VOICU FILIPESCU
Attorneys at Law
News in Laws – Legal Monthly Newsletter
November 2020

EU Data transfers after Schrems II - What would be a defensible position going further? A few recommended practical steps

by Marta Popa, Senior Partner Voicu & Filipescu

On July 16, 2020, the European Court of Justice has resolved, in its ruling granted in cause C-311/18 - Data Protection Commissioner against Facebook Ireland and Maximillian Schrems, upon invalidation of Decision no. 2016/1250 on the adequate character of protection offered by the EU – U.S. Privacy Shield and rendered valid Decision no. 2010/87 of the Commission regarding the standard contractual clauses for the transfer of personal data to processors established in third countries.

Subject matter of the case brought before the European Court of Justice (ECJ)

ECJ Ruling in case C-311/18 - Facebook Ireland and Maximillian Schrems is of special importance, highlighting the fundamental right to privacy in case of transfer of personal data to third countries as well as a series of non-compliances in the treatment of personal data mainly as regards observance of the necessity and proportionality principles, which eventually led to the invalidation of the Privacy Shield previously applicable between the EU and the US.

The case was initiated in 2015 by Max Schrems, a data privacy activist who succeeded in getting the previous 'Safe Harbor' transfer mechanism invalidated. Following the success of his safe harbor challenge, he turned his attention to Facebook's use of model clauses (also known as standard contractual clauses or 'SCCs') fortransferring personal data to its US headquarters and made a further complaint to the Irish Data Protection Commission ('DPC'). As part of his complaint, Schrems argued that the US approach to personal data undermined the EU's high data protection standards, and that personal data should not be exported to the US irrespective of the transfer mechanism.

The Irish DPC also raised concerns about the use of model clauses in general, and the case ended up before the ECJ).

The ECJ has found that the Privacy Shield is no longer a valid mechanism of transfer of personal data between the EU and the US and although SCCs remain a valid mechanism for cross-border transfers of personal data, they cannot be relied on by Facebook in this instance to transfer personal data to its US headquarters on the basis that Facebook is subject to US surveillance laws.

In more concrete words, "the requirements of US national security (from CIA or FBI or NSA – our note) and the requirements of public interest and law enforcement have primacy, thus condoning interference with the fundamental rights of persons whose data are transferred to that third country".

Furthermore, it was found that the complaint mechanism within Privacy Shield (the ombudsman mechanism) did not give any real right of to EU data subjects who wanted to complain about the way their data was being processed in the US.

Thus, even though SCCs do remain, in principle. a valid mechanism for cross-border transfers of personal data, in order to rely on SCCs the data exporters and the data importers must undertake assessments of the level of protection and take supplementary measures/additional safeguards to show that the receiving country can guarantee the same protections for EU data subjects, if there is no equivalent protection.

BCRs are also affected by Schrems II just like the SCCs, as U.S. law has primacy over this transfer tool too.

A rather unique ruling, as it obligates the Data Protection Authorities to order the deletion of data, suspension or end of unlawful data transfers rather than to impose penalties

The ECJ ruling generated many concerns for controllers and processors regarding mainly the level of due diligence they have to carry on in relation to SCCs and whether or not other transfer tools are still valid. Other difficult questions include how to effect transfers to countries where the level of data protection is not deemed adequate, such as China or Rusia, or non-EU countries such as UK or Japan.

Further, the ECJ also emphasized that supervisory authorities (DPAs) have the right to audit and review SCCs and suspend or stop data transfers where they find there is no adequate protection afforded by the receiving country. And these orders that DPAs may take can actually affect much more a company or a business than a fine.

Schrems II has thus become a Board/CEO-Level issue for entities involved in the international transfer of data.

A few recommended practical steps in consequence of "Schrems II" ruling

What kind of analysis is required to controllers and processors to demonstrate the due-dilligence they took in regard of the SCCs to comply with EU data protection law? Should it be the same standard applied for an EC adequacy decision under Article 45 GDPR? Could derogations set under Article 49 apply, since even SCCs are sometimes not enough? What paperwork needs to be put in place and what is to be done in case of a control from a supervisory body and what if such body is not in agreement with the due-diligence findings and strikes down the transfers? And how about countries with less protection for the transferred data, such as China or Russia?

However, on October 29, 2020, the European Data Protection Board (the "EDPB") has pointed out, in its document for approval of the Strategy for European institutions regarding Schrems II ruling, that compliance with such ruling should build around **cooperation and responsibility** of controllers in order to **achieve a compliance degree essentially equivalent to that guaranteed within the EU**. Also, the ECJ advised EU institutions to:

i. not transfer data within new processing activities (which includes US-owned Cloud and SaaS providers, regardless of where servers are located) or conclude new contracts with services provided located in the U.S.;

ii. complete Transfer Impact Assessments (TIAs) for all data transfers; and

iii. expect joint EDPS/EDPB guidance, compliance audits and enforcement actions for transfers towards the U.S. or other third countries on a case-by-case basis.

We are proposing below a few steps aimed at minimizing the risk of an inadequate analysis and use of the SCCs in case of ongoing and future international transfers:

1. Map cross-border transfers;

2. Perform Transfer Impact Agreements (TIAs);

3. Look into derogations under Article 49 GDPR;

4. Put supplementary measures/additional safeguards in place (pseudonymization, for example);

5. Improve contractual provisions with processors for legal and commercial comfort; and

6. Keep cross-border transfers under review.

On November 11, 2020, the EDPB put under public consultation a series of recommendations containing a roadmap of the steps that data exporters must take to find out if they need to put in place supplementary measures to achieve a level of compliance and protection essentially equivalent to that in the EU as well as recommendations on the European Essential Guarantees for surveillance measures. At the date hereof, the recommendations were not yet published; however, we will revert with more details once recommendations will be published.