COMPARISON OF DATA PROTECTION LAWS IN INDIA WITH RESPECT TO GDPR

By Varsha Gehlot[*]

ABSTRACT

This academic legal analysis compares the General Data Protection Regulation (GDPR) of the European Union with India's Digital Personal Data Protection Act (DPDPA) to determine whether the two pieces of legislation are compatible with one another. As we live in an increasingly digital world where information is freely shared across borders, data protection has become a pressing legal and societal concern. In 2018, the General Data Protection Regulation (GDPR) became law, setting a global standard for stricter data protection procedures with an emphasis on protecting people's rights and privacy. The Data Protection and Privacy Act (DPDPA's) development has been influenced by India's diverse economic and social landscape and the country's aspirations to become a digital superpower. However, the European Union's General Data Protection Regulation (GDPR) was developed to meet the needs of the integrated European economy. By comparing various legal systems, this research gives a more in-depth understanding of how data protection laws deal with the varied needs and challenges of different countries. Policymakers, legal experts, businesses, and individuals looking for guidance on data privacy regulations may all benefit from this research. Add to the ongoing discussion around data protection, this research compares and contrasts two pieces of legislation: the General Data Protection Regulation (GDPR) and the Data Protection Directive for Police and Criminal Justice Authorities (DPDPA).

Keywords- Data Protection, Data Privacy, GDPR, Personal Data Security etc.

[*] Law Student, Christ University, India.

I. INTRODUCTION

Information for the knowledge-based industry is like blood to the life of living beings. Information is worthy supplies not only for businesses like service and manufacturing, but adscititious it is perilous for the economy and security of a nation. The utilization of data/information and its capability to get converted into progressive information is paramount for businesspeople, policymakers, scientists, engineers, etc. Having worthwhile and at times exclusive information can have betterment in productivity and quality which can advance the field of education, research, and it supplemental benefits to make denizens more erudite. Indian culture's point of difference from Western culture begins with the non-distinctive concept of the autonomous individual[1].

The Western world conceives an individual with the incredible idea, imagining him living within an inviolate protected region, having the liberty "to choose". The holistic Indian culture embraces the very socio-centric belief of collectivism, where the privacy of an individual loses its supremacy, whereas the West encourages the very notion of individualism. India is a collectivist society where individualism or privacy is given less consequentiality as compared to the UK or the US, where an individual's paramountcy is at least equipollent to, if not more preponderant than the importance of the collective. This further leads to a varied understanding of data protection in the minds of individuals hailing from these two cultures. When one from the West takes it to be an issue concerning his privacy, which is paramount to him, an Indian would not only be concerned about his privacy, but also the societal value combined with his privacy. Data protection is indistinctively associated with "privacy".

With the technological advancements and economic reforms, there is now an extensive demand for protection against incongruous accumulation and handling of data[2]. There has also been a remarkable intensification of internet users, consuming the net for information, communication, and e-commerce, accentuating the authoritative ordinance of an efficacious regulatory system, and shedding new light on the accumulation, processing, and handling of data. The information acquired by the websites may be relegated as either "individually identifiable information", or as "mass undisclosed information". Elaborate on each of these

[1] Chawla, N., & Kumar, B. (2022). E-commerce and consumer protection in India: the emerging trend. Journal of Business Ethics, 180(2), 581-604

[2] Walia, H., & Chakraborty, S. (2021). Data Protection Laws and Regulation India 2021-2022. ICLG. com.

terms, one may say that "individually identifiable information" entails authentic information, which has more to do with the identification of an individual. It may incorporate data such as names, addresses, telephone numbers, credit card numbers, or email IDs, and other person-specific information[3].

This information may also be linked to the identifiable information of other sources, from which the other related personal information can be extracted with ease. The IP address may also be associated with this information. Another example could be, the processor Serial Number or PSN is a Pentium III processor identifier chip, which is a number fixed to the individual's laptop, desktop, or computer and is used to approve one's identity through a scope of communications with any association or statistic. The internet also fosters a trail of data every time a person makes a cessation which may or may not be related to certain personal information.

On the other hand, "Mass undisclosed information" is aggregated or categorized by a website or a third party according to the geographical areas (information such as postal codes and non-consumer concrete information engendered from innominate transactions), to help merchants manage their business and advertising better. Regardless, several technologies are used to accumulate both classes of information on consumers. "Cookies" can be one such example, which saves information in the form of computer code on a user's browser automatically. Cookies are information about the user's personal predilections exhibited during their visit to a website.

