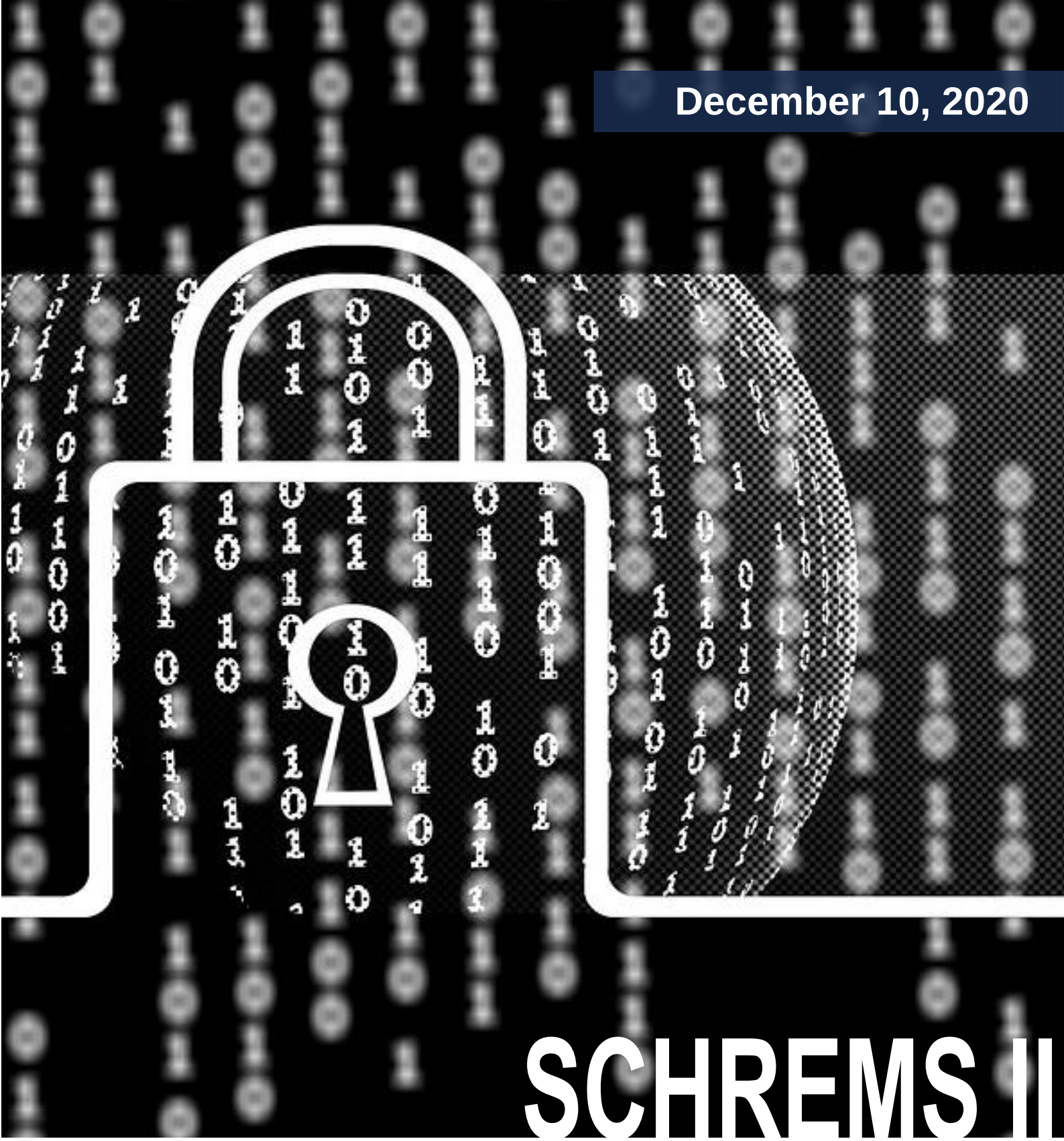
December 10, 2020



SCHREMS II

IMPACT ON INDIAN COMPANIES

argus partners
SOLICITORS AND ADVOCATES

MUMBAI I DELHI I BENGALURU I KOLKATA I AHMEDABAD

The Court of Justice of the European Union ("**CJEU**") on July 16, 2020 passed a landmark decision in *Data Protection Commissioner* v. *Facebook Ireland Ltd, Maximillian Schrems*, Case C-311/18 ("**Schrems II**") that invalidated the European Union-United States Privacy Shield ("**Privacy Shield**") and upheld the validity of Standard Contractual Clauses ("**SCC**"). With this decision, the Privacy Shield can no longer be used to justify the transfer of personal data from any member state of the European Union ("**EU**") to the United States of America ("**US**") other than in accordance with the applicable data privacy law. Entities transferring data from the EU to the US shall now be compelled to use SCCs to ensure an uninterrupted flow of data. In this article, we look at how this case impacts companies in India and the transfer of data from the EU to India.

The Privacy Shield: A Brief History

With high volumes of data flowing between the EU and the US, in 2000 the two regions had agreed to adhere to a set of data privacy principles titled "Safe Harbour" that would permit the transfer of personal data from the EU to the US. US companies that were regulated by either the Federal Trade Commission or the Department of Transportation were allowed to gain Safe Harbour certification and receive personal data from the EU, provided an adequate level of safeguards was in place to protect the data.

Following the public disclosures of large-scale surveillance programs run by the US Government on its own citizens, the Safe Harbour principles were challenged before Irish Courts and were subsequently referred to the CJEU. In its October 6, 2015 decision in *Maximillian Schrems* v. *Data Protection Commissioner*, Case C-362/14 ("**Schrems I**"), the CJEU declared the Safe Harbour principles as invalid and noted that if US companies were to find themselves in conflict with national security, public interest or the law enforcement requirements of the US government, such requirement would inevitably prevail over Safe Harbour requirements. The CJEU further noted that US companies that had provided undertakings under the Safe Harbour principles were bound to disregard, without limitation, the protective rules laid down by the principles when in conflict with national requirements, giving rise to potential interference by the state.

