Court of Justice of European Union Invalidates EU-US Privacy Shield

On 16 July 2020, the Court of Justice of the European Union (***CJEU***) delivered its judgment in the *Facebook Ireland and Schrems case* (C-311/18, ***Schrems II case***). The CJEU invalidated Decision 2016/1250 on the adequacy of the protection provided by the EU-US Privacy Shield. The CJEU ruled that the EU-US Privacy Shield does not provide adequate protection and can therefore no longer serve as a legal instrument permitting the transfer of personal data from the EU to the US. As a result, transfers of personal data between the EU and the US that rely on the EU-US Privacy Shield are now illegal. However, the CJEU considered that Commission Decision 2010/87 on standard contractual clauses (***SCCs***) for the transfer of personal data to processors established in third countries is valid and can be relied upon, provided that the applicable legislation does not prevent the recipient from complying with its contractual obligations under the SCCs.

International transfers under GDPR

The General Data Protection Regulation (Regulation 2016/679 – the ***GDPR***) ensures that personal data are protected in the EU (and the European Economic Area – ***EEA***). However, if personal data are transferred outside the EU/EEA, this protection must travel with such data. The GDPR permits personal data transfers to those third countries that the European Commission has declared do provide for an adequate level of protection for personal data by way of a so-called "adequacy decision". In this adequacy decision, the European Commission looks at the laws and regulations of a third country (or a part thereof) to determine whether the level of protection that is provided for personal data is "essentially equivalent" to the protection provided under the GDPR.

If the data importer is not covered by an adequacy decision, exporting data controllers (i.e., the party determining the purpose and means of the processing) should implement appropriate safeguards to permit the international transfer, unless one of the derogations of Article 49 of the GDPR applies.

In most cases, these appropriate safeguards take the form of a contractual arrangement between the exporter and the importer containing standard contractual clauses set out by the European Commission and aimed at ensuring the adequate protection of personal data transferred outside the EU. The *Schrems II case* concerns the validity of the SCCs adopted by the European Commission in Decision 2010/87/EU. The case questions the adequacy of the level of protection related to the SCCs mechanism.

History of the case

In 2015, the CJEU delivered its judgment in the *Schrems I case* (C-362/14), which invalidated the Commission adequacy decision on the EU-US Safe Harbour scheme, the predecessor of the Privacy Shield.[1]

---

[1] Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (OJ 2000 L 215, p. 7).

The case originated from a complaint filed in 2013 by Mr. Schrems with the Irish Data Protection Commission (***IDPC***) challenging Facebook Ireland's transfers of user data to Facebook Inc., located in the United States. In view of the then recent revelations by Edward Snowden on the methods used by US national security agencies, Mr. Schrems argued that US legislation did not offer adequate protection against surveillance of the data transferred to that country, and asked the IDPC to suspend the data transfer to the US. The IDPC rejected the request and Mr. Schrems appealed to the Irish High Court which referred questions to the CJEU for a preliminary ruling. In response to these questions, the CJEU invalidated the European Commission's Safe Harbour decision.

Following the *Schrems I* judgment, Facebook continued its transfers of personal data, now relying mainly on SCCs, and later on its registration under the EU-US Privacy Shield scheme, which had replaced the Safe Harbour and received an "adequacy" finding from the European Commission on 12 July 2016 (Commission Decision 2016/1250). At the same time, the proceeding was referred back to the Irish High Court who now had to determine the validity of the SCCs adopted by Facebook Ireland. The Irish High Court subsequently referred new questions to the CJEU asking whether the US ensures the adequate protection of EU citizens' personal data and whether the SCC mechanism and/or the EU-US Privacy Shield offer sufficient safeguards for the protection of EU citizens' freedoms and fundamental rights.

CJEU judgment

The CJEU started by recalling that EU law, in particular the GDPR, applies to the transfer of personal data for commercial purposes by an economic operator established in the EU to another economic operator established in a third country, even if the data may be processed by the authorities of the third country for the purposes of public security, defence and State security.

With regard to the protection required for such transfer, the CJEU held that the requirements laid down by the GDPR must be interpreted as meaning that data subjects must be granted a level of protection essentially equivalent to that guaranteed within the EU by the GDPR, read in conjunction with the Charter of the Fundamental Rights of the European Union (the ***Charter***). When assessing the level of protection, the CJEU looked at both the substantive provisions of the contractual clauses, and the relevant aspects of the legal system of that third country.

On this basis, the CJEU examined the validity of Commission Decision 2010/87 (on controller-to-processor SCCs) and found that it establishes the level of protection required by EU law since: (i) it imposes an obligation on both the data exporter and the recipient to verify, prior to any transfer, whether the level of protection required by EU law is respected in the third country, and (ii) it requires the data recipient to inform the data exporter of any inability to comply with the SCCs, in which case the data exporter must suspend the transfer of data. In other words, the CJEU underlined that a correct application of the SCCs requires the parties to assess whether they can comply with their respective obligations under the SCCs in light of the facts at hand and the legal system in the third country where the data recipient is established.

The CJEU also added that supervisory authorities are required to stop or prohibit such transfer to a third country where the SCCs are not or cannot be complied with in that country, and if the protection of the data that is required by EU law cannot be ensured by other means.

Finally, the CJEU examined the validity of Commission Decision 2016/1250 (on the EU-US Privacy Shield) in light of the requirements of the GDPR, read together with the provisions of the Charter governing respect

for private and family life, personal data protection and the right to effective judicial protection. In that regard, the CJEU noted that the decision allows the requirements of US national security, public interest and law enforcement to have primacy and therefore interfere with fundamental rights of persons whose data are transferred to the US. The CJEU also noted that the limitations on the protection of personal data arising from US law are not restricted in a way that satisfies the requirement of equivalent protections under EU law since certain surveillance programmes are not limited to what is strictly necessary. In addition, there are no limitations on the power of such surveillance programmes and insufficient guarantees for non-US citizens. Moreover, the CJEU considered that the Ombudsman mechanism set up under the EU-US Privacy Shield provides insufficient judicial protection against interference by US authorities.

The CJEU declared Commission Decision 2016/1250 to be invalid. Therefore, it can no longer be used for the transfer of personal data from the EU to the US. However, transfer of personal data from the EU to the US can still take place using SCCs, provided that parties assess whether their obligations under the SCC are not in conflict with US laws – including surveillance laws – that apply to their activities. This guidance on the application of SCCs will also be relevant for recipients in third countries other than the US which receive personal data from EU controllers based on SCC.

Another important take-away of this judgment is that EU supervisory authorities are called into action assessing, on a case-by-case basis, whether the use of SCCs is justified.

The full text of the *Schrems II* judgment can be found here.

23 July 2020