GDPR: LEGAL IMPACT ON EXTRA - TERRITORIAL COMMERCIAL PRESSURE ON INDIAN BUSINESS, TRADE AND INVESTMENT

Dr. Bindu Samuel Ronald
Professor and Deputy Director,
Symbiosis Law School, Pune, Symbiosis International (Deemed University)

Mr. Abhijit Vasmatkar
Assistant Professor, Symbiosis Law School, Pune,
Symbiosis International (Deemed University)

Dr. Shashikala Gurpur
Professor and Director, Symbiosis Law School, Pune,
Dean, Faculty of Law, Symbiosis International (Deemed University)

Abstract

The GDPR was implemented in 2018 to provide a balance between protecting personal data and privacy of data subjects. The implementation of GDPR has impacted various sectors. The extraterritoriality of the law on GDPR puts a pressure on companies and policy makers to re-examine the existing legal framework and India has not been insulated from the effects of implementation of GDPR. It puts a pressure on Indian trade bodies and upon government agencies to formulate a regulatory regime to achieve a synergy between Indian and EU laws.

The paper will look at the GDPR law in the EU, as well as at international responses to the implementation of the GDPR and will consider the effect it will have on Indian businesses, the trade and investment between India and EU. The paper will study the consequences that the law will have in commercial exchanges especially in the context of EU-India bilateral trade negotiation.

The authors have used the descriptive and analytical method research and have studied the implications of the introduction of GDPR especially for India.

Key words: GDPR, Data Protection, Trade, Business, Extra-territoriality

Introduction and the origin of GDPR

The General Data Protection Regulation (GDPR) central to Europe's digital privacy legislation aims to provide a balance between protecting personal data

and privacy of data subjects[1] ensuring growth of internal market to which free flow of data is imperative. The regulation became enforceable in EU in 2018 providing companies with a 2-year window to become GDPR compliant. The GDPR was promulgated to adapt to the current digital era and formulate a structure that would allow the EU to benefit from digitalisation. Technology controls our lives to such an extent, that every facet of our being revolves around data. There is always a fear of data breach. Information collected from individuals for various reasons gets stolen, stored and released into the hands of persons who misuse personal information of individuals.

With newer technologies getting introduced in the 1980s and 1990s, there was a huge shift in the way information began to get collected, stored and transferred from customers. It led to the introduction of Directive 95/46/EC. Based on the Data Protection Directive 95/46 /EC the member countries could formulate their own laws on the right to privacy and data protection. As a consequence, each country began to come up with its own legislation causing huge ambiguity.

However, subsequently with technology transforming lives of individuals in a way that nobody could have imagined 3 decades ago, it was imperative to review the Data Protection Directive of 1995 which was adopted at a time when the internet was still in its embryonic stage. This resulted in Europe's data protection authority recognising the need for a comprehensive approach on personal data protection"[2]. The regulation replaced the Data Protection Directive 95/46/EC[3] of 1995 and the individual laws of EU member states.

The GDPR is designed to 'harmonise' data privacy laws across all its member countries[4], but it was promulgated to mainly provide greater protection and rights to the individuals thus strengthening the fundamental rights of the citizens, giving them more control over their personal information[5].

The GDPR regulates the procedure of maintaining and processing EU citizens' personal data by data controllers[6] and data processors[7]. Under the GDPR regime the companies and individuals are under an obligation to see to it that the personal data collected by them from EU data subjects are collected as per the provisions of GDPR. They also have the responsibility to ensure that those who collect the information and manage the information are under an obligation to protect it from misuse, respecting the rights of those who are the owners of the data. However, in a world today where data storage is shared on the cloud most of the times, there are constraints and although the GDPR

---

1 Charter of Fundamental Rights of the European Union, 2000; Treaty on the functioning of the European Union, 2009.

2 *A comprehensive approach on personal data protection in the European Union* (2011), OJ C 181/01, p.1.

3 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995

4 Art. 1, of GDPR.

5 Art. 1(2), of GDPR.

6 Art 4(7), of GDPR.

7 Art 4(8), of GDPR.

has an extra-territorial applicability, in a space which is borderless, applicability of law poses challenges[8]. There are challenges to adjusting extra-territorial issues against conventional principles of territoriality.

