PSL Advocates & Solicitors

# Cross-border data transfers: (In)Adequate protection?

*"Data is the New Oil, the New Gold"*. If there is one thing which unites businesses all over the world, it is, above all else, their collection, use, processing or storage of personal/financial data of clients, consumers, service providers and business associates.

Across the nations , data protection laws have changed remarkably over the past two decades. Now more than ever, an individual's digital existence is a common phenomenon. Our reliance on smartphones, laptops and wearable technology has increased manifold and payment through online digital modes, is a way of life. At an individual level, there is a huge amount of personal data that is being shared, collected, and stored online on the pretext of making our online existence customized and therefore, comfortable. Due to this boom in digital space and economy, one of the most frequent concerns to arise is regarding the 'adequacy' of protection of our personal data.

Generally speaking, personal data is any data or set of data which can be used to identify a person directly or indirectly. This would include one's name, characteristics, personality traits, appearance etc. which may not necessarily be closely guarded. However, certain other types of data, such as those relating to one's religious or political belief, health, or private life would be closely guarded as their dissemination, or knowledge could have significant impact on a person or may be treated with greater care simply by virtue of their sensitive nature. With varying legal systems and societal standards, all jurisdictions have their own definition of what type of data should be categorised as 'Sensitive Personal Data' or be put in a special category of personal data ('SPD') requiring a relatively higher level of regulation or protection.

In the digital economy space businesses are global, requiring cross-border transfer of personal data. It is imperative that each business must understand the common basic principles pertaining to data protection and privacy laws regulating the legal environment of the jurisdictions within which such business operates or transacts. At a high level, jurisdictions having dedicated data protection law usually permit crossborder transfer of personal data on five broad principles – adequacy, informed consent, contractual necessity, interests of data subjects or other persons, and overriding legal or state functions.

The principle of adequacy requires that data can be transferred across national borders only if the receiving nation or territory offers sufficient protection for data under its own laws, which is comparable to or, at the very least complies with the minimum protection accorded in the transferor state.

The last few weeks have been particularly busy for the data protection activists and businesses alike, as both find themselves grappling with the issues resurrected by the ruling of the Court of Justice of European Union ('CJEU'), European Union's highest court, in the much-awaited case of Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems (usually known as the 'Schrems II') wherein the legal basis of international transfer and

processing of personal data between the EU and the United States of America ('USA') was tested for the second time.

European privacy laws [previously the Data Protection Directive – Directive 95/46/EC ('Directive'), and now the General Data Protection Regulation ('GDPR')] permit free flow of personal data within the EU. Cross-border transfer of personal data to non-EU country is also permitted provided the personal data enjoys 'adequate' level of protection in such country which is essentially 'equivalent' to that within the EU. USA came up with a set of guidelines or principles to be followed by businesses receiving data from EU known as the EU-US Safe Harbour framework ('Safe Harbour framework'). Vide order dated July 26, 2000, the European Commission accepted the adequacy of Safe Harbour framework. This resulted in free flow of personal data from EU to USA provided the entity receiving the personal data was compliant with the privacy principles contained in Safe Harbour framework.

In 2013, Edward Snowden publicly disclosed that intelligence agencies in USA have wide access to the personal data of EU users being collected by the electronic communication/service providers in USA. Following these revelations regarding the invasive surveillance mechanisms employed by authorities in USA, questions were raised about the integrity of the Safe Harbour framework and the adequacy of protection provided by it.

In the year 2015 an Austrian national, 'Maximillian Schrems' approached the Irish Data Protection Commissioner ('DPC') claiming that the Safe Harbour framework did not guarantee the requisite level of data protection mandated under the Data Protection Directive, the EU's data protection law in force at the time, and thus, data collected by Facebook Ireland Limited from EU residents must not be transferred to servers of Facebook Inc. in USA, as it violated the guaranteed rights of EU residents. The DPC ruled that it was bound by the Order dated July 26, 2000 passed by the European Commissioner; the Safe Harbour framework provided adequate protection; and, rejected the complaint as "frivolous and vexatious". The matter travelled up to the CJEU which gave its decision in this case of Maximillian Schrems v. Data Protection Commissioner, which came to famously be known as the 'Schrems I' case, in the year 2015. The CJEU also observed that "legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life" as guaranteed under the Charter of Fundamental Rights of the European Union ('CFR'). The CJEU held that a third country such as the USA must provide an "essentially equivalent" level of protection, that the decision of the DPC was invalid and that the protection pursuant to the Safe Harbour framework was inadequate.

