Three Ways You May Be Affected by the EU Safe Harbor Ruling

hugheshubbard.com — eALERT

Earlier this month, the European Union Court of Justice invalidated the U.S. Safe Harbor, a mechanism that permitted the transfer of personal data from the European Economic Area to the United States. The Court's ruling is expected to affect companies (i) that send personal data from Europe to the United States, (ii) that store European information in the Cloud, and (iii) that use third parties who do either of the above.

Background

The EU Data Protection Directive prohibits the transfer of personal data from the European Economic Area to non-member countries, absent certain defined exceptions. For the past 15 years, the principal exception for the United States has been the Safe Harbor. The Safe Harbor permits U.S. companies to transfer personal data by self-certifying to the Department of Commerce that they have taken reasonable precautions to protect personal information. Approximately 4,500 U.S. companies have used this procedure to transfer data from Europe to the United States.

In 2013, Maximilian Schrems lodged a complaint with the Irish data protection authority, alleging that data he provided to Facebook had been sent from Facebook's Irish subsidiary to computer servers in the United States. In the wake of Edward Snowden's claims concerning the data-gathering activities of the National Security Agency, Mr. Schrems argued that the United States offered no real protection of his data. The Irish data protection authority rejected Mr. Schrems's complaint on the ground that the EU Commission's Safe Harbor decision had found that the U.S. Safe Harbor program provided adequate protection for personal data.

On October 6, 2015, the EU Court of Justice declared the Commission's Safe Harbor decision invalid. The Court observed that the Safe Harbor does not apply to "U.S. public authorities" and that those who self-certify under the Safe Harbor scheme are "bound to disregard, without limitation, the protective rules laid down by that scheme where they conflict with" U.S. national security or law enforcement requirements. The Court held that permitting public authorities to have generalized access to data - without limits on such access or the data's subsequent use - compromises the fundamental right to privacy. It directed the Irish authority to reconsider Mr. Schrems's complaint and decide whether to suspend the transfer of the European Facebook data to the United States.

Discussion

Despite the initial furor over the Court's ruling, it is not yet clear how current business practices may be required to change. The U.S. Commerce Department has issued an advisory regarding the *Schrems* ruling, but is continuing to administer the Safe Harbor program while it awaits clarity from Europe. The data protection authorities in each EEA country are bound by the Court's ruling, but there is no telling how they will enforce the ruling, and there have been calls on both sides of the Atlantic for practical considerations to prevail. There may be a grace period to allow companies to adopt other measures permitting data transfers, such as model contracts and binding corporate rules. There may also be a compromise that would allow the Safe Harbor program to continue with additional data protections. The U.S. government has been negotiating a new Safe Harbor with the EU Commission since the Edward Snowden revelations in 2013, and both sides have recently indicated that they were close to agreement.

In light of the *Schrems* ruling and the uncertainty that it has created, companies should be reviewing their data-handling practices. The ruling affects data transfers under the Safe Harbor, including:

1. Direct Transfers of EU Personal Data to the United States
2. Transfers of EU Personal Data to the Cloud
3. Transfers of EU Personal Data by Agents and Vendors

Direct Transfers of EU Personal Data to the United States
The *Schrems* ruling most obviously affects the direct transfer of personal data from Europe to the United States. In reviewing their current practices, companies should keep in mind that the concept of personal data is much broader in Europe than it is in the United States, and includes virtually any identifying information. Human resources information, sales data, and customer information may all fall into this category.

Transfers of EU Personal Data to the Cloud
The transfer of personal data to the Cloud may also be implicated if the Cloud servers are located in the United States. In recent years, companies and their employees have begun using Cloud vendors to host email, track sales activities, store payroll and other human resources data, and enable employee collaboration on documents. Companies should review arrangements with Cloud vendors to determine whether their European data is being stored on servers in the United States.

Transfers of EU Personal Data by Agents and Vendors
Even if a company is not directly transferring data from Europe to the United States, its third-party consultants, tax advisors, or data vendors may be doing so on the company's behalf. Companies should also review these arrangements to ensure that third parties are not transferring company data from Europe to the United States without adequate protections in place.

Next Steps

Companies should not wait to begin reviewing their data-handling procedures. There is optimism that a new Safe Harbor arrangement will be reached soon, but there is no way to predict how long this might take, what interim measures may be agreed upon, or whether it will happen at all. There is also no telling how vigorously European data protection authorities may seek to enforce their individual data protection laws.

Adding to the current uncertainty is the expectation that there may soon be a new data protection regime. The EU Commission and the EU Parliament have been negotiating a new General Data Protection Regulation, which would supersede the Data Protection Directive. The General Data Protection Regulation is expected to impose stricter data protections, which may complicate efforts to reach a new Safe Harbor agreement.

There is no reason to overreact to the *Schrems* ruling, but prudent companies will want to be prepared for what might come next. Companies should identify any European data that is being transferred to the United States and begin considering whether they need to adopt alternative measures for transferring that data to the United States.

This Advisory is for informational purposes only and is not intended as legal advice. For more information on the subject of this advisory or Hughes Hubbard's eDiscovery practice, please contact any of the following attorneys:

Seth Rothman
(212) 837-6872
seth.rothman@hugheshubbard.com

Charles Cohen
(212) 837-6856
charles.cohen@hugheshubbard.com

Ignatius Grande
(212) 837-6120
ignatius.grande@hugheshubbard.com

eDiscovery Practice

October 2015

Hughes Hubbard & Reed LLP | A New York Limited Liability Partnership
One Battery Park Plaza | New York, New York 10004-1482 | +1 212-837-6000