Salient features of the provisions in the GDPR

The GDRP introduced changes in the way subjects are protected in relation to their personal data and has imposed duties on the State, businesses, people and organizations.

In a digital economy where technology is growing at a phenomenal speed, personal data is essentially a valuable resource which needs to be properly and systematically regulated in terms of processing, storage and transfer to third parties and other countries. Introduction of GDPR is an important step forward. There are cases where companies accumulate personal data relating to race, age, religion, political views, health conditions, device location etc which the company can later cash in many ways including sale of data to third parties. A lot of times companies providing online services collect data and later share the data with hardly any restrictions as regulators and law enforcement agencies do not have any mechanism to uphold and protect the privacy of people.

The GDPR provides extensive guidelines for transfer of personal data to third parties, third country location, international organisations or any other third party.[9] This puts a pressure on countries transacting or dealing with companies in EU. Thus countries like India are delving on strengthening their 'Data Protection and Data Localisation' laws. The provision under the GDPR states that companies should have the infrastructure to be able to provide any information relating to the data subject in a concise and transparent manner and in an accessible form.[10]

In terms of extra-territorial application, it is important to delve into the provision under Article 3 of the GDPR. A plain reading of the text could mean that the data subject could be any person irrespective of the nationality or the place of residence. It could mean that if an organisation possesses personal data of an individual who is a citizen of EU but is located outside the EU will not by itself trigger Article 3 of the GDPR. For example, if an enterprise based in India provides cleaning services of residences of persons located in India and the person during a travel meeting in Germany downloads the mobile app for the cleaning services while in Germany, does not attract the provisions of the GDPR as although the person downloads the app while in Germany and provides personal data as required in the app, the services are not for people in the EU.

---

[8] Newcombe Lee, *Securing Cloud Services: A Pragmatic Approach*, 2nd edition, IT Governance Publishing, 2020.

[9] Chapter 5, of GDPR.

[10] Article 12, of GDPR.

The GDPR provisions apply to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, irrespective of whether the processing takes place in the European Union or not.

In case a controller or processor is in the Union, it is irrelevant where it is doing business and whose personal data it is processing.[11] However, what is new in the GDPR is that in terms of the extra-territorial application of the provisions of the GDPR the scope of its application is widened outside the EU in two cases:

1) where goods or services are offered to EU data subjects;
2) it relates to tracking of behaviour of EU data subjects in EU.[12]

According to the provisions of the GDPR[13] anyone who has and processes personal data is accountable for guaranteeing that such data is:

- Processed in a legal, fair and transparent fashion (lawfulness);
- Collected and used for specified, explicit and legitimate purposes only (purpose limitation);
- Limited only to what is necessary for the specific purpose of processing (data minimisation);
- Accurate, with inaccurate data rectified and erased (data accuracy);
- Retained only as long as needed (data retention); and
- Protected (integrity and confidentiality).

Consequence of the GDPR on Business

Implementation of the GDPR for a company comes with a heavy cost which includes investment in various arena including investing in software and technology training personnel, hiring experts and lawyers to ensure compliance to the provisions of the law. It means processing personal data as per the provisions in the regulations, setting timelines to identify security breaches and informing the authorities. It also means sending communications to the customers to seek their consent and revalidating their consent. Non-compliance to the provisions of GDPR law means incurring heavy penalty. Big businesses have the advantage of customer trust which is not available to smaller businesses.

Earlier on, when personal data were collected by companies, they were stored physically in certain physical locations. However, today's business models and practices are different. Today, companies collect data through websites and then they are stored in remote servers located at places anywhere in the world. Many a times the data are saved on the cloud. The system of data storing allows people to use the information on the cloud from any remote locations. Now, under the GDPR regime, the place where the data will be stored is strictly

[11] Article 3(1) of GDPR.
[12] Article 3(2) of GDPR.
[13] Article (5) of GDPR.

regulated by the GDPR and the domestic law on the subject. Transfer of personal data of EU subjects can be made to a non-EU country only as per the provisions of the GDPR. Data subjects of the EU now also have the right to be forgotten[14]. They now have control over their data[15].

