LEGAL UPDATE

November 2015

By Robert J. deBrauwere, Jeffrey C. Johnson and Francesca N. Djerejian

EUROPEAN COURT OF JUSTICE DECLARES EU DATA PROTECTION DIRECTIVE 'SAFE HARBOR' INVALID

On October 26, the European Union announced that an agreement in principle had been reached with the United States on a pact (the "New Safe Harbor") to replace the U.S.-EU Safe Harbor Framework, which was invalidated early last month by the Court of Justice of the European Union.[1] Until the New Safe Harbor is negotiated and formally adopted, however, all American companies with subsidiaries, operations, employees and customers located in Europe that transfer personal data from the EU and the European Economic Area (EEA) to locations outside the EU/EEA can no longer rely on the Safe Harbor Framework. Instead, these companies must either implement, or ramp up their existing use of, alternative mechanisms for compliance with the standards established by the EU Data Protection Directive.

For almost 20 years, the transfer of personal data to countries outside the European Economic Area (EEA) has been subject to Article 25 of the Data Protection Directive, which allows such transfers to take place only if non-EU/EEA countries ensure adequate levels of protection for the transfer and processing of personal data originating in the EU.[2] The Safe Harbor Framework, implemented in 2000, has allowed U.S. companies to transfer, process and store data outside of the EU in a manner consistent with the EU Data Protection Directive, provided such companies "self-certified" to the U.S. Department of Commerce that they were compliant with EU data privacy standards.

This month's ruling stemmed from the data privacy-infringement lawsuit brought against Facebook by Max Schrems, an Austrian citizen who argued to the Irish Data Protection Authority that the allegations made by Edward Snowden regarding mass surveillance tactics in the United States were evidence that the protection afforded by the Safe Harbor agreement was inadequate. Pursuant to the Data Protection Directive, factors including the purpose and duration of the proposed processing operation, the country of origin and final destination of the data, and the rule of law and security measures in place in the destination country must all be considered in making a determination regarding the adequacy of the level of protection afforded by a non-EU/EEA country.[3] The case was brought to the Irish High Court on appeal and ultimately to the European Court of Justice. In reaching its decision, the Court noted that the Safe Harbor framework as applied in the U.S. fails to meet the required standard of data protection because, among other reasons, (i) U.S. national security, public interest and law enforcement requirements are prioritized over the EU standard, ii) U.S. government authorities are not subject to the Directive, and (iii) mechanisms for redress are lacking. The Court also considered that a significant number of certified companies were non-compliant with the Safe Harbor principles.

The new agreement, which is expected to be negotiated between the EU and the U.S. by January of 2016, will likely require stronger oversight by the Department of Commerce and feature additional enforcement mechanisms such as the imposition of sanctions. Companies now have little choice but to

[1] Court of Justice of the European Union, Press Release No. 117/15, Luxembourg, 6 October 2015.

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31).

[3] *Id.*

begin planning how to best ensure ongoing compliance in anticipation of the heightened safeguards that will likely be imposed by the New Safe Harbor regime, and keeping in mind that there is no assurance the EU will not enforce the current requirements of the EU Data Protection Directive against companies who are no longer entitled to rely on the Safe Harbor Framework and are therefore noncompliant. Accordingly, companies should first assess their data transfer operations and risk profile in light of the ruling and seek counsel on alternative mechanisms for compliance with the EU Data Protective, including the following:

1. The establishment of Binding Corporate Rules (BCR) for transfers of data, which refer to internal rules such as Codes of Conduct used by multinational companies to guarantee adequate safeguards for data protection.[4]
2. The adoption of Model Contracts, or data protection clauses (which must be executed each time a company needs to transfer personal data). The Commission has thus far issued model standard contractual clauses for both transfers from data controllers to non-EU/EEA data controllers and transfers to processors established outside the EU/EEA.[5]

Alternative strategies may also be considered as companies await further rulemaking. For example, companies may choose to restructure their data processing operations by implementing standalone European operations so that the processing of U.S. and European data is segregated. This is an expensive and time consuming approach, however, and one that raises the specter of the "splinternet." A less extreme approach involves putting in place data storage solutions which modify data pathways in order to minimize the risk of transfers which would violate the EU Data Protection Directive. Companies who outsource data processing operations should also be vigilant in ensuring that the third party vendor agreements are compliant with the post-safe harbor regime.

These ad hoc approaches to ensuring compliance are likely to be costly, difficult and inconvenient to implement. However, until the New Safe Harbor is adopted, U.S. companies that transfer personal data collected in the EU/EEA to the U.S. or other non-EU/EEA jurisdictions have little choice but to do their best to ensure compliance with the EU Data Protective and should keep a close eye on developing policies and prospects for the New Safe Harbor. Gaining a better understanding of the European data protection regulatory framework and being ready to take advantage of the New Safe Harbor when adopted may prove critical to successfully doing business in Europe.

***

The foregoing is merely a discussion of the New Safe Harbor Directive. If you would like to learn more about this topic or how Pryor Cashman LLP can serve your legal needs, please contact or Robert J. deBrauwere at (212) 326-0418, rdebrauwere@pryorcashman.com, Jeffrey C. Johnson at (212) 326-0118, jjohnson@pryorcashman.com or Francesca N. Djerejian at (212) 326-0138, fdjerejian@pryorcashman.com.

[4] http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm

[5] http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm