LAW AND INTERNATIONAL LAW

Poalelungi Mihai
Assessor of law (DE)
Fourth-year doctoral student at the
State University of Moldova, Republic of Moldova

EU – U.S. PRIVACY DATA RELATIONSHIP AND THE ONGOING IMPACT OF «SCHREMS II»

The best way to bring more security to exported data of citizens is a planned agreement between the concerned countries. The European Union (EU) attempted to regulate in a legally secure and uniform manner such data transfers after the European Court of Justice (ECJ) overturned the at the time applicable Safe Harbour Privacy Principles between the USA and EU mainly blaming the European Commission (EC) for exceeding its authority. The ECJ stated: "*The Court holds that the Commission did not have competence to restrict the national supervisory authorities' powers in that way*.

For all those reasons, the Court declares the Safe Harbour Decision invalid." [1]

As a result, both States reached a new agreement the so-called "Privacy Shield". Yet, just after few years the ECJ overturned the latter one too. This time the Court found that the United States cannot satisfy the requirements imposed by the EU law. The ECJ stated inter alia: "[…] *the limitations on the protection of personal data arising from the domestic law of the United States on the access and use by US public authorities of such data transferred from the European Union to the United States, which the Commission assessed in the Privacy Shield Decision, are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required, under EU law* […] "[2]

The US government criticised the ECJ's decision and argued that the Court, on the one hand, did not consider the, at the time, lately improvements. The US Foreign Intelligence Surveillance Court actively monitored the US intelligence agencies in

order to determine whether they properly target individuals.[3] On the other hand it stated that the vast majority of the companies simply do not have relevant information of an interest to the US national security, therefore their data is unlikely to be subject of a FISA-request (Foreign Intelligence Surveillance Act).

It may remain undecided whether it is enough to look away from such a concern of data privacy, based on the hope of each individual that his/her information isn't worth considering for the national security. As a fact it is certain that the "Privacy Shield" violates the EU law. Nonetheless the ECJ did not left the legal situation totally uncertain and upheld the validity of the Standard Contractual Clauses (SCCs).

The EC was fast to react with a new version of the SCCs which regulations meanwhile, as of today, are over the grace period and must be followed.

The invalidation of the "Privacy Shield" and the upholding of the SCCs results in an accountability to firms. Some use the Binding Corporate Rules (BCR), but it should be pointed out that BCRs offer much less legal certainty for international data transfers, not to mention the painful process of adopting them.

The consequence of applying SCCs is that every corporate entity must undertake a verifiable risk assessment (the so-called Transfer Impact Assessment, "TIA") on the level of data protection in the third country of the data importer. Third countries are all countries that don't belong to the EU/EEA. As a result, the question must be answered whether there is a risk that the data will be accessed by authorities or not. Yet, effective defence mechanisms could be taken into account, but also their effectiveness. For it would be of no benefit if the mechanism could not allow an effective enforcement. The European Data Protection Board (EDPB) also highlights that every corporate entity must critically review the adequacy level of data protection in the data recipient country.[4] For example, the FISA allows US authorities to access critical data. However, it is to mention, that there is a significantly reduced risk of data access if the data importer isn't an electronic communications service provider.

Should the company come to a conclusion that the legal regulations or other practices in the third country don't meet the requirements of the SCCs, it must take

additional steps to ensure them. They may consist in technical and/or contractual measures. If even then it's not possible to assure data privacy standards, it only remains to prevent the transfer to the certain third country and if necessary, develop an exit-strategy for the data.

In the past months the US-President and EC-President reached basically an agreement on a new framework for transatlantic data flow. As learnt from the decisions Schrems I and II it should be this time "predictable and trustworthy". Nonetheless there is no draft available for the new regulatory framework agreement. In addition to that the European Centre for Digital Rights (NOYB) alleged that the US has no plans to change any of its surveillance laws, but only to ensure the prosecution according to the relevant orders. Complicating that, the Supreme Court of the United States decided in the recent case – FBI v. Fazaga –, a case challenging FBI surveillance of allegedly gathering information on Muslims through a confidential informant, that effectively the US government has more freedom to invoke "state secrets" in spying cases. The reason is that the Supreme Court of the US finds inter alia that the Congress did not eliminate the state secrets privilege regarding spying cases when it enacted reforms in FISA. [5] As a result it comes again to the FISA, which doesn't satisfy the requirements of the EU data privacy law. According to this, a renewed agreement between the USA and EU is even further away than before.

As a conclusion it can be stated that even if in an unlikely scenario the US and EU would reach in the near future an agreement on the transatlantic data flow, Mr. Schrems already announced his intention to challenge the agreement at the ECJ. In the light of the current acts as FISA it is highly possible that he will win again and the ECJ will strike down the new agreement.

The corporate entities must better not rely on a new agreement and concentrate themselves on developing and optimizing their risk assessments so that they will in either case be able to deal with the transatlantic data flow.

References:

1. Press release of the ECJ No. 117/15, Luxembourg, 6 October 2015, Judgment in Case C-362/14 Maximillian Schrems v. Data Protection Commissioner – https://curia.europa.eu/

jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf

2. Judgement of the ECJ (Grand Chamber) in Case C-311/18, edge number 185, – https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=4584826
3. Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II, pag. 6, 7, – https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF
4. European Data Protection Board document on the judgment of the ECJ in Case C-311/18 – Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems adopted on 23 July 2020 – https://edpb.europa.eu/sites/default/files/files/file1 /20200724_edpb_faqonc jeuc31118_en.pdf
5. Supreme Court of the United States No. 20 – 828 “FEDERAL BUREAU OF INVESTIGATION, ET AL., PETITIONERS v. YASSIR FAZAGA, ET AL.” (FBI v. Fazaga), pag 13, – https://www.scotusblog.com/wp-content/uploads/2022/03/20-828.pdf