Pepper Hamilton LLP
Attorneys at Law

CLIENT ALERT

September 24, 2015

Advocate General of the EU Court of Justice: EU-U.S. Safe Harbor Act Is Not Safe for EU Citizens

Sharon R. Klein | kleins@pepperlaw.com
William M. Taylor | taylorw@pepperlaw.com
Katherine B. Puccio* | pucciok@pepperlaw.com

*** Ms. Puccio is a law clerk in Pepper Hamilton's Philadelphia office. She is not admitted to practice.**

THE DECISION COULD AFFECT THE THOUSANDS OF U.S. COMPANIES IN DIVERSE INDUSTRIES THAT RELY ON THE EU-U.S. SAFE HARBOR AGREEMENT TO LEGALLY TRANSFER PERSONAL DATA OF EU CITIZENS FROM THE EU TO THE UNITED STATES.

Key Points

- The Advocate General of the Court of Justice of the European Union (CJEU), Yves Bot, recommended the CJEU declare the EU-U.S. Safe Harbor Agreement invalid, thereby threatening the pact that permits thousands of U.S. businesses to transmit personal data from the EU to the United States.

- Bot's recommendation is **not binding**; however, the CJEU often reaches the same conclusion as the Advocate General. A decision from the CJEU is expected by the end of the year.

- Bot stated that the EU's national data privacy supervisory authorities have the power to conduct investigations and suspend data transfers to the United States, regardless of the EU Commission's 2000 decision that, under the Safe Harbor, the United States adequately protects data.

- Bot opined that, because the United States conducts "mass and indiscriminate surveillance," as exposed by Edward Snowden, it cannot ensure the protection of any data transferred from the EU.

The September 23, 2015 decision of Yves Bot, the Advocate General of the Court of Justice of the European Union (CJEU), in *Schrems v. Data Protection Commissioner*, Case C 362/14, threatens to end the current version of the EU-U.S. Safe Harbor Agreement. This agreement was reached in 2000 to address the finding that the United States did not provide an adequate level of protection for the privacy of personal data. To participate in the Safe Harbor program, a U.S. company must self-certify that it complies with seven privacy principles required to meet the EU's adequacy standard: notice, choice, onward transfer, security, data integrity, access and enforcement. The program is critical to the thousands of U.S. companies in diverse industries that rely on it to legally transfer personal data of EU citizens from the EU to the United States.

Bot recommended the CJEU declare the 15-year-old data-transfer pact invalid because of concerns over U.S. surveillance practices and lack of adequate measures for enforcement and redress of grievances. Bot specifically cited concerns over the "mass, indiscriminate surveillance" under the National Security Agency's "PRISM" program, exposed by Edward Snowden in 2013. Although the recommendation of the Advocate General is nonbinding, the CJEU more often than not reaches the same result as the Advocate General's recommendation, although sometimes with a different rationale. If the CJEU accepts Bot's recommendation, U.S. companies will have to comply with alternative schemes in order to transfer data from the EU to the United States. These alternatives are typically costly and time-consuming, making them less-than-ideal solutions.

In the case, Maximillian Schrems, an Austrian citizen and well-known privacy activist, lodged a complaint with the Irish Data Protection Commissioner (DPC) regarding data that Facebook Ireland transferred to Facebook USA servers in the United States. All EU Facebook users are asked to sign a contract with Facebook Ireland, the location of Facebook's European headquarters. Mr. Schrems contended that the "law the practices of the United States offer no real protection of the data kept in the United States against State surveillance" in light of the Snowden revelations. The Irish DPC decided not to investigate the complaint because (1) there was no evidence that the U.S. National Security Agency (NSA) accessed Schrems' data and (2) the complaint had to be rejected in light of the European Commission's (the Commission's) July 2000 decision (Decision 2000/520), which declared that the United States provided an adequate level of protection for the personal data pursuant to the "safe harbor" scheme and, therefore, Ireland had no authority to investigate Mr. Schrems' claims. The High Court of Ireland then asked the CJEU to decide whether the Decision 2000/520 prevented a national data protection supervisory authority (such as Ireland's) from investigating a complaint alleging that a third country (such as the United States) does **not** ensure an adequate level of protection. Further, the court asked whether the authority could suspend the transfer of data upon a finding of inadequate protection.

In his surprisingly far-reaching opinion, Bot found national supervisory authorities do have the power to investigate complaints regarding data security and to suspend the transfer of data where appropriate, irrespective of any general assessment made by the Commission. In no uncertain terms, Bot stated, "the Commission is not empowered to restrict the powers of the national supervisory authorities." Bot reasoned that individual countries have a duty to protect the rights and privacy of their citizens and the Commission can in no way interfere with this duty through Decision 2000/520.

Bot opined that, although national supervisory authorities are bound by Decision 2000/520, that decision cannot preclude investigations into the merits of complaints brought by EU citizens. While acknowledging Decision 2000/20 is very important to ensuring uniformity in the transfer conditions in the EU member states, Bot held that uniformity can only continue so long as the finding that a third country adequately protects data is not called into question.

Further, Bot argued that Decision 2000/520 must be declared invalid because the Safe Harbor does not "ensure an adequate level of protection of the personal data which is transferred to the United States from the European Union." Because U.S. laws "permit the mass and indiscriminate surveillance and interception of such data," the United States cannot be regarded as adequately protecting the data and privacy of EU citizens. Bot was particularly concerned with the NSA surveillance program, but also found

significant weaknesses in the Safe Harbor scheme, which relies on self-certification and self-assessment with little independent oversight and enforcement. In particular, Bot noted that neither the Federal Trade Commission nor any private entity possesses the power to monitor possible breaches of privacy by public actors, such as U.S. security agencies. Without such oversight, there is no way to ensure the effective protection of data, according to Bot.

Bot's opinion comes after U.S. and EU authorities have spent the last two years trying to update the Safe Harbor agreement. Discussions have stalled as representatives from both sides have struggled to address data transfers by U.S. companies. Many now speculate that Bot's recommendation will push the EU and the United States to reach a new agreement quickly so that the CJEU will have no reason to declare the agreement invalid. Any new agreement is expected to deal with the problems highlighted by Bot. In the interim, Bot's opinion is almost certain to push U.S. companies towards alternatives to the Safe Harbor, such as Binding Corporate Rules and Model Contractual Clauses. Both of these options require significant time and cost investments, making them far-from-ideal solutions. In light of these challenges, Pepper Hamilton stresses the importance of seeking opt-in consent for personally identifiable information in advance from all data subjects.

Pepper Points

- Although there are some alternatives to the Safe Harbor (such as opt-in consent, Binding Corporate Rules and Model Contractual Clauses), each of these alternatives has significant shortcomings. Alternatives to the pact are time-consuming and expensive; U.S. companies hope ongoing negotiations between U.S. and EU authorities fix the agreement before data transfers from the EU to United States are suspended. Nonetheless, U.S. companies will be forced to consider these alternatives unless the EU and U.S. authorities quickly address the Safe Harbor's problems.

- Pepper stresses the wisdom of opt-in consent for personally identifiable information. For example, a global business with European employees should obtain opt-in consent to allow access by U.S. human resource executives to the European employees' data. It is important to pay attention to transparency in disclosing onward transfer of European data as part of the broad consent. The details of the opt-in consent regarding the purpose and the use of the personally identifiable information are essential.