

EUROPE'S HIGHEST COURT INVALIDATES U.S.-EU SAFE HARBOR REGIME

The European Court of Justice (ECJ) today invalidated the transatlantic Safe Harbor Regime that permits U.S. companies to transfer consumers' and employees' personal data from Europe to the United States under a presumed level of "adequate" privacy protection. Although the ruling doesn't order an immediate end to such transfers, it does permit EU regulators to stop them if they feel that privacy protections are inadequate.

One possible consequence of today's decision is that U.S. companies might be forced to house their employee or customer data on servers located in Europe and quickly become familiar with multiple regulatory environments.

The Safe Harbor Regime, an agreement approved by the EU in 2000, has been used by some 4,000 U.S. and EU companies, including Apple Inc. and Alphabet Inc.'s Google. The agreement has been a mechanism for participating corporations to protect themselves from interruptions in their transatlantic business and prosecution by data protection authorities (DPAs) in individual European countries under their applicable privacy laws. The agreement created a voluntary program, whereby corporations self-certify annually that they are abiding by the regime's seven principles of privacy protection (Privacy Principles) and publically declare that they do so.¹

Today's decision stems from a 2013 complaint, known as the Facebook case, which was filed with the Irish DPA. The plaintiff, privacy activist Max Schrems, alleged Facebook violated his privacy rights by permitting his personal data to become subject to one of the mass surveillance programs of the U.S. National Security Agency. Although the DPA initially rejected the case, Schrems appealed the matter to the Irish High Court, which in turn referred to the ECJ the specific question of whether the respective country DPAs have the authority to investigate and suspend transfers of personal data under the Safe Harbor Regime without limitation by the EU Commission. Today, the ECJ has answered that question in the affirmative. But the ECJ went a step further and actually declared the 2000 implementation of the Safe Harbor Regime invalid, nullifying its legal basis.

Accordingly, in addition to the economic cost created by the uncertainty and

PEOPLE

Lucas Amodio, C|EH

Jeffrey Schultz, CIPP/US

SERVICES AND INDUSTRIES

Data Innovation, Security and Privacy
International



disruption, today's decision has significant practical and legal consequences for the many U.S. corporations that are (at times daily) transferring personal data from the EU to the U.S. The decision will certainly light a fire under the negotiations between the European Commission and the U.S. Commerce Department to reform the Safe Harbor Regime, which likely means additional compliance challenges for companies.

Further, corporations that do not have good contingency plans in place could find themselves flat-footed and arguably in violation of various European countries' data privacy laws. There are alternatives to the Safe Harbor Regime if you are one of the 4,000 corporations currently relying upon it as the legal basis for the transfer of personal data from the EU to the U.S., including obtaining explicit and fully informed consent from the data subject, implementing binding corporate rules for intracompany transfers, executing pre-approved model contracts between the data exporting and importing entities, and pursuing ad hoc adequacy determinations by the relevant DPAs.

In light of the swiftly changing sands in the data privacy/protection landscape, members of Armstrong Teasdale's Privacy and Data Security Group will continue to closely monitor the situation.

The seven Privacy Principles of the Safe Harbor Regime are notice, choice, onward transfer, access, security, data integrity, and enforcement.