As it is infeasible to differentiate between visitors to a website, the server will somehow mark the visitor by storing information on them. The introduction of the internet has made data transfer much facile which was time-consuming earlier[4]. The entire world can be accessed now on a small laptop screen through the internet. Every person's life is profoundly affected by this internet. The internet has expunged the territorial barriers to an extent that till now was a major impediment to the progress of trans-border business. Along with giving simplified answers to many critical questions, the World Wide Web has major side effects in terms of involuntary disclosure of data.

[3] Burman, A. (2019). Will a GDPR-style Data Protection Law Work for India? Carnegie India.
[4] Sharma, S. (2019). Data privacy and GDPR handbook. John Wiley & Sons.

II. BACKGROUND

The recent opinion by the Supreme Court has made obligatory for production of only PAN card and not Aadhaar Card for filing IT return. The court also ruled out that Aadhaar does not infringe on an individual's right to privacy and upheld its constitutional validity. Several sections of the Act were struck down. Court struck down Section 57 of the Aadhaar Act considering it as "unconstitutional"[5]. This implies no organization or private substance can seek for Aadhaar ID from you, this implies no privately owned business can constrain you to present your Aadhaar data to buy or avail of their service benefits. A circular issued by TRAI in March 2017 mandating the linking of mobile numbers with Aadhaar was struck down referring it to be illegal and unconstitutional as it is not supported by any law.

As indicated by the judgement given by the apex court, banks and other financial institutions cannot seek Aadhaar data. The top court additionally included that educational organizations alongside UGC, NEET, and CBSE cannot take Aadhaar for admissions or enrolment which was a fundamental condition before. The judgement mandated parental or guardian's consent before the enrolment of children under the Aadhar Act. The judgement further provides that children attaining the age of majority have the right to exit from Aadhaar in case they are enrolled under Aadhaar through their parental consent. Section 33(2) of the Aadhaar Act, which says that it is legal to disclose the identity and authenticated data in the interest of national security on the direction of an officer not below the rank of Joint Secretary to the government of India was struck down by the apex court[6].

Section 47 of the Aadhaar Act, which says that no individual was allowed to file a complaint if he/she felt their data was leaked or misused, was also ruled out by the Supreme Court. Under this Section, the law only allowed the court to take cognizance of a complaint filed by UIDAI or anyone authorized by it.

Authentication data records should not be kept beyond six months was made clear in the judgement by the Supreme Court and the provision that allowed archive records for five years has also been struck down. Storage of metadata of transactions by individuals is excluded by

[5] Goldberg, S., Johnson, G., & Shriver, S. (2019). Regulating privacy online: The early impact of the GDPR on European web traffic & e-commerce outcomes. Available at SSRN, 3421731.
[6] Von Schomberg, R., & Hankins, J. (Eds.). (2019). International handbook on responsible innovation: A global resource. Edward Elgar Publishing.

the apex court in the judgement. This banning implies that UIDAI cannot collect data sets and mine them for more data or analysis. Data sharing with the corporates is also ruled out. The Supreme Court also called for Parliament to draft and pass a data protection law as early as possible.

After effect of judgement has forced UIADI to make provisions for unlinking Aadhar cards which was deemed mandatory previously[7]. UIADI has now asked all private entities like banks and telecom companies to submit a plan to stop the use of Aadhar data. In 2017 and 2018 status of data protection in India was the focal point of numerous discourses. The presence of privacy as one of the fundamental rights was confronted by the government before the Supreme Court. Promoters favouring privacy were viewed as differentiating the estimations of Indian culture. Endeavours for framing separate legislation for data protection were in vain. The most recent judgement of the Supreme Court on Aadhaar confronted the manner personal data is protected in India[8].

On 24 August 2017, a nine-judge bench of the Supreme Court laid down judgement, together upholding that privacy was a fundamental right, retaining an individual's nobility and independence and expressing it as the core of the constitutional order. Privacy in this technologically advanced world is no longer an extravagance concern; it influences each person as it is pervasive through the mode of the web. By the end of July, Justice B. N. Shrikrishna Committee was appointed by the government who produced a report along with a draft bill for data protection for India.

