ROPES & GRAY

ALERT

Privacy & Data Security

September 25, 2015

EU - US Personal Data Transfers - Safe Harbor Under Threat

Attorneys
Rohan Massey
Heather Egan Sussman
James S. DeGraw
Mark Barnes

Following a private challenge by an Austrian law student to the storage by Facebook of his personal data on servers located in the United States, the EU Advocate General (the "Advocate General") has filed an advisory opinion with the European Court of Justice (the "Court of Justice") recommending that the EU-U.S. safe harbor of privacy principles (Commission Decision 2000/520/EC) (the "Safe Harbor") be invalidated. The Safe Harbor is a framework developed by the U.S. Department of Commerce and European Commission (the "Commission") that permits the transfer of personal data from the EU to the U.S. if the receiving entity adheres to certain privacy protection principles. The Safe Harbor thereby provides a legal basis to transfer data to the U.S. notwithstanding the fact that the Commission has found that the data privacy laws of the United States do not otherwise offer an adequate level of protection for personal data. Therefore, firms that are, or are planning to become, Safe Harbor certified should closely monitor whether the Court of Justice adopts the Advocate General's opinion and consider preparing for a situation in which the Safe Harbor is invalidated.

According to the Advocate General, revelations stemming from the Edward Snowden matter have recently brought to light the existence of large-scale information-gathering programs in the United States that are inconsistent with the privacy protections of the EU Data Protection Directive (Directive 95/46/EC) (the "Data Protection Directive"). As a result, the Safe Harbor scheme can no longer guarantee EU residents' rights to privacy and should therefore be found invalid and immediately suspended.

Over 4,000 companies rely on the Safe Harbor to transfer personal data to the U.S. "Personal data" is defined broadly under the Data Protection Directive "to include any information relating to an identified or identifiable natural person," meaning that even relatively mundane information like payroll and company phone books can be considered personal data. Given this broad definition of "personal data," companies that send personal information from the EU to the U.S. (including EU companies that use servers located in the U.S.) often rely on the Safe Harbor for their everyday operations.

As background, the proceeding on which the Advocate General commented is between an Austrian law student and the Irish Data Protection Commissioner (the "Commissioner"). The law student brought the proceeding to the High Court of Ireland (the "High Court") based on the Commissioner's refusal to investigate his complaint that Facebook Ireland Ltd keeps subscribers' personal data on servers located in the U.S. According to the High Court the issue is not the fact that Facebook stores Europeans' personal data in the U.S., but rather the fact that the Commissioner has not reconsidered its determination that the Safe Harbor framework ensures adequate privacy protection following Snowden's disclosures that U.S. authorities "can have access on a mass and undifferentiated basis to personal data of the population living in the territory of the European Union." Accordingly, the High Court stayed proceedings to ask the Court of Justice whether EU member states' national supervisory authorities are bound by the Safe Harbor to find that U.S. entities that are Safe Harbor certified ensure adequate protections, or whether, in light of the factual developments since the Safe Harbor was created in 2000, national supervisory authorities can conduct their own investigation into the adequacy of U.S. data privacy protections.

The Advocate General's opinion on these questions is not binding on the Court of Justice. However, such opinions are followed more often than not. Here, the Advocate General concluded that the Safe Harbor does not prevent a national supervisory authority from investigating a complaint that the U.S. does not ensure an adequate level of protection of personal data and, where appropriate, suspending the transfer of that data. The Advocate General

reasoned that residents of the EU have a right to the protection of their personal data, and if an investigation concludes that there are strong indications of a breach of this right due to failure to ensure such protection, the cognizant national supervisory authority must be able to suspend the transfer of data to a third country irrespective of restrictive condition laid down in an adequacy decision of the Commission (*e.g.*, the Safe Harbor). The Advocate General elaborated that whether or not a country "ensures" an adequate level of protection must be considered in the present – *i.e.*, at the time of a challenge – not only at the time of passing an adequacy decision.

Importantly, the Advocate General also addressed whether, if such an investigation had properly been conducted, the Safe Harbor could have been found valid, and concluded that the Safe Harbor should have been found invalid. This conclusion was based in part on the court's finding that personal data transferred by entities such as Facebook Ireland to the U.S. are capable of being accessed by the NSA and by other U.S. security agencies in the course of a mass and indiscriminate surveillance and interception of such data. Accordingly, the Advocate General concluded that under current circumstances the Safe Harbor cannot ensure an adequate level of protection of the personal data transferred from the EU to the U.S.

Notably, the Advocate General commented that on the basis of the allegations made, Facebook itself had not breached the requirements of the Safe Harbor. Rather, Facebook's disclosure of personal information to the U.S. authorities in order to comply with U.S. legislation would be consistent with the principles of the Safe Harbor. Nevertheless, the Advocate General found that this provision of the Safe Harbor itself is derogation from the EU Data Protection Directive's requirement that distribution of personal data must be limited to what is strictly necessary and is reason enough to invalidate the Safe Harbor.

To date, the EU has stopped short of suspending the Safe Harbor and is instead conducting a review of the Safe Harbor scheme. Specifically, the U.S. and EU authorities are negotiating an umbrella agreement that may assist in clarifying the situation addressed by the Advocate General. Similarly, the EU's new General Data Protection Regulation is currently nearing final form and should shed light on the ability to transfer personal data from the EU to the U.S. However, it is possible that the Court of Justice will align itself with the Advocate General's opinion prior to a change in the law or other agreement being reached, and the Safe Harbor could thereby be suspended in the interim.

Meanwhile, firms that are Safe Harbor certified should analyze which of their current personal data transfers from the EU to the U.S. rely on the Safe Harbor. Such firms should consider undertaking an analysis of whether these personal data transfers could take place under an alternative legal basis. Possible alternatives may include the use of the Commission's model contractual clauses, establishing "binding corporate rules" that permit transfers of personal data within a multinational corporation or international organization, or obtaining the "unambiguous consent" of the data subject to the transfer of personal data. Firms that are not yet Safe Harbor certified but that were considering undertaking such certification should analyze the feasibility of relying on one or more of these alternative mechanisms of transfer. Because each legal basis for transfer of personal data from the EU to the U.S. requires adhering to specific requirements, firms should not underestimate the amount of time required for such analyses.

[The case before the Court is Justice is titled, *Maximillian Schrems v. Data Protection Commissioner*, case number C-362/14]

If you have any questions about this alert, please contact Rohan Massey, Heather Sussman, James DeGraw, Mark Barnes, or any other member of Ropes & Gray's leading privacy & data security team.