Privacy Shield – Decision C-311/18

The CJEU overturned the "Safe Harbour" system on 6 October 2015, allowing data transfers between the European Union and the United States, in the famous "Schrems I" case. Following this ruling, Facebook Ireland continued to transfer data to US servers, but on the basis of standard contractual clauses under Commission Decision 2010/87. Schrems proceeded with this "battle" for the protection of personal data through a second request to the Irish Privacy Authority. The request from the well-known Austrian lawyer was aimed at stopping and prohibiting any transfer of data to the US because, according to the petitioner, North American data protection legislation would not provide sufficient protection for European citizens. The Irish Privacy Authority, therefore, had to determine the validity of Decision 2010/87, bringing the matter before the High Court. In the meantime, the Commission Decision 2016/1250 intervened, establishing the adequacy of the data transfer system between the European Union and the United States known as the "Privacy Shield".

The Irish High Court thus asked the following questions to the CJEU: whether the GDPR is applicable to transfers of personal data that occur on the basis of standard contractual clauses under Decision 2010/87; what level of protection is required by the GDPR in relation to such data transfers; what are the responsibilities of the Authorities in these circumstances; finally, the High Court requested the CJEU to rule on the validity of Decision 2010/87 and Decision 2016/1250.

The court with reference to the first question raised by the High Court ruled that in the present case, since the transfer of personal data is carried out by Facebook Ireland to Facebook Inc., by two legal persons, such transfer does not fall within the scope of Article 2(2)(c) of the RGPD, which concerns the processing of data carried out by a private individual in the course of a strictly personal or domestic activity. Nor does such transfer fall within the exceptions appearing in Article 2(2)(a), (b) and (d) of said Regulation, since the activities mentioned therein by way of example are, in all cases, activities specific to States or State authorities, which are outside the areas of activity of private individuals. However, the possibility that personal data transferred between two economic operators for commercial purposes may, during or after the transfer, be processed for public security, defence, and State security purposes by the authorities of the third party country concerned cannot exclude such transfer from the scope of application of the RGPD.

Regarding the second question raised by the Irish High Court, the Court of Justice stated that the expression 'adequate level of protection' must be understood, as confirmed by recital 104 of the GDPR, as requiring the country to which the data is directed to effectively ensure, in view of its national legislation or international commitments, a level of protection of fundamental rights and freedoms substantially equivalent to that guaranteed within the Union under that Regulation, read in light of the Charter of Fundamental Rights of the European Union

By shifting the focus to measures that the supervisory authorities themselves could take to limit the transfer in the event of a transfer carried out on the basis of standard clauses deemed by the same authority to lack adequate safeguards, the Court of Justice has ruled that in the version resulting from Implementing Decision 2016/2297, Article 4 of Decision 2010/87 contains a reference to the power of these authorities, currently under Article 58(2)(f) and (j) of the GDPR, to suspend or prohibit such transfer, without in any way limiting the exercise of this power to exceptional circumstances.

The Court finally focused on the analysis of the validity of the 2010/87 and 2016/1250 decisions.

Decision 2010/87 provides for so-called standard protection clauses, which, according to Article 46(2)(c) of the same Regulation only aim at providing data controllers or processors established in the Union contractual safeguards that apply uniformly in all third party countries and, therefore, are irrespective of the level of protection guaranteed in each of them. Rather, the standard protection clauses may, depending on the situation in one or another third party country, require additional measures to be taken

by the data controller to ensure compliance with this level of protection. Indeed, where the controller or the processor, established in the Union, cannot take adequate additional measures to ensure such protection, they or, alternatively, the competent supervisory authority, are required to suspend or terminate the transfer of personal data to the third party country concerned. Therefore, the sole fact that standard data protection clauses contained in a Commission decision adopted pursuant to Article 46(2)(c) of the GDPR, such as those contained in the annex to the Decision 2010/87, do not bind the authorities of the third party countries to which personal data may be transferred cannot affect the validity of that decision, which must therefore still be considered to be in force.

The Court also examined the validity of the decision on the “Privacy Shield” and found that the requirements of US domestic law, and in particular certain programs that allow public authorities in the United States to access personal data transferred from the EU to the United States for the purposes of national security, involve limitations on the protection of personal data that are not designed to meet requirements substantially equivalent to those provided for in EU law and that such legislation does not grant the interested parties legally actionable rights against the U.S. authorities. In particular, the decision "Privacy Shield", in point I.5 of its Annex II, under the heading "Principles of the Privacy Shield regime", also points out that the adherence to such principles may be limited to the extent necessary to meet national security requirements, public interest, or administration of justice. Consequently, that decision establishes the primacy of the aforementioned requirements over these principles. In consideration of its general character, the exception contained in point I.5 of Annex II of the Decision "Privacy Shield" therefore makes possible interference based on security requirements, national interest, and the public interest or the domestic legislation of the United States, in the fundamental rights of persons whose personal data are or may be transferred from the Union to the United States (for example, the FISA Court does not authorize individual surveillance measures, but rather programmes of monitoring, such as PRISM and UPSTREAM, based on the annual certifications prepared by the General Attorney and the Director of National Intelligence).

In view of the above, what could the future hold for Data transfers between European countries and the USA? It is likely that the privacy authorities will publish a *vademecum* or guidelines on additional safeguards for the transfer of personal data to third party countries that do not provide an adequate level of protection. It is also possible that the EU Commission may anticipate any decision of the European Data Protection Board (Edpb) by publishing a new version of Standard Contractual Clauses (SCCs) or a negotiated and correct version of the Privacy Shield in order to resolve the risks identified by the Court of Justice. In the meantime, however, the following three categories of additional safeguards can be identified:

a) Contractual guarantees that restrict the data importer's ability to allow access to third parties, even if they are government agencies, or that create additional forms of support and assistance for the data subject in order to protect its rights against third parties;

b) additional clauses requiring prior notification and authorisation of the data exporter in the event of a request for disclosure by the foreign public authority or the right of the data exporter to block the flow of data and effectively prevent further transfer;

c) clauses providing for forms of cooperation between the data exporter and the data importer in order to allow the data subject, in addition to transparency with regard to the further transfer of its data, the possibility of using, without bearing the economic charges and legal costs, the procedural tools and rights of action provided for by the legislation of the importing country to oppose the disclosure of its personal data.