Since the government delayed the implementation of a legal framework for the prosecution of data and privacy breaches, Indian BPO companies have therefore implemented unified processes such as the BS7799 and the ISO17799 standards for information security management, which also explicitly restrict the quantity of data available to employees of BPO and call centres. The Indian government needs to implement a strong Data Protection Act to sustain the BPO business and parallelly have a secured Aadhaar Card system. Still, if the government doesn't act on effective data protection, then there are chances that India may

[7] Staunton, C., Slokenberga, S., & Mascalzoni, D. (2019). The GDPR and the research exemption: considerations on the necessary safeguards for research biobanks. European Journal of Human Genetics, 27(8), 1159-1167.
[8] Ardic, O, H Gradstein, I Istuk and L Michaels (2019): "Financial inclusion beyond payments: policy considerations for digital savings", World Bank Group Working Papers, no 136101, April.

completely lose BPO business and if data is misused under the Aadhaar Scheme then it can lead to an undesirable result and can even cause a threat to the nation once huge amount to citizen record is easily accessible without any proper protection. A data protection authority with a proper framework in place would have helped in curbing the present issues[9].

The Authority would have had all mandates for collecting, processing, archiving, and purging Aadhaar information and the current mess could have been avoided. Apart from this, an immensely colossal data has been accumulated by the private agencies for the Aadhaar card; this Aadhaar number contains the personal details of the citizen of India. Hence, protecting the Aadhaar number under a stringent law is much more obligatory to evade any disastrous offense that can bring a citizen into extreme trouble.

III. DATA PROTECTION AND PRIVACY DATA

The word data (pronounced /ˈdeɪtə/, /ˈdætə/, or /ˈdɑːtə/) is the Latin plural of datum, neuter past participle of dare, “to give”, hence “something given”. The past participle of "to give" has been used for millennia, in the sense of a statement accepted at face value; one of the works of Euclid, circa 300 BC, was the Dedomena (in Latin, Data). “In discussions of problems in geometry, mathematics, engineering, and so on, the terms givens and data are used interchangeably. Such usage is the origin of data as a concept in computer science: data are numbers, words, images, etc., accepted as they stand.” Data refers to information or facts usually collected as the result of experience, observation, experiment, or processes within a computer system, or premises. Data may consist of numbers, words, or images, particularly as measurements or observations of a set of variables[10]. Data are often viewed as the lowest level of abstraction from which information and knowledge are derived.

Data protection/information assurance refers to the combination of technology and the legal right of privacy guaranteed by the constitution of India but not explicitly provided by any law in India yet. These issues surface wherever personal data relating to a person or persons are collected and stored in digital form or otherwise. Another dimension of the concern is how the data is garnered, stored, and used unauthorizedly. Access to information is also one of the issues

[9] Bank of England (2019): Future of finance: review on the outlook for the UK financial system, June, https://www.bankofengland.co.uk/-/media/boe/files/report/2019 /future-of-finance-report

[10] Bank for International Settlements (2019): “Big tech in finance: opportunities and risks”, Chapter III, Annual Economic Report 2019, June.

which includes in it's the issue of who gives access to whom and how. Further, the importance and value of such data enhances because of the effect the misuse and abuse of such data may have on the individual, commerce, or society as a whole.

Personal data and ancillary issues can be protected under a spectrum of different regimes including intellectual property rights, contractual obligations, interception of communications, etc. all of which are very much within the scope of this writing. The current paper is concerned with the data protection laws and the regulatory schemes working under it[11]. Thus, issues that may arise when a contract for outsourcing information or data is undertaken are as follows:

- Undetected intrusions
- Lack of predictable data and configuration integrity
- Loss of privacy of one's sensitive and personal information

Importance of data/Information

One must be wondering by now as to how all this data debate is material and consequential, as to how these entities in control and possession of data misuse it. Some may find it mere rhetoric and call it an abstract discussion having no visceral arguments vindicating it, but history has demonstrated time and again the value and utility of any data, from the advent of the internet (which is premised on the U.S Army's attempt to collect, share and gather information expeditiously) to new age portable computing (which is a Pandora box, having and offering myriad services and usages) which heavily relies and functions on data transfer. In modern times data is deemed a most valuable asset of any entity and organization or country for that matter.

