STINSON LEONARD STREET

EU Strikes Down the Safe Harbor Framework for Transatlantic Data Transfers: What You Should Know and What to Do Next

By Steve Cosentino, Tim Feathers and Jessica Kracl

After weeks of speculation, the Court of Justice of the European Union (CJEU) ruled on Oct. 6, 2015 that the European Commission's determination 15 years ago upholding the adequacy of the U.S. Department of Commerce Safe Harbor mechanism for transfers of personal data from the EU to the U.S. is "invalid."

Background

The EU's Data Protection Directive provides that companies operating in the EU may not transfer personal data to a country outside the European Economic Area (EEA) unless the receiving country ensures an adequate level of data protection by way of its domestic law or its international commitments. The U.S. Department of Commerce developed the Safe Harbor in consultation with the EU as a mechanism for allowing individual organizations to self-certify that their internal controls meet the EU requirements for data protection. The European Commission decided in July 2000 that the Safe Harbor framework ensured an adequate level of protection for personal data transferred from the EEA to organizations in the U.S. The Safe Harbor is relied upon by over 4,400 U.S. organizations to access the data of their EU partners and subsidiaries.

The present case was brought by Maximillian Schrems, an Austrian citizen and Facebook user whose data is transferred from Facebook's subsidiary in the EU to servers located in the United States, as is the case with other Facebook users residing in the EU. Facebook has been certified with the Safe Harbor framework since May 10, 2007. Schrems lodged a complaint before the Irish Data Protection Authority alleging that, in light of the revelations made in 2013 by Edward Snowden concerning the activities of the National Security Agency (NSA), the laws and practices of the United States do not offer sufficient protection against surveillance by public authorities.

In its decision, the CJEU invalidated the European Commission's July 2000 finding that the Safe Harbor framework ensured an adequate level of protection, holding that the Commission was required by the Data Protection Directive to "assess the content of the applicable rules in that country resulting from its domestic law or international commitments" and that the Commission's decision concerned only the adequacy of the Safe Harbor framework, a voluntary certification program with which U.S. public authorities are not required to comply. The CJEU held that the Commission's decision did not contain sufficient findings regarding the measures by which the U.S. ensures an adequate level of protection by reason of its domestic law or international commitments.

Impact of the Decision

The CJEU's decision invalidated the Safe Harbor framework effective immediately, meaning that organizations that are currently transferring personal data from the EEA to the U.S. without an alternate legal mechanism in place could face fines or orders to cease data transfers. That said, regulators will need time to assess their approach and are likely to understand that organizations will need time to implement new legal mechanisms upon which to base transfers of personal data. David Smith, the Deputy Commissioner of the Information Commissioner's Office in the United Kingdom, acknowledged as much when he said recently, "The judgment means that businesses that use the Safe Harbor will need to review how they ensure that data transferred to the U.S. is transferred in line with the law. We recognize that it will take them some time for them to do this."

The U.S. Department of Commerce has posted an advisory on its website, stating that in "the current rapidly changing environment, [we] will continue to administer the Safe Harbor program, including processing

submissions for self-certification to the Safe Harbor framework. If you have questions, please contact the European Commission, the appropriate European national data protection authority, or legal counsel." Further, the European Commission has expressed its intent to continue renegotiating a Safe Harbor with the Department of Commerce.

In the EU, the Article 29 Working Party held an extraordinary plenary meeting on October 15 to discuss the implications of the decision and, on October 16, released a statement regarding the landmark ruling. The Working Party called on EU member states to open discussions with the U.S. regarding "political, legal and technical solutions enabling data transfers to the territory of the United States that respect fundamental rights" and acknowledged that "current negotiations around a new Safe Harbor could be a part of the solution."

In its statement, the Working Party went on to say that data protection authorities consider that Binding Corporate Rules and Model Contract Clauses (as discussed below) can still be used, though data protection authorities may investigate particular cases where these are not sufficient. Finally, the Party signaled a possible grace period, stating that if by the end of January 2016, no appropriate solution is found with U.S. authorities, "EU data protection authorities are committed to take all necessary and appropriate actions, which may include coordinated enforcement actions", but also made quite clear that any transfers taking place under the Safe Harbor following the October 6 judgment of the CJEU are considered unlawful.