The invalidation of Safe Harbour principles by the CJEU led to renewed negotiations between the EU and the US, which culminated in a new arrangement titled the "Privacy Shield". The Privacy Shield retained the core of the Safe Harbour principles but added additional safeguards that focused on individual rights for EU citizens, stricter requirements for US businesses, and restrictions on access to personal data by the US Government. The changes included options to file complaints regarding data privacy through an Ombudsperson, increased monitoring of Privacy Shield compliant companies, and stricter reporting obligations for companies. By enabling US based companies to self-certify and publicly commit to compliance with Chapter 5 (five) of the EU General Data Protection Regulation ("**GDPR**") which pertains to the transfer of personal data to third countries or international organisations, the Privacy Shield facilitated cross-border transfer of large volumes of personal data from the EU to the US and underpinned Trans-Atlantic trade.

Impact of Schrems II

As mentioned above, the CJEU invalidated the Privacy Shield in Schrems II. The court expressed concern over US intelligence activities in relation to personal data that was transferred to the US, especially under Section 702 of the Foreign Intelligence Surveillance Act ("**FISA**") which enabled the surveillance of non-US citizens located outside the US, in order to collect intelligence. The CJEU also noted that Executive Order 12333 of the US Government allowed the National Security Agency (intelligence agency of the United States Department of Defense) to collect personal data that was being transmitted through underwater cables on the floor of the Atlantic Ocean, in bulk. Further, the Ombudsperson mechanism set up under the Privacy Shield was inadequate as it neither guaranteed the independence of the Ombudsperson nor could it guarantee actionable rights for data subjects of substantial equivalence to the standards imposed by the GDPR.

