EPSTEIN BECKER GREEN
labor and employment
CLIENT ALERT

# European Court of Justice Invalidates U.S.-EU Safe Harbor

**By Adam S. Forman, Patricia M. Wagner, and Evan J. Nagler**

**October 2015**

On October 6, 2015, the European Court of Justice ("ECJ"), the top court of the European Union ("EU"), released its opinion[1] in *Maximillian Schrems v. Data Protection Commissioner* (C-362/14), invalidating the U.S.-EU Safe Harbor program.

## Background: EU Data Protection

While the United States has taken a patchwork approach to privacy with laws like the Health Insurance Portability and Accountability Act (for health care entities), the Gramm-Leach-Bliley Act (for financial institutions), as well as various state and federal laws (for employment relationships), the EU has a broad overarching law covering all industry sectors: Data Protection Directive 95/46/EC ("Directive"). The Directive provides a minimum set of protections that each EU member state must offer for personal data. Some member states have national laws that provide even more protection to personal data.

In order to facilitate business between the United States and EU, the United States and EU negotiated an agreement whereby U.S. companies wishing to process EU residents' personal data could do so by qualifying for, and meeting, certain principles and guidelines. These principles and guidelines were set forth in the U.S.-EU Safe Harbor Framework ("Safe Harbor").[2] The Safe Harbor required adherence to guidance materials and seven basic principles: notice, choice, onward transfer limitation, security, data integrity, access, and enforcement. Companies could self-certify that they were in compliance with the Safe Harbor and process (which, under the Directive, includes transferring) EU data.

Companies that did not proceed with the U.S.-EU Safe Harbor certification could export personal data from the EU by one of two alternative methods: Model Contract Clauses[3]

[1] Maximillian Schrems v. Data Protection Commissioner, E.C.J. C-362/14 (Oct. 6, 2015), *available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=145571.

[2] The principles and relevant information may be found at http://www.export.gov/safeharbor. A similar agreement exists with Switzerland and is unaffected by the *Schrems* ruling. The principles are also enshrined in the EU as Decision 2000/520/EC.

[3] Commission Decision 2010/87/EU.

or Binding Corporate Rules ("BCRs").[4] The EU Model Contract Clauses, when inserted in agreements, provide for the collection and processing of personal data in compliance with EU law regarding transfers to third countries. BCRs can be adopted by multinationals or multinational groups of companies to ensure that a company maintains standards compliant with EU data protection rules.

## The *Schrems* Case and Ruling

An Austrian law student and Facebook user, Max Schrems, brought a challenge related to the fact that his data from Facebook was being exported from Ireland to the United States.[5] Schrems raised significant concerns after the leaks from Edward Snowden about the U.S. government's Prism program revealed the extent to which the U.S. government routinely accesses and processes data from the Internet and from U.S. companies' servers. Because the surveillance was sufficiently broad and routine, Schrems contended that it violated EU law.

Since Facebook's subsidiary is located in Ireland, Schrems raised his complaint with the Irish Data Protection Authority, and, after appeals through the EU system, the ECJ issued its ruling. The ruling held that the Safe Harbor is incompatible with the Directive and its associated laws and rulings. In addition, the ruling held that national data protection authorities do have the power to investigate complaints regarding the export of data to non-EU countries over violations of EU residents' rights in those countries.

## Impact of Ruling

Any company that has been relying on the Safe Harbor certification is affected by this ruling. This could include U.S. companies selling to EU customers if EU customer information is transferred to the United States and companies that may be transferring employee information between the United States and the EU. The ECJ did not offer a grace period for compliance, so affected companies relying on the Safe Harbor must now find alternate methods to demonstrate compliance. To move towards compliance, there are several steps companies can take, including the following:

1. *Institute Binding Corporate Rules or Model Contract Clauses*

Some companies will be able to switch to BCRs or Model Contract Clauses for compliance in exporting personal data from Europe. These two methods, described above, provide alternate means for compliance with EU law. Companies, however, should be advised that EU Data Protection Authorities are likely to scrutinize companies switching to BCRs or Model Contract Clauses. If pursuing this option, companies should conduct thorough reviews to ensure that they are appropriately compliant with the guidelines for BCRs or Model Contract Clauses before making the change. Additionally, there is the danger that the nature of Schrems's complaint regarding the Prism surveillance program may lead to claims that BCRs or Model Contract Clauses allowing export to the United States are invalid.

