Privacy Shield Struck Down in Europe: What Companies Should Do Now

The Court of Justice of the European Union (CJEU), the European Union's (EU) highest court, on July 16, 2020, struck down Privacy Shield—a trans-Atlantic framework that allowed companies to move data between the EU and the United States by self-certifying adherence to various privacy principles. As a result of the decision, the more than 5,000 businesses who relied on Privacy Shield must cope with the court's decision and reevaluate the legal basis for their transfers of personal data between the EU and the U. S.

Privacy Shield was created in 2016 to address concerns that the U. S. lacked adequate measures to protect the personal data of EU residents by giving Europeans more control over how their personal data was used. Privacy Shield also provided certain mechanisms to raise and resolve complaints relating to alleged violations of Privacy Shield principles.

The importance of Privacy Shield to U.S. companies was amplified in 2018 when the EU's General Data Protection Regulation (GDPR) became effective. The GDPR prohibits the transfer of personal data to countries outside the EU unless that data is covered by certain transfer mechanisms. Chief among these mechanisms were "adequacy decisions" (such as Privacy Shield) and "appropriate safeguards." The most widely used safeguards include standard contractual clauses (SCCs), ready-made contractual clauses written by the European Commission and executed between US and EU companies, and binding corporate rules, internal codes of conduct governing cross-border transfers within a multinational group.

In its highly anticipated ruling last week, the CJEU found that Privacy Shield did not adequately address U.S. government surveillance programs, which the court criticized as "not limited to what is strictly necessary" and as "condoning interference with the fundamental rights of persons whose data are transferred." The CJEU further found that Privacy Shield does not grant EU residents actionable rights before a body that are substantially equivalent to those required under EU law.

While the CJEU generally upheld the validity of SCCs, the CJEU stressed the need for companies to evaluate whether or not the use of SCCs will, in fact, provide "a level of protection essentially equivalent" to EU law. In particular, the CJEU stressed the need for companies to evaluate legal protections for the data in the

POSTED:

Jul 20, 2020

RELATED PRACTICES:

Corporate Law
https://www.reinhartlaw.com/practices/corporate-law

RELATED SERVICES:

Data Privacy and Cybersecurity
https://www.reinhartlaw.com/services/data-privacy-and-cybersecurity

RELATED PEOPLE:

Collin S. Weyers
https://www.reinhartlaw.com/people/collin-weyers

Melissa A. Zabkowicz
https://www.reinhartlaw.com/people/melissa-zabkowicz

non-EU recipient country. Given the CJEU's view of U.S. legal protections for non-citizen data, it remains to be seen whether SCCs for transfers to the United States will withstand further scrutiny. Nevertheless, SCCs may be the best candidates for a speedy alternative transfer mechanism for companies who have relied on Privacy Shield.

What Now?

Although the Privacy Shield is no longer a valid trans-Atlantic data transfer mechanism and cannot be used as the legal basis for transferring personal data from the EU to the United States, the U.S. Department of Commerce will continue to administer Privacy Shield. Participating organizations must continue to abide by their obligations under the Privacy Shield framework.

The bottom line is this: if you are transferring the data of EU users to the United States, the time is ripe to reevaluate those transfers, including by making sure that you are keeping promises made under Privacy Shield, signing SCCs (or adopting another appropriate safeguard) and ensuring that they can be complied with in practice. Privacy policies that rely upon Privacy Shield should also be reviewed and updated.

When Safe Harbor (Privacy Shield's predecessor) was struck down in October 2015, EU authorities allowed a roughly three-month grace period during which organizations could adopt alternative transfer mechanisms. During the grace period, EU authorities retained the power to investigate specific cases following individual complaints. The first post-Safe Harbor fines were issued in June 2016, almost nine months after Safe Harbor was invalidated. As of this writing, EU authorities have not announced whether there will be a similar grace period this time and, if so, how long it will be.

We will continue to monitor further developments and guidance on the invalidation of the Privacy Shield. If you have any questions regarding any aspect of this decision or your company's ability to comply with GDPR, please reach out to your Reinhart attorney.