The companies in possession of personal data have to notify the users of the ways in which they use the data relating to them to provide insight into their data, provide a copy of data, or change incorrect data.[16] An individual has the right to get from the controller the erasure of personal data about him or her without delay and the controller has the obligation to erase personal data without any undue delay where one of the grounds mentioned in the provision of the regulation are present.[17]

Automated individual decision-making, including profiling, is made contestable under the law now.[18] Citizens now have the right to question and fight decisions that affect them that have been made on a purely algorithmic basis.[19]

Under the regulation it is necessary to implement appropriate measures so that processing would be carried out only on personal data collected for a specific purpose. This effectively means that every company will, from the beginning, have to adjust its business model to privacy protection standards when making a business plan or strategy which includes handling or collecting data.[20] Privacy by Design and by Default require that data protection measures are designed into the development of business value proposition processes for products, services and processes of product and services.[21]

The number of complaints brought by consumers is increasing since the implementation of the GDPR[22].

In landmark *Google case*[23] the Court of Justice held that there is no obligation under EU law that compels Google to apply provision under the GDPR on the right to be forgotten to every country in the world. The court stated that under the law EU residents certainly have the right of erasure, but this right is only available within the borders of EU Countries. The court in the case set the territorial boundaries of an individual's right to be forgotten. In this case Google was only required to remove the links of the search engines within the EU.

---

14 Article 17 of GDPR.

15 https://www.researchgate.net/publication/325914966_Impact_of_GDPR_on_Business_Focus_on_Data_Controllers_and_Processors_not_Established_within_the_EU/link/5bf3d10992851c6b27cc290a/download accessed on 24 May 2020.

16 Article 7 of GDPR.

17 Article 17 of GDPR.

18 Article 22 of GDPR.

19 https://www.riverpublishers.com/journal.php?j=JMBMIT/4/3.

20 Article 25 of GDPR.

21 https://www.riverpublishers.com/journal.php?j=JMBMIT/4/3.

22 https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/risk/deloitte-nl-risk-part3-received-complaints.pdf, accessed on 25th May 2020.

23 Case C-507/17 *Google v CNIL*

Another landmark international privacy case was brought against *Facebook* by Max Schrems which was brought to the Irish Data Protection Commissioner where Mr. Schrem had challenged the transfer of his data along with that of EU citizens to the U.S. by Facebook. The Court of justice of the European Union invalidated the Safe harbour arrangement, which governed data transfers between the EU and U.S.

International response towards becoming GDPR compliant

The implementation of the GDPR has not just affected the companies from the 28 (now 27) EU countries but it has had a direct impact on the countries across the globe where any kind of personal data from customers from EU are collected and processed. The GDPR may be a EU regulation, however, its implication is not limited to the EU and thus it is not completely a EU issue. The global reach and extra territorial application of the GDPR cannot be denied. The enforcement of rights by the consumers, the growth in the awareness about the GDPR and the potential fines that will be imposed for violations of the GDPR provisions will create external pressure upon companies across the world doing business with the EU to comply with the GDPR framework and meet the demands of the Data Protection Authorities[24]. The Extra-territorial scope of the GDPR increases the scope of the regulation and echoes the borderless nature of the digital world and the internet[25]. Countries outside the EU are also introducing new data protection regulations and upgrading their existing law[26]. Countries transacting with the EU have to ensure they consider issues relating to security controls, data management and automation

Transfer of personal data to a non-EU country can only take place if the Commission considers that this country provides the necessary and adequate level of protection. The transfer is allowed if appropriate safeguards are available in the other country in the form of contract clauses, binding corporate rules, adherence to Codes of Conduct or certification schemes and if the individual has given explicit consent to transfer the private data to such other country. Although there is the extra-territorial application of the GDPR, there is no standard provided to measure the 'adequacy' of the level of protection that should be available.

While some countries are welcoming the GDPR as a benchmark around which they are structuring their national data protection laws, other countries are still skeptical about the new data protection regime simply because their own *existing laws are too weak* to support the GDPR model.[27] Companies from

---

[24] Blume, J. (2018), A Contextual Extra Territoriality Analysis of the DPIA and DPO Provisions in the GDPR, 49 *Geo. J Int'l* 1425.

