Post Safe Harbor – What's Next?

Oct 08, 2015

Categories:

Publications

On October 6, 2015, the European Court of Justice (ECJ) sealed the fate of the U.S.-EU Safe Harbor ("Safe Harbor") for cross-border transfer of personal data. In this much-anticipated decision, the ECJ ruled that in light of Edward Snowden's revelations concerning the surveillance by the U.S. National Security Agency, the Safe Harbor was "invalid." In so ruling, the ECJ adopted the recommendation of the Advocate General arising out of the case of *Shrems v. The Data Protection Commissioner of Ireland*.

This decision has left the roughly 4,000 U.S. companies that have self-certified to Safe Harbor in a quandary as to a course of action. Transfers of personal data from locations in the EU to the U.S. by companies that have not taken other measures considered adequate protection under the Directive 95/46/EC ("Directive"), are in violation of the Directive and the law of the EU jurisdiction where the data is located.

The U.S. Department of Commerce said in a statement that it is "deeply disappointed in [the decision], which creates significant uncertainty for both U.S. and EU companies and consumers, and puts at risk the thriving transatlantic digital economy." It has pledged to continue to work with the European Commission to strengthen the Safe Harbor and to issue an updated Safe Harbor as soon as possible.

As mentioned in our advisory late last month, discussing the Advocate General's recommendation, the next steps for an organization that relied upon the ECJ Decision approving the Safe Harbor as a means for compliance in connection with transfers of personal data from the EU to the U.S. is far from clear. At this point, the prospects for a Safe Harbor 2.0 are unclear, and the three remaining options to meet the "adequate protection" requirement – the adoption of binding corporate rules (BCRs), the use of the approved model contractual clauses, and obtaining the express and informed consent of the data subject – though tempting to fall back on, are all burdensome and daunting to adopt. But a rush to a solution may not be advisable. There is an expectation that the Commission will caution the EU's data protection authorities not to

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

clamp down on U.S. companies immediately. In fact, many Data Protection Authorities (DPAs) have openly admitted they are under-resourced, and this decision will place additional burdens upon their offices.

Organizations should take a step back and analyze what data transfers to the U.S. rely upon the Safe Harbor. Then they can evaluate their various options. Having made the commitment to the Directive's privacy principles by self-certifying to the Safe Harbor, organizations should already have a privacy and security program in place that with some enhancement may prove to be the foundation for adoption of Binding Corporate Rules (BCRs). Even before the ECJ decision, BCRs were being viewed more favorably, with 70 firms having thus far completed the process. In fact, they bear a strong resemblance to APEC's cross-border transfer rules. Consideration should be given to whether an organization's existing program that complied with the Safe Harbor can be enhanced to meet the BCR requirements, or to evaluate where there might be an opportunity for obtaining data subject consent. The requirements imposed by use of the model contract clauses should be reviewed as well, although these requirements are considered to be stricter than the requirements of the Safe Harbor.

But before making any firm decision, organizations should bear in mind that the ECJ's basis for invalidating the Safe Harbor – U.S. government surveillance with no judicial protection – will not be changing in the foreseeable future, and impacts the potential viability of all means to provide guarantees for adequate protection, including the BCRs. Concerns abound about the ability of U.S. companies to withstand requests for data by U.S. governmental authorities. Ultimately, the political process needs to work itself out, and until a political solution is found, businesses do not have a clear viable option for complying with the adequate protection requirements of the Directive.

For more information, contact Michael Nitardy, or any other member of Frost Brown Todd's Privacy & Data Security Team.

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

FBT Gibbons