DATA TRANSFER TO THIRD COUNTRIES OUTSIDE EUROPEAN UNION- SCHREMS II CASE AND ITS IMPACT

ABSTRACT: In the world of globalisation and digitalisation, conduct of business involves multiple parties located at various parts of the world. Today, business not only involves delivery of products/services across the borders but even "Data". Data in its various forms/kinds and its access and process has become an integral part of business. There are various regulations that control the transfer of data across borders. The General Data Protection Law (GDPR) being the most comprehensive and stringent. The GDPR came into effect on May 25, 2018. The primary aim of the legislation is to give individuals control of their data. The law applies to all enterprises within the European Economic Area (EU countries plus Iceland, Liechtenstein, and Norway) and companies that process the personal data of EU subjects, regardless of location. GDPR lays down certain restrictions/mechanisms for Cross Border Data Transfer.[1] The European Court of Justice in the case of *Data Protection Commissioner Vs Facebook Ireland and Maximillian Schrems*[2](Schrems II) invalidated the adequacy of protection provided by the EU-US Data Protection Shield. This judgement which came on 16th July, 2020 has huge implications on transfer of data from EU countries to US and any other third country (including India).

This article will discuss (A) what is Cross Border Data Transfer (B) what is EU-US Data Protection Shield (EU-US Privacy Shield) (C) Schrems I judgment and (D) Schrems II judgement (E) Impact of Schrems II judgment.

A. CROSS BORDER DATA TRANSFER

Cross Border Data Transfer means transfer, access or processing of Personal Data[3] of any EU resident outside the European Economic Area (**EEA**). It includes any or all of the below:

[1] Article 44-50 of GDPR.
[2] Case -311/18 Schrems, see also Press Release No.91/20.
[3] Article 4 (i) of the GDPR

a. Physical transfer of Personal Data outside EEA.

b. Access, or processing[4], including viewing of Personal Data from any country outside EEA.

c. Access or processing, including viewing Personal Data via remote desktop connection from any country outside EEA.

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or international organization shall take place only, subject to the mechanisms permitted under GDPR[5]

(i) if the third country in question ensures an adequate level of data protection. According to the GDPR, the Commission may find that a third country ensures, by reason of its domestic law or its international commitments, an adequate level of protection.[6] The EU Commission has granted adequacy to certain countries like Switzerland, Argentina, Andorra, Faroe-Islands, Guernsey, Isle of Man, Israel (partly), Japan, Jersey, Canada (only for commercial organisations), Newzealand and Uruguay. India has not been granted adequacy.

(ii) In the absence of an adequacy decision, such transfer may take place only if the data exporter established in the EU has provided appropriate safeguards, which may arise, in particular, from standard data protection clauses adopted by the Commission, and if data subjects have enforceable rights and effective legal remedies.[7] The standard data protection clauses are known as Standard Contractual Clauses (SCC). Furthermore, the GDPR details the conditions under which such a transfer may take place in the absence of an adequacy decision or appropriate safeguards.[8]

(iii) Transfer under binding corporate rules.[9]

(iv) Transfer based on international agreements.[10]

B. EU-US DATA PROTECTION SHIELD (EU-US PRIVACY SHIELD)

[4] Article 4 (ii) of the GDPR
[5] Article 44 of the GDPR
[6] Article 45 of the GDPR
[7] Article 46 of the GDPR
[8] Article 49 of the GDPR
[9] Article 47 of the GDPR
[10] Article 48 of the GDPR

The EU-US Privacy Shield is an agreement between EU and United States for protection of data transferred from EU to US. It was announced by the EU Commission on 2nd August 2016. It includes privacy principles to be adhered to by the US companies and restrictions on data access by the public authorities. Such restrictions were promised by US Federal Government to be published in the US Federal Register. The EU-US Privacy Shield also granted rights to EU citizens against the US companies in case of breach or misuse of their data by such US companies.[11]

