Page 601 - 612 **DOI:** *https://doij.org/10.10000/IJLMH.113618*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 5 | Issue 5

2022

Data Protection Regulations and Compliance Requirement: Analysis of Regulations From EU, Singapore and India

SHUBHANGI UPADHYAY[1], KULDEEP KUMAR YADAV[2], PRINGLE SINGH[3] AND SHASHI SHUKLA[4]

ABSTRACT

In the present era, cybercrime and other similar offenses including identity theft, data breach, etc, have increased the concern towards data security over the last decade. On one side, we cannot avoid our everyday life without data transferring transactions and on the other side, the data transferring transactions are becoming riskier and riskier. Sensing the urge of the hour, many States globally have come up with their Data Protection Laws. However, among all such regulations, the General Data Protection Regulation of the European Union has had a large impact on the world. In order to determine how effective and similar the General Data Protection Regulations are, the author has reviewed the legislation and made a few other regulations, such as the Personal Data Protection Act, 2012 of Singapore, a point of comparison. The provisions of the compliance requirements that are the same and different in each of these rules have also been considered by the author. The corporate entities' perspective has been used to evaluate compliance requirements. Since the regime is still in its infancy at the moment, the author has also provided a brief introduction to the data protection laws already in place in India and any potential future developments. With the aim of comparing and developing a better understanding of the regulations of the respective three countries, the author derives an analysis in this article.

Keywords: *Data Protection, GDPR, Cyber Crime, Privacy, Aadhar, EU*

I. INTRODUCTION

Over time, as Internet usage has grown, so has the significance of data privacy. In order to deliver services, websites, software, and social media platforms frequently need to gather and preserve personal data about users. However, some platforms and applications could go beyond what consumers had anticipated in terms of data gathering and utilisation, giving users less

[1] Author is an Advocate in India.
[2] Author is an Advocate in India.
[3] Author is an Advocate in India.
[4] Author is an Advocate in India.

 [ISSN 2581-5369]

privacy than they had anticipated. Other platforms and apps might not put enough protections in place for the data they gather, which could lead to a data breach that breaches user privacy.

In simple words, one can say that data privacy refers to a person's right to decide for themselves when, how, and to what extent their personal information is shared with or conveyed to others. These details can include a person's name, address, phone number, online or offline conduct, or other personal information. This is similar to how someone might desire to keep others out of a private chat, many online users want to regulate or stop the flow of specific kinds of personal information.

No digital transaction in the modern world is free from the influence of communications and other data-related chores because they have merged into our daily lives. The development of internet services has greatly facilitated electronic transfers, making them easier and quicker, but this convenience does not come without a price, since the risk of hacking, fraud, data theft, and other related cybercrimes has also increased. The risk has increased significantly with the development of technology transactions and the sharing of data between users, as compared to other paperwork that is often completed offline.

According to various estimates, the amount of data traveling across borders increased by 45 times between 2005 and 2014, and e-commerce sites like Alibaba and Amazon account for up to 12% of all international trade, particularly in the realm of products (Manyika, 2016). According to the US International Trade Commission, increased productivity and decreased trade costs resulted in a more than 3.4 percent increase in the US Gross Domestic Product (GDP) in 2014. This can be attributed to global digital trade, which includes data processing and other data-based services.

Numerous nations have already taken action in response to the concerns surrounding data protection by creating their own regulatory frameworks to address the issue. Data protection issues have already attracted attention in many countries around the world. The GDP Regulations, which were recently adopted by the European Union, were the most recent shift in the realm of data protection. These regulations had a tendency to have an impact on nearly every nation, forcing them to modify in order to meet their new compliance standards. The EU's definition of privacy is more centered on the idea that it is a fundamental human right, therefore a transition in which the international regulatory bodies modify their legislation in accordance with the European GDPR ideology is a pretty high-hoped move. This idea is deeply ingrained in the rich history and culture of the European Union, and it is not always a viewpoint that other nations in the world.

 [ISSN 2581-5369]

II. WHY DATA PROTECTION REGULATIONS ARE IMPORTANT FOR EVERY STATE?

By creating rights to shield individuals from the misuse of their personal data and obligations to hold companies accountable for their use of data, effective data protection laws and regulations contribute to the growth of public trust in digital tools and systems. Theoretically, this increased trust should result in a higher level of acceptance of services that depend on data sharing and usage, which will increase investment in the tools and knowledge required to accelerate a nation's digital transformation and promote evidence-based government.

