Pepper Hamilton LLP
Attorneys at Law

CLIENT ALERT

October 7, 2015

EU Court of Justice: Safe Harbor Decision Permitting EU-U.S. Personal Data Transfers Is Invalid

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.**

Ruling affects approximately 5,000 U.S. companies that have relied on the Safe Harbor to transfer personal data from the EU to the United States.

In a stunning ruling rendered on October 6, 2015, the Court of Justice of the European Union (CJEU) declared invalid the European Commission's (Commission's) July 2000 decision, identified as Decision 2000/520, which had authorized companies to transfer personal data from the EU to the United States pursuant to certain "Safe Harbor" principles that were meant to ensure that the United States adequately protected personal data (Safe Harbor Decision). Finding that the Commission never declared that the United States did in fact "ensure" an adequate level of protection through domestic law or international commitments, the CJEU held that it was forced to invalidate the Safe Harbor Decision. Although the CJEU could have stopped there, it went on to admonish the United States for allowing public authorities to have access "on a generalised basis" to electronic data. The CJEU's ruling suggests that, until the United States passes legislation that restricts the power of the government to access personal data, there can be no transfers of data from the EU to the United States.

The ruling's key points are:

- The approach of the U.S. government to personal electronic data must be regarded as "compromising the essence of the fundamental right to respect for private life."
- The EU Commission's 2000 Safe Harbor Decision improperly restricted EU member states' supervisory authorities' ability to protect the fundamental rights and freedoms of individuals who question the Decision.
- Only the Court of Justice of the European Union, and not the EU supervisory authorities, has the power to declare an EU act such as the Safe Harbor Decision invalid. Where a national authority finds there is a foundation for finding an act invalid, it must refer the question to the court.
- Following the ruling, the EU Commissioner confirmed that alternatives to the Safe Harbor are still viable.

In the case, known as *Schrems v. Data Protection Commissioner*, Case C 362/14, an Austrian citizen (Maximillian Schrems) lodged a complaint with the Irish Data Protection Commissioner (DPC) regarding data that Facebook Ireland transferred to Facebook USA servers in the United States. In order to use Facebook, all EU Facebook users are asked to sign a contract with Facebook Ireland. Facebook had located its European headquarters in Ireland because Ireland's data protection authority had marketed itself as the most pro-business of the EU's 28 different data protection authorities.

Mr. Schrems contended that the law and the practices of the United States "offer no real protection of the data kept in the United States against State surveillance" in light of Edward Snowden's 2013 revelations regarding the U.S. National Security Agency's (NSA's) surveillance program. The Irish DPC decided not to investigate the complaint because (1) there was no evidence that the NSA accessed Schrems' data and (2) the complaint had to be rejected in light of the Safe Harbor Decision, 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 Schrems' claims. The High Court of Ireland then asked the CJEU to decide whether the Safe Harbor Decision 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 its October 6 ruling, the CJEU first dealt with the High Court of Ireland's threshold questions. The CJEU found that a Commission decision that a country adequately protects personal data cannot eliminate or reduce the power of an EU member state's national supervisory authority. When a national supervisory authority receives a complaint about data privacy from a citizen, it has a duty to investigate whether the transfer of the data complies with the Safe Harbor Decision. If a claim is considered to have merit, the citizen must have access to legal proceedings that could result in the suspension of the data transfer.

The CJEU next considered the validity of the Safe Harbor Decision. It found that the Commission, in considering the adequacy of a non-EU member state's protection of personal data, was required to find explicitly that the country at issue does in fact ensure "a level of protection of fundamental rights essentially equivalent to that guaranteed in the EU legal order," either through domestic law or international agreement. Observing that the Commission never stated in the Safe Harbor Decision that the United States does in fact ensure an adequate level of protection through domestic law or international agreement, the CJEU concluded the Safe Harbor Decision must be declared invalid. The CJEU did note, however, that it was not "examin[ing] the content of the Safe Harbor principals."

In reaching its ruling, the CJEU highlighted that the Safe Harbor Decision is applicable solely to those self-certified organizations that choose to comply with its directives. The Safe Harbor Decision had no binding effect on U.S. public authorities, and the CJEU noted that national security and law enforcement directives preempt any agreements

under the decision. The CJEU found this completely unacceptable, stating that "legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life." According to the CJEU, the EU must protect this right and permit derogations and limitations only where strictly necessary.

According to the press release accompanying the ruling, the Irish DPC will now be required to "examine Mr Schrems' complaint with all due diligence and, at the conclusion of its investigation, is to decide whether, pursuant to the directive, transfer of the data of Facebook's European subscribers to the United States should be suspended on the ground that that country does not afford an adequate level of protection of personal data."

Although the CJEU's ruling focused specifically on the Safe Harbor Decision, its reasoning appears broad enough to apply to Binding Corporate Rules and Model Contractual Clauses — two alternatives to the Safe Harbor for the transfer of personal data. That is, the CJEU's principal concern appears to be the ways in which the U.S. government can access data and that such access is not limited to data transferred pursuant to the Safe Harbor. The early indications from the EU following the ruling, however, appear to show that the Safe Harbor alternatives are still viable. At a press conference concerning the ruling, Vera Jourová, the European Commissioner for Justice, Consumers, and Gender Equality, explained that alternative mechanisms, such as Binding Corporate Rules and Model Contractual Clauses, are still available for companies to share data.

Pepper Points

- The CJEU's ruling will push U.S. companies to adopt alternatives to the Safe Harbor. The most obvious alternatives are Binding Corporate Rules, Model Contractual Clauses, obtaining data subject consent and anonymizing data. The ruling is likely to make Binding Corporate Rules and Model Contractual Clauses more expensive and time-consuming because it enhances the role of each of the 28 different data protection authorities by clarifying that each one must examine complaints from EU citizens regarding the processing of personal data in another country. In addition, neither Binding Corporate Rules nor Model Contractual Clauses shield companies from U.S. government requests for personal information. Consequently, these mechanisms are subject to the same issues cited by the CJEU, and it remains to be seen whether they will be challenged in the future.

- 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. Consent must be specific, informed and freely given. Transparency in disclosing onward transfer of European data and the purpose and the use of the personally identifiable information are crucial when obtaining opt-in consent.

- If a company's business purposes may be achieved by using anonymous data, it may wish to explore anonymizing the data to be transferred. Anonymous data is not subject to EU data protection laws. Special attention should be paid to guidance on anonymizing data provided by EU data protection authorities (*e.g.*, guidance (available at https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf) from the United Kingdom's Information Commissioner's Office).

- The U.S. Department of Commerce and the Federal Trade Commission have been attempting to address concerns regarding the Safe Harbor for several years now via negotiations with their EU counterparts. It is unlikely, however, that these negotiations contemplated the significant changes to U.S. surveillance laws that would appear to be the only way to address the CJEU's concerns. Nevertheless, given the impact of the ruling on U.S. companies doing business in the EU, the parties may be incentivized to bring these negotiations to a quicker resolution.