your Legal Lab

"Safe Harbour Principles" – Are they really safe?

(Decision of the Court of Justice of the EU on case No. C-362/14)

If you have questions or would like additional information on the material covered in this article, please contact:

Katerina Christodoulou, Partner
+302103388831
katerina.christodoulou@yourlegalpartners.gr

Maria Golfinopoulou, Partner
+302103388831
maria.golfinopoulou@yourlegalpartners.gr

www.ylp.gr

Introduction – Legal Framework

According to article 25§1 of Directive 95/46 the transfer from a Member State of the EU to a third party of personal data, which are undergoing processing or are intended for processing after transfer, may take place provided that the third country in question ensures an adequate level of protection. On the basis of article 25§6 of the said Directive 95/46, according to which the Commission may find that a third country ensures an adequate level of protection by reason of its domestic law or of the international commitments it has entered into for the protection of the private lives and basic freedoms and rights of individuals, the Commission adopted Decision 2000/520. By virtue of the aforementioned Decision 2000/520 it was concluded that the "Safe Harbour Principles" issued by the US Department of Commerce on 21 July 2000 are considered to ensure an adequate level of protection for personal data transferred from the EU to organisations established in the United States.

i) Factual Background of the case brought before the Court of Justice of the European Union.

Mr. Maximilliam Schrems, an Austrian national residing in Austria, has been a user of the Facebook social network since 2008. On 25 June 2013 Mr. Schrems filed a complaint before the Data Protection Commissioner of Ireland, by virtue whereof he asked the latter to exercise his statutory powers by prohibiting Facebook from transferring his personal data to the United States, on the ground that the law and practice in force in the United States did not ensure adequate protection of the personal data held in its territory against the surveillance activities of competent public authorities (i.e. National Security Agency – "NSA"). The Commissioner rejected Mr. Schrems' complaint on the ground that (a) there was no evidence that Mr. Schrems' personal data had been accessed by the NSA and (b) his complaint could not be admissible since any question of the adequacy of data protection in the United States had to be determined in accordance with the aforementioned Decision 2000/520 and the Commission had found in that decision that the United States ensured an adequate level of protection. Consequently, Mr. Schrems brought an action before the High Court of Ireland challenging the decision at issue in the main proceedings.

The High Court considered that the evidence adduced by the parties demonstrated a "significant over-reach" on the part of the NSA and other federal agencies of the United States. Once the personal data has been transferred to the United Stated, it is capable of being accessed by the NSA and other federal agencies, such as the Federal Bureau of Investigation (FBI), in the course of indiscriminate surveillance and interception carried out by them on a large scale. According to the High Court, Decision 2000/520 does not satisfy the requirements set out by Articles 7 and 8 of the Charter, since the right to respect for private life would be rendered

meaningless if State authorities were authorised to access electronic communications on a casual and generalized basis without any objective justification based on considerations of national security or the prevention of crime that are specific to the individual concerned and without those practices being accompanied by appropriate and verifiable safeguards. Under those circumstances, the High Court decided to stay the proceedings and to refer the following questions to the Court of Justice of the EU for a preliminary ruling: (a) whether in the course of determining a complaint which has been filed before a national independent data protection authority, according to which personal data is being transferred to another third country (in this case, the United States of America) the laws and practices of which, it is claimed, do not contain adequate protections for the data subject, the said data protection authority is absolutely bound by the Community's contrary Decision 2000/520, (b) or, alternatively, the national independent data protection authority may and/or must conduct its own investigation of the matter in the light of factual developments in the meantime since the said Commission decision was first published?

ii) The Decision of the Court of Justice of the EU (Grand Chamber)

The Court of Justice of the EU considered that pursuant to the fourth paragraph of Article 288 TFEU, the Decision 2000/520 of the Commission, issued by virtue of Article 25§6 of Directive 95/46, is binding on all Member States to which it is addressed and is therefore binding on all their organs, in so far as it has the effect of authorizing transfers of personal data from the Member States to the third country covered by it. Thus, until such time as the Commission Decision is declared invalid by the Court of Justice, the Member States and their organs, including their independent data protection authorities, cannot adopt measures contrary to that decision, such as acts intended to determine with binding effect that the third country covered by it does not ensure an adequate level of protection.