Data rules and regulations, however, must be well-thought-out, adapted to local realities, and regularly and successfully implemented in order to achieve these goals. Sadly, early data reveals that many nations with data privacy laws have insufficient enforcement, independent regulatory bodies, and policies that are not tailored to the available resources.

Fair Information Practices were established in the United States in the 1970s, and the OECD later codified and expanded on these principles in the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, which were published in 1980. These events are credited with the development of modern approaches to data protection. National data protection frameworks founded and expanding on these principles have been gradually spread over the years that too mostly in wealthier nations.

Notably, the number of countries that have adopted data protection legislation has significantly increased over the last two decades. Since 2010, in most countries of Africa, Asia, and Latin America, 64 countries over the globe have come up with their data protection laws.

Interestingly some factors like growing general awareness of the risk of personal data misuse, the demand for responsible data acquiring and processing, smooth international trade, etc are the pulling force for the recent rapid adoption of national data protection frameworks by multiple countries. More than 60 countries have enacted new data protection laws and among them, almost all have taken GDPR and the EU Data Protection Directive of 1995 as their base model in their framework.

III. GENERAL DATA PROTECTION REGULATION: EUROPEAN UNION

The General Data Protection Regulation (GDPR, 2016) of the European Union (EU) places great emphasis on the fact that any individual's personal data is significant. As a result, from every angle, the GDPR has been structured to appear as though dealing with data required a lot of planning. The GDPR, which the EU adopted in May 2018 to replace the previous Data Protection Directive, is a reflection of the value of privacy as a human right in the EU. It

broadens the implementation of the EU Data Protection Directive and increases its extraterritorial reach.

The GDP Regulations were passed into law in 2016, although they were not implemented until the year 2018 (GDPR, 2016). Prior to the GDPR, the European Union's Data Protection Directive was in effect which also established the framework for the GDPR as it exists today. But the earlier action had greatly inadequate compliance and poor enforcement. The fact that the regulations include significant fines for failing to comply with the requirements as set forth, as well as the incorporation of several external mechanisms to encourage compliance as soon as is practicable by corporate entities and other individuals included within the regulations, is one of the main reasons why the GDPR has attracted the attention of corporate entities in the current time period. This has had a significant impact globally, making the GDPR one of the most well-known laws that affects practically the whole world. The GDPR's scope has been designed in a way that makes the electronic domain impervious to illegal access. The regulations thereby address a broad range of information-related issues.

The GDPR is strategically constructed in a way that instills in businesses a sense of the value of data and the range of ways in which it may be used in their operations. Additionally, the design places these rules almost on par with rules that businesses typically take seriously, such as antitrust statutes and other laws pertaining to corrupt conduct. There have been cases in the past where businesses that engaged in data-related wrongdoings received fines that were less than what they would pay to one of their employees, so the firms themselves are not all that motivated to follow the law. The current GDPR, in contrast, has updated penalty allocation and enforcement for strict compliance standards that must be adhered to by those who have implemented the mechanism incorporated inside the scope of the GDPR.

Any organisation that has operated within the EU as well as any organisation outside the EU that provides goods or services to clients or enterprises in the EU is subject to GDPR. The law applies to two main categories of data handlers: "processors" and "controllers." A processor is a "person, public authority, agency or other body which processes personal data on behalf of the controller" and a controller is "a person, public authority, agency or other body which determines the purposes and means of the processing of personal data, either alone or jointly with others." For instance, if you were governed by the UK's Data Protection Act, you'll probably also need to comply with GDPR. "If you are accountable for a breach, your legal liability will increase dramatically. Under the GDPR, these requirements for processors are a new duty "the UK's Information Commissioners Office, the body in charge of registering data controllers, enforcing data protection laws, and responding to complaints about data processing

 [ISSN 2581-5369]

practices. In the end, GDPR imposes legal responsibilities on processors to keep track of personal data and how it is processed, resulting in a far higher amount of legal exposure in the event that the organisation is violated. Additionally, controllers must make sure that any agreements with processors adhere to GDPR.

