European Court Rules That Safe Harbor Does Not Legitimize Personal Data Transfer

Cyber Law and Data Protection Alert | October 13, 2015
By: Randy M. Friedberg and Michael Jervis

On October 6, 2015, the Court of Justice of the European Union (CJEU) ruled in Schrems v. Data Protection Commissioner that the EU-US Safe Harbor for personal data transfers is not valid as it does not provide adequate protection for personal data. This ruling has significant implications for U.S. companies doing business in Europe.

The Safe Harbor Framework

In general, transfers of personal data from countries in the European Economic Area (EEA) to outside countries are prohibited unless the outside country has adequate personal data protection measures in place. Many non-EU countries, including Canada and Switzerland, were found to have such adequate protections. The United States was not. In response, in 2000, the U.S. and EU negotiated the Safe Harbor framework, and the European Commission then ruled that the framework provided an adequate level of protection. This action enabled U.S. to self-certify compliance with the Safe Harbor framework, allowing them to legally transfer personal data from the EU to the U.S. That ability to self-certify is no longer available.

The Schrems Ruling and its Implications

Schrems is an Austrian privacy activist and Facebook user. He filed a complaint against Facebook Ireland claiming it did not comply with European personal data protection rules. The Irish Data Protection Commission found it did not have authority to consider his complaint because Facebook certified its compliance with the Safe Harbor, and the European Commission had already ruled that the Safe Harbor provided adequate protection. Schrems challenged this ruling with the Irish High Court, which certified to the CJEU the question of whether the Data Protection Commission could nonetheless examine Facebook’s privacy protection despite the European Commission’s existing ruling. In a decision notable both for the speed in which it came down as well as for its holding, which goes far beyond the specific question presented, the CJEU eviscerated the Safe Harbor as it currently exists. It did so in two distinct but related ways.

The CJEU’s first key holding was that an individual member state’s data protection commission had authority to investigate a company’s protection of personal data, even though the European Commission had already ruled that there was an adequate level of protection. The CJEU next considered whether the European Commission’s ruling that the Safe Harbor provided an adequate level of protection was correct. It found that it was not; the Safe Harbor does not provide adequate protection because U.S. law requires companies to turn over personal data upon request for national security purposes that go beyond those seen as legitimate under European law.
As a result of this ruling, the Safe Harbor framework is no longer valid, and transfers of data between the EU and U.S. which were based solely on the Safe Harbor are no longer legitimate. The short term ramifications of this ruling will depend on the reactions of regulators in the various European Union Member States. It is possible that some Member States, such as Germany which has long been critical of the Safe Harbor, may suspend all personal data transfers to the US. Even those that don’t will likely receive a sharp increase in the number of administrative complaints against U.S. companies involving personal data transfers.

**Alternative Methods for Compliance**

Fortunately, all is not lost. There are three other ways to comply with European data privacy law including consent, binding corporate rules and model contracts. However, all have potential pitfalls.

Directive 95/46 of the EU also allows for transfer of personal data with the “unambiguous consent” of the individual. This alternative approach may work but for the consent to be valid it needs to be explicit and fully and clearly informed. Facebook Ireland, for example, includes such consent in its terms of use. However, some EU data protection authorities do not look upon this method favorably, particularly where there is a significant power imbalance between the parties. Consent is even more questionable when applied retroactively.

Binding Corporate Rules (BCRs), allows for the “intragroup transfers” of data. However, BCRs require approval from the relevant country’s data protection commission, which can take upwards of 18 months. Additionally, BCRs may be vulnerable to the same arguments made against the Safe Harbor framework, to the extent that companies still must comply with U.S. national security rules not seen as legitimate under European standards.

Model contracts are another possible mechanism for compliance. The European Commission has provided standard model clauses which can be incorporated into agreements between exporting and receiving entities. These clauses are designed to ensure adequate protection of the data. However, the model clauses are also potentially vulnerable to the same attacks as are the BCRs.

In addition to the existing compliance methods, having recognized some of the infirmities noted by the CJEU, the U.S. and EU have been working towards agreement on a new “Safe Harbor II” for the past two years. When and if that is eventually implemented, it may again provide a streamlined method for compliance. At the moment, however, there is no projected deadline for finalization of the new Safe Harbor. Further, the Schrems decision indicates that more stringent compliance with EU law will be required if such a Safe Harbor II is to be deemed adequate protection by the court. This may delay its implementation. Regardless, the first part of the CJEU ruling indicates that any new Safe Harbor will be subject to scrutiny on a country-by-country basis.

**Where Do We Go From Here**

In light of this development, companies doing business in the EU, particularly those previously relying on the Safe Harbor, must promptly take affirmative steps to evaluate their operations and determine compliance with EU laws to ensure continued transfer of data.
Initially, companies should consider whether transfers of personal data across EEA boundaries are truly necessary. If such transfers are occurring simply because, for example, redundant backup servers are on opposite sides of the border or because of the location of third-party cloud computing server farms, it may be worth considering whether operations can be consolidated either entirely outside or inside EEA borders.

Where it is decided that cross-border transfers are required, alternative compliance methods should be considered. For those entities transferring data only within their own company, BCRs may be an appropriate compliance method. For those transferring data to and from third parties, model contracts may be considered. Additionally, entities should continue closely monitoring the reactions of member state data protection authorities.

As some EEA states inevitably use this ruling to more strictly limit data transfers, while others take a more lenient approach and allow for a grace period to respond to the ruling, we will continue to monitor and analyze whether certain member states within the EEA provide a more hospitable environment for locating operations.

For additional information on this matter, contact Randy Friedberg (friedbergr@whiteandwilliams.com | 212.714.3079), Michael Jervis (jervism@whiteandwilliams.com | 215.864.7042), or another member of the Cyber Law and Data Protection Group.

This correspondence should not be construed as legal advice or legal opinion on any specific facts or circumstances. The contents are intended for general informational purposes only, and you are urged to consult a lawyer concerning your own situation and legal questions.