

Important European Court Ruling On Personal Data Transfer To The U.S.

July 17, 2020

On July 16, 2020, the Court of Justice of the European Union delivered its decision in *Data Protection Commissioner v. Facebook Ireland Ltd. and Maximillian Schrems*, which invalidated EU Commission Decision 2016/1250 (the "**2016 Decision**") on the adequacy of the protection provided by the EU-US Privacy Shield. The court decision confirmed the validity of EU Commission Decision 2010/87 (the "**2010 Decision**") on standard contractual clauses for the transfer of personal data to processors established in third countries.

Background

The case involved the transfer of personal data outside of the European Union. According to the European regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, which became effective in 2018 (the "**GDPR**"): "when personal data is transferred from the Union to controllers, processors or other recipients in third countries ... the level of protection of natural persons ensured in the Union by this Regulation should not be undermined" (Preamble 101 of the GDPR). Based on this principle, the GDPR lists several legal bases that make a transfer of personal data outside of the EU legal, including: a decision adopted by the Commission finding that a third country ensures an adequate level of protection; binding corporate rules; approved code of conduct or approved certification mechanism; and standard data protection clauses adopted by the EU Commission.

Based on these principles, and as a result of the European Commission's previous invalidation of the EU-US Data Privacy Safe Harbor Framework, on July 12, 2016, the European Commission adopted the 2016 Decision on the adequacy of the protection provided by the EU-U.S. Privacy Shield. Based on the 2016 Decision, the U.S. Department of Commerce adopted rules that incorporated the EU-U.S. Privacy Shield Framework Principles and allowed U.S. entities receiving personal data from the EU to self-certify for the purpose of qualifying for the Privacy Shield Framework.

Implications for U.S. Entities

In invalidating the benefits of the Privacy Shield Framework, the court held that "limitations on the protection of personal data arising from the domestic law of the United States on the access and use by U.S. public authorities of such data transferred from the European Union to the United States ... are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required under EU law." However, at the same time, the court affirmed the validity of contractual clauses derived from the 2010 Decision, due to the fact that they set forth "effective mechanisms that make it possible ... to ensure compliance with the level of protection required by EU law and that transfers of personal data pursuant thereto are suspended or prohibited in the event of the breach of such clauses or it being impossible to honor them." However, it was also stressed that the data exporter and the data recipient, prior to the transfer, shall verify that such level of protection is actually available in the country where data would be received. If not, transfer of data should be suspended, and the contract terminated. Based on the same presumption, a competent supervisory authority can suspend such transfer.

In practical terms, this judgment requires all U.S. entities to reevaluate the mechanisms they have employed to transfer personal data from the EU to the U.S. Moreover, U.S. entities that were utilizing the Privacy Shield Framework must be aware that, as of July 16, 2020, any transfer based thereon will no longer be compliant or legal.

Continued

If you have questions about the impact of this ruling or other data security issues, please contact any of the authors or your Miller Canfield attorney.