BRACEWELL

INSIGHTS

Dangerous Waters in the Safe Harbor: The EU-U.S. Safe Harbor for Data Transfer is Safe No More

November 16, 2015

*By: **Jeffrey B. Andrews**, **Constance Gall Rhebergen** and **Brad Y. Chin***

On October 6, 2015, the European Court of Justice (ECJ), abolished the 15 year old Safe Harbor agreement between the EU and the U.S. Over 5,000 businesses have relied on the Safe Harbor to receive personal data from EU member countries. While this creates a massive upset on how US companies do business, there are clear guidelines on actions to take in order to comply with the EU Data Protection Directive going forward.

The ECJ's invalidation of the EU-U.S. Safe Harbor disrupts every business that transfers personal data collected from residents in the EU to the U.S. This decision impacts global data flows and raises jurisdiction issues over personal data for multinational companies that operate data centers in the EU, rely on cloud based storage by European subcontractors, and transfer data intra-company from EU subsidiaries.

Companies in the U.S. can no longer transfer EU data to U.S. servers without adequate protections. Such companies will not be able to store, process, or transfer data from EU citizens using the Safe Harbor Framework through an annual self-certification with the U.S. Department of Commerce. Instead, EU national regulatory authorities will now investigate data transfer to determine whether companies comply with EU law under an "adequate level of protection" standard.

After the end of January 2016, companies that violate the ruling will risk significant EU civil and criminal fines and face orders to halt data transfers. In some EU member states, officers and employees of a non-compliant company may face personal criminal liability for a failure to comply.

Companies will face huge costs to remove personal data from Europe or implement alternative processing in the EU in order to comply. Three main methods for validating a transfer of data of an EU data subject include 1) obtaining personal consent to data transfers, 2) implementing binding corporate rules for intra-company transfer, and 3) using model contract clauses that incorporate the EU Directives principles. While personal consent is one option, there are many challenges to this approach to ensure validity. A more cost effective solution is to enter into data transfer agreements based on EU approved Commission's model contract clauses. These are essentially contracts that allow companies to transfer data out of the EU by going through different approval processes. Large internet and technology companies, global multinationals, and cloud providers that employ model contract clauses will ensure meeting the new EU data protection obligation in a cost-effective manner.

Similarly, all companies that transfer data from Europe to the US need to take action to ensure compliance under the new regulatory system. Such companies should consider the differences in model contract clauses between a data processor (a supplier that processes personal data) and a data controller (a customer that determines the purposes for the processing of data) in order to be in compliance. The distinction will consider the kind of personal data to be processed, the method and frequency of the transfer, and whether to utilize an electronic of automated means of processing.

All companies with European subsidiaries that transfer data to the US would benefit from a brief audit of their corporate rules to ensure compliance under the new regulatory system in the event reliance was previously on the Safe Harbor exemption. The EU Directive recognizes the implementing of binding corporate rules for intra-company transfer as another prong for proving compliance.

For further information on analysis and actions to ensure compliance, please contact any of the authors.