Deciphering Schrems II

W-INVESTMENT
Digitally Present

Shivani Agarwal | Samaksh Khanna | Mustafa Rajkotwala

Email- winvestmentofficial@gmail.com

Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems

1. INRODUCTION

The case of *Data Protection Commissioner ("**DPC**")* v. *Facebook Ireland Limited and Maximillian Schrems* (**"Schrems II"**) has been pivotal for enterprise data transfer processes, specially from the European Union ("**EU**") to the United States ("**US**"). Enterprises, across the globe, have for a time and since the inception of the General Data Protection Regulation (**"GDPR"**), been making the use of Standard Contractual Clauses (**"SCC"**) for transferring data outside the EU. The Schrems II judgment, Case C-311/18, delivered on July 16, 2020 by the Court of Justice of European Union ("**CJEU**"):

(i) asserted the validity of these SCCs, in the sense that SCCs shall still remain valid and enterprises may rely on their SCC models to transfer data outside the EU;

(ii) invalidated the Decision 2016/1250 which provided for the adequacy of the privacy shield (**"privacy shield decision"**) between the EU and the US.

The invalidation of privacy shield comes as a major shock to US companies. Almost 5384 organisations in the US have relied upon the privacy shield for data transfers from the EU to the

US. These companies must suspend their practice of using the privacy shield for data transfers into the US as the US does not provide any effective remedy to the EU citizens as per the Schrems II ruling. While SCC remain valid, transfers shall not be made as progressively as pre-Schrems II. The CJEU has directed the national supervisory authorities, as provided by Article 51(1) of GDPR, to have an explicit duty towards ensuring a more fair and stringent practice of data transfers. The national supervisory authorities now have the duty to suspend or prohibit data transfers if they consider that the EU SCC cannot be effectively implemented within the destination or recipient jurisdiction.

2. BACKGROUND

The case is a direct result of data practices by Facebook. Maximillian Schrems (**"Max Schrems"**), an Austrian lawyer, brought out a complaint against Facebook Ireland, a subsidiary of Facebook Inc. and the data processor of Facebook Inc., concerning the transfer of his personal data by Facebook Ireland to Facebook Inc. in the US. As per Article 44 of the GDPR, data transfer to recipient outside the EU can only be done when the level of protection in the destination country is 'adequate' as per the GDPR standards and comparable with the EU. In this context, Max Schrems submitted that the US was a mass surveillance state with data being processed by the intelligence agencies without having any adequate remedies in place for the EU citizens. In December 2019, the Advocate General of the CJEU, in his opinion to the CJEU stated that SCCs were a valid mechanism, provided that the parties to the SCC need to ensure that the countries outside the European Economic Area (**"EEA"**) have proper data protection laws and remedies, equivalent to that of the EEA. In Max Schrems' opinion as well, SCCs were a valid mechanism of data transfer. He only questioned the enforcement of rights provided by the GDPR in the US.

Moreover, in this context it is also important to understand that privacy shield was implemented as Safe Harbour (predecessor) was invalidated in Max Schrems v. Facebook Ireland Limited (**"Schrems I"**). The background of both decisions, Schrems II and Schrems I, remain the data transfer practices of Facebook Inc.

CJEU has validated the SCC but not the privacy shield.

3. STANDARD CONTRACTUAL CLAUSES LEGALITY

SCCs are used to transfer personal data outside the jurisdiction of the EU, to third countries, for the purpose of processing. It is interesting to note that even when the data is being collected in the EU and is not being processed but merely being *accessed* outside the EU, it would amount to as transfer of data. However, in the context of the GDPR and the EU laws, SCC are not the only mechanism used for the transfer of data from a data exporter to a data importer. Other mechanisms under Article 46 of GDPR include binding corporate rules, approved code of conduct as provided in Article 40 of the GDPR. In the present Schrems II case, the DPC argued that SCC was not a valid arrangement as it violated Articles 7, 8 and 47 of the EU Charter of Fundamental Rights **("EU Charter"**). The DPC argued that the clauses of the SCC do not necessarily bind the public authorities of the third country to provide effective remedy. The CJEU refused to invalidate the SCC mechanism solely on this fact. Taking into account the AG's view on December 9, 2019, the CJEU ruled that EU SCCs were an adequate mechanism as per GDPR and EU Law standards and provided for sufficient safeguards towards protecting freedom and fundamental rights of EU citizens. This is because data controllers and supervisory authorities are obliged as per the Commission Decision on standard contractual clauses, 2010/87/EU of 5 February 2010, as implemented by Decision (EU) 2016/2297 of 16 December 2016 (**collectively "SCC Decision"**), to suspend or prohibit data transfers in cases of conflict between obligations arising under EU SCCs and those imposed by laws or international commitments of the third country. Moreover, the CJEU also stated that data transferors or data exporters shall not merely pay attention to the SCC agreement but also to the laws of the data importer or the destination country.

