CUATRECASAS

Intellectual Property, Media and IT

Legal Flash | Portugal

July 22, 2020

Judgment of the Court of Justice of the European Union (CJEU) in case C-311/18 (Schrems II)

On July 16, 2020, the CJEU published the long-awaited judgment on case C-311/18 (Data Protection Commissioner vs. Maximillian Schrems, Facebook Ireland), with significant consequences for the transfer of personal data between the European Union (EU) and the United States (US).

I. Background

The current General Data Protection Regulation (Regulation (EU) 2016/679 of April 27 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (GDPR)) establishes limitations on the transfer of personal data obtained in the European Economic Area (EEA) to other countries outside this area.

Specifically, such transfers are only allowed if the European Commission reaches an adequacy decision with the third country (the country outside the EEA that receives the data), or, failing that, if the organizations that export and import personal data adopt adequate guarantees.

This is not a new feature of the GDPR, as its predecessor, Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995 on the protection of natural persons with regard to the processing of personal data and the free movement of such data (Directive 95/46/EC), clearly stipulated these limitations. It was precisely while Directive 95/46/EC was still in force that the adequacy decision between the European Commission and the US, known as the "Safe Harbor" decision at the time, was legally challenged in the Schrems I case.

To put this into context, Maximillian Schrems was an Austrian citizen residing in Austria who had been a Facebook user since 2008. As with other users residing in the European Union, the personal data of Mr. Schrems was, in whole or in part, transferred by Facebook Ireland to servers belonging to Facebook Inc. located in the US, where it was processed. Mr. Schrems lodged a complaint with the Irish supervisory authority, essentially seeking to ban these transfers. He maintained that US law and practices did not duly protect data transferred to that country from access by public authorities, and that the Safe Harbor adequacy decision did not effectively protect his rights as the data subject. In its Judgment of October 6, 2015, the CJEU, which was called to issue a preliminary ruling on a matter referred by the High Court of Ireland, declared the Safe Harbor decision invalid.

The invalidation of the Safe Harbor decision had a considerable impact on transfers of personal data to the US. For almost a year, and until the European Commission managed to come up with a new adequacy decision with the US, organizations exporting personal data to the US could not do so based on it and had to adopt additional guarantees to ensure this international flow of data was legal.

It was only on July 12, 2016 that a new adequacy decision between the European Commission and the US was published, i.e., the "Privacy Shield." Until July 16, 2020, this was the legal mechanism for transferring personal data from the EEA to the US, and more specifically to American companies that had adhered to the Privacy Shield.

The CJEU has now declared this new adequacy decision invalid, with the consequences indicated below.

II. Facts and decision

The case essentially involved two claims:

1) The validity of standard contractual clauses, which, basically, are a kind of adhesion contract drawn up by the European Commission that can be used by organizations that wish to export personal data to third countries with those that import such personal data; and

2) The validity of the Privacy Shield, which was the adequacy decision in force that allowed the transfer of personal data from the EEA to the US, provided that the organization based in the US had adhered to this mechanism.

The CJEU confirmed that the standard contractual clauses provided by the European Commission were legal, but it made it clear that it was up to the data controller to ensure that the legal context of the country where the data was imported allowed the full and effective adoption of these contractual clauses: *"For this purpose, the assessment of the level of protection provided in the context of such a transfer must, inter alia, take into account both the contractual stipulations agreed between the data controller or its subcontractor in the European Union and the recipient of the transferred data in the third country and the relevant elements of the third country's legal system, insofar as public authorities in the third country may be able to access the personal data thus transferred."*

The adequacy decision in force with the US until that time, the Privacy Shield, was declared invalid, as occurred with its predecessor, the Safe Harbor decision. Briefly, the CJEU ruled that US public authorities could disproportionately and inappropriately interfere with the personal data transferred, and that there were no mechanisms in place to ensure that data subjects would be able to contest abusive use of their data by US authorities.

In the specific context of the main issue raised in this judgment, Facebook Ireland cannot transfer personal data collected in the EEA to Facebook Inc. based on the Privacy Shield. Furthermore, the ruling makes it clear that recourse to standard contractual clauses is allowed, insofar as they are compatible with the requirements of the domestic jurisdiction of the country that imports this personal data.

III. Future alternatives:

Companies that have so far used the Privacy Shield as a mechanism to ensure an adequate level of protection when transferring personal data to the US for processing are advised to review their international personal data flows and assess alternative mechanisms to ensure an adequate level of protection.

In particular, companies that transfer data to the US based on the Privacy Shield, standard contractual clauses or binding rules that apply to companies should seek further guidance from the competent

supervisory authorities. Of particular concern are companies that are subject to collaboration obligations with US intelligence services.

However, if the data importer is not subject to US requirements concerning access to data by intelligence services, additional protections such as encryption or "tokenization" should still be required, which will allow the exporter to conclude that adequate (technical) safeguards for the data have been put in place, given that access to the content is protected.

The CJEU also requires the data importer to inform the exporter whether it meets the necessary conditions to receive the imported data in compliance with the requirements of the GDPR. Therefore, before transferring personal data to organizations based in third countries in the future, the data controller is advised to ask the data importer for specific information and a statement confirming that it meets the necessary legal and operational conditions to ensure a level of personal data protection that is equivalent to the level provided by the GDPR.

Finally, although the Schrems II case has specific implications for data transfers to the US, it is important to remember that standard contractual clauses effectiveness in the jurisdiction of the importing country will always be a precedent condition, whether or not this is the United States.

Therefore, it will be important for legal partners from different parts of the world to collaborate closely, as the global (and not just European) impact of the GDPR is now becoming increasingly clear.

Contact

Cuatrecasas, Gonçalves Pereira & Associados,
Sociedade de Advogados, SP, RL
Sociedade profissional de responsabilidade limitada

Lisbon
Praça Marquês de Pombal, 2
1250-160 Lisboa I Portugal
Tel. (351) 21 355 3800 I Fax (351) 21 353 2362
cuatrecasasportugal@cuatrecasas.com I www.cuatrecasas.com

Oporto
Avenida da Boavista, 3265 - 5.1
4100-137 Porto I Portugal
Tel. (351) 22 616 6920 I Fax (351) 22 616 6949
cuatrecasasporto@cuatrecasas.com I www.cuatrecasas.com

For additional information on the contents of this document, please contact Cuatrecasas.

Information about the processing of your personal data

Data Controller: Cuatrecasas, Gonçalves Pereira & Associados, Sociedade de Advogados, SP, RL ("Cuatrecasas Portugal").
Purposes: management of the use of the website, of the applications and/or of your relationship with Cuatrecasas Portugal, including the sending of information on legislative news and events promoted by Cuatrecasas Portugal.
Legitimacy: the legitimate interest of Cuatrecasas Portugal and/or, where applicable, the consent of the data subject.
Recipients: third parties to whom Cuatrecasas Portugal is contractually or legally obliged to communicate data, as well as to companies in its group.
Rights: access, rectify, erase, oppose, request the portability of your data and/or restrict its processing, as described in the additional information.
For more detailed information on how we process your data, please go to our *data protection policy*.

If you have any questions about how we process your data, or if you do not wish to continue receiving communications from Cuatrecasas Portugal, we kindly ask you to inform us by sending a message to the following email address data.protection.officer@cuatrecasas.com