

EU-U.S. Privacy Shield

The EU has not recognized the U.S. as providing an adequate level of data protection. As a result, the EU and U.S. entered into the EU-U.S. Privacy Shield program. The

program served as a certification mechanism to transfer personal data from the EEA to commercial entities in the U.S. in a manner that ensures a level of protection essentially equivalent to EU law. Over 5,000 U.S. companies have certified under the Privacy Shield since its 2016 effective date.

Schrems II

In *Schrems II*, the CJEU invalidates the EU-U.S. Privacy Shield program because it fails to provide an adequate level of protection to personal data transferred from the EEA to the U.S.

The CJEU noted that the breadth of U.S. national security bulk surveillance laws (FISA 702, E.O. 12.333, PPD 28, which permit bulk surveillance and monitoring activities) violate the basic minimum safeguards required by the GDPR for proportionality: the U.S. government's processing of EEA personal data is not limited to what is strictly necessary.

The CJEU further found these surveillance programs fail to provide EEA data subjects with enforceable rights and effective legal review.

As of the date of the decision, data exporters and U.S. data importers can no longer rely on EU-U.S. Privacy Shield certification as a mechanism to transfer personal data from the EEA to the U.S.

Standard Contractual Clauses

The CJEU affirmed the validity of controller-processor SCCs as an adequate mechanism for transferring personal data from the EEA to a third country lacking an EU adequacy determination.

While it reviewed SCCs for transfers to any third country without an adequacy determination, the CJEU's decision is particularly relevant to U.S. data importers in light of its decision on the EU-U.S. Privacy Shield.

The SCCs are approved, standardized contractual clauses executed by a data exporter and non-EEA data importer for each transfer of personal data out of the EEA. These clauses are drafted to ensure adequate safeguards for personal data transferred to and processed in a third country.

In affirming the validity of SCCs as an adequate transfer mechanism, the CJEU highlighted three stakeholder obligations:

1. The data exporter's responsibility to verify the importer's ability to provide an essentially equivalent level of protection in the third country;
2. The data importer's responsibility to notify the exporter immediately if it cannot comply with the SCCs, including where it is compelled to produce EEA data at the request of law enforcement; and
3. The data exporter's responsibility to immediately suspend or terminate the transfer upon notice from the importer that it cannot comply with the SCCs.

Based on these requirements, the SCCs may not be an adequate transfer mechanism in every case, or they may require the negotiation of additional provisions to satisfy these obligations.

The CJEU further highlighted the affirmative obligation of supervisory authorities to identify and suspend or terminate transfers based on SCCs where the importer cannot provide EEA data with an adequate level of protection.

Implications

Effective immediately, data transfers performed in reliance on the EU-U.S. Privacy Shield are no longer valid. Currently, there is no grace period. However, the EU enacted a grace period shortly after the EU-U.S. Safe Harbor was invalidated and it is conceivable one will be announced as the EU and U.S. assess the implications of this decision.

Data exporters and U.S. importers who rely on the EU-U.S. Privacy Shield to transfer personal data from the EEA to the U.S. should review the applicability of alternate transfer mechanisms, taking into consideration the nature of their processing activities, the types of personal data, the data flows, type of industry, and the transferee country.

In consultation with the EEA data exporter or data controller, U.S. importers must determine whether to retain, return, or delete data received under the EU-U.S. Privacy Shield.

The U.S. Department of Commerce will continue to administer the EU-U.S. Privacy Shield program, including processing submissions by U.S. organizations for self-certification and re-certification to the Privacy Shield Framework and maintaining the Privacy Shield List. The CJEU's decision does not relieve certified organizations of their obligations under the Privacy Shield.

Organizations may continue to use SCCs. Since SCCs are executed for each transfer, data exporters should review on a case-by-case basis the content of the SCCs, the specific circumstances of the transfer, and the laws of the third country to determine whether supplemental measures are necessary to ensure an essentially equivalent level of data protection. How data exporters will make this determination and what additional measures may address satisfactorily EU concerns about U.S. surveillance activities is unclear. The European Data Protection Board (EDPB) and member state data protection authorities are reviewing additional measures and the European Commission is drafting updated SCCs to replace the 2010 controller-processor SCCs currently in use.

U.S. data importers must determine how or whether certain U.S. surveillance laws may affect them, or their sub-contractors and service providers, and whether these laws conflict with EU privacy laws, as well as their ability to provide an adequate level of data protection.

In addition, organizations should anticipate increased scrutiny from supervisory authorities and data subjects seeking to ensure the data exporter performed due diligence and verified an importer's ability to provide an adequate level of data protection, particularly in countries conducting mass surveillance activities. Supervisory authorities are tasked with investigating, in light of all the circumstances, whether the data importer can comply with the SCCs or appropriate data protection can be provided by other means. Data exporters will want to document their due diligence and findings.

Compliance Risks

Under the GDPR, an impermissible transfer can result in assessment of fines 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.

Thus, a transfer of personal data under the invalidated EU-U.S. Privacy Shield, a failure to verify the existence of essentially equivalent protections in the transferee country, or a failure to suspend, terminate, or report the importer's inability to comply with the SCCs creates significant risk. 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.

What to Expect

While the CJEU's decision has and will continue to have a significant impact on transatlantic trade, various stakeholders appear committed to addressing and resolving issues arising out of the transfer of personal data from the EEA to the U.S. The U.S. Department of Commerce is working with the EU to resolve this issue, the EDPB will provide further guidance, and the European Commission has been preparing in anticipation of the decision's potential impact. Numerous member state data protection authorities advise they are reviewing the decision to provide guidance. For example, the Berlin data protection authority has published specific instructions to data controllers based on the CJEU's decision, including a requirement that data controllers transferring data to the U.S., especially when using cloud service providers, use service providers based in the EU or in a country with an adequate level of protection.

For additional information, see our FAQs.

If you have questions or need assistance, please reach out to the Jackson Lewis attorney with whom you regularly work.