FUNKHOUSER VEGOSEN LIEBMAN & DUNN LTD.

Legal Update

November 2015

THE STORM IN THE SAFE HARBOR

By Peter T. Berk

Recently, the Court of Justice of the European Union (CJEU) invalidated a major method thousands of companies used to comply with European Union (EU) law when storing and processing personal data from the EU. U.S. businesses need to be mindful of their actions in this time of uncertainty as decisions made now may need to be changed later and inaction may result in unintended violation of the EU's strict privacy laws. Authorities in the EU and the U.S. Department of Commerce are currently working on a solution, but we don't have one yet.

The EU-U.S. Safe Harbor

In July 2000, the European Commission made a decision approving transfers of personal data between the EU and the U.S. pursuant to what is known as the "Safe Harbor" program. Under that decision, the program was determined to provide the adequate protections required under European law for data transferred outside the EU. The Safe Harbor consisted of certain requirements, which included, among others, notice to users about the disclosure and use of their data, providing users with choice about the disclosure of their information, giving users the ability to access and correct their information, and ensuring the security of information.

A company that complied with all of these requirements would then submit a self-certification form to the U.S. Department of Commerce indicating that it complies with all of the Safe Harbor requirements. That certification was required every year. Upon submitting the certification, the company would be listed as certified on the Safe Harbor website.

Certified companies could rely on that certification and continued compliance with the requirements to protect them against claims from the EU that they were not complying with EU law on protecting personal information.

The Court of Justice of the European Union Invalidates the Safe Harbor

In June 2013, a European Union citizen, Maximillian Schrems, made a complaint with the Data Protection Commissioner against Facebook that it was not sufficiently protecting his personal information when it was sent from Ireland, where he lived, to Facebook's servers in the United States. Schrems claimed that the revelations made by Edward Snowden about the U.S. National Security Agency's PRISM surveillance program made the transfer of his data to the U.S. improper under EU privacy law.

FVLD®

The Commissioner took the complaint, but determined that there was no evidence that the NSA looked at Schrems' data. Further, because of the directive finding that the Safe Harbor was sufficient, the transfer was proper and the Commissioner had no ability to investigate the adequacy of protection further.

The CJEU decided the opposite. Among other things, the CJEU stated that (a) the Commissioner had the ability, and the duty, to investigate claims that data was being improperly transferred, or that a previously approved transfer method was no longer in compliance with EU law, and (b) the directive approving the Safe Harbor program, given Snowden's disclosures, was no longer valid. Thus, the CJEU eliminated the existing Safe Harbor scheme as a protected way for companies to transfer data from the EU to the United States in compliance with EU law.

The Current Situation

What companies currently should, and in the future will be required to, do regarding data transfers from the EU to the U.S. is unclear, but manageable. While the U.S. Department of Commerce is continuing to operate the Safe Harbor system, and its requirements do ensure high standards of privacy, that program no longer provides the assurance of compliance that companies are looking for, at least in its current form.

The relevant local privacy authorities in the EU, who are part of a group called the Article 29 Working Group, have stated that they will not initiate complaints themselves regarding transfers from the EU to the U.S. until the end of January, 2016. They are doing so to allow the EU and the U.S. to attempt to negotiate and gain approval for a new system. While the authorities will still need to investigate complaints brought by individuals, the refusal to institute actions themselves should calm some fears.

Further, there are currently other methods for complying with EU privacy laws that were not directly impacted by the CJEU's ruling. These include Binding Corporate Resolutions (BCRs) that have been approved by the EU for U.S. companies sharing data with affiliates and subsidiaries in the EU, and Model Contract Clauses for companies that are sharing data with unaffiliated companies. Companies using BCRs and Model Clauses should not alter the language and should ensure that (a) all appropriate information is included, and (b) their actual practices match the BCR/Model Clause. Finally, companies can obtain express consent from the "Data Subject" (the person whose data is being transferred) for transferring their data to the U.S. Such consent, however, must be clear, informed, specific, and not a "forced" consent (where the individual has no choice but to consent).

It is worth noting, however, that shortly after the CJEU's ruling, the German data protection authority raised a question whether, given the revelations by Edward Snowden and the CJEU's ruling, even BCRs and Model Clauses remain sufficient for transfers from the EU to the U.S. Other data protection authorities, both in the EU and elsewhere, have also questioned the security of data sent to the U.S. under EU sanctioned model rules or BCRs, other "Safe Harbor" programs (such as the U.S.-Swiss Safe Harbor), or other country specific authorizations and have considered requesting halts to certain transfers. Thus, companies must keep close watch as this issue is sorted out, even if they do not receive data from the EU, to determine what actions will provide proper compliance.

Overall, companies should not rush to implement a solution without fully thinking it through. If a company rushes to utilize BCRs or Model Clauses that do not match actual practice, the company is no better protected than if it did nothing. Moreover, rushing to utilize currently authorized methods of protection that may later be determined to be insufficient can create internal and external confusion about a company's practices, not to mention being a waste of resources. Rather, companies should look at what,

and how, they share data between the EU and U.S., its necessity to their business, what procedures they have in place, and other circumstances to determine what, if anything, the correct solution is for the time being. Something the company does today may be insufficient by January.

Given the uncertainty and fluid nature of this situation, companies should contact legal counsel as soon as possible if they have any questions or concerns regarding transfers of data from outside the U.S.

FVLD publishes updates on legal issues and summaries of legal topics for its clients and friends. They are merely informational and do not constitute legal advice. We welcome comments or questions. If we can be of assistance, please call or write Peter T. Berk 312.701.6870 pberk@fvldlaw.com, or your regular FVLD contact.

FVLD®