[25] Azzi, A.dele (2018), The Challenges faced by the Extra Territorial Scope of the General data Protection Regulation, *JIPITEC* 9 (2).

[26] Kessler, J. (2019), Data Protection in the Wake of the GDPR: California's Solution for Protecting the World's Most Valuable Resource, 93 S. *Cal. L. Rev.* 99.

[27] Schwartz P., Peifer K., (2019), Structuring International Data Privacy Law, *Int'l Data Privacy Law* 21, p.33.

these lesser compliant countries will have a tough time transacting business with EU nations.

Trade between India and Europe

The last two decades have been important as far as the EU - India trade and business relationship is concerned especially with both the EU and India having undergone considerable social, economic and political changes. Over this period of time, the EU grew as an economic power on the International arena, while India underwent a social and economic growth emerging as an important player on the international market. Over the past two decades India has emerged as an attractive place to do business and Indians have also grown to widen their business bases in Europe. India has emerged as a reliable business partner on the International arena and the European market has also been quick to realise this fact.

While the European Commission and trade leaders of the EU and India look at ways to strengthen the trade partnership between the countries and even at easing FDI regulations to facilitate establishment of Indian companies in the EU and European companies in India, the introduction of the GDPR has raised several concerns especially in the light of the concern relating to the impact of the implementation of the GDPR and concerns about data localisation although that has not been the intent of introducing the GDPR *perse*[28].

With the new set of Cross-Border restrictions[29] and extra-territorial commercial pressure exerted by the implementation of the GDPR the ease of transacting business for many Indian companies will now become cumbersome. Many companies outsourcing their information management sector are concerned with the greater risk of penalties and litigation due to the higher threshold of accountability under the GDPR regulation. The clear increase in infrastructural cost for companies[30] in order to make their business module more GDPR-compliant is a taxing and stressful challenge faced by Indian companies as well as companies across the globe. Although the GDPR is relatively comprehensive, lack of guidance on what constitutes an effective data de-identification scheme and the grey area on what is inadequate causes confusion among countries. These are some of the apparent challenges faced by companies in their quest to becoming more GDPR-compliant.

The EU is India's largest trading partner and accounted for €80 billion worth of trade in goods in 2019 and 11.1% of the total Indian trade. This was on par with the USA and ahead of China which stood at 10.7%. India was the EU's

---

[28] https://www.europeindia.eu/wp-content/uploads/2018/01/EICC-Newsletter-January-2018.pdf accessed on 20th May 2020

[29] Krishnan, S. (2016), *Cyber Security, How can Indian organisations prepare for the GDPR regime?,* PwC India, https://www.pwc.in/consulting/cyber-security/blogs/how-can-indian-organisations-prepare-for-the-gdpr-regime.html.

[30] *Ibid.*

10th largest trading partner accounting for 1.9% of the total EU trade in goods in 2019. On the other hand, trade in services between the EU and India has increased considerably to €29.6 billion in 2018 while it stood at €22.3 billion in 2015. Another interesting figure is that the EU's share in foreign investment inflows to India has doubled from 8% to 18% in the last decade, making the EU a very large foreign investor in India. The EU's foreign direct investment stocks in India were €68 billion in 2018. There are over 6,000 European companies in India, providing over 1.7 million direct jobs in India and providing 5 million jobs indirectly in a broad range of sectors[31]. The uncertainties and fear of law suit for any possible violation have created tremendous commercial pressure on Indian businesses operating in and from the EU.

The extended territorial scope and huge fines are prompting not only Indian companies but also countries and companies outside the EU, trading with the EU and dealing in data relating to EU citizens to comply with the provisions of the GDPR[32]. What makes GDPR compliance much more challenging is the stringent codification requirements, along with fines that can be as much as four percent of a company's global revenue or €20 million ($21.3 million), whichever is higher.[33]

