MILLER CANFIELD

European Court Invalidates EU-US Data Privacy Safe Harbor Framework

October 9, 2015

The Grand Chamber of the Court of Justice of the European Union recently invalidated the Safe Harbor Framework for data transfer from the E.U. to the U.S. The Safe Harbor Framework has provided a method to transfer personal data outside the European Union to U.S. companies in a way that is consistent with the EU Data Protection Directive. Now, U. S companies receiving personal data from a subsidiary, branch or established commercial presence in the E.U. can no longer rely on the Safe Harbor Framework.

The EU Data Protection Directive generally prohibits organizations from transferring personal data from the E.U. unless there is an adequate level of data protection (the adequacy requirement). Until now, a U.S. entity could satisfy this requirement and lawfully receive the personal information of EU citizens (personal data) from organizations located in the E.U. if it complied with a set of privacy principles developed by the U.S. Department of Commerce and approved by the European Commission (the "Safe Harbor Decision").

On October 6, 2015, the Court of Justice of the European Court delivered a judgment in *Maximilian Schrems v. Data Protection Commissioner.* The case stemmed from the request made in proceedings between Mr. Schrems and the Data Protection Commissioner concerning the Commissioner's refusal to investigate a complaint made by Mr. Schrems regarding transfers of personal data of Facebook users made by Facebook Ireland Ltd. to the U.S., and storing the data on servers located in the U.S. The case arose because the Commissioner originally rejected Mr. Schrems' claim, referring to the Safe Harbor Decision. The Commissioner concluded that Mr. Schrems' allegation about his data being accessible by U.S. surveillance services was unfounded and that the Safe Harbor Decision prevents the complaint from being brought forward.

Against this background, the Irish High Court referred the matter to the Court of Justice of the European Union, as to the binding character of the Safe Harbor Decision for a preliminary ruling. The CJEU was asked whether the national authority should conduct its own investigation or instead rely on the Safe Harbor Decision only in the event of doubt about the U.S. ensuring an adequate level of protection of personal data.

In its judgment, the Court of Justice of the European Union made two main findings. First, it held that any European decision which finds that a third country ensures an adequate level of protection does not prevent a supervisory authority of a Member State from examining a complaint brought by a person claiming to the contrary. In other words, any decision of this kind does not introduce a binding presumption which would prohibit any contradictory statement.

Second, and even more far-reaching, the Court found the Safe Harbor Decision itself invalid. The CJEU explained that the Safe Harbor Decision did not state that the U.S. in fact "ensures" an adequate level of protection by reason of its domestic law or its international commitments, as required by the EU Data Protection Directive. In addition, by restricting the powers available to national supervisory authorities, the Commission, in adopting the Safe Harbor Decision, exceeded the power conferred to it by that EU Data Protection Directive.

The CJEU's ruling triggers serious implications for subsidiaries of U.S. companies in Europe as well as for any organization that was relying on safe harbor privacy principles when transferring data from the E.U. to the U.S. What was legal and in compliance with E.U. data protection law before October 6, 2015, is no longer considered safe.

Continued

So what is a U.S. company having subsidiaries in Europe to do now? On the day the decision in *Schrems v. Facebook* was delivered, the European Commission published a press release confirming that it would keep working with U.S. authorities on a renewed and safe framework for the transfer of personal data across the Atlantic. In light of the judgment, it also promised to come forward with clear guidance for national data protection authorities on how to deal with data transfer requests to the U.S.

In the meantime, U.S. companies should review their data privacy policies, certifications and practices to ensure that they will comply with U.S. and European data protection law.

Miller Canfield, with offices in Europe, can help US companies navigate the EU data privacy laws. If you have questions or concerns about the above or any issue involving EU data privacy laws, please contact us.

Richard A. Walawender
+1.313.496.7628
walawender@millercanfield.com