The European Court of Justice Invalidates Safe Harbor

Written by Catherine Muyl, Colin J. Zick

October 6, 2015

The European Court of Justice has just issued a **decision** (ECJ 6 October 2015 Case C-362/14, Maximillian Schrems v. Data Protection Commissioner) that invalidates the so-called US-EU "Safe Harbor" system. Suddenly, what 3,500 U.S. Companies (including some of the largest companies in the world) have been doing with personal data now potentially becomes illegal.

What is the background to this decision?

In 1995, the European Union adopted a **Directive** 95/46/EC aimed at providing a high level of protection of personal data throughout the European Union. According to Article 25 of said Directive, the transfer of personal outside the European Union is prohibited unless the receiving country has an adequate level of protection of personal data and the ECJ interprets this to mean "substantially equivalent" to European standards.

The European Commission was granted the authority to decide whether a particular non-EU country ensures an adequate level of protection "by reason of its domestic law or of the international commitments it has entered into." The Commission has so far recognized for example Argentina, Australia, Canada, Switzerland and New Zealand as providing adequate protection.

With respect to the United States, the European Commission entered into an Agreement called the "Safe Harbor" with the U.S. Department of Commerce based on self-certification. Under the US-EU "Safe Harbor," transfer of personal data from the EU to a US organization was lawful if the US organization receiving the data has unambiguously and publicly disclosed its commitment to comply with the "Safe Harbor Privacy Principles" as set out in the **Commission Decision 2000/520/EC of 26 July 2000**.

After the revelation by Edward Snowden of surveillance programs involving large-scale collection of personal data, the European Commission issued two Communications on 27 November 2013 (Communication **(2013)846** "Rebuilding Trust in EU-US Data Flows" and Communication (**2013)847** on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU) in which it found:

> that the United States authorities were able to access the personal data transferred from the Member States to the United States and process it in a way incompatible, in particular, with the purposes for which it was transferred, beyond what was strictly necessary and proportionate to the protection of national security.

The Commission also noted that "the data subjects had no administrative or judicial means of redress enabling, in particular, the data relating to them to be accessed and, as the case may be, rectified or erased."

What did the European Court decide?

In its decision of 6 October 2015, the European Court of justice held, in response to a preliminary question raised by the Irish High Court, that:

> even if the Commission has adopted [the above mentioned Commission Decision], the national supervisory authorities, when hearing a claim lodged by a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him, must be able to examine, with complete independence, whether the transfer of that data complies with the requirements laid down by the directive (Recital 57).

Although the question has not been expressly submitted by the Irish Court, the European Court of Justice decided to examine whether the Commission Decision 2000/520/EC complied with the Directive 95/46 and the Charter of Fundamental Rights of the European Union.

The Court pointed out that:

- the reliability of the Safe Harbor system which is based on the self-certification of companies, "is founded essentially on the establishment of effective detection and supervision mechanisms enabling any infringements of the rules ensuring the protection of fundamental rights, in particular the right to respect for private life and the right to protection of personal data, to be identified and punished in practice" (Recital 81);
- "United States public authorities are not required to comply with [the Safe Harbor principles]" (Recital 82);
- "Decision 2000/520 lays down that 'national security, public interest, or law enforcement requirements' have primacy over the safe harbor principles, primacy pursuant to which self-certified United States organizations receiving personal data from the European Union are bound to disregard those principles without limitation where they conflict with those requirements and therefore prove incompatible with them" (Recital 86);
- "In the light of the general nature of the derogation set out in the fourth paragraph of Annex I to Decision 2000/520, that decision thus enables interference, founded on national security and public interest requirements or on domestic legislation of the United States, with the fundamental rights of the persons whose personal data is or could be transferred from the European Union to the United States" (Recital 87);
- The European Commission stated in its Communication of 27 November 2013 "that the United States authorities were able to access the personal data transferred from the Member States to the United States and process it in a way incompatible, in particular, with the purposes for which it was transferred, beyond what was strictly necessary and proportionate to the protection of national security" and that "the data subjects had no administrative or judicial means of redress enabling, in particular, the data relating to them to be accessed and, as the case may be, rectified or erased." (Recital 90).

The Court concluded that the Decision 2000/520 was invalid.

In practice, this decision means that US organizations can no longer rely on the Safe Harbor system to permit transfer personal data from the EU to the US consistent with Directive 95/46/EC.

What are the risks for those transferring data who are no longer protected by the Safe Harbor and do not comply with Directive 95/46/EC?

The transfer of personal data to a country outside the EU which does not afford adequate protection is prohibited by Directive 95/46/EC, but the enforcement of that rule is left into the hands of Member States.

Penalties are laid down by the law of each Member-State.

In France, for example, the unlawful transfer is a criminal offence which can give rise to imprisonment and a maximum fine of 300,000 € (Article 226-22-1 of the Criminal Code).

In addition, Article 28 of the Directive provides that national Data Protection Authorities are entitled to impose "a temporary or definitive ban on processing" and according to EU case law (C-317-04 and C-318-04) the transfer of personal data outside the EU constitutes a processing. It is on that basis that Max Schrems asked the Irish Data Protection Authority to prohibit Facebook Ireland from transferring his personal data to the United States.

What steps should US organizations take to comply with the EU data protection regime?

There are two options available to comply with EU requirements:

Standard contractual clauses

The European Commission has issued standard contractual clauses which impose obligations on both the exporter and the importer of the data (which may or may not be entities of the same group) to ensure that the transfer arrangements protect the rights and freedoms

of data subjects. In short, the US entity undertakes contractually to comply with the European privacy standards.

Binding corporate rules

Binding Corporate Rules ("BCR") are internal rules which define the global policy with regard to the transfers of personal data within a corporate group.

BCR ensure that all transfers are made within a group benefit from an adequate level of protection.

This is an alternative to the company having to sign standard contractual clauses each time it needs to transfer data to a member of its group.

The company which wants to implement BCR has to apply for authorization with a national Data Protection Authority.

The **list of companies** which successfully applied is available.

Contact **Catherine Muyl**, **Colin Zick** or **Alice Berendes** if you need assistance determining what would be the most appropriate method for your organization to move forward in light of the decision.
