EU Court Invalidates Privacy Shield – What’s Next for Data Transfers and International Trade?

Shrems II – Groundhog Day, All Over Again

Past is Prologue

One of the keys to the European Union's data protection regime has been the prohibition against transferring personal data from EU countries to jurisdictions that do not have regimes that, in the determination of the EU, provide adequate protection to consumers. Beginning in 2000 the U.S. – EU Safe Harbor Framework allowed U.S. companies to certify their compliance with EU data protection requirements, and facilitated the transfer of data between the EU and the U.S. On October 6, 2015, the Court of Justice of the European Union, the European Union's highest court, overturned the Safe Harbor Framework. In response, the EU and the U.S., primarily through the Department of Commerce, developed International Safe Harbor Privacy Principles, commonly called the “Privacy Shield," and a more robust framework was adopted, allowing substantially the benefits of the Safe Harbor.

On July 16, 2020, the CJEU held that the EU-U.S. Privacy Shield arrangement — which includes more than 53,000 participating companies — is invalid. The CJEU said in a press release that, in the court’s view, “the 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 … are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required under EU law, by the principle of proportionality, in so far as the surveillance programmes based on those provisions are not limited to what is strictly necessary.” The Court also said that the United States ombudsman is neither independent enough, nor has adequate authority, to provide an effective cause of action to guarantee the protections under EU laws and regulations.

In particular, the court said that the ombudsperson mechanism in the U.S. — a role created by the Privacy Shield arrangement — “does not provide data subjects with any cause of action before a body which offers guarantees” at the level of EU law. The CJEU said the ombudsperson, which sits under the U.S. Department of State, is neither empowered nor independent at an adequate level.

Impact of the Decision

Like the invalidation of the Safe Harbor, the rejection of the Privacy Shield is likely to create substantial disruptions in data transfers, a key to international trade, until a resolution is found. It is hard to overstate the significance of this decision. The U.S. Commerce Department estimates that the value of the transatlantic economic market at $7.1 trillion, and that a multitude of companies, large and small, rely on the ability to transfer personal, employee and other data from the EU to the U.S. The impact on individual firms will be wide:

- Companies that have relied on participating in the Privacy Shield program will have to update privacy policies and, likely, publicize those changes; this could create a perception that those companies are less secure. In addition, companies that don’t update their privacy polices risk Federal Trade Commission enforcement for not living up to privacy promises.
While the Department of Commerce has stated that companies can continue to rely on the Privacy Shield for now, including for processing self-certifications and updating the program’s list, companies will need to consider other, less flexible, alternatives to maintain uninterrupted data transfers. While the decisions upheld the validity of standard contractual clauses (agreements that many companies have entered into which impose the obligations of the General Data Protection Regulation on contracting parties), standard contractual clauses are cumbersome and create potential liabilities for U.S. companies.

As noted above, a key element of the decision lies in concerns over U.S. surveillance activities and legal remedies. The CJEU decision requires EU regulators to bar data transfers—even using standard contractual clauses—to a third country where privacy protections fall short of EU law. The Irish Data Protection Commission, which acts as the main regulator for some of the biggest tech companies in Silicon Valley, said that “[W]hatever mechanism is used to transfer data to a third country, the protection afforded to EU citizens in respect of that data must be essentially equivalent to that which it enjoys within the EU,” and “in practice, the application of the SCCs transfer mechanism to transfers of personal data to the United States is now questionable.” This creates doubt as to whether the standard contractual clauses may actually be effective. This is particularly of concern to the banks, which were not able to qualify under the Privacy Shield and are more likely to have relied on standard contractual clauses to transfer data out of the EU.

Companies may be forced to find ways to avoid any transfer of data from the EU to the U.S., interrupting the ability of companies to operate efficiently, if at all. Companies will need to analyze what types of data are transferred to the U.S. that might be subject to monitoring by the U.S. The ruling could force some companies that are major players in the storage and processing of data, including tech giants such as Amazon, Facebook, Alphabet, and Apple Inc.—to decide between a costly transfer to EU data centers or cutting off business with the region.

**What Next?**

One potential byproduct of the CJEU’s decision is renewed interest in a federal comprehensive privacy law, attorneys and advocates said. Since the ability of the U.S. to surveil data and the lack of effective enforcement mechanisms is at the heart of the CJEU decision, privacy legislation addressing those concerns would be the most direct, and likely most effective, means of freeing the flow of data between the EU and the U.S.

It should be noted that while the impact of the decision is enormous, it is limited to the EU; other countries, like Switzerland, that have adopted laws similar to the GDPR, have not rejected the Privacy Shield. However, since those countries often move in tandem with the EU, that situation may be short-lived.

It is likely that EU and U.S. regulators will, again, attempt to create a regime similar to the Safe Harbor or Privacy Shield that allows for voluntary compliance with EU requirements. The question is whether the third time will be the charm.

*Robert E. Braun* is the co-chair of the Cybersecurity and Privacy Law Group at Jeffer Mangels Butler & Mitchell LLP. Bob helps clients to develop and implement privacy and information security policies, negotiate agreements for technologies and data management services, and comply with legal and regulatory requirements. He helps clients to develop and implement data breach response plans, and he and his team respond quickly to clients’ needs when a data breach occurs. Contact Bob at RBraun@jmbm.com or +1 310.785.5331.
JMBM’s Cybersecurity and Privacy Group counsels clients in a wide variety of industries, including accounting firms, law firms, business management firms and family offices, in matters ranging from development of cybersecurity strategies, creation of data security and privacy policies, responding to data breaches and regulatory inquiries and investigations, and crisis management. The Cybersecurity and Privacy Group uses a focused intake methodology that permits clients to get a reliable sense of their cybersecurity readiness and to determine optimal, client-specific approaches to cybersecurity.