Online personal data is gathered in a variety of ways, including through e-commerce, social media use (such as Twitter and social networks), internet browsing, and location information from smartphones. When collected and analysed to create a personal profile, personal data can also be inferred from non-personal data. It is not always easy to tell personal data from non-personal data, as this taxonomy of personal data illustrates. Even if each individual piece of data collected is not personal, gathering information on habits, places, and health conditions can be used to build a personal picture of a person so it would always be a matter of concern.

Even if a corporation doesn't have a presence in the EU, but it maintains or processes personal data about EU citizens there, it must abide by the GDPR. Companies needing to comply must meet the following criteria:

- An existence in an EU nation.

- Does not have a physical presence in the EU yet handles personal data of citizens there.

- There are over 250 workers.

- Less than 250 employees, but where data processing that affects data subjects' rights and freedoms, is ongoing or involves certain forms of sensitive personal data. That essentially means that all businesses.

The GDP Regulations tend to have an effect on a number of different third party and customer contracts in addition to the businesses that meet each of the aforementioned requirements, imposing an equal obligation on both data controllers and data processors. In Europe, the right to privacy is increasingly recognised as distinct from data protection. While privacy upholds the Athenian ideal of private life, data protection concentrates on whether data is utilised fairly and in accordance with due process.

The Data Privacy Directive's geographical application is not as broad as that of the GDPR. This has been characterised as a "major shift in extraterritorial application" by one analyst. Another person said the idea that the GDPR can be applied globally to protect personal data from the EU while it is being transmitted throughout the world "illusion."

The Directive that came before the GDPR was causing problems for the European Union since it was impossible to maintain consistency across national privacy regulations. As a result, some

 [ISSN 2581-5369]

internet companies started abusing the directive's existing flaws, which prompted a revision of the directive. The older directive was redesigned in an effort to fill the gap left by the earlier directive, and this is how the GDPR came to be. It also applies to the monitoring of individuals' behaviour insofar as it occurs within the Union when processing activities are related to either (a) offering goods or services to such individuals in the Union, regardless of whether a payment from the individual is necessary; or (b) monitoring their behaviour insofar as it occurs within the Union (GDPR Article 3). However, the Regulation mandates that the controller name a representative in the Union in cases where the controller is not based in the EU (GDPR, 2016).

The GDPR's Recitals 23 and 24 add to the basic information. Online offers of products or services that include the usage of the language of an EU member and the ability to make a purchase are likely to qualify as an offering for sale under the GDPR, according to Recitation 23. A person is "monitored" when they are "tracked on the internet with data processing techniques that consist of "profiling" a person, particularly in order to take decisions about her or him or for analysing or predicting her or his preference, behaviours, or attitudes," according to Recital 24 of the Regulation. When considered as a whole, this seems to encompass a sizable portion of internet usage.

The GDPR's compliance with EU trade commitments in the WTO might theoretically be contested by developing nations because privacy measures have an impact on international data transfers, which are essential to digital trade. The fundamental issue highlighted by the GDPR—how to retain digital commerce possibilities while maintaining nationally accepted privacy standards—is unlikely to be addressed by WTO action, though. However, WTO action may persuade the EU to be less rigid in its implementation of the GDPR and provide other nations with the chance to negotiate agreements similar to the one with the USA (Department of Commerce, 2016).

IV. THE PERSONAL DATA PROTECTION ACT, 2012: SINGAPORE

Singapore is amongst the first few Nations who comprehensively drafted and enacted Data Protection Act. Singapore’s Data Protection Act i.e Personal Data Protection Act (PDPA) was enacted in the year 2012. With recent amendment in 2020 PDPA is one of the most effective and the most comprehensive law on data protection.

Before Understanding the PDPA and its effectiveness, firstly it should be understood that what is personal data. Personal data is defined simply as any data regarding an individual who can be identified either from that or data or from that data and other additional information to which the organization or authority has or is likely to have access.

The PDPA regulates the use of personal data and also monitors its collection and its disclosure. However, PDPA does not applies to public sector, which is subject to separate data protections laws and regulations. Generally, the PDPA requires that consent must be obtained by the organization. Consent can be either expressed or implied under the PDPA.