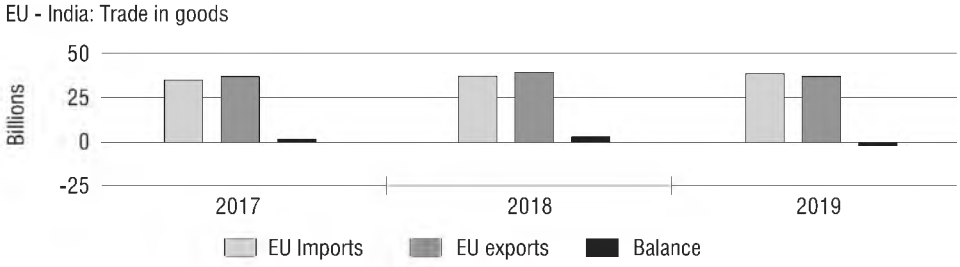

Fig. 1. Trade in Goods for 2017, 2018 and 2019[34]

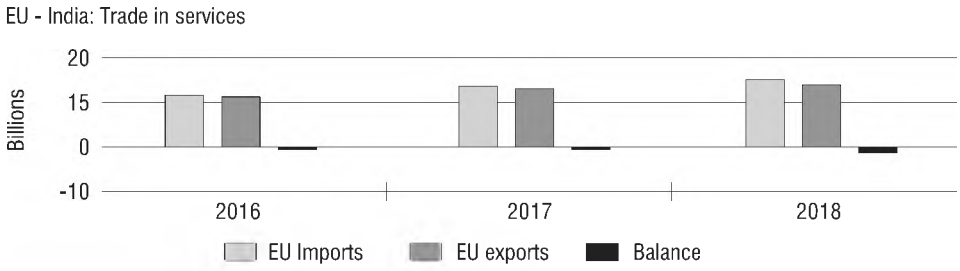

Fig. 2. Table on trade in Services for 2016, 2017 and 2018[35]

[31] https://ec.europa.eu/trade/policy/countries-and-regions/countries/india/ accessed on 20th May, 2020.
[32] California Consumer Privacy Act 2020, in US, India's Data Privacy Bill 2019.
[33] GDPR, RSA, Available at https://www.rsa.com/content/dam/en/e-book/how-gdpr-could-impact-your-business-organization.pdfaccessed on 24th May 2020.
[34] Source: European Commission Trade Policy Report.
[35] Source: European Commission Trade Policy Report.

The EU-India trade regime and regulatory environment is relatively restrictive with technical barriers to trade, sanitary and phyto-sanitary measures, deviation from international standards and agreements. Adopted legislative or administrative measures such as the GDPR can also affect a wide range of sectors, including goods, services and investment.

One of the sectors amongst others that is going to have a great impact on the implementation of the GDPR is the Information Technology arena. India is one of the countries which will be impacted from cross border transfer that happen between India and the EU in the field of IT. IT companies in India will face numerous challenges in building applications that use personal data. The problem will be bigger for smaller companies than for larger ones.

The GDPR seems to be the new wave of protectionism emerging on the international arena and refers to a broader range of domestic actions restricting international trade[36]. Restrictions on cross-border flows of personal data or data localisation requirements do hamper digital trade. With a substantial market in the pharmaceutical sector IT and BPO, restrictions on personal data will affect digital trade. The impact of the extra-territorial commercial pressure on Indian trade and business is big. With the EU as one of the big markets for Indian outsourcing sector, India will need to strengthen its own systems. Weak data protection laws make India less competitive on the global market and there is a lot of pressure to brace ourselves by legislating a strong law relating to data privacy and data protection. Indian companies require proper safeguards as required under the GDPR so as to be able to transfer data beyond the EU. There will not be enough prospects for Indian companies that do not comply with the GDPR or increase compliance costs. The decision in the case of Justice K. S. Puttaswamy (Retd.) & Anr v Union of India & Ors[37] paved the way for a comprehensive Bill on Data Protection in India.

India introduced the Data Protection Bill 2019 in December 2019 in the *Lok Sabha* (House of the People). The 2019 Bill has taken India a step closer to having a comprehensive legislation on Data protection and data privacy. Once it is enacted, the law will have huge implications on investments and trade in sectors such as IT, BPO, Artificial Intelligence and in the pharmaceutical sector which are key areas in case of trade in services between India and the EU and also other countries such as the United States and the United Kingdom. The Bill proposes to bring about certain data localisation restrictions although there has been resistance from global giants such as Google and Apple. The Bill also allows the Data Protection Authority to create 'Sandbox' where business undertaking such as those in Artificial Intelligence, machine learning, etc. can seek certain relaxation on the applicability of some of the data protection obligations. Although the 2019 Bill in India is based on the GDPR, there are also differences between the two.

