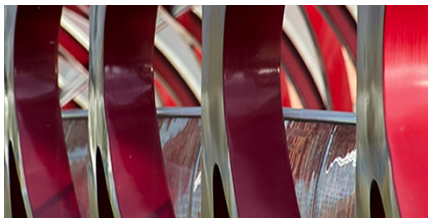
masuda funai



News & Types: Commercial, Competition & Trade Update

EU Court of Justice Invalidates US-EU Privacy Shield and Spares SCCs in Landmark Schrems II Data Privacy Decision

7/17/2020

By: Kenton P. Knop

Practices: Commercial, Competition & Trade, Intellectual Property & Technology

EXECUTIVE SUMMARY

The Court of Justice of the European Union invalidated the US-EU Privacy Shield mechanism for compliance with the GDPR, citing US government surveillance laws. The Court did not invalidate the Standard Contractual Clauses ("SCCs") for GDPR compliance, but indicated that data exporters are responsible for verifying that the laws of the receiving country ensure adequate protection of EU residents' data. Although companies may continue to use SCCs for their GDPR compliance strategies for EU-to-US data transfers, the long-term effects of this decision may ultimately lead to increased involvement of EU data privacy regulators in suspending or terminating data transfers to the United States and other countries with far-reaching government surveillance programs.

On July 16, 2020, the Court of Justice of the European Union issued its long-awaited decision in the *Facebook Ireland Ltd. v. Maximillian Schrems* (*Schrems II*) case, concerning the adequacy of the US-EU Privacy Shield Framework ("Privacy Shield") and Standard Contractual Clauses ("SCCs") for compliance with the EU General Data Protection Regulation ("GDPR"). In the latest chapter to the long-running data privacy controversy between the United States and the European Union, the Court declared the Privacy Shield invalid, citing concerns that US government surveillance programs based on Section 702 of the Foreign Intelligence Surveillance Act ("FISA") do not provide adequate levels of protection to EU residents' personal data as required under the GDPR. This decision comes as a blow to the over 5,300 Privacy Shield participants that based their GDPR compliance strategy for EU-to-US data transfers on the now-invalidated framework.

In contrast to the Privacy Shield, the Court did not invalidate SCCs as an appropriate mechanism for ensuring that data transfers outside of the EU guarantee EU residents' data privacy rights. However, the Court expressed concerns that SCCs, as a contractual mechanism, do not bind the actions of public authorities, and that it is the responsibility of data exporters to verify that the laws of the receiving country ensure adequate

protection of EU residents' data in accordance with EU law. The Court further indicated that if a data exporter does not take measures to ensure adequate protection of data, then competent EU supervisory authorities must suspend or end the transfer of data outside of the EU.

Although this decision means that companies can for now continue to rely on SCCs for GDPR compliance, usually as part of a Data Processing Agreement, the questions that remain are: (1) how data exporters can ensure "adequate protection" of data when sent to countries with far-reaching government surveillance programs, such as the United States; and (2) whether EU supervisory authorities are willing to order the suspension or termination of data exports to the United States and similarly-situated countries in response to privacy complaints from EU residents, such as the one that gave rise to this *Schrems II* case. Unfortunately, answers to these questions may not be forthcoming until the United States and European Union reach a resolution on data privacy. If you have questions about GDPR compliance and whether your company needs to take measures in response to the *Schrems II* ruling, please contact your Masuda Funai relationship attorney for a consultation.