nota bene

UPDATE

26 October 2021

This Update has been prepared by Sucharita Basu and Ronodeep Dutta.

Personal Data Protection: New EU GDPR Standard Contractual Clauses

A. Setting the Context

On 16 July 2020, the Court of Justice of the European Union ("**CJEU**") vide its judgment in the *Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems*[1] (the "**Schrems II Case**") held the EU-US Privacy Shield, one of the primary data transfer mechanisms for the safe and free flow of data between EU and US organizations, as invalid. While the CJEU upheld the use of Standard Contractual Clauses ("**SCC**s") for transfer of personal information outside European Economic Area ("**EEA**"), it required that organizations perform a case-by-case analysis to determine whether the laws in the country to which the data is being transferred, ensures adequate protection. For those transfers where the recipient country does not provide adequate protections, the CJEU requires that data exporters provide additional safeguards or suspend transfers.

In November 2020, the European Data Protection Board ("**EDPB**") adopted the recommendations[2] ("**Supplement Transfer Tools**"), firstly to supplement transfer tools and secondly to imbibe the 4 (four) European Essential Guarantees[3] ("**EEG**"), namely (i) processing based on clear, precise and accessible rules, (ii) demonstration of necessity and proportionality, (iii) independent oversight mechanism, and (iv) effective remedies for the individual, being the core elements when assessing the level of interference or surveillance measures by the third countries. While the former assisted data controllers and data processors to implement appropriate measures for ensuring an *'essentially equivalent'* level of protection to the data transferred to third countries, the latter provided guidance on whether surveillance measures by national security agencies or law enforcement authorities in a third country can be regarded as a justifiable interference or not.

Consequently, on 4 June 2021, the European Commission (the "**Commission**") adopted 2 (two) sets of updated SCCs ("**New SCCs**"). One, for use between Controllers and Processors under Article 28 of the General Data Protection Rules ("**GDPR**")[4] and another, for the transfer of personal data to third countries under Articles 44 – 50 of the GDPR.

B. Key elements of New SCCs

[1] In Case C-311/18

[2] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, version 2.0

[3] Recommendations 02/2020 on the European Essential Guarantees for surveillance measures

[4] Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016.

1. Compared to the old SCCs[5], the New SCCs are an entirely new data transfer tool to reflect the present day data transfer realities by covering additional processing and transfer situations with a more flexible approach. For instance the New SCCs provide for a 'docking clause' which enables the original signatories to add more parties to the SCCs as and when required;

2. The New SCCs also provide for a liability mechanism similar to the one under GDPR. The key obligations include (i) liability for any material or non-material damages; (ii) joint and several liability in applicable cases; (iii) entitlement to claim back damages from the counterparty;

3. Under the New SCCs, the data importer is obligated to conduct a transfer impact assessment in conjunction with the data controller wherein the following five broad steps, namely, (i) risk assessment, (ii) warranty to the counterparty, (iii) documentation, (iv) notification if future laws subject the data importer to any additional obligations, and (v) remedying the situation if such laws override safeguards, need to be carried out;

4. To maintain the validity of these SCCs, it is important to note that they cannot be modified, however, they can be expanded upon, or included as part of a broader contract, as long as such additions do not contradict or detract from these SCCs as written;

5. The New SCCs mirror the basic data protection principles in Article 5 of the GDPR, which is reflected in extensive obligations for the parties around purpose limitation, transparency, data minimization, accuracy, and storage limitation. In most cases, the data exporter and data importer will have to make a copy of the new SCCs, including the appendix, available to the individuals, upon request;

6. In addition, the new SCCs introduce accountability obligations, requiring that each party must be able to demonstrate compliance with its obligations under the new SCCs. Data importers, in particular, will be required to keep records of the processing activities carried out under their responsibility, which they will have to make available to the relevant supervisory authority on request;

7. The New SCCs are based on a multifunctional, modular approach to increase contract efficiencies such as contracts between controller to controller, controller to processor, processor to processor and processor to controller;

8. Data importers will need to promptly deal with any complaints from individuals about the processing of their transferred data. Data importers may also opt to involve an independent dispute resolution body, at no cost, to offer to the individual. Individuals will need to be informed of the redress mechanism and that they are not required to use it;

9. Pursuant to the Schrems II Case decision, the new SCCs include elaborate provisions to address the effects of the laws of the third country on the data importer's compliance with the clauses, in particular, with respect to dealing with *'binding requests'* from public authorities in that country for disclosure of the transferred personal data;

10. Further under the New SCCs both the data exporter and data importer will have to warrant that they have no reason to believe that the laws and practices that apply to the data importer are not in line with these requirements.

[5] Decision 2001/497/EC and Decision 2010/87/EU

C. *The Transition Period*

The New SCCs entered into force on 27 June 2021, which means data exporters and importers can start using the new SCCs from that date and the Commission decisions implementing the old SCCs stands repealed, after a transition period of 3 (three) months i.e. on 27 September 2021 ("**Repeal Date**").

An additional period of 15 (fifteen) months has been provided to the data exporters and data importers, i.e. upto 27 December 2022, to continue with the old SCCs for the performance of contracts which have concluded before the Repeal Date, provided that the processing operations that are the subject matter of the contract remain unchanged and that reliance on the clauses ensures that the transfer of personal data is subject to appropriate safeguards.

D. *The Indian Perspective*

The extraterritorial application will require Indian controllers or processors who are not covered by Article 3 of the GDPR to implement the safeguards required in the SCCs.

Given the powers of access and surveillance that governmental and law enforcement authorities in India exercise, there may be significant difficulties with respect to reporting a disclosure request. The Indian government derives such powers from S 69 of the Information Technology Act, 2000 and the Sensitive Personal Data or Information Rules 2021, as well as under telephonic and internet communications' surveillance laws.

Considering India's endeavor to cement its position as a preferred global outsourcing hub, with more EEA entities engaging Indian companies for data processing, coupled with the absence of a specific data protection law and independent supervisory authority, increases the level of risk for data processors in India.

Further continual obligations on the data importer to notify the supervisory authority in cases where risk is high towards the freedoms and rights of data subjects, reviews and independent audits and certifications on the request of the data controllers would necessarily result in a significant increase in compliance requirements.

Lastly, the Supplement Transfer Tools categorically state that, supplementary measures are to be implemented by the data controllers, if it is determined that the law of the third country impinges on the effectiveness of transfer tools given under Article 46 of GDPR. In such cases the exporters may implement supplementary measures that fill the gaps, if any, in the protection and bring it up to the level required by GDPR. The exporters will need to identify them on a case-by-case basis in line with the principle of accountability under Article 5.2 of GDPR, which requires controllers to be responsible for, and be able to demonstrate compliance with the GDPR principles relating to processing of personal data.

Therefore, if the data exporter or EU supervisory authority deems that Indian law impinges on the effectiveness of the SCCs or that the power granted to public authorities to access the transferred data goes beyond what is necessary and proportionate in a democratic society, an Indian data importer may be required to implement these additional supplementary measures or suspend the transfer.

This Update has been prepared by Sucharita Basu and Ronodeep Dutta who can be reached at **sucharita.basu@aquilaw.com** and **ronodeep.dutta@aquilaw.com.**