---

[36] Yakovleva, S. (2020), Privacy Protection(ism): The Latest Wave of Trade Constraints on Regulatory Autonomy, 74 U. *Miami L. Rev.* 416.

[37] MANU/SCOR/31178/2018, ITEM NO.1502 COURT NO.1 SECTION PIL-W ITEM NO.1502 COURT NO.1 SECTION PIL-W Writ Petition Civil No.494/2012.

Many Indian companies are already GDPR-compliant. However, once the Bill is enacted, Indian companies will also have to ensure compliance with the incremental requirements set out under Indian law. This will also impact cross-border transactions, as the investor and the target will need to ensure acquiescence with data protection laws across multiple applicable jurisdictions.

Keeping in mind the expanded territorial application of the GDPR, Indian companies have to ensure that in case one possesses personal data of any EU citizens there is an obligation to appoint a representative on EU territory. It can be a branch office in some EU Member State, or a local lawyer or a person in charge of communication with the competent bodies of the EU. Risk assessment and mitigation will be required to be made and prior approval of the Data Protection Authorities (DPA) will be required for high risks[38]. Companies could face practical difficulties while transferring data to third countries with two different players, the data controllers and the data processors. Data processors will be bound by the provisions under the GDPR but there can be legal issues on the applicable laws regarding the latter. Although the GDPR does provide some basis to govern both players, in case of multinational technology companies which are situated outside the EU with no regional offices in the EU where the company is able to obtain data through worldwide users, there will be a problem in defining 'data transfer'.

Trade and GDPR

It becomes imperative for India to provide for proper safeguard measures and ensure compliance to the GDPR and also formulate its own law relating to data protection and data privacy with the EU making data protection and free trade two important areas of action. The connection between trade and data protection is increasing and this is because there has been a phenomenal increase in digital services being provided as part of trade in services and processing personal data is an integral part of ensuring competitive services. In provisions relating to cross-border transfer of data the companies have to comply with the provisions under the GDPR. There is no provision under the WTO which regulates cross-border data transfers, however, DSB has held that the WTO rules apply to cross-boarder data services[39]. The WTO has recognised the extension of world trade in information technology products[40].

FTAs between countries are on an increase. In the past, there has been an attempt to have an FTA between India and the EU and there have been dialogues for a comprehensive Free Trade Agreement between India and the EU that began in 2007, however, the same was suspended in 2013 because of the differences in ambitions between the two countries. However the EU has successful free trade agreements with many other countries and as part of

[38] Article 35 of GDPR

[39] DS285: Antigua and Barbudav. United States, United States - Measures Affecting the Cross-Border Supply of Gambling and Betting Services

[40] https://www.wto.org/english/docs_e/legal_e/itadec_e.htm

FTAs with countries the EU has been calling on the parties to maintain adequate data protection measures[41]. GATS provision positions trade interests above all and not in providing any guarantee for upholding data protection as envisaged by the EU under its GDPR regime, whereas the EU has prioritised data protection giving lesser priority to trade interests. Considering that there are strong trade links between India and the EU, India will have to take a strong stand as far as data privacy and protection is concerned keeping in mind the trade interests.