Soon thereafter, USA negotiated with EU to come up with another framework referred to as the EU-US Privacy Shield framework ('Privacy Shield') for providing adequate protection to data so that the companies in the USA can resume engaging in crossborder transfer of data on a self-certification basis. European Commission's Decision 2016/1250/EC of July 12, 2016 approved the Privacy Shield as providing 'adequate'/'equivalent' protection.

Since the Privacy Shield had failed to address the core issues pertaining to conflict of laws in USA with the fundamental right to respect for private life as guaranteed under the CFR of EU, the issue related to adequacy of protection granted by the Privacy Shield again travelled to the CJEU on account of a lawsuit filed by Irish DPC against Facebook Ireland Limited and

Maximillian Schrems. However, this time, the touchstone to judge the adequacy of the data protection was GDPR which replaced and repealed the Directive in the year 2018. On July 16, 2020, the CJEU issued a judgment declaring invalid the European Commission's Decision of July 12, 2016 on the adequacy of the Privacy Shield. The CJEU, amongst other things, declared the Privacy Shield as an invalid mechanism for transferring personal data, due to the limitations on its protection from the domestic law of USA which allow indiscriminate access to public authorities in USA to the EU data transferred there. It observed that though the Commission had held in its adequacy ruling that the authorities in USA would be bound by the limitation principles under the EU law, the laws of USA do not "grant data subjects actionable rights before the courts against the US authorities. Therefore, the Privacy Shield cannot ensure a level of protection essentially equivalent to that arising from the Charter contrary to the requirement in Article 45(2)(a) of the GDPR that a finding of equivalence depends, inter alia, on whether data subjects whose personal data are being transferred to the third country in question have effective and enforceable rights." The CJEU thereby declared that the Privacy Shield cannot be used as the legal basis for transferring personal data to USA where the recipient is subject to parting with such data as per its surveillance laws.

Back at home, the Supreme Court of India in the year 2018 had also given a ruling recognising the need to bridle the powers of the government while handling data of its citizens. It was noted that "informational privacy is a facet of the right to privacy. The dangers to privacy in an age of information can originate not only from the state but from non-state actors as well." To guard against such dangers, the Court recognised that "a careful and sensitive balance between individual interests and legitimate concerns of the state" needs to be achieved. In the past couple of months, lack of adequate protection has also been a growing concern. The Indian Government's recent ban on several Chinese applications including TikTok, UC Browser and BeautyPlus was also due to breach of users' data privacy. India under its current laws in the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 also recognises the requirement of adequate protection for cross-border transfer of SPD.

Should adequacy be lacking in laws, states such as Russia, Switzerland and those following the GDPR permit cross-border transfers provided treaties or data sharing frameworks have been established for it. It was under this route that the Privacy Shield was set up to allow EU companies to transact with businesses in USA. Even if there is no data sharing framework in place, entities intending to transfer the data can opt to be contractually bound by the model clauses or Standard Contractual Clauses ('SCC') approved by the transferor nation's data authorities. Even otherwise, parties can themselves provide contractual obligations respecting the higher protection standards. However, some jurisdictions such as Switzerland, would require prior approval of the data protection authorities if the SCCs terms are deviated from. The consequences of the CJEU judgment in Schrems II is that the businesses are now forced to rely on SCCs to legally support cross-border transfer of personal data from EU to USA. Contractual safeguards may even be put in place by way of binding corporate policies. The law proposed to be enforced soon in India i.e. the Personal Data Protection Bill, 2019 ('Proposed Bill') also envisages alternative mechanisms to facilitate cross-border transfer of data.

Even in case of glaring conflicts or inadequacy, all is not lost in the world of data transfer. In such situations, cross-border transfer can take place if the data subject or data principal, i.e.

the person to whom this personal data relates, consents to transferring such data despite being apprised of the risks associated with such inadequacy. What assumes importance then is the quality of consent and the riders attached to it, which vary from jurisdiction to jurisdiction. For instance, EU, UK, Mauritius and Switzerland would require that consent should be given after informing the data subject about associated risks and giving the option to refuse such consent. In fact, in Vietnam, financial data is considered as SPD and therefore, the e-commerce websites must seek purpose-specific informed consent before using or disclosing such data. On the other hand, as per Australian law, since financial data is not strictly included in SPD, it could even be disclosed based on an implied consent understood to have been given by the data subject. However, most recently enacted data protection laws do not consider a 'consent by default' sufficient for this purpose. The practicality of this is to give the data subject an opportunity to make a conscious decision for herself, being insulated from the self-interest of the data controller/transferor to export data, whether for ease of business or earning profits.

