OPINIONS

December 27, 2017

The EU-USA Data Transfer between Privacy Shield and alternative methods: the Standard Contractual Clauses

BY AGNESE SCHINELLI

Abstract

In a rapidly evolving regulatory framework, the strategies for the protection of personal data that companies engaged in EU-USA cross-border business activities have adopted so far risk to be no longer adequate.

* * *

Personal data are protected by a fundamental right of the person and, at the same time, represent a precious and valuable asset for companies: for this reason, in the global digital market, their transfer plays a fundamental role in business relations between the European Union and the United States.

The "essentially equivalent" protection and the Privacy Shield: a self-certification system with stronger safeguards

The transfer of personal data from the EU to third countries is permitted only provided that the level of protection granted by the third country to which the data is transferred is "essentially equivalent" to the one granted by European laws.[1]

In the attempt to provide a highly protective umbrella for the transfer of personal data, the European Union and the United States have adopted the Privacy Shield agreement, a framework deemed by the European Commission adequate to the European standards.[2] Such mechanism, managed by the US Department of Commerce, offers American companies intending to receive personal data from the EU the opportunity to self-certify their compliance to strict transparency, information and monitoring obligations.

The details relating to the companies adhering to the Privacy Shield are easily accessible to any interested party[3] who, for the first time, has the opportunity to address, and file claims before, the Ombudsperson, a mechanism specifically dedicated to review the claims of the data subjects relating to possible access by US intelligence authorities, for national security purposes, to personal data transferred from the EU to the US.[4]

---

[1] CJEU, decision C-362/14, *Schrems v. Data Protection Commissioner*, October 6, 2015.
[2] Commission Implementing Decision (EU) of 12 July 2016.
[3] https://www.privacyshield.gov/list
[4] The Privacy Shield Ombudsperson, a senior official within the U.S. Department of State, is a mechanism set up under the Privacy Shield to facilitate the handling of all complaints (not limited to complaints against Privacy Shield companies) relating to access to personal data transferred from the EU by US intelligence agencies for national security purposes.

If the Privacy Shield undoubtedly represents a mutual effort EU-USA in balancing the protection of the fundamental right to private life with granting an efficient prosecution of business activities, the adequacy of the level of personal data protection provided by US, state and local laws remains under the microscope of the EU institutions.

The alternative methods to transfer personal data to third Countries: the Standard Contractual Clauses to be invalidated?

The Standard Contractual Clauses (SCCs) constitute the alternative method that most companies use to transfer personal data outside the EU. Approved by the European Commission, the SCCs set forth mutual obligations of personal data protection on both the data exporter and the data importer such as, for example, the adoption of appropriate safeguards and the guarantee of the importer that applicable laws and regulations do not prevent the importer's compliance with the contractual obligation of data protection.[5]

In *Schrems* "Round II" the Irish Supreme Court: (i) expressed "well founded concerns" about the adequacy of the level of personal data protection granted by US, state and local laws; and (ii) clarified that the SCCs are not *per se* sufficient to remedy the potential inadequacy of the level of protection ensured by the laws of the third country to which the data are being transferred, thus deeming necessary a reference for preliminary ruling to the Court of Justice of the European Union about the validity of the relating adequacy decision.[6]

This means that **the standard-content agreements that have been in place so far in order to grant a continuous flow of personal data from the EU to third countries, might soon no longer constitute a valid instrument to implement such transfer**, not even, for example, to transfer data among companies within the same corporate group.[7]

A difficult dialogue between speakers communicating in two very different languages

The territory of personal data protection is a litmus test of the difference of approaches between the EU and the USA in the field of personal data protection, for example:

1. **The lack of a data protection authority in the American system.** The various decisions and interventions of the EU institutions, as well as the establishment of the Ombudsperson within the Privacy Shield framework, unveil the European attempt to create an American equivalent of the European data protection authorities, all in different ways independent from the respective governmental systems. However, the Ombudsperson is appointed by the US Department of State and the Privacy Shield is managed and administered by the US Department of Commerce, both branches of the executive power.

2. **The US laws protecting privacy and the common law "third party doctrine".** The US legal framework protecting the right to privacy is a patchwork of federal and state laws, the interpretation of which is still influenced by the "*third party doctrine*", i.e. the

[5] Commission Decision 2010/87/EU of February 5, 2010.
[6] Irish High Court, decision of October 3, 2017, *Data Protection Commissioner v. Facebook and Maximilian Schrems*.
[7] As of November 15, 2017, the questions of the reference for preliminary ruling have not been submitted to the CJEU yet: in the event the order of reference for preliminary ruling is filed by the end of 2017, the CJEU will not likely render its decision before 2019. Therefore, pending the CJEU's decision, the SCCs remain valid and enforceable.

common law legal theory that denies constitutional protection to the personal data that the data subject voluntarily discloses to third parties.[8]

Conclusions

The EU appears to remain under the illusion that the transfer of personal data to third countries, i.e. on a global scale, must occur only and exclusively applying the European standards, thus easily risking to slip into political evaluations and reactions.

In view of the "domino effect" triggered by *Schrems I*, the challenge, more topical than ever, for the companies engaged in EU-USA *cross-border* business activities is to proceed to an accurate revision of their own strategies and procedures of transfer of personal data, trying to protect the fundamental right to privacy, and at the same time keeping intact the business opportunities.

About the author

AGNESE SCHINELLI – Associate at K&L Gates

Attorney qualified both in Italy and in the State of New York, Agnese devotes her professional practice to corporate and commercial law, assisting Italian and foreign clients in domestic and cross-border M&A and private equity transactions, as well as in corporate governance, regulatory and privacy compliance issues.

[8] Katz v. United States, 389 U.S. 347, 351 (1967).