C. SCHREMS I JUDGEMENT[12]

Maximillian Schrems, an Austrian national, lawyer, author, and privacy activist, had been a Facebook user since 2008. As in the case of other users residing in the European Union, some, or all of Mr. Schrems's personal data was transferred by Facebook Ireland to servers belonging to Facebook Inc. that are located in the United States, where it undergoes processing. On 25th June, 2013, Mr. Schrems made a complaint to the Commissioner by which he in essence asked the Commissioner to exercise his statutory powers by prohibiting Facebook Ireland from transferring his personal data to the US. He contended in his complaint that the law and practice in force in United States did not ensure adequate protection of the personal data held in its territory against the surveillance activities that were engaged in United States by the public authorities. Mr. Schrems referred in this regard to the revelations made by Edward Snowden concerning the activities of the United States intelligence services, those of the National Security Agency ('the NSA'). The Commissioner rejected Mr. Schrems complaint on the ground, inter-alia, that, in the ***Safe Harbour Decision***[13], the Commission had found that United States ensured an adequate level of protection.

Safe Harbour Decision: *The Commission in the Safe Harbour Decision had held that the personal data of customers or internet users, as well as employees, could be transferred from states within the EU to the US and stored and processed there without any further requirements (such as the approval of the data subject/person concerned). The only*

[11] 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 (OJ 2016 L 207, p. 1).
[12] Maximillian Schrems v Data Protection Commissioner; Case:C-362/14 Schrems. Press Release No. 117/15.
[13] Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (OJ 2000 p.7).

requirement was that the US companies dealing in such receipt, access and process of data undertake to observe the "Safe Harbour Principles" (a commitment to comply with the EU data protection standards) and register on a "safe harbour list" held by the US Trade Department.

Mr. Schrems brought an action before the High Court of Ireland challenging the decision of the Commissioner. After considering the evidences provided by the parties at hand the High Court found that the electronic surveillance and interception of personal data transferred from the European Union to the United States serve necessary and indispensable objectives in the public interest. However, the High Court further noted that the mass and undifferentiated accessing of personal data by the United States federal agencies is clearly contrary to the principle of proportionality and the fundamental values protected by the Irish Constitution. According to the High Court, the Commissioner should have proceeded to investigate the matters raised by Mr. Schrems in his complaint and that he was wrong in rejecting Mr. Schrems complaint. The High Court decided to stay the proceedings and referred the matter to European Court of Justice for a preliminary ruling[14]. The questions laid before the European Court of Justice were the (i) what was the legality of the Safe Harbour Decision and (ii) whether the Commissioner should have conducted his own investigation in light of the new factual developments instead of just relying on the Safe Harbour Decision.

On 6thOctober, 2015, the European Court of Justice, declared that the Safe Harbour Agreement and the Safe Harbour Decision was invalid. It also held that the Commissioner was wrong in not conducting his own investigations.

D. SCHREMS II JUDGEMENT[15]

[14] A reference for a preliminary ruling allows the courts and tribunals of the Member States in EU, in disputes which have been brought before them, to refer questions to the Court of Justice about the interpretation of European Union law or the validity of a European Union Act.
[15] Case -311/18 Schrems, see also Press Release No.91/20.

After Schrems I judgment, the Irish supervisory authority asked Mr. Schrems to reformulate his complaint considering the Schrems I judgement. In his reformulated complaint, Mr. Schrems claimed that the United States did not offer sufficient protection of data transferred to United States. He sought the suspension or prohibition of future transfers of his personal data from the EU to the United States, which Facebook Ireland carried out pursuant to the standard data protection clauses. The Irish supervisory authorities brought Mr. Schrems compliant to the High Court (Ireland) who referred the matter to European Court of Justice for preliminary ruling.

The questions referred to the European Court of Justice (**Court**) were **(a)** whether the GDPR applies to transfers of personal data pursuant to the standard data protection clauses, **(b)** what level of protection is required by the GDPR in connection with such a transfer, and **(c)** what obligations are incumbent on supervisory authorities in those circumstances **(d)** what is the ***validity of standard contractual clauses (SCC)*** and **(e)** what is the ***validity of EU-US Privacy Shield.***

The European Court of Justice declared as under:

(a) ***GDPR did apply to transfer of personal data*** for commercial purposes by an economic operator established in EU to another economic operator established in a third country, even if, at the time of that transfer or thereafter, that data may be processed by the authorities of the third country in question for the purposes of public security, defence and State security. The Court added that this type of data processing by the authorities of a third country cannot preclude such a transfer from the scope of the GDPR.