However, a Commission Decision adopted pursuant to Article 25§6 of Directive 95/46, such as Decision 2000/520, cannot prevent persons whose personal data has been or could be transferred to a third country from lodging with the national data protection authorities a claim, concerning the protection of their rights and freedoms in regard to the processing of that data. Whilst the national authorities are admittedly entitled to question the validity of Decision 2000/520, they are not, however, endowed with the power to declare such an act invalid themselves.

Having regard to those considerations, in case a person whose personal data has been or could be transferred to a third country which has been the subject of Commission Decision 2000/520, lodges with a national data protection authority a claim concerning the protection of his rights and freedoms in regard to the processing of that data and contests, in bringing the claim the compatibility of that decision with the protection of the privacy and of fundamental rights and freedoms of individuals shall be examined, it is incumbent upon the national data protection authority to examine the claim with all due diligence. In case the said national authority concludes that the arguments put forward in support of such claim are unfounded and therefore rejects it, the person who lodged the claim must have access to judicial remedies enabling him to challenge such a decision before the national courts. Those courts must stay proceedings and make a reference to the Court of Justice for a preliminary ruling on validity, in case they consider that one or more grounds of invalidity put forward by the parties are well founded. In the converse situation, where the national data protection authority considers that the objections advanced by the person who has lodged with it a claim concerning the protection of his rights in regard to the processing of his personal data are well founded, that authority must be able to engage in legal proceedings before the national courts, in order for them, if they share its doubts as to the validity of the Commission decision, to make a reference for a preliminary ruling for the purpose of examination of the decision's validity.

As to the validity of the Decision 2000/520, the Court of Justice considered that a third country cannot be required to ensure a level of protection identical to that guaranteed in the EU legal order.

However, it is required by the third country to ensure that, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter. Moreover, when the validity of a Commission decision adopted pursuant to Article 25§6 of Directive 95/46 is examined, account must also be taken of the circumstances that have arisen after that decision's adoption.

In this case Decision 2000/520 a) does not include sufficient findings regarding the measures by which the United States ensures an adequate level of protection, within the meaning of Article 25§6 of the aforementioned Directive, by reason of its domestic law or its international commitments, b) 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 organisations 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, c) does not contain any finding regarding the existence, in the United States, of rules adopted by the State intended to limit any interference with the fundamental rights of the persons whose data is transferred from the European Union to the United States, interference which the State entities of that country would be authorised to engage in when they pursue legitimate objectives, such as national security, d) does not refer to the existence of effective legal protection against interference of that kind. **Consequently, the Court of Justice decided that without there being any need to examine the content of the safe harbor principles, Article 1 of Decision 2000/520 fails to comply with the requirements laid down in Article 25§6 of Directive 95/46, read in the light of the Charter, and that it is accordingly invalid.**

iii) Greek Data Protection Authority - Conclusion

Upon issuance of the above mentioned landmark decision of the Court of Justice, the EU data protection authorities assembled on 16.10.2015 in the Article 29 Working Party ("WP") and discussed the first consequences to be drawn at European and national level. The WP concluded that transfers from the EU to the United States can no longer be framed on the basis of Commission Decision 2000/520 and therefore **transfers that are still taking place under the Safe Harbour decision are unlawful.** Furthermore, it underlined the necessity of establishing new political, legal and technical solutions enabling data transfers to the territory of the United States that respect the fundamental right to private life, such as a new Safe Harbour that includes obligations on the necessary oversight of access by public authorities, on transparency and on redness mechanisms. In the meantime, Standard Contractual Clauses and Binding Corporate Rules shall be applied.

In accordance with the said statement of the WP dated 16.10.2015, **the Greek Data Protection Authority issued a statement on 23.10.2015,** by virtue of which**, it instructed the Greek data controllers that transfer personal data to the United States on the legal basis of Decision 2000/520 on Safe Harbour, to stop immediately such transfer and implement Standard Contractual Clauses and Binding Corporate Rules instead.** So, basically, the **Greek Data Protection Authority** requires all Controllers that have made a notification regarding trans-border transmission to the US based on the Safe Harbor, **to stop any data transmission to that country**. Until the WP and the Greek Data Protection Authority issue further guidance as per the legal grounds for trans-border transmission to the US, all Controllers that are interested in transmitting personal data to the US should either uphold Standard Contractual Clauses and Binding Corporate Rules (if applicable) or file a request to receive permission from the Greek Data Protection Authority. New developments on the safe harbor issue are likely to come, so close monitoring on the legal environment is necessary.