Top European Union Court Invalidates EU-U.S. Privacy Shield Framework for Cross-Border Data Transfers

07.16.2020

The Court of Justice of the European Union issued a landmark ruling on Thursday, July 16 that could immediately affect businesses in the United States by challenging data transfer arrangements that are currently in place for cross-border sharing of information between U.S. and EU companies.

The CJEU, the EU's highest court, struck down the EU-U.S. Privacy Shield framework, which was established in 2016 as a mechanism for companies to transfer data between the EU and the U.S. after the CJEU struck down the predecessor Safe Harbour framework in 2015. Effective immediately, Privacy Shield is not a valid mechanism for data transfers between the EU and the U.S. The full text of the ruling can be found here.

The Court's reasoning for the decision was based on the far-reaching scope of U.S. government surveillance practices. The Court held that the U.S.'s national security programs have too much power to view and collect individuals' data and the U.S. government does not provide sufficient remedies for EU residents who have concerns or complaints about how their data is being used.

Another notable part of the Court's Thursday ruling was that the CJEU upheld in principle the use of Standard Contractual Clauses (SCCs), which are uniform terms into which companies can enter in order to guarantee sufficient safeguards of data during international transfers. However, the Court's opinion calls into question whether U.S. companies will be able to rely

ATTORNEYS

Maureen E. Fulton

PRACTICE AREAS

Data Privacy and Security

Top European Union Court Invalidates EU-U.S. Privacy Shield Framework for Cross-Border Data Transfers

on standard contractual clauses going forward.

The Court stated that businesses can only use standard contractual clauses for data transfers if the country receiving data from the EU has "adequate" privacy protections in place. The European Commission, the executive branch of the European Union, has not recognized the U.S. as having an "adequate" level of protection. The Court stated that data protection officers located in European Union countries have the ability to decide adequacy and advised businesses to review SCCs on a case-by-case basis. Thus, while SCCs are still valid, it is unknown whether the clauses will survive long-term as an option for U.S. companies.

Prior to Thursday's decision, U.S. companies had at its disposal a handful of ways it could lawfully effectuate data transfers between the EU and the U.S.: (1) Privacy Shield certification through the U.S. Department of Commerce; (2) utilizing standard contractual clauses; and (3) implementing binding corporate rules (a rarely used device). Companies can also use "derogations for specific situations" as discussed in GDPR Article 49; a method that is typically only used sparingly and not as a regular transfer mechanism. Now, Privacy Shield is gone, and SCCs might not be the desired option at this point given the uncertainty surrounding how country-level Data Protection Officers will react to this ruling.

For advice on how to adapt to the European Union Court's ruling, or for other privacy and cybersecurity advice, please contact a member of the Koley Jessen Data Privacy and Security practice area.