Data Privacy and Cybersecurity

US-EU Privacy Shield Invalidated – What Now?

By: Kelly Hagedorn and David P. Saunders

The Court of Justice of the European Union (CJEU) ruled on 16 July 2020 in the case of *Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrem*s (**Schrems II**) that the US-EU Privacy Shield is invalid.[1] This important mechanism had previously allowed certain transfers of personal data from the European Economic Area (**EEA**) to the United States, and was widely used by international corporations. In many respects, the Privacy Shield was considered to be preferable to the other transfer mechanisms provided for by the General Data Protection Regulation (**GDPR**), and its demise will leave a substantial number of organisations looking for alternatives.

Background

As a starting point, the GDPR prohibits the transfer of personal data from the EEA to third countries. There are exceptions to this general position, including where the European Commission (the **Commission**) has determined that the third country has adequate laws to protect personal data.[2] Once the Commission has issued an adequacy decision, personal data can be transferred freely to organisations in the relevant country.

As regards the United States, however, the Commission has not decided that it has adequate data protection laws. However, the Commission issued a decision in 2016[3] that established the US-EU Privacy Shield (the **Privacy Shield Decision**). The Privacy Shield Decision permitted transfers of personal data to the United States if the recipient organisation had certified to the US Department of Commerce that it complied with certain privacy principles.[4] In that instance, the data recipient organisation was deemed adequate and transfers could take place freely, both from the certified entities' affiliated companies within the EEA, and also from unrelated persons located in the EEA. It was therefore a valuable mechanism to ensure compliance with the GDPR.

The other common mechanism to transfer personal data outside of the EEA in compliance with the GDPR is the use of Standard Contractual Clauses (**SCCs**). These are standard contractual provisions designed by the Commission[5] that are executed between a data exporter in the EEA and a data importer outside of the EEA. These were also subject to the CJEU's review in the instant case.

Schrems I

Max Schrems is an Austrian privacy advocate. He made a complaint to the Irish Data Protection Commissioner (**DPC**) concerning Facebook's transfer of his personal data from Ireland to the United States. At the time of his complaint, those transfers took place pursuant to the Safe Harbour regime, [6] which was the predecessor to the Privacy Shield scheme. The High Court of Ireland referred the question of the legitimacy of the Safe Harbour regime to the CJEU. In a 2015 decision colloquially known as Schrems I, the CJEU declared that the Commission's decision establishing Safe Harbour was invalid.[7]

Schrems II

The DPC asked Mr Schrems to reformulate his complaint following the Schrems I decision. Mr Schrems did so, in effect challenging the validity of the SCCs, the mechanism Facebook proceeded to use to transfer personal data from the EEA to the United States in compliance with the GDPR and its predecessor legislation. The DPC asked the Irish High Court to rule on the validity of the SCCs, which

in turn referred the question to the CJEU. The DPC also asked the Irish High Court – and therefore the CJEU – to consider the validity of the Privacy Shield Decision.

In its decision on 16 July 2020, whilst the CJEU declared that the use of SCCs was valid and that transfers of personal data out of the EEA pursuant to those arrangements was in accordance with the GDPR, it invalidated the Privacy Shield Decision, effective immediately.

The CJEU did so because the Privacy Shield Decision enshrines the position (as did Safe Harbour) that US national security, public interest and law enforcement will take priority over the rights of the European data subjects whose personal data has been transferred pursuant to the Privacy Shield. The US authorities can therefore obtain that personal data, and once they have it the law of the United States does not provide that data with protection equivalent to that provided by European law. In particular, US laws on surveillance, and data obtained via those surveillance programmes, go beyond what is permitted by equivalent European laws. In addition, there is no private right of action for individuals subject to US surveillance activities. The CJEU determined that the Ombudsman rubric provided for by the Privacy Shield was not an adequate means of protecting data subjects' rights in the absence of an ability to bring court proceedings.

The CJEU therefore declared that the Privacy Shield Decision is invalid. Upon publication of the Schrems II judgment, transfers of personal data to the United States pursuant to the Privacy Shield immediately ceased to be in compliance with the GDPR.

What Next?

This decision may cause Privacy Shield certified organisations – which number in the thousands – a significant degree of business interruption. Data transfers to the United States relying on the Privacy Shield mechanism should cease, and should only recommence once a new mechanism (such as SCCs) is put in place.

Fortunately, the GDPR does provide for alternative mechanisms to accomplish the data transfers. Organisations should consider whether these alternative methods need to be implemented both within corporate groups and with third parties from whom they receive personal data from Europe. Within corporate groups, binding corporate rules (a form of intra-group data transfer agreement, approved by a supervisory authority) may also be a good alternative.

Careful consideration should be given to ensure that – whichever mechanism is used – controllers and processors safeguard the personal data that they process in accordance with the applicable laws.

---

[1] Case C311/18 - https://files.lbr.cloud/public/2020-07/ecj judgment.pdf?lfEaIZBAlzPT0iT9teTLp.wk_PU3BtLZ.

[2] Andorra, Argentina, Canada (commercial organisations only), Faroe Islands, Guernsey, Isle of Man, Israel, Japan, Jersey, New Zealand, Switzerland and Uruguay.

[3] Decision 2016/1250 - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG.

[4] https://www.privacyshield.gov/eu-us-framework.

[5] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

[6] Decision 2000/520/EC - https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32000D0520.

[7] Case C362/14 - http://curia.europa.eu/juris/documents.jsf?num=C-362/14.

Contact Us

Kelly Hagedorn
khagedorn@jenner.com | Download V-Card

David P. Saunders
dsaunders@jenner.com | Download V-Card

Meet Our Team

Practice Leaders

David Bitkower
Chair
dbitkower@jenner.com
Download V-Card

David P. Saunders
Co-chair
dsaunders@jenner.com
Download V-Card