July 16, 2020

CJEU Invalidates EU-U.S. Privacy Shield Decision; Finds SCCs Valid, Emphasizing Need For Case-by-Case Scrutiny

The Court of Justice of the European Union ("CJEU"), the EU's highest court on matters of EU law, today announced landmark rulings on two different mechanisms relied upon by organizations for the transfer of personal data from the EU to other countries, including the United States. In its decision, the CJEU determined that the use of EU Standard Contractual Clauses (the "SCCs") remains valid, emphasizing the need for case-by-case scrutiny, and that the decision allowing organizations to rely on the EU-U.S. Privacy Shield Framework ("Privacy Shield") is invalid as being incompatible with EU data privacy law.

The EU General Data Protection Regulation (the "GDPR") provides data subjects with broad protections concerning the handling, processing, and transfer of their personal information. Under the GDPR, transfers of personal information from data controllers or processors established in the EU to other countries are allowable only under certain circumstances, including to a country for which the European Commission has issued an "adequacy decision" finding that the receiving country ensures and provides an adequate level of protection along with sufficient safeguards and recourse mechanisms for data subjects. The Commission has not issued an adequacy decision to the United States.

In the alternative, transfers to the U.S. and other countries lacking an adequacy decision are only permitted if done via another approved mechanism, including the SCCs and, until today's decision, Privacy Shield. The SCCs are EU-approved model contractual clauses used for the transfer of personal data for commercial purposes. Privacy Shield allowed U.S. companies to self-certify that they provide the necessary protections required under EU data privacy law; in 2016, the Commission issued an adequacy decision regarding Privacy Shield (the "Privacy Shield Decision").

Privacy activist Maximillian Schrems, whose successful challenge to the U.S.-EU Safe Harbor framework – the predecessor framework to Privacy Shield – was the subject of the prior "Schrems I" decision of the CJEU, here challenged the reliance upon, and validity of, the SCCs, again arguing that the U.S. fails to provide the necessary adequate protections required under EU data privacy law. In this action, dubbed Schrems II, Ireland's High Court sought a preliminary ruling from the CJEU on whether the GDPR applies to transfers made pursuant to the SCCs, the corresponding level of data protection required, and the supervisory authorities' role and responsibilities in such transfers. In addition to addressing the SCC's validity, the CJEU additionally considered the question of whether the Commission's Privacy Shield Decision was valid under the requirements of EU data privacy law.

In Schrems II, the CJEU found that the SCCs, read in light of the Charter of Fundamental Rights (the "Charter"), remain valid because they provide appropriate safeguards, enforceable rights, and effective legal remedies that are essentially equivalent to those guaranteed under the GDPR. Importantly, the CJEU emphasized that "[i]t is therefore, above all, for that controller or processor to verify, on a case-by-case basis and, where appropriate, in collaboration with the recipient of the data, whether the law of the third country of destination ensures adequate protection, under EU law, of personal data transferred pursuant to standard data protection clauses, by providing, where necessary, additional safeguards to those offered by those clauses." Should compliance prove not possible, such transfers should be suspended. The CJEU also noted that data protection authorities have the ability to assess transfers made under the SCCs and to suspend or prohibit such transfers upon a finding of non-compliance with the requirements. The CJEU's focus on conducting adequacy assessments prior to data transfers indicates an intention to impose a higher level of scrutiny on the reliance on SCCs.

With respect to Privacy Shield, the CJEU concluded that, as read against the Charter, Privacy Shield failed to protect transferred personal data and, in turn, data subjects, from U.S. surveillance initiatives. The CJEU explained in its decision, "the limitations on the protection of personal data arising from the domestic law of the United States on the access and use by US public authorities of such data transferred from the European Union to the United States, which the Commission assessed in the Privacy Shield Decision, are not circumscribed in a way that satisfies the requirements that are essentially equivalent to those required, under EU law, by the second sentence of Article 52(1) of the Charter." In addition, the CJEU concluded that the Privacy Shield ombudsperson mechanism, in reality, does not truly afford impacted data subjects actionable rights against U.S. authorities in U.S. courts that are comparable to those available within the EU. Specifically, the CJEU, in its decision, noted that "the ombudsperson mechanism to which the Privacy Shield Decision refers does not provide any cause of action before a body which offers the persons whose data is transferred to the United States guarantees essentially equivalent to those required by Article 47 of the Charter." Thus, the CJEU invalidated the Commission's Privacy Shield Decision.

The impact of the CJEU's decision is sure to be significant. First, companies will no longer be able to rely on the EU-U.S. Privacy Shield program as a means to legitimize transfer of data between the EU and the U.S. – though, as noted today by the Department of Commerce, companies that do certify to Privacy Shield must still continue to comply with its requirements. Second, although the SCCs are still valid, the CJEU paid particular attention to the higher scrutiny now directed towards the data exporter's requirement to assess and ensure on a case-by-case basis that the data importer can and will provide adequate protections. Whether data transfers to the U.S. can be authorized on a case-by-case basis will likely depend, in part, on whether the data transferred will be subject to review by U.S. authorities, as such review will raise the same issues discussed by the CJEU in its decision regarding Privacy Shield. Indeed, Ireland's Data Protection Commissioner opined today that "[I]n practice, the application of the SCCs transfer mechanism to transfers of personal data to the United States is now questionable. This is an issue that will require further and careful examination, not least because assessments will need to be made on a case by case basis." The

assessment requirement will raise future questions, as the CJEU did not set forth a standard that data importers must meet. And third, organizations, data protection authorities, and others may need to look to alternative means for the legitimization of transfers of data under the GDPR, including the potential development of new certification mechanisms or codes of conduct.

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

H. Christopher Boehning
+1-212-373-3061
cboehning@paulweiss.com

Roberto J. Gonzalez
+1-202-223-7316
rgonzalez@paulweiss.com

Jeannie S. Rhee
+1-202-223-7466
jrhee@paulweiss.com

Ross M. Gotler
+1-212-373-2979
rgotler@paulweiss.com

Steven C. Herzog
+1-212-373-3317
sherzog@paulweiss.com

E-Discovery Attorney Lidia Kekis contributed to this Client Memorandum.