To ensure compliance with the EU laws, the data transferors shall look further than the data transfer agreements based on the SCCs between the data exporter and the data importer in the third country. For this purpose, the CJEU paid emphasis on the fact that the data exporter must ascertain if there are any relevant aspects in the data importers legal system which gives the public authorities access to the data that is being transferred. If in this sense, the protection regime in the third or destination country is not guaranteed, then the data exporter shall terminate data transfers and any contract arising out of the same. This adequacy decision shall arise out of the terminology as provided in Article 45(3) of the GDPR. A proper due diligence is required on the part of the exporters to assess the laws of the destination country. The data exporters shall also ascertain if the laws of the destination country are posing any obligations on the importer that is contrary to the terms of the SCC.

CJEU refused the arguments that SCC is invalid as it does not bind the public authorities.

4. THE PRIVACY SHIELD DECISION

CJEU held the privacy shield which was formed as a successor to the safe harbour arrangement to be invalid. Previously, privacy shield had been used to transfer data from the EU to the US following the clauses as set out in the privacy shield decision. However, it is interesting to note that Annex II, under the heading EU-US Privacy Shield Framework Principles, of the privacy shield decision states that adherence to the principles as set out in the privacy shield decision may be limited to the "extent necessary to meet national security, public interest, or law enforcement requirements". This means that the US is bound to its domestic laws and such laws shall have primacy over the principles with matters related to the data transferred into the US from the EU. The US organisations in this sense may disregard the principles in case there is a conflict and the US laws prove incompatible with the principles. This in turn means that para 1.5 as set out in Annex II of the privacy shield decision allows for interference with the principles in matters concerning national security, public interest or matters concerning the domestic laws of the US. Annex II thus provided powers to US surveillance agencies to have access to the personal data that was being transferred from the EU to the US. The CJEU opined that this provision in the privacy shield decision interfered with the fundamental rights of the person whose personal data was being transferred into the US or whose personal data 'could be' transferred into the US. Moreover, any such data that is being transferred into the US could be under watch of surveillance programs like PRISM and UPSTREAM in the US under Section 702 of the Foreign Intelligence Surveillance Act of 1978 (**"FISA"**) which provides the Attorney General and Director of National Intelligence access to data of non-US persons for or persons located outside the US for a period of up to 1 (one) year.

The privacy shield in itself is an adequacy decision with reference being taken from Article 45(2)(a) of the GDPR which states the commission while making an adequacy decision must consider the rights of the data subjects, judicial redress, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation etc. The CJEU regarded that the Article 8(2) EU Charter specifically provides for limitations towards the access of data and processing of any data must be only done after obtaining necessary consents. However, in reference to the US laws, it is regarded that such provisions do not limit the power of the intelligence services and data subjects (outside the US) do not have actionable rights before the US courts. Further, Article 45(2) of the GDPR is violated since the EU citizens are not provided 'effective and enforceable remedy' against their personal data. Section 702 of FISA provided for unrestricted and unlimited rights to the US surveillance agencies which was in violation of the rights as set out in the EU Charter. The provision of the privacy shield 'ombudsman' is not sufficient enough to cure the deficiencies provided in US laws and such laws cannot ensure "*a level of protection essentially equivalent to that guaranteed by the EU Charter*", thus not being adequate and compatible as provided by the GDPR and the EU Charter. Considering such aspects, the CJEU declared the EU-US privacy shield agreement to be invalid with immediate effect.

5. STATEMENTS BY THE US AND THE EU ON SCHREMS II

The United States Department of Commerce has stated that they shall be continuing to process requests for self-certification and re-certification under the privacy shield and has stated that the ruling of the CJEU does not relieve organisations from their obligations to the privacy shield. However, it is best for organisations to consider alternate routes to the privacy shield. Since, currently there has been no grace period granted, the transition towards relying on SCCs and other mechanisms may be done swiftly. In this regard, the EU Commission had also previously announced that it shall be consulting with stakeholders in the US and other countries to look into alternative mechanisms and instruments for facilitating personal data transfers. European Data Protection Supervisor (**"EDPS"**) issued a statement clarifying that it is analysing the impact of Schrems II on contracts concluded by public bodies, institutions and offices in the EU. EDPS had further mentioned that it has initiated an investigation into the contracts with ICT providers like Microsoft. However, Microsoft issued a statement stating that it will continue to use SCC to enable transfer the data.

The task of enforcement of the GDPR is conferred on the supervisory authority from each member state, as per Article 55(1) and 57(1)(a) of the GDPR. The implications of the judgement has already started to follow with the Berlin Commissioner of Data Protection and Freedom of Information requesting the data entities in Berlin to transfer all data situated in the US back to Europe.

Microsoft continues to use SCC to enable data transfer despite Schrems II. It claims to be in compliance with the GDPR.

