Bloomberg BNA

WORLD DATA PROTECTION REPORT >>>

News and analysis of data protection developments around the world.
For the latest updates, visit www.bna.com

International Information for International Business

VOLUME 16, NUMBER 6 >>> JUNE 2016

European Union

Prohibition on Data Transfers to the U.S. Turns Into Protectionism

By Lokke Moerel

European companies that transfer data to the U.S. may find themselves deep in a legal minefield. The Irish privacy supervisory authority has just issued a draft decision finding that European citizens do not have sufficient rights to sue the U.S. government if the transfer takes place on the basis of the European Model Contracts . Negotiating a new political agreement between the European Commission and the U.S. seems to be the only solution, but it may be about time to ask whether Europe is going too far in its demands.

Lokke Moerel, is senior of counsel at Morrison & Foerster LLP in Berlin. Moerel specializes in data protection and information/communications technology (ICT) law, and is professor of global information, communications and technology law at Tilburg University in the Netherlands.

Earlier, the European Court of Justice ruled that the Safe Harbor agreement between the EU and the U.S. was not a valid basis on which to transfer data from European companies to U.S. companies . As a result of this judgment, European companies could no longer transfer personal data to U.S. companies that had joined the Safe Harbor program and had thereby been considered "safe" by the Commission. To re-legitimize their transfers, these companies implemented alternative transfer instruments, such as entering into the European Model Contracts.

The complaint by Max Schrems, a noted European privacy activist, which gave rise to the judgment of the European Court was referred back to the Irish authority, who then had to assess whether Facebook Inc. could rely on the European Model Contracts for its data transfers. That question was now answered negatively.

Because the Irish authority cannot itself nullify the Model Contracts, it has referred the case to the Irish court. If that court deems the objections valid, it will refer the case to the European Court to nullify the Commission's decisions authorizing the use of the European Model Contracts. This process would take at least two years.

If the European Model Contracts are invalidated as well, European companies will be left with no practical instruments through which to legitimize their data transfers to the U.S. Ceasing transfers may be the only option.

The only positive news is that the Irish authority has not suspended Facebook's data transfers pending the investigation. For the time being, therefore, companies can still use the Model Contracts. However, a number of other European supervisory authorities have announced that they will not grant new authorizations for international transfers based on the Model Contracts. It is also quite possible that other EU authorities will suspend transfers based on the Model Contracts until the court has ruled on the matter.

If the European Model Contracts are invalidated as well, European companies will be left with no practical instruments through which to legitimize their data transfers to the U.S.

The solution should come from the political agreement reached between the Commission and the U.S. on a new data transfer arrangement: the EU-U.S. Privacy Shield (16 WDPR 02, 2/25/16). But on this front, there is no good news to report, either. The joint European privacy supervisory authorities (Working Party 29) and the European Parliament have announced that they find the conditions of the Privacy Shield agreement insufficient in key areas—i.e. generic surveillance is still possible and the redress mechanisms against the U.S. government are not adequate—and urged the Commission to renegotiate the agreement with the U.S. (16 WDPR 06, 6/28/16). The Working Party 29 have even threatened to bring suit at the European Court should the Commission adopt the Privacy Shield agreement in its current form.

A committee of member state representatives will also issue advice, which the Commission must take into account as much as possible. This committee is apparently unable to reach an agreement, given the fact that two additional meetings have been scheduled to agree upon an advice. While the Commission can ignore the advice of the Working Party 29 and Parliament, under these circumstances it is hard to imagine that the Commission would dare to adopt the Privacy Shield agreement unaltered.

This means renegotiations with the U.S., with the main aim to further restrict the U.S. government's powers of bulk surveillance and improve legal redress for EU citizens. At first sight, these demands seem quite reasonable, but is that really the case? For starters, these requests would require changes to the U.S. Constitution and a fundamental change in the U.S. legal system.

Prohibiting data transfers to the U.S. alone appears to apply a double standard that is beginning to resemble an impermissible restriction on trade.

European privacy law further prohibits transfers of data to countries that do not provide "adequate protection" of personal data. What is considered adequate is also determined by the protection the EU provides to its own citizens. There are several recent reports available concluding that some member states permit bulk surveillance of personal information as well, and that the legal remedies afforded to individuals to enforce their privacy rights do not meet the requirements of the European Convention on Human Rights (ECHR). Indeed, there are currently three cases pending before the European Court of Human Rights against the U.K., arguing that the general surveillance powers of the U.K. intelligence services violate the right to privacy of Article 8 ECHR.

Similar concerns could be raised in respect of the surveillance powers and redress mechanisms of other major European trading partners, such as China, Russia, Brazil and India. Prohibiting data transfers to the U.S. alone appears to apply a double standard that is beginning to resemble an impermissible restriction on trade and may be viewed no differently than the efforts at data localization by countries such as Russia.

Puzzling is also that on June 3, 2016, the EU and U.S. signed an umbrella agreement, implementing a data protection framework for criminal law enforcement cooperation. The question raises why the EU and U.S. apparently can agree on what the appropriate data protection safeguards are when data are transferred for their own law enforcement purposes—which concerns the most sensitive data and may have serious ramifications for individuals—but yet find it impossible to come to a consensus on what the appropriate safeguards should be when seemingly less sensitive data are transferred by companies. It begs the question whether double standards are applied here out of self-interest on both sides of the Atlantic.

   ISSN 1473-3579