Conclusion

The GDPR law enacted in Europe has its impact on India. Regarding the extra-territorial applicability of the provisions of the GDPR, there are extra territorial commercial pressures created which will impact trade and business between the EU and India and other countries. There has to be further clarity regarding jurisdictional scope and provisions relating to cross-border data transfer. In spite of the gaps, EU data protection law is the fore runner in upholding data privacy and upholding privacy rights of EU nationals and residents. Irrespective of the location of an organisation or business, in case of businesses processing personal data of individuals from the EU or in case of businesses having a presence in the EU, they should be GDPR-compliant. Countries across the world are updating their existing law relating to data privacy. One of the driving forces behind updating data privacy law has been the high administrative fines that will be imposed in case of non-compliances to the provisions of the GDPR and the fear of legal battles. India's trade with the EU has been substantial as far as IT, BPO and the pharmaceutical industry sector are concerned. For the Indian industries - be it the IT sector, the BPO or the pharmaceutical industry - to keep continuing to do business in Europe, it needs to comply with the GDPR. Introducing the Data Protection Bill, India has moved a step closer to having comprehensive data protection legislation. The Bill which is to a great extent based on the EU General Data Protection Regulation of 2018 goes a long way in implementing an all-and-inclusive legislation to uphold data privacy, promoting trade between countries further strengthening the trade between India and the EU. It is a legislation that will have great implications in financial investment activities and this will be especially true for financial investment activity in data intensive targets such as the IT sector, the BPO sector, the Artificial Intelligence sector and the pharmaceutical sector where India has been strong. It also becomes imperative for Indian companies to review their policies and data privacy and protection policies and also impart regular training programmes for their employees. Indian companies also need to be equipped to deal with the audit process. The GDPR as a law cannot be considered to be a piece of legislation which only has a local implication. In the past 2 years it has shown that the GDPR has a far-reaching implication and countries will have to review their existing laws thus ensuring a better trade and investment environment between countries.

[41] See EU - Japan FTA, EU - South Korea FTA.

Bibliography

1. Azzi, A. (2018), The Challenges Faced by the Extra Territorial Scope Of The General Data Protection Regulation, *JIPITEC* 9 (2).
2. Blume, J. (2018), A Contextual Extra Territoriality Analysis of the DPIA and DPO Provisions in the GDPR, 49 *Geo. J Int'l* 1425.
3. Kessler, J. (2019), Data Protection in the Wake of the GDPR: California's Solution for Protecting the World's Most Valuable Resource, 93 S. *Cal. L. Rev.* 99.
4. Krishnan, S. (2016), *Cyber Security, How can Indian Organisations Prepare for the GDPR Regime?,* PwC India, https://www.pwc.in/consulting/cyber-security/blogs/how-can-indian-organisations-prepare-for-the-gdpr-regime.html
5. Lindgren, P., and Rasmussen, O. H. (2013), The Business Model Cube, *Journal of Multi Business Model Innovation and Technology*, 1(3), 135-180.
6. Newcombe, L. (2020), *Securing Cloud Services: A Pragmatic Approach*, 2nd edition, IT Governance Publishing.
7. Schwartz, P., Peifer, K. (2019), *Structuring International Data Privacy Law*, Int'l Data Privacy Law 21.
8. Tarhonen, L. (2017), *Pseudonymisation of Personal Data According to the General Data Protection Regulation,* In Korpisaari, Päivi (edit.). Viestinnän muuttuva sääntely - Viestintäoikeuden vuosikirja 2016. Forum Iuris, Helsingin yliopiston oikeustieteellisen tiedekunnan julkaisuja 2017, p. 10-32.
9. Yakovleva, S. (2020), Privacy Protection(ism): The Latest Wave of Trade Constraints on Regulatory Autonomy, 74 U. *Miami L. Rev.* 416.

Cases

1. DS285: Antigua and Barbudav. United States, United States - Measures Affecting the Cross-Border Supply of Gambling and Betting Services.
2. Justice K.S. Puttaswamy (Retd.) &Anr v Union of India &Ors, MANU/SCOR/31178/2018, ITEM NO.1502 COURT NO.1 SECTION PIL-W ITEM NO.1502 COURT NO.1 SECTION PIL-W Writ Petition Civil No.494/2012.
3. Maximilian Schrems v. Facebook Ireland Limited (2013).

Legislation and Other

1. California Consumer Privacy Act 2020
2. Charter of fundamental rights of the European Union, 2000;
3. Data Protection Directive 95/46 /EC
4. General Data Protection Regulation, 2018
5. Treaty on the functioning of the European Union, 2009.

Acknowledgement

1. The research presented in the paper has been done under the EU-funded Erasmus+ project EURASIA: European Studies Revitalised across Asian Universities (Project ID: 585968-EPP-1-2017-1-BG-EPPKA2-CBHE-JP.)