(b) As regards what level of protection is required in connection with such transfer, the Court held that a ***level of protection essentially equivalent to that guaranteed within the EU by the GDPR read in light with the EU Charter should be provided to the data subjects.*** The Court further held that in assessing the level of protection, the following aspects must be taken into consideration:

- the contractual clauses agreed between the data exporter in EU and the recipient of the data established in the third country, and
- the relevant aspects of the legal system of such recipient country (as regards access of such data by the public authorities of that recipient country).

(c) As regards the obligations of the supervisory authorities, the ***Court held that the supervisory authorities are required to suspend or prohibit a transfer of personal data to a third country*** where the supervisory authorities opine that the SCC are not or cannot be complied with in such third country or where protection of the data transferred to such third country cannot be ensured by any other means whatsoever.[16]

(d) As regards the validity of use of SCC for data transfer, ***the Court held that data transfer could take place based on SCC as long as they met the data protections adequacies (after assessing on case to case basis)***. The Court held that the Decision 2010/87[17] establishes such mechanisms. The Decision imposes an obligation on a data exporter and the recipient of the data to verify, prior to any transfer, whether that level of protection is respected in the third country concerned. Further, the recipient is required to inform the data exporter of any inability to comply with the SCC, in which case, the data exporter is required to suspend the transfer of data and/or to terminate the contract with the data recipient.

(e) As regards the validity of the EU-US Privacy Shield, the Court ***held that it was invalid and no more a lawful basis of transfer of data from EU to US.*** The Court held that FISA (Foreign Intelligence Surveillance Act) do not set out limitations on the powers of the intelligence services and do not give data subjects actionable rights before US courts.

E. IMPACT OF SCHREMS II JUDGEMENT

- With Schrems II judgement, all Cross-Border Data Transfer from EU to US which relied on the EU-US Privacy Shield are to be **immediately** suspended. This may lead to huge business disruption for companies including Indian companies whose major clients reside in US and the processing of such US client data takes place in data centres in EU Member States. Many Indian companies operate with their data centres based in Ireland or EU Member State countries. With this Judgement, such Indian companies must resort to other modes of data transfer. Transfer of data to US and third country like India can now be done only through SCC after assessing the same. However, even with SCC, the risk of lack of

[16] This would apply where the data exporter in EU has not himself suspended or put an end to such data transfer to such third country.

[17] Commission Decision 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 of the Council, as amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 (OJ 2016 L 344, p. 100).

adequate protections still exists. For example, the US **Foreign Intelligence Surveillance Act, 1978 (FISA)** stipulates that US telecommunication companies are obliged to provide information to the US services and **that no court order is required to access data** at such companies. This applies not only to social network providers, for example, but also to cloud providers such as Amazon or Microsoft. Under the US Cloud Act, 2018 US intelligence services have permission to even access the EU-servers of US companies. **Even in India, Rule 6 of the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011** confers power on the Government agencies to seek information including personal sensitive data from body corporates without the consent of the provider. With these regulations in place, the rights of such regulatory authorities is far reaching. This may lead to more claims by data subjects (for examples, clients and employees) in case of doubt about protection of their data in such countries. Such claims by them can lead to ban or suspension or prohibition of data transfer to such countries.

- Schrems II Judgement has also increased the obligations of the data exporter as they are required to carry the assessment and recommend additional protections, safeguards needed to be implemented by their service providers for protection of their data. The data recipient on the other hand is also required to provide all assistance to the data exporter in conducting the assessment. The data recipient is also required to inform the data exporter of its inability to comply with recommendation of the data exporter. Companies operating at a global scale have now, a two -fold role to play. On one hand as the data exporter and on the other hand as the data importer. A company may act in both capacities as data importer for its client and data exporter for its vendors/partners/subcontractors. With such dual role, they must be on their tip toes to full fill the obligations towards their client and at the same time ensure that necessary checks and balances are put in place with their vendors. Only then the data transfer can be water- tight.

- ***Failure on the part of data exporter and importer to put adequate measures in place for data protection and transfer in line with the requirements set out in GDPR, can lead to suspension or ban of data transfer by the Supervisory authorities along with huge***

administrative penalties to data exporter and data importer. [18] Such penalties can range upto 20 million euros or 4% of the annual global turnover whichever is greater.[19] This can lead to huge financial and reputational loss for the companies.

[18] Article 58, para 2 of the GDPR.
[19] Article 83 of the GDPR