Where transfer is necessary for purpose of contractual or pre-contractual obligations, the same may be transferred in the absence of specific informed consent for cross-border transfer by the data subject. However, the requisite parties to the contract eligible to transfer data in this manner also vary under different laws. In countries such as Brazil, Mauritius and Russia, so long as it is in the best interest of the data subject, even contracts entered into by the data collector/transferor with other third parties to the exclusion of but for benefit of the data subject would be valid ground for availing leeway under this basis. Whereas in Switzerland, for intra-group cross-border transfer in case of inadequacy, data subject should be a party to the contract.

The next basis for international transfer is vital or compelling interest. This means that cross-border transfer may be permitted on the grounds of vital interest of data subject, or on account of compelling legitimate interests of the data controller and/or processor, and in some cases, a third party. Different legislative frameworks have different standards for exercising this basis for cross-border transfer. In some jurisdictions, such as Germany, Russia and Luxembourg, such a ground of data subject's interest would be permitted only where data subject is not in a position to give an informed consent. Interestingly, Mauritian authorities can even call upon the data exporter to demonstrate that compelling legitimate interests did in fact exist. Further, under the GDPR and Mauritian law, data from publicly accessible records can be shared, in compliance with other conditions of the data protection law or where the requesting third party, can demonstrate a legitimate interest where access is regulated. It is likely that issues relating to demonstrability and compelling nature of such interest, being subjective elements, would require frequent intervention of data protection authorities and courts.

The ground of necessity for legal or state related functions for data transfer is, perhaps, a ground as widely observed as that of consent. Laws of almost all nations recognise that data to at least a limited extent could be transferred even without strictly complying with otherwise applicable law where disclosure is necessitated by reasons of national security or defence, public interest, protection of life or health, complying with court procedure or establishing or enforcing legal rights. It must be appreciated that it is not only in case of national or international exigencies that cross-border flow of data occurs. In the present day and age where international cooperation has expanded in all spheres, be it to improve global

health, fight terrorism or to catch economic offenders, countries are likely to share data proactively to achieve their goals. Such cooperation amongst countries has been seen in the past when Herve Falciani in 2008 fled to France with data of account holders who were hiding money from taxmen in the Swiss branch of the Hongkong and Shanghai Banking Corporation (H.S.B.C.) Bank, and details of those individuals were shared with India by the French authorities in 2011 and later, the Swiss authorities in 2019. Being bound by their respective national laws to some extent, even the authorities would be expected to exercise a degree of caution while disclosing such data.

The protection of personal data in cross-border transfers has gained enormous importance in recent times and would continue to be of vital interest to the businesses in times to come given the fact that data flows are bound to grow with more and more businesses going digital. Judgments of CJEU in Schrems I and Schrems II has served notice to businesses and nations alike that the right to privacy must be upheld and respected.

India has proposed a new law for protection of personal data. In fact, the Indian Government is also considering regulating the processing and transfer of non-personal data to promote a healthy business environment. Earlier this year, the Indonesian President is reported to have signed a draft law on personal data protection, which leans towards the Indian Proposed Bill and defines general personal data and SPD in a similar fashion. Unlike the GDPR, the Indonesian bill includes personal financial data as a part of SPD and for cross-border transfer of personal data and adopts the mechanism of 'adequacy' of protection in the recipient states. Countries like China, Indonesia and Russia, that once banned cross-border data transfers, are now conscious of the need to open up the digital boundaries and harmonize themselves with the global pulse of data protection. Where Switzerland had a more stringent regulation in place, in light of its close geographical and economic ties with the EU, perhaps, it realized the need to introduce leniency and streamline its laws with that of its neighbours.

However, a view may be taken that it is not sufficient for countries to merely align their data protection policies. As seen above, a state of real adequacy of protection cannot be attained unless national laws overriding data protection laws are also brought in sync with one another. In absence of coming up with robust crossborder data transfer mechanisms, nations and entities might soon realise that the principle of adequacy is turning into an unforeseen trade barrier. Since international harmonization across legal issues seem more like a utopian vision than a soon to be achieved reality, data importers and exporters would have to make up for the disconnect on their own, to whatever extent it is possible. Depending on a case to case basis, one approach could be to transfer data not only on one of the many aforementioned legal bases but rather to use a combination thereof so that even if one of the basis is held to be invalid, like the Privacy Shield in Schrems II, business is not thrown in a state of absolute frenzy and rather already has provisions for enabling stop-gap arrangements to be put in place.

While countries can take time to decide whether or not to review their respective legislations, the business entities are forced to amend their policies and contracts to protect their businesses so that they earn 'adequate' profits while arranging to provide for 'equivalent' protection for cross-border flow personal data.