6. IMPLICATION OF SCHREMS II ON BREXIT

The United Kingdom ("**UK**") had left the EU on by signing a Brexit Withdrawal Agreement on January 24, 2020 with effect from January 31, 2020. Thereafter, a transition period of 1 (one) year has been implemented which will be in place till December 31, 2020. During such transition period, the EU laws continue to apply to the UK including Schrems II. Therefore, the corporations in the UK making use of privacy shield must review its alternatives. Post the transition period, the Schrems II ruling will continue to apply to the UK unless it is explicitly struck down by the courts in the UK. However, it is uncertain if the UK will incorporate the GDPR into its laws. The UK's independent authority Information Commissioner's Office ("**ICO**") in its statement stated that it is working with the organisations to ensure global data flows while ensuring the personal data protection. Organisations in the UK are expecting a guidance from the ICO in this regard which will further clarify the effective compliance mechanism with the Schrems II.

7. GLOBAL IMPACT OF SCHREMS II

Schrems II changes the landscape for SCCs and data compliances between the US and EU. With the reluctance of the US to make amends in its domestic laws, the companies in the US will be paralysed in terms of providing effective remedy to the EU citizens. As per the ruling in Schrems II, if the third country companies are unable to comply with the SCC, they must inform the controller in the EU. Even if the data processor outside the EU is prohibited from their national laws from disclosing such inability to comply with the SCC Decision, must nonetheless disclose to the controller in the EU of its inability to comply with SCC. Currently, in the US, due to the carve out in the form of FISA, the companies in the US may not be able to comply with SCC. Therefore, they would be under an obligation to inform the controller in the EU of its ability to do so. However, as discussed above, Microsoft has already issued a statement stating that the data will continue to flow through SCC.

On the other hand, authoritarian regimes such as Russia and China, would have a tougher time with this judgment coming in, owing to the fact the protections offered as per their laws should be "essentially equivalent" to that in the EU. Further, it is well known that the as such regimes are known for their misuse of power, it shall be interesting to see whether the EU would be able to sufficiently address this aspect. This would have an immense impact on the enforcement of their privacy framework across continents. While the US shares privacy values closer to that the of the EU, China has stringent regime where there is a lack of transparency on the how the data is being processed. With the wider adoption of internet marketplaces like Alibaba and TikTok, the data flows to China is more than one imagines.

Most companies in India currently rely on SCC to transfer data from the EU since India does not have a data protection regime equivalent to the GDPR standard. The Personal Data Protection Bill, 2019 (**"PDP Bill"**) has been considered by the parliament and likely to be passed. PDP Bill provides for a carve out power in favour of the central government which may not be looked at favourably by the EU. Therefore, it is not certain that India will get its adequacy status even after the PDP Bill is enforced. Though on a positive note, right to privacy is an extension of right to life under Article 21 of the Constitution of India, 1950 (**"Indian Constitution"**) and Article 21 extends to even the foreign nationals. Therefore, the remedy for enforcing the data privacy may also be available to the EU citizens.

What is the way forward for organisations now?

8. W-INVESTMENT COMMENTS

Through the Schrems II judgment, CJEU has provided for enhanced procedures to be followed while using SCCs to transfer data. CJEU has stated that the domestic laws and international obligations of the third world country or the destination importing country shall also be taken into account. Many organisations will have to revamp their SCCs to be fully GDPR compliant. The result of this may be that while organisations may rely on SCCs to transfer data to certain third countries, it may not be possible to use SCCs for all third countries. The adequacy test will have to be followed at a heightened level than ever before. Any violation of the same may result in the termination of transfer of data and any agreement arising out of the same. Since the initial case in itself was filed due to Facebook having access to data in the US and the US being a mass surveillance state, it is necessary to understand the implications of a case where the public authorities have access to the data. However, the Schrems II judgment does not provide for a direct answer here. Through time and development of SCC, organisations will have a better picture with regards to the usage of SCCs in a case where public authorities have access to data in third countries and whether in such a case the level of protection would be deemed as inadequate. Therefore, the intention seems to be that where for the purposes like national security, a huge carve out has been provided in the data protection laws, it is likely to be not 'adequate' under Article 45 of the GDPR.

The judgment is to have immediate effect on cross border data transfers and hence, organisations who are using the privacy shield shall relook into their practices to ascertain a better mechanism. Any surveillance laws that are being provided in the importer or destination countries and obligations of such a country arising out of them shall be ascertained while considering data transfers outside the EU. Since such laws are sophisticated and different in every jurisdiction, a proper due diligence mechanism will have to be in place. Whether, the current regime followed by organisations provide for safeguard mechanism and has justified recourse is what needs to be understood. All US entities shall most likely be transitioning from the privacy shield to SCCs very soon, however, it is also opined by the authors that organisations in the US shall not just place reliance on SCCs and shall act with more prudence by looking into all obligatory laws in the US and those provided in the EU Charter, especially disclosure obligations. Data entities such as Microsoft have provided reassurance to their clients and users that Schrems II shall not impact their mechanism for cross border transfer of personal data and that they shall comply with all GDPR governance norms. However, in the US, with its surveillance laws, the SCCs that organisations are utilising, may in all likelihood have to be restructured.