COHEN & GRESSER LLP

October 9, 2015

The End of the Safe Harbor Framework – and the Threat to Model Clauses and BCRs

Karen H Bromberg, Partner
Duane A Cranston, Associate

Earlier this week, the European Court of Justice (CJEU) invalidated the Safe Harbor framework between the United States and the European Union -- effective *immediately*. This decision significantly disrupts the flow of data from Europe to the U.S. and will have a major impact on U.S.-EU trade.

What is the Safe Harbor

Some background may be helpful. The Safe Harbor framework was implemented in 2000 in response to the European Union Data Protection Directive, which forbids the transfer of personal data to countries outside the European Union that have been determined not to have adequate data protection measures in place (including, importantly, the United States). The Safe Harbor was critical because it enabled companies to transfer personal data from the EU to the U.S. by certifying that the companies themselves complied with EU privacy standards – notwithstanding the fact that the U.S. standards were lower. To participate in the U.S.-EU Safe Harbor program, a company had to publicly declare its compliance with the Safe Harbor Framework's requirements, including the framework's specific set of privacy principles, and state in its published privacy policy statement that it adhered to the Safe Harbor Privacy Principles. Once a company self-certified and became part of the Safe Harbor program, the company could legally transfer personal data from the EU to the U.S. in a relatively headache free-way.

The CJEU Decision

In recent years, American data protection laws have come under increasing scrutiny in the EU, as individuals and regulatory agencies have challenged the right of companies such as Google and Facebook to collect and use personal data in connection with online searches and social media applications. The CJEU's ruling resulted from an action brought by Max Schrems, an Austrian citizen and privacy activist, before the Irish Data Protection Commissioner to prohibit Facebook from transferring his personal data from the EU to the U.S. According to Schrems, the disclosure of government surveillance programs by Edward Snowden demonstrated that the Safe Harbor Framework was insufficient to protect his personal data from unauthorized or impermissible governmental surveillance and disclosure in the U.S.

The Commissioner refused to investigate the complaint, citing European Commission Decision 2000/520, which set out the Safe Harbor Privacy. Schrems challenged the Commissioner's decision before Ireland's High Court which determined, based on evidence including Snowden's disclosures of widespread surveillance by the NSA and other federal agencies, that Schrems was, in effect, challenging the legality of Decision 2000/520. The High Court stayed the case in order to get a ruling from the CJEU as to whether the Commissioner could review Decision 2000/520, and the CJEU ruled that the Commissioner could do so, on the grounds that "the large scale access by intelligence agencies to data transferred to the U.S. by Safe Harbor certified companies raises…serious questions regarding the continuity of the data protection rights of Europeans when their data is transferred to the U.S." and that "a significant number of certified companies did not comply or did not comply fully with the safe harbor principles."

The CJEU's decision unwinds a legal framework on which thousands of companies across a range of industries, including technology, finance, and healthcare, have relied for the past 15 plus years. While suggesting that bilateral agreements between individual EU member states and the U.S. should be overseen by each country's privacy regulators, the decision nonetheless, leaves a legal vacuum and means that companies can no longer rely on certification within a single data privacy regime. The decision potentially impacts any company that transmits personal data between the EU and the U.S., including human resources information concerning the company's own employees.

What this means for Companies

For the past two years, the EU and the U.S. have been negotiating a new safe harbor framework. While this ruling will certainly add urgency to that process, it may also add a layer of complexity as negotiators must now be mindful of what is and is not permissible under the CJEU decision. Significantly, while the judgment is limited to the Safe Harbor mechanism and does not invalidate other existing means to transfer data from the EU to the U.S., such as U.S. "Model Clauses" which have been approved by the European Commission for data transfer contracts with an EU-located subsidiary, and binding corporate rules ("BCRs") that can be applied throughout an entire corporate group regardless of location, the CJEU's first rationale for striking down the Safe Harbor Framework – the large scale access to private data enjoyed by U.S. intelligence agencies – seems at least potentially applicable to Model Clauses and BCRs as well, and companies relying on these mechanisms should expect future legal challenges. In any event, the approval process for Model Clauses and BCRs can be both lengthy and expensive, making them potentially unsuitable for all but the largest companies.

Because the CJEU has not provided a transitory period, companies concerned about their compliance with EU privacy laws applicable to any personal information they may collect, store, or transmit should immediately begin reviewing the sources and types of such information, and determine the extent to which personal information of their employees or customers may be implicated.

Companies should also review this information with any third party vendors they engage that may be involved in the process of data collection, storage, analysis or transmission, review those vendors' privacy policies, and stay informed of any updates these vendors may be contemplating.

Alternative methods of addressing data transfers will be needed. Consideration should be given to obtaining individual consent, or implementing strong encryption, establishing European servers in order to locally store any personal data of EU residents, or ensuring that all personal data from EU residents is segregated from other information and not transmitted to the U.S. In the interim, companies and their counsel should be closely monitoring the ongoing negotiations for a new safe harbor framework so that adjustments can be made accordingly.

About the Authors

Karen Bromberg is the head of the firm's Intellectual Property and Technology group. Her intellectual property practice focuses on litigation, counseling, and dispute resolution in all aspects of intellectual property, including patents, trademarks, trade dress, copyrights, unfair competition, trade secrets, and internet related issues. She regularly negotiates and drafts license agreements for clients in a diverse range of industries including consumer products, software, and financial services.

Duane Cranston serves as outside general counsel for a number of early to mid-stage companies industries ranging from technology to healthcare, representing clients in intellectual property licensing, commercial transactions, data privacy, and employment matters. He counsels employers on compliance with Title VII, ADEA, FMLA, and state level employment regulations and develops employment policies including insider trading and data privacy policies. He also advises on M&A and financing transactions.

October 9, 2015

About the Firm

Cohen & Gresser is an international law firm with offices in New York, Paris, and Seoul. We represent clients in complex litigation and corporate transactions throughout the world. Founded in 2002, Cohen & Gresser LLP has grown to nearly sixty lawyers in six practice areas: Litigation and Arbitration, Intellectual Property and Technology, White Collar Defense, Corporate, Tax, and Employment Law.

New York | Paris | Seoul

www.cohengresser.com
info@cohengresser.com
+1 212 957 7600

View C&G's profile