International Journal of Education, Modern Management, Applied Science & Social Science (IJEMMASSS)
ISSN : 2581-9925, Impact Factor: 6.882, Volume 05, No. 03(II), July - September, 2023, pp. 149-155

COMPARATIVE ANALYSIS OF DATA PROTECTION LAWS: GDPR VS. OTHER GLOBAL PRIVACY REGULATIONS

Dr. Sangeeta Sharma*

ABSTRACT

This research compares the General Data Protection Regulation (GDPR) with other significant worldwide privacy standards and discusses its essential components and ramifications. To stay compliant and manage risks efficiently, companies must appreciate the intricacies of data protection requirements in today's data-driven, globally networked environment. Since its 2018 implementation, the General Data Protection Regulation (GDPR) in the European Union has operated as a model for data protection regulations across the world. This study investigates the General Data Protection Regulation (GDPR) and draws similarities to different privacy laws throughout the world, including the CCPA in California, the PIPL in China, and the Personal Data Protection Bill in India. duties, enforcement mechanisms, and extraterritorial repercussions are essential issues to examine while examining the rules' reach and relevance. This research adds to the constant debate regarding data protection and aids stakeholders in understanding the challenge of complying with a wide range of regulations, which is vital because privacy concerns are now influencing legislative frameworks.

Keywords: *Data Protection, Laws, GDPR.*

Introduction

Within the context of today's data-driven and always-on environment, everyone, from individuals to governments, is becoming increasingly concerned about the means by which they can protect the privacy of individuals' information. Since there has been an increase in the number of people who are concerned about their privacy, various countries and regions all over the world have implemented stringent regulations regarding the collection, processing, and storage of personal information. One such framework that has established a standard for the protection of personal information is the General Data Protection Regulation (GDPR), which is a comprehensive and extensive piece of legislation.

General Data Protection Regulation (GDPR)

It was finally determined that the Data Protection Directive was no longer relevant after the enactment of the Global Data Protection Regulation (GDPR) in the year 2016. The General Data Protection Regulation (GDPR) was ultimately given the go-ahead after being discussed for forty days and undergoing a number of revisions. According to the adverse data limits imposed by the EU, which have resulted in legal confusion among member states, the acts of the EU are supposedly responsible for distorted competition and the stalling of economic progress. The issue of conflicting legal regimes was able to be brought to a satisfactory conclusion by means of the execution of regulatory measures that were immediately applicable to the addressees and that removed the demand for extra processes. There has been a considerable reduction in the possible hurdle that may be faced when travelling with an endless quantity of data as a consequence of law that is consistent across the member states of the European Union.

The General Data Protection Regulation (GDPR) was brought into effect with the intention of regaining the trust of the general public in the internal market of the European Union. In order to make this a reality, businesses must first acknowledge that they have broken the previous obligations of the General Data Protection Regulation (GDPR), and then they must satisfy their new promises for the protection of individual data. The General Data Protection Regulation (GDPR) was developed with the

* Associate Professor, Department of Law, RNPILJ, Anand, Gujarat, India.

purpose of ensuring that it is applicable to the maximum number of enterprises that are practically possible from the beginning. The obstacles that are provided by a global economy, new technology, and business models were taken into consideration, which allowed for the successful completion of this task.

The General Data Protection Regulation (GDPR) is a piece of legislation that, from a judicial and legal standpoint, combines twenty-eight separate frameworks into a single, conventional framework. This framework replaces the twenty-eight frameworks that were previously in operation. In the event that this were to take place, it would be advantageous not just to companies but also to the economy as a whole. This is because it would guarantee that all firms, whether they are new or already established, would be processed in the same manner. In light of the fact that the former way of notifying the Data Protection Authority (DPA) is both time-consuming and unnecessary, the General Data Protection Regulation (GDPR) made it obligatory for individuals to accept responsibility for their activities. As an additional requirement, the General Data Protection Regulation (GDPR) demanded that public agencies adhere to additional criteria on the transparency and friendliness of their operations towards customers. As a consequence of this, a more comprehensive comprehension of the concept of "consent of consumer" in correlation with the safeguarding of personal data was achieved. The General Data Protection Regulation (GDPR) has developed a variety of mechanisms in order to promote a healthy level of competition and, ultimately, to result in superior data protection services and products. This is the ultimate goal of the GDPR. Some of the measures that fall under this category are as follows: the right to data portability, the implementation of standard privacy symbols, and the implementation of data protection by design by default. The deployment of the deterrent strategy is now being carried out in order to evaluate the results of data protection and to avoid breaches in reporting.

The processing of data has undergone a considerable transition as a direct consequence of the General Data Protection Regulation (GDPR), which was implemented in May of this year. Previously, it was necessary to notify designated payment administrators (DPAs) whenever controller actions were being carried out. This was a requirement. As a result of the fact that the notification responsibilities of the member states were distinct from one another, this particular occurrence took place. A number of multinational companies (MNCs) were confronted with a significant challenge as a direct result of this. The requirements for internal recordkeeping that are defined in the General Data Protection Regulation (GDPR) have rendered this structure obsolete. Data protection officers will only be assigned to designated controllers. This structure has been replaced.

Throughout the course of this investigation, a comparison will be made between the General Data Protection Regulation (GDPR) and several other privacy regulations from across the world. The objective of this comparison is to offer readers with a better knowledge of the characteristics of the General Data Protection Regulation (GDPR), variations on the GDPR, and the current state of laws pertaining to data protection measures. As a result of the process of comparing and contrasting the guiding principles, scope, enforcement methods, and cultural subtleties of the various nations, it is possible that we will be able to get a more comprehensive knowledge of the varied ways in which nations protect the privacy of individuals.

The document in question is one that is always undergoing changes, and we are working hard to expand it in significant areas. It offers connections to further material that has been published by the material Commissioner's Office (ICO) and guidance that has been issued by the Article 29 Working Party of the European Union. Additionally, it offers links to important sections of the General Data Protection Regulation (GDPR). The Working Party is comprised of individuals representing the data protection agencies of each of the member states of the European Union (EU), with the Information Commissioner's Office (ICO) serving as the representative pertaining to the United Kingdom.

On the 25th of May in 2018, the General Data Protection Regulation (GDPR) became operational in the United Kingdom. The government has confirmed that the decision of the United Kingdom to depart from the European Union will not have any effect on the implementation of the General Data Protection Regulation (GDPR). This was verified by the government.

In order to assist businesses and public bodies in preparing to comply with the requirements of the General Data Protection Regulation (GDPR) before May 2018 and beyond, the Information Commissioner's Office (ICO) is committed to providing assistance. However, this should not be a diversion from the necessity of complying with the General Data Protection Regulation (GDPR), which is becoming increasingly important. After the United Kingdom exits the European Union, we are aware that there may still be questions about how the General Data Protection Regulation (GDPR) will be implemented in the United Kingdom.

Additional Reading in the Details of the GDPR Agreement

- **Personal Data**

The Data Protection Act (DPA) and the General Data Protection Regulation (GDPR) both relate to what is commonly referred to as "personal data." However, the definition of personal data that is contained in the General Data Protection Regulation (GDPR) is more detailed and makes it clearly clear that information such as an online identifier, such as an IP address, can be deemed personal data. According to the definition that is more comprehensive, a wide range of personal identifiers might be regarded to constitute personal data. This is a reflection of the method in which organizations acquire information about individuals as well as the changes that have taken place in the field of technology.

The majority of organizations, who are responsible for storing HR data, customer lists, or contact details, among other things, should not see a significant change in practice as a result of the revision that was made to the definition. Because it is fair to assume that if you have information that is protected by the Data Protection Act (DPA), then it will also be protected by the General Data Protection Regulation (GDPR), it is recommended that you make this assumption.

Personal data that has been pseudonymized, such as by being key-coded, may or may not fall under the ambit of the General Data Protection Regulation (GDPR), depending on how difficult it is to connect the pseudonym to a specific individual. This is because the GDPR is designed to protect consumers' personal information.

- **Sensitive Personal Data**

In accordance with the General Data Protection Regulation (GDPR), sensitive personal data are referred to as "special categories of personal data." These categories are, for the most part, the same as those that are contained in the DPA; however, there are a few minor adjustments that have been made. An example of something that is specifically included in the special categories is the collection of genetic and biometric data. The processing of this data was done in order to create a one-of-a-kind identity for each and every individual.

It is not included that any personal information that refers to criminal convictions and offences is included; nevertheless, the processing of this information is subject to extra measures of a similar nature.

Principles and Rights

- **Principles**

The key responsibilities that fall under the purview of businesses are stated in the General Data Protection Regulation (GDPR), which is a set of rules that govern data protection. A new accountability duty has been introduced, and the notions that it contains are akin to those that are included in the DPA. At crucial locations, however, there is a greater degree of specificity. There is not a single concept that pertains to the rights of individuals or the transit of personal data anywhere in the globe that is included in the General Data Protection Regulation (GDPR).

The most significant change that was made was the introduction of the concept of responsibility. In accordance with the General Data Protection Regulation (GDPR), you are obligated to provide evidence that you adhere to the principles. One way to demonstrate this is by keeping a record of the choices that you make on certain processing activities.

- **Explanatory Text on Consumers' Rights**

Numerous concerns have been voiced regarding the potential risk to the privacy of customers that may arise as a consequence of the influence of big data. When information from a number of different sources is combined, this comes about, which eventually leads to the creation of consumer profiles that are meticulously crafted. In spite of the fact that the data sets are extremely extensive, it is possible to make use of them in order to accurately identify individual requirements, routines, and patterns of financial activity. The majority of the time, however, customers are unaware that they are contributing to the development of data that has an effect on analytical models.

"Consumers also need to have transparent, affordable, and convenient access and correction rights," as mentioned in the most recent G20 DFI HPLs, which were highlighted in the preceding phrase. This is something that consumers need to have.28, an ARCO rights are especially relevant in the context of DFS, which is a situation in which the data of a person is maintained by a number of different institutions or may be accessed by those institutions, and the data may be in a variety of various forms. There is a potential that consumers are ignorant of who is holding their data or who has access to it, the

reason for which it is being used, the place where it is being held or by whom it is being held, as well as the type of data that is being held and the scope of the data that is being stored. In addition, even if consumers are aware of all of this information, it is extremely improbable that they will be able to exercise their rights. In particular, this is the case in circumstances in which customer-recourse methods are not expressly established, as well as in circumstances in which data is hosted on the cloud and/or is unstructured data.

In General Principle 4 of the GPCR, there is a collection of proposals that concern to the rights of consumers. The regulations that regulate the protection of consumers and data subjects need to be established in a manner that leaves no room for interpretation. At the very least, these regulations ought to incorporate the ARCO rights, which are defined as follows:

- The right to object to their information being collected for certain purposes and/or used for certain purposes;
- The right to be informed on the conditions of collection, processing, and distribution of data held about them;
- The right to access data held about them periodically at little or no cost; and
- The right to challenge the accuracy of information about them."

It is important to note that the General Principles recognize the agreement of consumers whenever third parties access their data. This is the case even if the General Principles mandate the thorough collection of information, which includes positive data. In an open environment, where it is impossible to identify the data controller and the aim of data usage may be entirely different from the purpose of data collection, it may become increasingly vital for consumers to have the ability to make decisions on their own personal data. When customers are confronted with circumstances in which third parties make considerable use of their information, consent procedures, in conjunction with the idea of portability, may offer them some degree of protection.

The Individual Participation Principle of the Organization for Economic Co-operation and Development (OECD) gives customers the right to know whether or not a data controller holds certain information about them; 29 to access the data within a reasonable amount of time, in a form that can be understood, and at a cost that is not unreasonable; and to dispute the data and, if we are successful, to have the data destroyed or amended. Several concepts that are comparable to those that pertain to the right of access, as well as the rights to edit and delete, are incorporated into the Madrid Resolution. thirty percent Additionally, the Madrid Resolution Data Quality Principle requires that data be anonymized or erased when it is no longer required for the legitimate objectives of collection. This is a requirement whenever the data is no longer required. To fulfil this condition, it is necessary to do so.