The invalidation of the Privacy Shield has led to significantly greater importance being attached to SCCs as one of the few remaining means of continuing unimpeded cross-border data transfer from the EU to third-party countries, including the US. The SCCs are a set of standard contractual terms and conditions recommended by the EU for data transfer from the EU to non-EU countries, with which both the data exporter and importer have to comply. The aim of SCCs is to protect personal data leaving the European Economic Area through contractual obligations, in compliance with GDPR requirements, to territories that are not considered to offer adequate protection for personal data.

The CJEU considered the validity of SCCs and discussed the factors which need to be considered to determine whether the adequacy of the level of protection offered through the SCC is of the standard required by the GDPR under Article 45. Under Article 45 of the GDPR, transfer of personal data to a third country or an organisation may take place only where the European Commission ("**Commission**") has decided that the third country or organisation can offer an "adequate" level of protection while taking into account a variety of conditions such as the rule of law, respect for human rights, national security and criminal law, access of public authorities to personal data, data protection rules, existence of one or more independent supervisory authorities etc. The Commission shall also consider whether the third country has effective and enforceable data subject rights and effective administrative and judicial redress for data subjects whose personal data are being transferred.

With *Schrems II*, data exporters and importers may now have to put in place additional safeguards to ensure that the level of protection given by SCCs is equivalent to the GDPR, in order to compensate for the lack of data protection in a third country. The CJEU concluded that the non-exhaustive list of criteria prescribed in Article 45 of the GDPR for assessment of adequacy by the Commission corresponds to the list of criteria required by the SCCs to be taken into consideration by a data exporter when determining whether the level of protection offered by a data importer is adequate for that specific data transfer to a jurisdiction outside the EU. When performing the assessment, the exporter must take into consideration the content of the SCCs, the specific circumstances of the transfer, as well as the legal regime applicable in the importer's country. The assessment should include:

i) Consideration of the laws that apply to the data importer;
ii) The type of data imported, as some data may be inherently less at risk;
iii) The categories of data subjects;
iv) Consideration of the business sector in which the data importer operates, and the odds of the importer becoming the subject of surveillance; and
v) The identity of the data importer.

The CJEU also noted that SCCs may not always sufficiently ensure effective protection of transferred personal data, particularly when the laws of the third country allow its public authorities to interfere with rights of the data subjects. It based the validity of the SCCs on whether the additional effective mechanisms and safeguards make it possible to ensure compliance with a level of protection equivalent to that guaranteed within the GDPR. In the event of a breach of the SCC clauses, or if it is impossible to honour the clauses, the transfer of personal data must be suspended or prohibited. If data has already been transferred under SCCs, it must be returned or destroyed immediately.

Repercussions for Indian Companies

Indian companies receiving data from the EU have generally relied on SCCs and Binding Corporate Rules ("**BCR**") to meet compliance requirements under the GDPR. BCRs are rules that govern an entity or a group of entities, and apply to data transfers within the group. However, with India yet to be considered by the EU as having an established legal or regulatory framework that ensures data protection and privacy, existing SCCs and BCRs will have to be revisited to ensure unimpeded flow of data from the EU to India, post *Schrems II*. India's law enforcement apparatus

has a wide range of powers that may be exercised in the interest of national security, with such powers being recognised by the Courts as an exception to the fundamental right to privacy. Much like in the US, if law enforcement authorities were to approach an Indian company for access to personal data of EU citizens, the company would generally have to comply- irrespective of any contractual obligations between the company and a data importer/exporter.

India has made progress towards establishing a legal framework for data protection, with the Personal Data Protection Bill ("**Bill**") being tabled in the Lower House of India's Parliament on December 11, 2019. While the Bill has been modelled along the lines of the GDPR, there are a few significant differences between the two data protection laws:

- The Bill gives India's Central Government ("**Central Government**") the power to exempt government agencies from the provisions of the bill, on the grounds of national security, national sovereignty, and public order. While the GDPR includes similar clauses, they are tightly regulated by different EU directives and judicial oversight. The Bill does not have similar safeguards, and may potentially give the Central Government the power to access personal data, over and above the existing GDPR framework.
- The Bill permits the Central Government to order companies to share any "nonpersonal" data that they collect, with the Central Government. While the reason for such a provision is ostensibly to improve the delivery of government services, the provisions are silent on how the data will be used, whether it might be shared with other private businesses, or whether compensation will be provided for the data.