There is no definition of sensitive information under the PDPA. However, guidance published by the Personal Data Protection Commission provides that certain types of information, such as national idtentity numbers, passport numbers and work permit numbers, should not be collected unless certain narrow exceptions apply. The PDPA does not apply to business contact information. The exclusion of business contact information encompasses an individual's name or title, business telephone number, business address, business electronic mail address or business fax number or any other similar information about the individual that is provided for business and not solely for personal purposes.

Express consent is only valid if the individual has been provided with adequate notice of the purposes of data collection, use and disclosure. However same is not the condition with the implied condition. Deemed consent includes situation firstly, where an individual either voluntarily provides the personal data and such providing is obvious or reasonable in doing so. Secondly, a situation where an individual voluntarily gives personal data to the organization but for a notified purpose. In addition to the above situations consent may also be deemed when personal data is provided to an organization for the purpose of entering into a ccontract where such providing of personal data was reasonably necessary. With the Amendmend of the Law in the year 2020, scope of deemed consent is widened. In addition the amendmend added two new bases for the processing of personal data i.e (1) legitimate interests and (2) business improvement purposes.

Other condition where data protection needs to be monitered is situation where transfers of data take place outside of Singapore, in such case the PDPA requires that organizations should provide a standard of protection that is comparable to the protection under the PDPA.

V. LEGAL SCENARIO FOR DATA PROTECTION: INDIA

In contrast to the GDPR or the Data Protection Directive, India is not a signatory to any treaty on the protection of personal data. However, India has ratified or is a signatory to several international declarations and conventions that uphold the right to privacy, including the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.

There are in fact provisions for data protection in India. However, there isn't a single, focused

piece of legislation; instead, the provisions are dispersed throughout a number of other pieces of legislation and some court rulings. Although India does not have a comprehensive law for data protection like the EU GDPR or the PDPA in Singapore, or like the sectoral laws that are present in many other nations, this does not imply that India has no provisions at all.

The Information Technology Act, 2000 ("IT Act") and the rules created thereunder, provides for collection, storage, disclosure, and transfer of electronic data, include the legal principles of data protection (Information Technology Act, 2000). IT Act also provides punishment for offences like illegal downloading/destruction/alteration/deletion of data, any kind of data theft, identity theft, cheating by personation, breach of confidentiality, etc.

However, IT Act was amended by the Government of India and Sections 43A and 72A, which grant a right to compensation for incorrect disclosure of personal information, were added. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (the "Rules") were subsequently published by the Central Government in accordance with Section 43A of the IT Act. On August 24, 2011, a clarification to the aforementioned Rules was published (the "Clarification"). With respect to the gathering and dissemination of sensitive personal data or information, the Rules have brought new responsibilities for commercial and corporate enterprises in India that bear certain resemblances to the GDPR and the Data Protection Directive.

Aadhaar which is a biometrically based resident unique identification number, was launched in India. The Aadhaar (Targeted Delivery of Financial and Other Subsidies Act) of 2016 ("Aadhaar Act"), as well as any rules and regulations made thereunder, govern Aadhaar. According to sectoral regulations, organisations in regulated industries like the financial services and telecommunications must maintain the privacy of client personal information and only use it as specified by the customer or for purposes that have been specifically authorised by law. The Supreme Court of India recognised the right to privacy as a fundamental right under Article 21 of the Constitution as a part of the right to "life" and "personal liberty" in a landmark decision issued in August 2017 (Justice K.S. Puttaswami & another Vs. Union of India). An aspect of the right to privacy known as "informational privacy" has been recognised, and the court has ruled that information about a person and the right to access that information also require the protection of privacy ("Privacy Judgment"). The court ruled that everyone should be able to control how their identity is used for commercial purposes, and that this right gives people the "exclusive right to commercially exploit their identity and personal information, to control the information that is available about them on the internet, and to disseminate certain personal information for specific purposes only." For the first time, the Supreme Court has

 [ISSN 2581-5369]

explicitly recognised a person's right to their own personal information.