Additionally, this is the case in situations where the data is no longer necessary. In addition to providing for rights that are comparable, the additional safeguards that are contained in Convention 108 mandate that any data that is used for a purpose that is banned by law must be erased. This is a requirement that must be met.31 a 31 There are rules that are extremely explicit regarding access and rectification rights, and these may be found in Part V of the APEC Privacy Framework. On the other hand, these fundamental principles are open to a great deal of variation in a variety of contexts. In certain circumstances, such as when granting access would result in an unreasonable expense for the company, when the information should not be disclosed due to legal or security reasons, or when access could put confidential commercial information at risk or violate the privacy of another individual, the right to refuse a request is one of the rights that can be exercised.

Objectives of the Study

- To study on General Data Protection Regulation (GDPR)
- To study on challenges to achieving and maintaining privacy regulation compliance

Other Global Privacy Regulations

- **California Consumer Privacy Act (CCPA)**

Businesses who have a gross yearly turnover of more than $25 million are entitled to comply with the California Consumer Privacy Act (CCPA), which is a law that was passed in California. that derive at least fifty percent of their annual revenue from selling the personal information of residents. For example, businesses that sell the personal information of residents can be subject to the CCPA. Businesses that sell the personal information of residents, for instance, may be liable to the California

Consumer Privacy Act (CCPA). With regard to the California Consumer Privacy Act (CCPA), for example, companies that sell the personal information of residents may be held accountable for violations of the law. For instance, in accordance with the California Consumer Privacy Act (CCPA), businesses who sell the personal information of residents of the state may be held liable for any violations of the law that they commit. Compliance with the legal requirements that are classified as mandatory is a need that must be met by each and every one of these sorts of businesses. The California Consumer Privacy Act (CCPA) is a piece of legislation that regulates the individual rights of consumers with regard to their privacy. consumers are subject to this law. Whoever residing within the boundaries of the state of California is subject to the California Consumer Privacy Act (CCPA).

In order for businesses to successfully establish that they are in compliance with the California Consumer Privacy Act (CCPA), they are needed to publish a statement that addresses the "notice at collection" requirement. In accordance with the terms of this legislation, businesses are obligated to provide consumers with information regarding the collection of their personal information as well as the reasons for doing so. It is mandatory for businesses to show this statement in order to demonstrate compliance with this rule. Under any and all circumstances, this is done in order to ensure that the customers' personal information is protected from being compromised in any way. Additionally, it includes a whole part that is devoted to the regulation of the operations that are carried out by data brokers. This section is included in the document. This indicates that it is a piece of legislation that meets all of the requirements. In addition to the numerous other responsibilities that they have, this is one of the many activities that they are responsible for. Individuals who violate the rules may be subject to fines that range from $2,500 for an incidental offence to $7,500 for a deliberate infringement or one that is done on purpose. These fines can be imposed on those who disobey the laws. This is the amount of the fine that is levied on the individual who has broken the law. There is a possibility that the penalties will be imposed for those who have committed offences that were either intentional or purposeful. There is a possibility of both of these outcomes.

- **California Privacy Rights Act (CPRA)**

The year 2020 marked the commencement of its implementation, which was to increase the rights of customers with regard to the privacy and security of their data. The goal of this implementation was to strengthen the rights of consumers. The Consumer Privacy and Data Protection Act (CPRA) is an enlarged version of the California Consumer Privacy Act (CCPA), which was created in the same year to protect the privacy of consumers in the state of California. The CCPA served the purpose of protecting the privacy of customers in the state of California. Following the establishment of a new category known as sensitive personal information (SPI) by the Consumer Protection and Electronic Records Act (CPRA), businesses are required to provide additional safeguards that are differentiated according to the level of sensitivity of the personal information that they collect. This obligation is imposed on businesses. This responsibility is a consequence of the fact that businesses are obligated to offer additional precautions for their employees. Furthermore, it comprises criteria for opting in and opting out totally, as well as disclosure rules that have been tightened, requirements for purpose limitation, and requirements for purpose restriction. All of these elements are included in the document.

Additionally, the Consumer Privacy Rights Act (CPRA) provides customers with four extra rights, in addition to broadening the scope of the restrictions that are now in existence. One of these rights is the right to correct inaccurate personal information, another is the right to limit the use and disclosure of sensitive personal information (SPI), a third is the right to access information about automated decision-making, and a fourth is the right to opt out of using technology that uses automated decision-making. All of these rights are included in the right to privacy. The laws that are already in existence are being extended, and in addition to that, these rights are also being awarded. If these new rights are put into force, consumers will be safeguarded against the inappropriate use of their data by AI-driven systems. This will guarantee that customers are protected from being exploited in any way.