Data collection, processing, and analysis is considered game game-changing act. If one looks at new-age mergers and acquisitions of big companies, one can patently make out the utility of data being transferred as an asset of high importance. We share a voluminous amount of data with the companies which we use regularly. Google, Facebook, Yahoo all collect out data and they use it to target users through advertisement[12]. Lately, Comcast (Pioneer ISP) has asked the

[11] Bapat, D, R Bijapurkar, B Chakravorti, B Mazzotta, K Ramesha, D Roy and R Shukla (2019): "The cost of cash in India", Tufts University, January, https://sites.tufts.edu/ibgc/files/2019/01/COC-India-lowres.pdf.
[12] Cangiano, M, A Gelb and R Goodwin-Groen (2019), "Public financial management and the digitalization of payments", CGD Policy Paper, no 144, June.

Federal Communications Commission to allow it to share the browsing history of users with advertisers, so that it can provide cheap and bargained services to the users. Other ISPs are already doing it without the authorization and permission of the customers and perhaps this is the reason for the differential pricing of ISP services at different places. We are blissfully unaware that it's happening, even though every user of Yahoo, Facebook, Google, etc. experiences it routinely. Don't we get to see different advertisements appearing invariably on our Facebook accounts and Google pages?

Through our social networking accounts, we have become products for big companies, almost half a decade ago the concept of free services provided by big companies like Facebook, Yahoo, and Google was like a quagmire and hard to discern, but now with the way these big companies are functioning it has become grossly manifest that they are monetizing voluminous data of individuals and are deeply into the business of data transfer and that too without prior authorization of the individuals who have become a mere commodity into the hands of these unscrupulous entities. This is the sheer dismantling of one's privacy without information and permission[13].

IV. MILIEU OF DATA SECURITY LAWS IN INDIA

Before delving into the issues of the data security milieu in India, it is important to see its evolution in India. In the late 80's General Electric was the first company in India which start the inter-country outsourcing of business processes and information technology. In September 1989, it was only after the meeting of Mr. Jack Welch, Chairman and CEO at the time with the Chief Technical Advisor to then Prime Minister Rajiv Gandhi, which led to convincing Mr. Welch of the possibilities for GE in India.30, GE collaborated &formed a joint venture with Wipro Ltd. within a year to develop and market medical equipment in India. GE then began the processing of credit card applications, call centres, and other business-specific consumer activities and used India as a base for data entry[14].

[13] Carstens, A (2019a): "Central banking and innovation: partners in the quest for financial inclusion", speech at the Reserve Bank of India, C D Deshmukh Memorial Lecture, Mumbai, 25 April, https://www.bis.org/speeches/sp190425.htm

[14] Cook, W and A Raman (2019): "National Payments Corporation of India and the remaking of payments in India", Consultative Group to Assist the Poor Working Paper, May.

Till 1991 India's foreign opportunities were very scarce, it was only after the year 1991 that India opened its borders to foreign investors Indian economy for foreign investment saw a great surge in the rein of Dr. Manmohan Singh, Finance Minister then (later who became India's Prime Minister) when he started opening and introducing competition into the Indian telecom industry to bring down prices.

Satellite downlink stations were installed and set up to attract more foreign investment under the leadership of Dr. Manmohan Singh when he made flexible certain stringent rules that were obstructing foreign investors from investing in India Market. Satellite downlink stations were established in Bangalore with the newly relaxed rules instituted by Dr. Singh, and it made it much easier for foreign companies to avoid the erratic Indian phone network and connect with their home bases and other distant locations. Earlier they used to have their own satellite downlink, an Indian government official was required to oversee it and had the right to examine all data going in or out of the country. "Since then, many foreign companies like Citigroup, Microsoft, Delta Airlines, IBM, Accenture, and countless other multinational companies have developed outsourcing relationships with leading Indian outsourcing companies, such as Infosys Technologies, Wipro, Mphasis, and Tata Consulting".

Due to excessive outsourcing practices today personal information about customers of various companies can be accessed easily [15]. This comprises information of potential misuse like numbers of credit card, social security numbers like ZIP codes etc., driver's license details, and dates of birth, medical records, and other important personal information. The work culture of Indian BPO employees engages them in several tasks that expose them to customers sensitive personal data in transactions. "Transcription of medical records, preparation of tax returns, processing of credit card applications and bills, managing of mortgage applications, reviewing of insurance claims, analysis of patients X-rays, and help-desk services" and many more activities involving handling of sensitive information and personal information of customers are some of the works which are managed and processed by Indian employees.

