

## CLIENT ALERT

### Transfer of Personal Data from the EU to the U.S.

October 2015

*European Court of Justice (i) confirms powers of national Data Protection Authorities and (ii) declares the EU Commission's U.S.-EU Safe Harbor Decision invalid.*

On October 6, 2015, the European Court of Justice (ECJ) issued a decision in "Schrems v. Facebook," that had two major effects.

First, the ECJ held that, even if the EU Commission decides that a third country provides an "adequate level of protection" that permits personal data of EU citizens to be transferred to a "third country" outside the European Economic Area (such as the EU-U.S. Safe Harbor Framework allowing transfers from the EU to the U.S.) this decision:

(i) does not prevent individuals whose personal data has been or could be transferred to a third country from challenging the adequacy of the protection by lodging a claim with the competent national data protection authority (DPA) based on protection of their fundamental rights and freedoms; and

(ii) does not eliminate or reduce the powers available to the DPAs under the Charter of Fundamental Rights of the European Union and EU Directive 95/46 and national laws to examine *that claim*.

As a result, EU citizens can lodge claims with any DPA arguing that the transfer of their personal data to a third country, such as the US, is improper even if the basis for that transfer was negotiated between the third country and the EU and even if the Commission accepted the basis for the transfer as satisfying the adequacy requirements of EU Directive 95/46. This analysis is not limited to Safe Harbor transfers, and thus potentially affects all data transfers from the EU to the U.S. Although there have not yet been additional cases similar to the one brought by Schrems against Facebook to challenge other data transfers from the EU to the U.S., such cases seem inevitable.

Second, the ECJ held that the EU Commission decision finding that the Safe Harbor Framework provided an adequate level of protection is invalid.

The ECJ based its opinion on U.S. national security surveillance and data collection practices, finding that Safe Harbor "*thus enables interference, by United States public authorities, with the fundamental rights of persons, and the Commission decision [finding Safe Harbor adequate] does not refer either to the existence, in the United States, of rules intended to limit any such interference or to the existence of effective legal protection against the interference.*"

Over 4,400 companies relied on Safe Harbor to lawfully and practically transfer data from the EU to the U.S. Now that Safe Harbor has been declared invalid, they have to look for alternative options to legally transfer personal data to the United States (such as using of Model Contracts or Binding Corporate Rules, or invoking the derogations in which case transfers are also allowed).

However, putting alternative data transfer mechanisms into place may require a lot of time and effort, and some of the are not suitable in all situations. In addition, as the ECJ judgment makes clear, concerns about U.S. Government surveillance are not unique to the Safe Harbor Framework, so all of the alternative mechanisms for transferring data from the EU to the U.S. are potentially vulnerable, and, at the very least, will not automatically protect companies against data subjects in the EU who wish to challenge the adequacy of the data transfer.

The EU data protection authorities and Commission officials, assembled as the Article 29 Working Party, issued a statement on October 16, 2015 in which they made clear that:

1. The U.S.-EU Safe Harbor is no longer a valid basis for EU-U.S. data transfers, and companies must find alternative solutions;
2. Standard Contractual Clauses and Binding Corporate Rules can still be used, at least for the time being;
3. Individual member state data protection authorities may investigate specific data transfers, for instance on the basis of complaints against particular companies;
4. The data protection authorities expect the U.S. and EU to develop solutions to deal with the "massive and indiscriminate surveillance" in the U.S. and to provide an "adequate" framework by the end of January 2016; and
5. If no solution is found by the end of January 2016, then "EU data protection authorities are committed to take all necessary and appropriate actions, which may include coordinated enforcement actions."

It is clear that companies that have relied on Safe Harbor must find another basis for transferring personal data belonging to EU citizens from Europe to the U.S. It is equally clear that, until this matter is resolved between the EU and the U.S., all such data transfers are potentially at risk of challenge, whether by DPAs or by individual citizens.

---

#### Other Articles in This Month's Edition:

- [Proposed Updates to the Motor Vehicle Safety Act](#)
- [A Highlight Reel: FTC's Amendment to Fair Packaging and Labeling Act Rules](#)
- [Advertisers in the Ring – A Roundup of This Month's Competitor Advertising Challenges: Measuring '#1' and 'Free' Claims](#)

---

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

#### **Frederik Van Remoortel**

Partner – Brussels

Phone: +32.2.282.1844

Email: [fvanremoortel@crowell.com](mailto:fvanremoortel@crowell.com)