Next Steps

- Don't panic, but start looking to the future. Transatlantic transfers of personal data have not been banned and alternate legal bases for such transfers exist.
    - *Binding Corporate Rules*
      Binding Corporate Rules (BCRs) allow multinational companies to transfer personal data from the EEA to their affiliates outside the EEA. BCRs take some time to develop and implement, and the lead data protection authority (DPA) for the organization (e.g. the Information Commissioner's Office if the organization has its EU headquarters in the U.K.) must authorize the BCRs once it is satisfied with the safeguards contained therein. The DPA of each EU jurisdiction where the company operates also must then authorize use of the BCRs, a process that is facilitated by the lead DPA. Given the time involved, multinational companies that previously relied upon the safe harbor for the transfer of data among their affiliates may wish to begin the process for implementing BCRs now.
    - *Model Contract Clauses*
      The European Commission has approved a set of Model Contract Clauses that impose obligations on both the exporter and the importer of the data to ensure that the transfer arrangements protect the rights and freedoms of the data subjects. The clauses must be included in the agreement without amendment. Companies that previously relied on the Safe Harbor for the transfer of their EU resident data to companies with servers located outside of the EEA, for example, may wish to review their contracts with vendors to ensure that the model contract language exists or there is an appropriate mechanism to deal with processing for companies that import data from the EEA. That being said, and notwithstanding the Working Party's recent statement that the Model Contract Clauses are valid, they present a potentially problematic issue. Use of the clauses requires an organization to assert that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter. In light of this and the overwhelming focus of the Schrems case on the surveillance laws and practices of the United States, reliance on the Model Contract Clause may also be subject to attack by individual DPAs.
    - *Consent*
      The Data Protection Directive permits the transfer of personal data outside the EEA with the data subject's consent. Consent must be "freely given," "specific" and "informed." To date, European privacy regulators have been reluctant to accept consent as a valid data transfer method for ongoing and systematic data transfers, particularly where the consent is provided as a part of a privacy policy that is hard to find, difficult to understand or rarely read. At a minimum,

users should be required to affirmatively click to accept the terms of a privacy policy that includes consent for the transfer of their data outside the EEA.

- *Other Derogations Allowing the Transfer of Personal Data*
  The Data Protection Directive contains a handful of other instances in which data may be transferred outside of the EEA, such as when the transfer is necessary for the performance of a request of the data subject, the transfer is necessary for substantial public interest, the transfer is necessary in connection with legal proceedings or the transfer is necessary to protect the vital interests of the data subject. These derogations are most likely to apply, however, only to single instances of data transfers and not to the common and routine data transfer activities of the organization.

- Review references to the Safe Harbor framework in your online privacy policy. While the current Safe Harbor framework will not serve to ensure compliance with the EU Data Protection Directive, there may be some value in using the framework as shorthand to communicate the principles that the organization follows to protect personal data. That said, it would be prudent to review the context in which you mention the Safe Harbor and remove any references to it being the legal basis for permitting cross-border transfers of personal data.
- Don't rush to cancel your certification or opt not to renew. The Department of Commerce has said that it will continue to administer the Safe Harbor program. Though organizations can no longer rely on it as the legal basis for transferring data from the EEA to the United States, organizations that have executed contracts that include representations regarding certification with the Safe Harbor framework or adherence to its principles, should consider any such contractual obligations prior to non-renewing your certification. Further, there remains a possibility that a re-worked or updated Safe Harbor may be a part of the ultimate solution and maintaining current certification could potentially streamline the process for certification with Safe Harbor 2.0. If, however, you are considering becoming newly certified with the Safe Harbor, it may be best to hold-off until further guidance emerges.

For additional information on the impact of the decision and recommendations for next steps, please consult with the attorneys listed below or your usual Stinson Leonard Street LLP attorney.

Steve Cosentino
816.691.2450
steve.cosentino@stinson.com

Timothy Feathers
816.691.2754
timothy.feathers@stinson.com

Jessica Kracl
612.335.1537
jessica.kracl@stinson.com