[15] Desai, S, N Jasuja and P Khandekar (2017): "Your guide to UPI – the world's most advanced payments system", Wharton Fintech, 11 May, https://medium.com/wharton-fintech/your-guide-to-upi-the-worlds-mostadvancedpayments-system-b4e0b37.

The companies would be remiss to ignore that "…these kinds of business process applications create thorny issues about personal data protection for the customers[16]…" As offshore vendors deal more often with customers and specific customer data, the potential for abuse rises.

Right to privacy under article 21

The law of privacy provides an inviolable right to do things in privy; it's a right which has many manifestations. To what extent you want to share your information, your whereabouts, your desires, and your self is the supreme right provided under Article 21 of the constitution of India. Individuals have the choice under the above-mentioned article to keep his/her information out of the purview of the public. But this right of privacy sometimes is seen as a limitation to the right to information and that leads to a whole tussle between privacy on the one hand and information on the other[17].

The Personal Data Protection Bill, 2006

This bill was passed This bill was introduced in the Rajya Sabha on December 8th, 2006, and the attempt was to replicate the foreign laws. "The purpose of this bill was to provide protection of personal data and information of an individual collected for a particular purpose by one organization and to prevent its usage by other organization for commercial or other purposes and entitle the individual to claim compensation or damages due to disclosure of personal data or information of any individual without his consent and for matters connected with the Act or incidental to the Act. Provisions contained in this Act relate to the nature of data to be obtained for the specific purpose and the quantum of data to be obtained for that purpose. Data controllers have been proposed to be appointed to look upon the matters relating to violation of the proposed Act. Further, the Act recognizes an organization to be a Government Authority or Private company, collecting the data for processing[18].

IV. GENERAL DATA PROTECTION REGULATION (GDPR)

The General Data Protection Regulation (GDPR) has become a benchmark of personal data regulation and protection. GDPR addresses a comprehensive list of existing and potential issues

[16] FinRegLab (2019): The use of cash-flow in underwriting credit, July.
[17] Stucke, M (2018): "Should we be concerned about data-opolies?", Georgetown Law Technology Review, vol 2, no 2.
[18] Schumpeter, J (1911): A theory of economic development, Cambridge, Harvard University Press

regarding data; hence it is widely assumed as the working standard for data regulation. It has been used as a template for other countries striving to create their own data protection bills.

India is the largest democracy, and currently, the fifth-largest economy in the world. India is one of the largest generators of data over the last few years[19]. There have been calls for India to have a nationalized data protection law that was fulfilled in 2019 with the Personal Data Protection Bill or PDP. While the PDP has adapted GDPR in many major ways, several important differences serve as a contrast between the different prevailing local realities and the unique requirements of India.

Scope

The scope of sensitive personal data is much broader in the PDP than in the GDPR. The PDP provision regarding critical personal data has no appropriate parallel to the GDPR. PDP names three categories of data- personal data, sensitive personal data, and critical personal data. The PDP authorizes the central government to define and determine the nature of critical personal data and recommend new categories of sensitive personal data. There are also provisions to exempt certain government entities from the bill[20]. Unlike the GDPR, the PDP has provisions for governmental access to non-personal data held by any data processor or data fiduciary for certain purposes relating to better delivery of government services and more effective policy making.

Residency and Cross-Border Data Flow

GDPR places no demand for hard data residency. Depending on the type of data, getting authorization from the appropriate SAs or Supervisory Authority might or might not be a requirement. There are conditions and restrictions in place regarding the overseas transfer of data. Under the PDP, sensitive personal data must be stored locally. However, in certain conditions, this data can also be approved for cross-border transfer, although with explicit

[19] Ruhela, S (2019): "Data empowerment and protection architecture explained", Indian Software Product Industry Roundtable – iSPIRT, 23 June, https://pn.ispirt.in/dataempowerment-and-protection-architecture-explained-video/

[20] Riley, T and A Kulathunga (2017): Bringing e-money to the poor: successes and failures, World Bank Group.

consent. The same holds for sensitive personal data. Non-sensitive personal data can be sent and processed outside India without any restriction[21].

Broadly speaking, the standards of data residency would be much stricter under PDP than it is under GDPR. Transferring personal data outside India, in many cases, would be the purview of either the central government or the relevant Data Protection Authority or DPA.

Consent and Notice

GDPR requires clear notice regarding the collection of data. This notice needs to be simple and easily understandable. It also needs to include details about the relevant Data Protection Officer or DPO and the identity of the data controller, among other things. GDPR also requires valid consent before the data is processed. Valid consent is specific consent, informed, given without ambiguity, capable of being withdrawn at any point and given freely without coercion.

