WILLKIE FARR & GALLAGHER LLP

NEW YORK WASHINGTON HOUSTON PARIS LONDON FRANKFURT BRUSSELS MILAN ROME

CLIENT MEMORANDUM

European Court of Justice Declares EU-U.S. Safe Harbor Framework Invalid in a Landmark Decision – What to Do Now?

October 7, 2015

AUTHORS

Dr. Christian Rolf | Francis M. Buono | Patrick Wacker

Overview

On October 6, 2015, the European Court of Justice (the "ECJ") declared invalid[1] the longstanding decision of the European Commission (the "Commission") that compliance with the EU-U.S. Safe Harbor ("Safe Harbor") framework is a legitimate basis for the transfer of personal data from the European Union to the United States. The impact of this decision will be dramatic, since companies that previously relied on the Safe Harbor to justify such transfers may violate EU data protection laws unless they implement alternative transfer compliance mechanisms. Such alternative mechanisms include EU model contract clauses, the use of Binding Corporate Rules ("BCRs"), explicit consent of the data subject, and reliance on various exceptions under certain national data protection laws.

The Safe Harbor Framework

EU data protection law[2] generally prohibits transfers of personal data to any country outside the European Economic Area that does not provide an "adequate" level of data protection. The July 26, 2000[3] decision of the Commission permitted the

1 Decision of October 6, 2015 – Case No C-362/14.

2 EU Directive 95/46 EC October 24, 1995.

transfer of personal data from a Member State of the European Union to U.S. companies that had agreed to comply with certain data protection principles regarding the usage, disclosure, and protection of personal data broadly based on the EU model. Although the Safe Harbor model is widely used by over 5,000 U.S. companies to facilitate transfers of personal data between the European Union and the United States, the framework has been subject to criticism by EU data protection regulators in recent years in the wake of the revelation of U.S. and other government surveillance programs following publication of classified material by former NSA contractor Edward Snowden.

The Case: Maximilian Schrems against the Irish Data Protection Commissioner

Maximilian Schrems is an Austrian citizen and subscriber to Facebook. As a European user of Facebook, he had to agree to the general business terms of Facebook's Irish subsidiary, which operates the Facebook service throughout Europe. He filed a complaint with the Irish Data Protection Commissioner arguing that even with respect to companies that comply with the Safe Harbor framework, the United States does not provide for an adequate level of data protection, as U.S. authorities (in particular the NSA) may access and process his personal data that Facebook is forwarding to its servers in the United States. The Irish Data Protection Commissioner rejected the complaint on the grounds that because the Safe Harbor rules (which Facebook adopted) were deemed by the Commission to ensure an adequate level of data protection, national data protection authorities are obliged to follow such decision. Mr. Schrems then took his claim to the Irish High Court, which submitted the matter to the ECJ. Prior to the decision of the ECJ, the court's Advocate General, or chief legal advisor, had issued an opinion[4] that the decision of the Commission approving the Safe Harbor framework does not prevent national data protection authorities from performing an independent assessment as to whether the level of data protection in a non-EU country is adequate. Further, the Advocate General also expressed his opinion that the Commission's Safe Harbor decision is invalid altogether.

The Decision of the ECJ

The ECJ agreed with the Advocate General's position and declared the 2000 decision of the Commission approving the Safe Harbor framework invalid. It based its decision principally on a finding that the United States is *not* able to provide for an adequate level of data protection even using the Safe Harbor, because the Safe Harbor essentially has too many loopholes. For example, the ECJ cited with concern the fact that the Safe Harbor may not apply if "national security, public interest or law enforcement requirements" are at stake, and that U.S. public authorities are not required to comply with the Safe Harbor requirements at all.[5]

---

[3] EC 2000/52.

[4] Opinion of September 23, 2015.

[5] The ECJ did not address the issue whether the Safe Harbor rules by themselves provide for such adequate protection, but argued that the Safe Harbor rules restrict only corporations and not U.S. authorities.