Given the above, it is unlikely that the Bill in its current form would allow India to meet third-party "adequacy" requirements as prescribed under Article 45 of the GDPR, and thus making it increasingly important for data importers to put in place SCCs with adequate safeguards.

Mitigation Measures by Companies

With the increased importance of SCCs in data transfer agreements between EU and third-party countries, both importers of data from India and exporters of data from EU will need to undertake several measures to ensure that the SCCs are of equivalency with the protection standards of the GDPR to ensure the unimpeded flow of data across jurisdictions. Companies may take the following measures to ensure compliance:

- A company should first assess the nature of data transfers that are made, the regularity of such transfers, and the existing safeguards in place for the transfer. It would be advisable to identify whether the transfers are international, intra-group transfers, or third-party transfers.
- Companies must identify what personal data is being transferred, the sensitivity of the personal data, and whether some/all of the personal data is already in the public domain.
- Data exporters are recommended to carry out due diligence on the data importer to determine whether the importer is bound by any laws which might be in contravention with GDPR requirements.
- Data transfers must be reviewed on a case by case basis, and companies must assess whether the SCCs are adequate, or whether additional supplementary measures are required.
- Companies may implement enhanced notice requirements under which data importers notify data exporters and data subjects of law enforcement or surveillance requests, to the extent practical and permitted by law.
- Companies may also enhance encryption requirements for data that is transferred. This may be done by encrypting data such that only the data exporter has the key, and cannot be decrypted by intelligence agencies. Data can be further anonymised or pseudonymised in such manner that only the data exporter can link the data to a natural person.

- BCRs may be an alternative to SCCs. It is pertinent to note that EU authorities are generally supportive of organisations that elect to adopt BCRs because of the enterprise-wide commitment to data protection that BCRs generally require. BCRs however might not adequately protect from governmental interference, potentially leading to the need for implementation of additional safeguards depending on the country in question. BCRs also may take several years to prepare and obtain approval from the relevant EU authorities, and may be considered a long-term solution.

EPDB Recommendations

Following *Schrems II*, the European Data Protection Board ("**EDPB**"), an independent body of the EU in charge of application of the GDPR, released recommendations on November 10, 2020 ("**EPDB Recommendation**") on measures that can be taken to ensure compliance with the EU level of protection of personal data. A summary of the recommendations are as follows:

i) Data exporters must know their transfers and map where and how the data travels. Exporters must also verify that the data transferred is adequate, relevant and limited to what is necessary in relation to the purposes for which it is transferred and processed in a third country.
ii) Data exporters must verify the transfer tool they rely on, and assess whether the European Commission has declared the country, region or sector to which data is being transferred to as having adequacy under the GDPR. Exporters must monitor the validity of the adequacy decision, in absence of which exporters may rely on other transfer tools (as under Article 46 of the GDPR) or any of the derogations provided for under Article 49 of the GDPR.
iii) Data exporters must assess the law of the third country that might impinge on the effectiveness of the safeguards included in the transfer tools that are relied on for the specific transfer. The assessment must be conducted with due diligence and documented thoroughly, as the exporter may be held accountable for any decision that is taken on that basis.
iv) If the exporter finds that the legislation of the third country impinges on safeguards, supplementary measures must be identified and adopted to ensure essential equivalency with the GDPR. The exporter will be responsible for assessing the effectiveness of the measures in the context of the third countries laws and the transfer tool being relied on. In cases where no supplementary measure is suitable, the exporter must avoid, suspend, or terminate the transfer to avoid compromising protection of the personal data.
v) The data exporter must take into account any formal procedural steps that may be required for adoption of the supplementary measures, depending on the transfer tool relied on.
vi) The level of protection afforded to the data being transferred must be re-evaluated at appropriate intervals, and monitored for any potential developments that may affect it.