As a result, the Indian government established a committee to develop a draught statute for data protection. The Data Protection Bill, 2021 ("Bill") is the most recent of several draughts of the data protection law that have been published. Technology companies and start-ups condemned the Bill for its contentious nature and the related high cost of compliance. On August 3, 2022, the Government withdrew the Bill. The new data protection measure, which the government has promised will replace the current one, is anticipated to be submitted to the parliament for ratification during its winter session in December 2022.

VI. CONCLUSION AND SUGGESTIONS FOR INDIA

Limitations on the use of personal data without the citizens' express consent were included in the abandoned Bill. Additionally, it had tried to provide the government the authority to exempt its investigative agencies from the Act's requirements, a proposal that was vehemently opposed by the opposition MPs who had submitted their dissent notes.

To inform the Lok Sabha members of the withdrawal, a statement was distributed. According to reports, the statement mentioned that the government was developing a thorough legislative framework while taking 81 modifications and 12 recommendations from the JPC into account.

However, if one derives the comparison in a nutshell one can find out that on the ground of applicability EU’s GDPR has a much wide coverage as it covers almost all organisations within or outside EU upon satisfaction of certain criteria, while PDPA only covers the businesses in Singapore. The withdrawn bill of Personal Data Protection in India was previous covering the data which is being processed in India as well as outside India. If we see the ground of consent Chapter 2, Article 7 of GDPR EU laid down the conditions for a valid consent and similar to that, in PDPA Singapore Section 13 requires subject’s consent to be taken for data collection, processing and release. Chapter 4, Article 33 provides for the requirement of notification of breach within 72 hours where as in Singapore there is no such requirement. Also, there is right to be forgotten provided by GDPR EU but no such specific right is there in PDPA Singapore. In India even the withdrawal Bill provided provisions for both the requirements.

Although there are differences in how these policies approach the method or data privacy in general, there are still some features of the regulations that tend to stay the same. In light of this, it is important to note that despite the ways in which these laws address data privacy vary greatly, the concept tends to be shared by all of them.

*****

 [ISSN 2581-5369]

VII. REFERENCES

- Aaditya Mattoo, Joshua P Meltzer, International Data Flows and Privacy: The Conflict and Its Resolution, Journal of International Economic Law, Volume 21, Issue 4, December 2018, Pages 769–789
- Christopher Kuner, 'Reality and Illusion in EU Data Transfer Regulation Post Schrems', German Law Journal 18 (04) (2017)
- Christopher Wolf, 'Overextended: Jurisdiction and Applicable Law under the EU General Data Protection Regulation', The Future of Privacy Forum White Paper, January 2013
- Department of Commerce Fact Sheet: Overview of the EU–US Privacy Shield, https://www.commerce.gov/news/fact-sheets/2016/02/fact-sheet-overview-eu-us-privacy-shieldframework.
- Justice K S Puttaswamy v Union of India and Ors, Supreme Court of India, Writ Petition (Civil) No. 494.https://sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf
- Pal Dalmia, Vijay. (December 12, 2017). India: Data Protection Laws in India – Everything You Must Know. Retrieved from http://www.mondaq.com/india/x/655034/data+protection/Data+Protection+Laws+in+India.
- Shamma Iqbal, Singapore to Introduce Data Protection Law (Inside Privacy, 13 May 2011), http://www.insideprivacy.com/international/singapore-to-introduce-dataprotection-law/
- Sindhuja Balaji, India Finally has A Data Privacy Framework – What Does it Mean For Its Billion-Dollar Tech industry, (August 3rd, 2018), https://www.forbes.com/sites/sindhujabalaji/2018/08/03/indiafinally-has-a-data-privacy-framework-what-does-it-mean-for-its-billion-dollar-techindustry/#63a9f7e670fe
- Singapore Legal Advice. (December 27, 2018). Essential PDPA Compliance Guide for Singapore Businesses. https://singaporelegaladvice.com/law-articles/essential-pdpa-compliancеguide-singapore-businesses/
- Economic Laws Journal Data Protection & Privacy Issues in India, http://elplaw.in/wp-content/uploads/2018/08/Data-Protection-26-Privacy-Issues-in-India.pdf
- Adv. Prashant Mali, Founder & President – Cyber Law Consulting (Advocates & Attorneys), Data Protection Laws and Compliance Requirements - Analysis of Laws from Europe, Singapore and India, 2019 JETIR June 2019, Volume 6, Issue 6