There are also a number of additional laws that deal with the right of customers to privacy and the collection of data. These laws are referred to as "data acquisition laws." In addition to the three principles that have been discussed previously, these laws are required to be followed. In the context of the government, laws such as these are examples of what are known as rules. A piece of law known as the Health Insurance Portability and Accountability Act (HIPAA) is a piece of legislation that regulates the healthcare industry and prohibits the unauthorized collecting and distribution of health information about individuals without first obtaining their knowledge and consent. The year 1996 saw the passage of this statute. In order to ensure that customers are able to acquire the information that is relevant to their

insurance plans, this law was created in order to do so. According to the Gramm-Leach-Bliley Act (GLBA), financial institutions are required to comply with its rules in order to ensure the confidentiality and safety of the financial information of their customers while also protecting their customers' privacy. These details may contain facts about their debts, financial statuses, transactions, and other characteristics that are related with their financial conditions. It is probable that this information will include these details.

- **The Challenges to Achieving and Maintaining Privacy Regulation Compliance**

It is quite probable that certain organisations may discover that compliance with regulations concerning the protection of personal information and the right of an individual to privacy is more challenging than they had imagined it to be. There is a possibility that they will find out about this. In matters pertaining to regulation, the individual is always responsible for a great deal of responsibilities and obligations that are placed on their shoulders. It is always the individual who is responsible for bearing these responsibilities. "And from a practical point of view, it is very often a challenge to operationalize new regulations like this," says Andreas Klug, chief privacy officer at GVC Ladbrokes Coral, a leader in the gambling industry situated in the United Kingdom. According to Klug, "it is very often a challenge to operationalize new regulations like this." "And from a practical point of view, it is very often a challenge to operationalize new information." "And from a practical point of view, it is very often a challenge to operationalize new information."

In order to fulfil the requirements for compliance, there are a great number of challenges that need to be conquered. All of the following are included in this, but the list is not exhaustive:

- Enhancements to the systems that involve information technology
- Maintaining the most recent versions of the policies and standards
- The process of identifying and cultivating talented individuals.

The road to compliance has not been devoid of its fair share of challenges, even for companies that have taken these obstacles head-on and overcome them. According to the information that was provided to us by an additional executive with whom we had a conversation, "Even the implementation of some of the smallest of requirements under the law can require a significant investment."

Legacy IT Systems Challenges Compliance

When it comes to the constraints that prevent comprehensive compliance with the General Data Protection Regulation (GDPR), dealing with legacy information technology systems emerges as the most critical obstacle (see Figure 5). By a margin of more than one in three, or 38 percent, chief executive officers are of the opinion that it is exceedingly difficult to bring the information technology that is now being utilised into compliance with the regulations. The General Data Protection Regulation (GDPR), which was enacted in May of this year, requires that this be done in compliance with current regulations. In his role as an employee at GVC Ladbrokes Coral, Andreas Klug underlines the necessity of being able to include compliance controls into the tools as well as the technology itself. There is a member of the personnel at the firm named Klug.

Legacy information technology was ranked as the most critical difficulty that was identified, and it earned 42 percent of the total votes that were cast. When CEOs were asked to describe the most significant problems that companies face in the process of preparing for the CCPA, the most significant difficulty that arose was legacy information technology at the top of the list. Furthermore, organisations have expressed their worry that they are perplexed by the lack of information offered by data protection authorities regarding the system by which they would be evaluated. Many of these organisations have expressed their concern. Organisations have expressed their concern on this matter. The issue in question is one that has been brought up by a number of different groups. Fourty-two percent of the companies that took part in the poll responded that this was an issue for the way that they conduct their operations. Forty percent of businesses describe the difficulty of convincing staff of the relevance of the standards and bringing about a shift in thinking as some of the difficulties they confront as a challenge to the culture of the firm. This is one of the challenges that they face. Among the difficulties that they must contend with is this one.