[4] Information about BCRs may be found at http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm.
[5] Facebook Ireland is Facebook's EU subsidiary.

2. *Strengthen Privacy Practices Generally*

In line with the BCR and Model Contract Clause methods, companies looking to continue their US-EU data transfers should strengthen privacy protections generally. In addition to EU law, there are several proposed U.S. laws that would move the United States towards an EU-type set of personal data protection principles. Instituting EU-friendly practices now may save time and effort later if and when such proposals become law.

3. *Wait It Out*

For several years, the EU has been discussing the successor to the Directive: the General Data Protection Regulation ("GDPR"). This law would address many of the changes in global business since the 1995 Directive. EU bodies have declared that their objective is to agree to the terms of the GDPR by the end of 2015.[6] With the *Schrems* ruling, it is likely that the EU will seek to address the gap left behind by the invalidation of the Safe Harbor, either through the GDPR itself or through a side agreement negotiated with the United States.

The U.S. Department of Commerce responded to the *Schrems* decision by stating that a new Safe Harbor Framework has been in negotiations for two years and that the Department of Commerce and the EU will work to finalize the new Framework "as soon as possible."[7] Additional responses from both the Department of Commerce and the EU will likely be forthcoming,[8] potentially including new guidance. We will keep you posted regarding if or when those bodies respond further.

4. *Halt All Transfers of Data from the EU to the United States*

Though highly impractical, halting all transfers of data from the EU to the United States is one of the only ways to guarantee compliance in the short term. However, this may not even be technically possible for many businesses, depending on network structure and the software tools in place.

* * *

*This Client Alert was authored by* **Adam S. Forman, Patricia M. Wagner,** *and* **Evan J. Nagler***. For additional information about the issues discussed in this Client Alert, please contact one of the authors or the Epstein Becker Green attorney who regularly handles your legal matters.*

---

[6] *E.g.*, http://www.privacyanddatasecurityinsight.com/2015/07/new-eu-cybersecurity-regulations-on-the-way-things-to-know-now/.

[7] *Statement from U.S. Secretary of Commerce Penny Pritzker on European Court of Justice Safe Harbor Framework Decision*, U.S. Department of Commerce (October 6, 2015), *available at* https://www.commerce.gov/news/press-releases/2015/10/statement-us-secretary-commerce-penny-pritzker-european-court-justice.

[8] UK Information Commissioner Christopher Graham commented that his office will not be "knee-jerking into sudden enforcement of a new arrangement," that EU Data Protection Authorities are coordinating their responses, and that companies should "keep calm" and pursue BCRs and Model Contract Clauses. *See, e.g.,* https://iapp.org/news/a/icos-graham-dont-panic.

*This document has been provided for informational purposes only and is not intended and should not be construed to constitute legal advice. Please consult your attorneys in connection with any fact-specific situation under federal law and the applicable state or local laws that may impose additional obligations on you and your company.*

### About Epstein Becker Green

Epstein Becker & Green, P.C., is a national law firm with a primary focus on health care and life sciences; employment, labor, and workforce management; and litigation and business disputes. Founded in 1973 as an industry-focused firm, Epstein Becker Green has decades of experience serving clients in health care, financial services, retail, hospitality, and technology, among other industries, representing entities from startups to Fortune 100 companies. Operating in offices throughout the U.S. and supporting clients in the U.S. and abroad, the firm's attorneys are committed to uncompromising client service and legal excellence. For more information, visit www.ebglaw.com.