International Data Transfers – Consequences of the European Court of Justice's Schrems II Decision

1 September 2020

I/ Introduction

On 16 July 2020, the **Court of Justice of the European Union** (CJEU) invalidated the **EU-US Data Protection Shield** (Privacy Shield)[1] in its *Schrems II* decision,[2] in light of the provisions of the **General Data Protection Regulation** (GDPR)[3] and the **EU Charter of Fundamental Rights** (ECFR).[4] In short, the decision strikes down one of the critical legal basis for transatlantic data transfers. However, the CJEU upheld the validity of **Standard Contractual Clauses** (SCCs) for the transfer of personal data to processors established in third countries.[5] The CJEU's decision has important implications for all businesses involved in both transatlantic and international data transfers.

II/ Background and Analysis of the CJEU's Decision

The CJEU's *Schrems II* decision is the result of proceedings brought in Ireland by **Max Schrems** against the **Irish Data Protection Commissioner** relating to **Facebook's** data transfers to the **US**. The questions referred to the CJEU were as follows:

- (1) Whether the provisions of the GDPR apply to the transfer of personal data by an economic operator established in the EU to another operator established in a third country in which the data is liable to be proceeded by the authorities for public security, defence and state security purposes?
- (2) Which factors need to be taken into account for the determination of the required level of protection of SCCs under the provision of the GDPR?
- (3) Whether **Data Protection Authorities** (DPA) are required to suspend or prohibit data transfers under SCCs if the required level of protection cannot be ensured?
- (4) Whether SCCs are valid in light of provision of the ECFR?
- (5) Whether the Privacy Shield ensures an adequate level of protection under the GDPR?

[1] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield.
[2] Court of Justice of the European Union, *Data Protection Commissioner v. Facebook Ireland Ltd, Maximilian Schrems*, Case C-311/18, 16 July 2020.
[3] Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 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 (General Data .
[4] Charter of Fundamental Rights of the European Union.
[5] Commission Decision 2010/87 of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and the Council.

In essence, the CJEU found that:

- The provisions of the GDPR apply to personal data processed for national security purposes.
- The principle of "essential equivalence" with EU law enshrined in Art. 45 GDPR applies to SCCs under Art. 46 GDPR and must be based on EU law, especially the ECFR.
- DPAs have a duty to suspend or prohibit data transfers if the SCCs cannot be complied with or if the required level of protection appears to be insufficient.
- The Privacy Shield does not provide a system of equivalent protection of personal data between the EU and the US and is accordingly invalid with immediate effect.

The CJEU's decision raises a number of questions for DPAs and future international agreements. The immediate consequences of the decision are accordingly difficult to assess for businesses across the EU and further guidance is urgently required.

III/ Consequences of *Schrems II* on international data transfers

On 30 July, a number of representatives of the global business community addressed a joint industry letter to European Commissioner for Justice **Didier Reynders** and European Data Protection Board Chairwoman **Dr**. **Andrea Jelinek**. The business representatives called for new negotiations on a successor to the Privacy Shield and asked for guidelines from DPAs combined with a reasonable enforcement moratorium. However, the **European Data Protection Board** (EDPB) **Frequently Asked Questions (FAQ) on the consequences of the CJEU's decision** released on 23 July underline that no grace period will be granted to businesses transferring data to the US.

Since the Privacy Shield cannot be used by businesses for transatlantic data transfers, companies have to use SCCs and ensure their compliance with the GDPR, the ECFR and the CJEU's additional requirements. In particular, companies should conduct a **self-assessment of their SCCs** and verify that the level of data protection in the third country is essentially equivalent to the protection provided under EU law, taking into account:

- The circumstances of the transfers.
- The supplementary measures that the company can put in place to ensure that U.S. (or foreign) law does not impinge on the adequate level of protection guaranteed under the SCCs.

If the assessment concludes that the appropriate safeguards cannot be ensured, the company is required to suspend or end the transfer of personal data. Otherwise, if the company intends to continue to conduct data transfers despite the results of the assessment, it has to notify its decision to the competent **data protection supervisory authority** (SA).

Moreover, companies can still rely on the derogations of Article 49 GDPR[6] to transfer data to the US, but must ensure that:

- Transfers based on the consent of the data subject are:
  - Explicit,
  - Specific for the particular data transfer or set of transfers,
  - Informed, particularly as to the possible risks of the transfers.
- Transfers necessary for the performance of a contract between the data subject and the controller remain occasional.

[6] For more information on the derogations, see EPDB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 adopted on 25 May 2018.

- Transfers necessary for important reasons of public interest do not take place on a large scale and a systemic manner and meet a strict necessity test.

IV/ Policy Options and next steps

On 10 August 2020, European Commissioner for Justice **Didier Reynders** and U.S. Secretary of Commerce **Wilbur Ross** issued a joint statement indicating that the EU and the US have initiated discussions to evaluate the potential for an enhanced EU-US Privacy Shield framework to comply with the CJEU's decision. However, it must be underlined that the CJEU's interpretation of the principle of essentially equivalent protection under the GDPR sets very high standards calling for more than an enhanced Privacy Shield. Rather, the Court's decision invites the Commission to come forward with new approaches to international data transfers. Doing otherwise risks not meeting the CJEU's standards and creates an environment of legal uncertainty for businesses and the 800 million citizens on both sides of the Atlantic.

Further guidelines from the EDPB are urgently needed, especially on the supplementary measures that companies can put in place to comply the CJEU's decision. On 4 September, the EDPB created a **Task Force** that will prepare recommendations to assist controllers and processors with their duties to identify and implement appropriate supplementary measures to ensure adequate protection when transferring data to third countries.

In the meanwhile, businesses are required to undergo a careful assessment of their SCCs. With a team of specialised digital policy experts, Lighthouse Europe is ideally situated to assist businesses and industry groups with an interest in the policy discussions and can assist with a better understanding of the evolving legal environment for international data transfers.

By Boniface de Champris