July 17, 2020 | Business, Corporate & Securities, Insights

EU Court Strikes Down EU-U.S. "Privacy Shield"

By: Rich May

On July 16, 2020, the Court of Justice of the European Union (the "Court") announced its decision to invalidate Commission Implementing Decision (EU) 2016/1250 (the "2016 Decision"). The 2016 Decision had ruled that the EU-U.S. Privacy Shield Framework (the "Privacy Shield") was adequate to enable transfers of personal data from the EU to the U.S. under EU law, including the then newly adopted General Data Protection Regulation ("GDPR"). Yesterday's decision (the "020 Decision") is poised to have potentially significant impacts on businesses operating in both the European Union and United States.

As discussed below, the primary impact on U.S. businesses is the immediate inability to rely on the Privacy Shield for GDPR compliance. While the Department of Commerce released a statement yesterday maintaining that the Privacy Shield program will continue to be administered and its participants are not relieved of their obligations, EU-U.S. data transfers by Privacy Shield participants will no longer be considered compliant under EU law and the GDPR.

Background

Prior to the adoption of the GDPR, data transfers between the EU and the U.S. were allowed under the International Safe Harbor Privacy Principles. The European Commission ruled in July of 2000, in the so called "Safe Harbour Decision," that U.S. companies complying with these principles met the data protection requirements under EU law (including the Data Protection Directive), and that such companies were allowed to transfer personal data from the EU to the U.S.

In October 2015, the Court invalidated the International Safe Harbor Privacy Principles. Soon after this decision, the European Union and the United States began talks over a new framework, and reached a political agreement regarding the same in February 2016. This new framework was the Privacy Shield, and was deemed adequate by the European Commission in its 2016 Decision.

The European Union adopted the GDPR in April 2016 and began enforcement in May 2018.

The GDPR applies to organizations involved in the processing of personal data of individuals located in the European Union. Personal data is defined broadly as "any information relating to an identified or identifiable natural person." The breadth of the GDPR means its application extends to many U.S. technology companies with European operations or that collect, process or handle the personal data of European Union residents.

The Privacy Shield program, administered by the International Trade Administration within the Department of Commerce, enabled U.S. companies to join the Privacy Shield framework (as well as the separate Swiss-U.S. framework), in order to benefit from the adequacy determination made in the 2016 Decision. To do so, U.S. companies had to self-certify and publicly commit to comply with the Privacy Shield requirements. While voluntary to join, once a commitment to the Privacy Shield requirements was made, such commitment would be enforceable under U.S. law.

The Privacy Shield was subject to a number of legal challenges, including one brought by Austrian national Maximillian Schrems in Ireland against Facebook. Schrems had challenged the transfer of his personal data from Facebook Ireland to servers belonging to Facebook Inc. located in the United States, where such personal data was then processed, as a violation of the GDPR. He claimed that despite the Privacy Shield, the U.S. does not offer sufficient protection of personal data. Schrems' challenge was referred by the Irish authorities to the Court, which led to the 2020 Decision yesterday.

The 2020 Decision

In yesterday's decision, the Court ruled that the transfer and processing arrangement conducted by Facebook and complained of by Mr. Schrems falls under the scope of the GDPR and that data subjects such as Mr. Schrems' must be afforded a level of personal data protection "essentially equivalent" to that guaranteed within the EU by the GDPR. In determining the sufficiency of personal data protection, the Court ruled that such an assessment should look at both the contractual arrangement between the EU data exporter (Facebook Ireland in Schrems' case) and the recipient of the personal data (Facebook Inc.) as well as the legal system of the country where the recipient is located.

The Court, in reexamining the 2016 Decision in light of the GDPR requirements, conducted such an assessment and ruled that (i) the requirements of US national security, public interest and law enforcement have primacy over the Privacy Shield, thus condoning interference with the fundamental rights of persons whose data are transferred, (ii) the limitations on the protection of personal data stemming from the permitted access and use of such data by U.S. authorities mean that personal data is not afforded an "essentially equivalent" level of protection as that required under EU Law, and (iii) accordingly, the 2016 Decision is invalid and the Privacy Shield is no longer deemed adequate to allow for data transfers under EU law. These rulings were based largely on the ability of U.S. authorities, through various surveillance programs authorized under the Foreign Intelligence Surveillance Act (which allows for mass collection of non-Americans' personal data from technology companies), to access personal data despite the Privacy Shield. The Court focused on the insufficient limitations on the implementation and use of such surveillance

programs, as well as the lack of actionable rights of EU data subjects before U.S. courts.

Although the 2016 Decision was invalidated and the Privacy Shield deemed inadequate, the Court stopped short of invalidating an alternative mechanism for GDPR compliance referred to as "standard contractual clauses" or "SCCs." These SCCs are contractual provisions drafted by the European Commission, outlining rights and responsibilities of data subjects and processors that comply with the GDPR. However, the Court left open the possibility of EU privacy regulators invalidating SCCs on a case-by-case basis if a company violates their terms or is unable to adhere to them.

Impact on U.S. Businesses

The primary impact on U.S. businesses is the immediate inability to rely on the Privacy Shield for GDPR compliance. While the Department of Commerce released a statement yesterday maintaining that the Privacy Shield program will continue to be administered and its participants are not relieved of their obligations, EU-U.S. data transfers by Privacy Shield participants will no longer be considered compliant under EU law and the GDPR.

U.S. businesses relying solely on SCCs for GDPR compliance should also keep abreast of upcoming developments in light of the 2020 Decision, especially if they are known to be subject to data collection under U.S. surveillance law, including the Foreign Intelligence Surveillance Act. While the system of SCCs will remain in place for now, the Court contemplates, and much of the commentary in the EU data privacy realm predicts, that EU regulators will reexamine and ultimately invalidate the SCCs on a similar basis as the Court used to invalidate the Privacy Shield.

Finally, U.S. businesses potentially affected by the 2020 Decision should be aware that exceptions remain in place under existing provisions of Article 49 of the GDPR. These exceptions will allow for the continued transfer of data, despite the Court's invalidation of the 2016 Decision and the Privacy Shield, where:

- the data subject has given explicit consent to such transfer after being informed of the absence of an adequacy decision and appropriate safeguards;
- the transfer is necessary for the performance of a contract between the data subject and the business controlling the data processing or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the business controlling the processing and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defense of legal claims;
- the transfer is necessary in order to protect the vital interests of the data

subject or others and the data subject is physically or legally incapable of giving consent; or
- the transfer is made from a register which according to EU or member state law is intended to provide information to the public and meets the prescribed legal conditions.

The Court highlighted that these exceptions, primarily that which allows for transfers necessary for the performance of a contract between the data subject and the business controlling the data processing, act to ensure that a "legal vacuum" is not created by 2020 Decision, disrupting crucial business activity.

Rich May continues to monitor the evolution of data protection and privacy laws and regulations that affect U.S. companies, both domestically and abroad, and will provide additional updates as they become available.

Disclaimer: This summary is provided for educational and informational purposes only and is not legal advice. Any specific questions about these topics should be directed to attorney Matthew Sweet.

