TECNOLOGY

SCHREMS II CASE - IMPACTS ON THE INTERNATIONAL TRANSFER OF PERSONAL DATA

03 AUGUST 2020

AUTHORS

JULIA AKERMAN SHINOHARA
LAWYER / SÃO PAULO

MARINA MORELLO ABBUD
LAWYER / SÃO PAULO

/

In a decision handed down on July 16, the Court of Justice of the European Union (CJEU) changed the understanding of the European Commission on international transfer of personal data between the United States and the European Union.

The decision, issued in the Schrems II Case,[1] raised two main issues:

> The first relates to the validity of the EU-U.S. Privacy Shield, which used to authorize the transfer of personal data of individuals located in the European Union to the United States. It was questioned whether this instrument would actually meet the requirements of the European Union's General Data Protection Regulation (GDPR), in view of the US government's surveillance programs, which authorize the country's public security authorities to access and use personal data imported from the European Union.

> The second issue concerns the validity of the standard contractual clauses approved by the European Commission as adequate and sufficient instruments for the international transfer of personal data, in cases in which there is no adequacy decision handed down by the European Commission in relation to the country receiving such data.

Privacy Shield Invalidation: consequences for international transfer of personal data

In 2016, the US Department of Commerce and the European Commission entered into the agreement known as Privacy Shield, which established a set of principles and safeguards to be guaranteed by the companies that are party to the agreement, in order to enable the transfer of personal data of individuals located in the European Union to those companies located in the United States.

Until now, the Privacy Shield was an instrument recognized by the European Commission as adequate to ensuring a level of protection compatible with the one afforded by the GDPR[2] and, as a result, adherence to the agreement was sufficient to authorize the transfer of data from individuals located in the European Union to companies and organizations located in the United States that were adhering to the Privacy Shield, without the need for additional safeguards or authorizations from the data protection authorities of each of the European Union member states.

However, the recent decision rendered by the CJEU in the Schrems II Case invalidated that understanding, ceasing to recognize the adequacy of Privacy Shield as a legal basis for the international transfer of personal data. According to CJEU's understanding, the surveillance programs implemented by the US government represent a disproportionate violation of the rights to privacy and data protection guaranteed by the GDPR. This is because, by failing to make clear the limitations on the powers granted to the intelligence services, the surveillance programs ultimately allow the public authorities to commit excesses and are not limited to what is strictly necessary to guarantee national security, as provided by the GDPR.

Furthermore, for the CJEU, US law does not guarantee judicial or other effective means for the data subjects to enforce the protection of their data against access and misuse by public authorities, nor the right to request rectification or deletion of their data.

That said, the CJEU concluded that US legislation and practices are not adequate to the GDPR and that the Privacy Shield is not sufficient to remedy these problems and, therefore, does not constitute a valid legal basis to legitimize the transfer of data from individuals located in the European Union to the United States.

Standard Contractual Clauses: guarantee of protection in international transfer of personal data?

Standard contractual clauses consist of standard template provisions, pre-approved by the European Commission, which should be included in contracts involving the international transfer of personal data as a safeguard measure to ensure minimum standards of security and protection of rights, as guaranteed by the GDPR. Since 1987, such clauses have been recognized by the European Commission as a valid and appropriate mechanism for authorizing international transfers of personal data, as laid down in decision No. 2010/87.

This understanding was confirmed by the CJEU in the Schrems II Case. However, the CJEU highlighted that the validity of standard contractual clauses is not absolute and is conditioned to their practical effectiveness in light of the laws, regulations and practices of the destination country, and it would be up to the controller to carry out this analysis.

That is, before transferring personal data to other countries, the controller must assess whether the standard contractual clauses will actually be effective or whether the data importer will be prevented from complying with them by legal provisions or by orders issued by the local public authorities, since the standard contractual clauses only bind the parties to the contract (data exporter and data importer), but not the public authorities of the destination country.

Should the controller believe that the standard contractual clauses will not be effective to ensure the protection of personal data, it must adopt additional safeguard measures. Otherwise, the controller may be prohibited by the data protection authorities of the European Union member states from transferring data to such countries. The CJEU also emphasized that this analysis shall be carried out periodically and that the controller must suspend the transfer of data if circumstances in the destination country change.

Consequences of the Schrems II Case at the global and national level

The decision in the Schrems II Case will have a great impact on the global market, since more than five thousand US companies used to resort to the Privacy Shield to legitimize the transfer of data from people located in the European Union, and now they will have to adopt new safeguard measures, as is already the case in other countries that have not had their adequacy recognized by the European Commission, such as Brazil.

In addition, the decision made it clear that standard contractual clauses are not absolute, which means that their mere insertion in the contracts may no longer be sufficient to legitimize the international transfer of data, especially in the case of countries whose laws and practices make their effectiveness unfeasible.

Finally, the decision highlights the importance of having local laws and practices compatible with the level of protection guaranteed by the GDPR, since the non-compliance may result in increased costs for the data transfer (due to the additional safeguards to be adopted by the controller) or, further, in the prohibition of transfer.

In this context, the entry into force of the Brazilian General Data Protection Law (LGPD) and the formation of the Brazilian Data Protection Authority (ANPD) become even more urgent. This is because, although it is clearly inspired by the GDPR, which may facilitate recognition of its adequacy, the LGPD must become effective and Brazil must have an independent ANPD capable of guaranteeing the effectiveness of the LGPD and, consequently, the protection of personal data processed here.

---

[1] The Schrems II Case arose from a complaint lodged by the Austrian data protection activist Maximillian Schrems with the Irish supervisory authority, seeking to prohibit the transfer of his personal data from Facebook Ireland to Facebook Inc, located in the United States, on the grounds that U.S. law and practices did not provide adequate protection against access to personal data by public authorities.

[2] The legal structure and standards set established in the Privacy Shield were subject to a decision by the European Commission (decision No. 2016/1250), issued in August 2016. It was recognized that the Privacy Shield is an appropriate tool to legitimize the international transfer of data between the US and the European Union.