Conclusion

After careful consideration, the authors have arrived at the opinion that the Personal Data Protection Board (PDPB) is a commendable endeavor, and that India's privacy regulations should be more stringent. The implementation of regulations concerning the privacy and security of data is

something that has to take place on a worldwide basis. Although a company may be in compliance with the General Data Protection Regulation (GDPR), this does not always mean that it is also in compliance with the standards set out by the Personal Data Protection Board (PDPB). Compliance with both of these standards is obligatory for every company that operates on a worldwide scale and deals with personal information. Unless an exemption is applicable, such as when an investigation is still ongoing, a logical circumstance is occurring, or a documented unique scenario is occurring, data controllers and processors are required to delete all personal data once a certain amount of time has passed or the agreement has been terminated. This is in accordance with the General Data Protection Regulation (GDPR), which mandates that they delete all personal data. The writers include a concluding table in which they present a comparison and contrast of the different pieces of legislation and speculate on the influence that the PDPB would have on the nation.

References

1. bn records compromised in Aadhaar breach since January. (2018). Gemalto.
2. Abir Roy. (2019). Data protection: Why a comprehensive law is needed. Financial Express. https://www.financialexpress.com/opinion/data-protection-why-a-comprehensive-law-is-needed/1694205/
3. Afroz, S., Islam, A. C., Santell, J., Chapin, A., & Greenstadt, R. (2013). How Privacy Flaws Affect Consumer Perception. 10–17. https://doi.org/10.1109/STAST.2013.13
4. Agrawal, S., Banerjee, S., & Sharma, S. (n.d.). Privacy and Security of Aadhaar: A Computer Science Perspective. 1–23.
5. Anirudh Burman. (2020). Will India's Proposed Data Protection Law Protect Privacy and Promote Growth? Carnegie Endowment for International Peace. https://www.jstor.org/stable/resrep24293.4
6. Anurag Vaishnav. (2019). The Personal Data Protection Bill, 2019: All you need to know. The PRS Blog.
7. Ardhapurkar, S., Srivastava, T., Sharma, S., Chaurasiya, V., & Vaish, A. (2010). Privacy and data protection in cyberspace in the Indian environment. International Journal of Engineering Science and Technology, 1(2), 942–951.
8. Aria Thaker. (2018). In a year of data breaches, India's massive biometric program finally found legitimacy.
9. Author, R., Jash, S., Kaushik, A. K., Mishra, S., Padmanabhan, A., Prakash, P., Ratna, T., Simons, J., & Srikumar, M. (2019). Key Differences Between the U.S. 1Social Security System and India's Aadhaar System Report Part Author (s): Kaliya Young Report Title : The Promise of Public Interest Technology : Report Subtitle : In India and the United States Key Differences B.
10. Ben Wolford. (n.d.). Everything you need to know about the "Right to be forgotten." GDPR.EU. https://gdpr.eu/right-to-be-forgotten/
11. Bhardwaj, I., & Himanshu. (2019). Regulatory measures of Data Protection in India: Need of the hour. 4(5), 75–78.
12. Bhattacharya, M., Agarwal, S., Iyer, V., Bansal, A., Vedashree, R., & Vishwanath, S. (2019). Cyber Security: India Market. December, 56.
13. The personal data protection bill, 2018, (2018) (testimony of BN Srikrishna Committee).
14. Womble Bond Dickinson (US) LLP. (2019). India's Proposed Privacy Law Allows Government Access and Some Data Localization. https://www.lexology.com/library/detail.aspx?g=9982a218-799c-4886-ad08- 3b414cda6571#: ~:text=The PDPB would grant the procedures%2C safeguards and oversight mechanism)
15. Determann, L., & Gupta, C. (2019b). India's Personal Data Protection Act, 2018: Comparison with the General Data Protection Regulation and the California Consumer Privacy Act of 2019. Berkeley Journal of International Law, 37:3.
16. P. T. J. Wolters, The security of personal data under the GDPR: a harmonized duty or a shared responsibility? (2017) 165-178 International Data Privacy Law.
17. Elizabeth Goitein & Faiza Patel, what went wrong with the FISA court (2015).
18. Caspar Bowden, The US surveillance programmes and their impact on EU citizens' fundamental rights 474,405 (2013).

❖◆❖