Suggested Changes to SCC Clauses

The EU, under decisions 2001/497/EC and 2004/915/EC, had issued sets of SCCs for personal data transfers from EU data controllers to non-EU data controllers. It had also issued a set of contractual clauses for data transfers from EU data controllers to non-EU data processors, under decision 2010/87/EU. These SCCs are likely to be superseded by a new set of draft SCCs that the Commission has released in response to *Schrems II.* The new draft SCCs include contractual clauses for data transfers from EU data processors to non-EU data processors, and from EU data processors to non-EU data controllers.

While supervisory authorities are still considering how *Schrems II* would impact these standard form clauses, the Commissioner for Data Protection and Freedom of Information for the German State of Baden- Württemberg ("**LFDI BW**") recently published indicative guidance on how

supplemental measures may be added to SCCs pursuant to *Schrems II*, by amending the following SCC Clauses:

- Clause 4(f): Inform the data subject that their personal data will be a transferred to a third country that does not provide an adequate level of protection as prescribed by the GDPR, not just in case of transfer of special categories of data, but for transfers of personal data of any category.
- Clause 5(d)(i): Data importers should promptly disclose any legally binding requests for disclosure of personal data by law enforcement not just to the data exporter, but also to the data subject, as long as it is not prohibited by the authority.
- Clause 5(d): Add a clause obligating data importers to take legal action against the disclosure of personal data, and to refrain from disclosing private data to public authorities until a competent court of the last instance has ordered the importer to disclose the data in a legally binding manner.
- SCC Clause 7(1)(b): While this clause obligates data importers to refer disputes to Courts of the member state in which the data exporter is established, the LFDI BW recommends extending this obligation in the event that a data subject claims rights as a third party beneficiary, and/or claims damages against the data importer under the SCC.

The EPDB Recommendations also provide examples of supplementary measures that can be adopted to ensure equivalence with the GDPR, including technical measures that may be implemented based on the circumstances of the data transfer, contractual measures that can be added to complement and reinforce safeguards, transparency obligations that can be annexed to the contract and bind the importer, organisational measures and data minimisation measures, internal policies for governance of transfers within groups of enterprises and adoption of standards and best practices.

While these recommendations by the LFDI BW and EPDB are non-exhaustive and recommendatory in nature, companies must remember to ensure that their SCCs or other transfer tools are suitably modified to meet GDPR adequacy standards based on the nature of data transfer they are engaged in, and evaluate the transfer tool on a case-by-case basis. Companies must also review data flows and consider putting in supplementary measures (such as further contractual obligations), while diligently documenting their GDPR compliance efforts.

This paper has been written by Suchita Ambadipudi (Partner), Vinod Joseph (Partner) and Pranav Pillai (Associate).

DISCLAIMER

This document is merely intended as an update and is merely for informational purposes. This document should not be construed as a legal opinion. No person should rely on the contents of this document without first obtaining advice from a qualified professional person. This document is contributed on the understanding that the Firm, its employees and consultants are not responsible for the results of any actions taken on the basis of information in this document, or for any error in or omission from this document. Further, the Firm, its employees and consultants, expressly disclaim all and any liability and responsibility to any person who reads this document in respect of anything, and of the consequences of anything, done or omitted to be done by such person in reliance, whether wholly or partially, upon the whole or any part of the content of this document. Without limiting the generality of the above, no author, consultant or the Firm shall have any responsibility for any act or omission of any other author, consultant or the Firm. This document does not and is not intended to constitute solicitation, invitation, advertisement or inducement of any sort whatsoever from us or any of our members to solicit any work, in any manner, whether directly or indirectly.

You can send us your comments at:
argusknowledgecentre@argus-p.com

Mumbai I Delhi I Bengaluru I Kolkata I Ahmedabad

www.argus-p.com