U.S. and EU Reactions

The Federal Trade Commission (the "FTC"), the Department of Commerce, and the White House released statements on the ruling. FTC Chairwoman Edith Ramirez issued a short statement that the FTC is reviewing the decision and evaluating its impact. Ramirez also said that the FTC will continue to work with its "European colleagues to develop effective solutions that protect consumer privacy with respect to cross-border data transfers." Secretary of Commerce Penny Pritzker expressed disappointment in the decision and encouraged reaching an agreement to an updated Safe Harbor framework as soon as possible. White House Press Secretary Josh Earnest told reporters, "We believe this decision was based on incorrect assumptions about data privacy protections in the United States. There is concern about the economic consequences of this particular ruling."

The Vice President and a Commissioner of the Commission released a statement on the court's ruling. Both said the Commission must ensure the continuation of transatlantic data flows and that clear guidance for national data protection authorities on how to deal with data transfer requests to the United States in the wake of the ECJ decision will be forthcoming. They also acknowledged the importance of continuing to negotiate a renewed Safe Harbor framework with the United States.

The Article 29 Working Party (an EU advisory body comprised of representatives of the data protection authorities in EU countries) plans to meet later this week to discuss the implications of the ECJ's decision and issue guidance. German and other EU authorities will also be meeting independently in their countries at the end of this week to discuss next steps.

Implications and What Companies Should Do Now

As the ECJ provided no transition period for its ruling, its decision is effective immediately for all companies. Thus, unless specifically authorized by national data protection authorities, the Safe Harbor is no longer a legitimate basis for the transfer of personal data from the EU to the United States, including transfers between EU companies and their U.S. customers or vendors, and intra company transfers between an EU and U.S. subsidiary and parent or different subsidiaries. However, it is important to stress that EU data flows to the United States are not per se unlawful. Rather, companies should analyze which of the following alternative mechanisms they will use instead of the Safe Harbor to justify permitting transfers of personal data from the EU to the United States going forward

- **The EU Model Contracts** provide a set of standard clauses, approved and published by the Commission, for the transfer of personal data between an EU data controller and a U.S. data controller or between an EU data controller and a U.S. processor (i.e., vendor) (http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm). However, model contract clauses cannot be altered. The current advantage of this alternative is that the model clauses are based on a valid decision of the Commission which must be presumed to be lawful.

- **Binding Corporate Rules** are internal company regulations governing how the flow of personal data is organized and the rights of concerned individuals are protected. BCRs can be adopted to the specific needs of the company,

but are subject to governmental approval, which is complicated and time-consuming – indeed, it has typically taken years for companies to complete the BCR approval process, and only a small number of companies have adopted BCRs. In particular, the German authorities are currently very reluctant to approve BCRs.

- **Clear Notice and Unambiguous Explicit Consent** of the individual whose personal data is being transferred. Consent can be difficult to manage in certain circumstances, however, and some EU countries' data protection authorities (e.g., Germany) discourage use of consent in certain situations.

- **Statutory Exceptions** may apply in certain countries that permit transfers of personal data if specified conditions are met. However, these exceptions are very fact-specific and are often narrowly construed by EU regulators.

As each of these alternative transfer mechanisms has certain pros and cons, they should all be carefully considered, with counsel, for each situation, based on the particular data, organizations, and purposes of the transfers at issue.

We expect regulators on both sides to continue their ongoing negotiations to update the Safe Harbor framework, and it is possible that the ECJ's ruling will expedite these discussions and result in a modified Safe Harbor approach that will again be able to legitimize transfers of personal data from the EU to the United States.

If you have any questions concerning the foregoing or would like additional information, please contact Dr. Christian Rolf (+49-69-79302-151, crolf@willkie.com), Francis M. Buono (202-303-1104, fbuono@willkie.com), Patrick Wacker (+49-69-79302-127, pwacker@willkie.com), or the Willkie attorney with whom you regularly work.

Willkie Farr & Gallagher LLP is an international law firm with offices in New York, Washington, Houston, Paris, London, Frankfurt, Brussels, Milan and Rome. The firm is headquartered at 787 Seventh Avenue, New York, NY 10019-6099. Our telephone number is (212) 728-8000 and our fax number is (212) 728-8111. Our website is located at www.willkie.com.

October 7, 2015