The PDP replicates the notice requirements of the GDPR and makes further additions to it. These additions include notice being available in multiple language options and the inclusion of any other information asked by the DPA, including data trust scores and reliability ratings[22]. The consent requirements are also like GDPR, with the addition that sensitive personal data would be processed only when there is explicit consent. To help oversee the consent of the principals better, PDP also introduced a new entity called "consent manager." Due to the different classification structures of personal data and separate rules governing each type, the PDP varies in a lot of ways from GDPR. Unlike GDPR, the PDP offers better clarity on the legal fallouts of the withdrawal of consent. Also, with the advent of the new "consent manager" entity, the process of channelling and handling consent would be fundamentally different from the prescriptions of GDPR.

Data Processing

Under the purview of GDPR, certain principles are attached to data processing. These include

- Fairness and transparency

[21] Raman, A and S Staschen (2017): "Is the unbundling of payments from banking regulation imminent?", Consultative Group to Assist the Poor blog, 22 March, https://www.cgap.org/blog/unbundling-payments-banking-regulation-imminent.

[22] Petralia, K, T Philippon, T Rice and N Véron (2019): "Banking disrupted? Financial intermediation in an era of transformational technology", 22nd Geneva Report on the World Economy, September

- Lawfulness
- Purpose limitation
- Collection limitation
- Storage limitation
- Accuracy
- Integrity
- Confidentiality and accountability

Along with this, the GDPR also spells out certain grounds for processing personal data. These include:

- Compliance with the law
- Consent
- Vital interest
- Public interest
- Legitimate interests
- Contract performance
- Self-motivated publication by the principal

Here there are some interesting differences with the PDP. While the principles of data processing under the PDP are similar, the bill also adds other grounds, including needs related to employment and other reasonable purposes as decided by the DPA[23].

Contract performance, while a ground for data processing under GDPR, is not considered valid ground under the PDP. Also, all grounds for processing personal data under GDPR carry equal weight. Under the PDP, the primary basis is consent, and all the other parameters are considered exceptions.

GDPR grants permission to retain data for prolonged periods due to research, statistical analysis, and archiving purposes. Under PDP, data can only be retained for a long duration with either explicit consent or due to a legal obligation. Also, legitimate interests are not viewed in

[23] Aridor, G., Che, Y. K., & Salz, T. (2020). The economic consequences of data privacy regulation: Empirical evidence from gdpr (p. 26900). Cambridge, MA, USA: National Bureau of Economic Research.

the PDP as valid grounds for data processing. Instead, they include data processing for reasonable purposes as specified by the relevant DPA[24].

Compliance and Security

GDPR specifies data protection by design. Data controllers and processors are required to enforce the proper data security measures for any kind of personal data. Controllers are also obligated to carry out Data Protection Impact Assessments or DPIAs before processing certain kinds of personal data. Data protection audits can be employed to investigate data controllers and processors.

In these measures, the PDP remains very similar to GDPR. Audits, privacy by design, and DPIAs are all included in the PDP. However, there are some differences regarding the approach.

GDPR obligates all data controllers to carry out DPIAs and maintain all records of data processing activities. In the PDP, this is only a requirement for "significant" data fiduciaries. Also, the DPA is permitted to bring regulations that specify the exact way in which data auditors would conduct the audits.

Furthermore, the PDP also proposes a data sandbox in which data fiduciaries with certified policies can participate. There is no provision for a data sandbox in GDPR. Therefore, PDP compliance might entail more processes and requirements than GDPR[25].

Data Breaches

In the event of a data breach, GDPR specifies that data controllers would need to provide notification to the relevant Supervisory Authority within a maximum period of 72 hours. If there is a chance of harm coming to the data subject, the subject also is required to be notified as soon as possible. Under the PDP, data fiduciaries are only required to notify data principals if they are instructed to do so by the DPA.

In such cases, the DPA determines the need to notify based on the degree of the potential harm the data subject can face. This is the main point of difference from GDPR, where every breach

[24] Wewege, L., Lee, J., & Thomsett, M. C. (2020). Disruptions and digital banking trends. Journal of Applied Finance and Banking, 10(6), 15-56.
[25] Martin, A., & Taylor, L. (2021). Exclusion and inclusion in identification: Regulation, displacement and data justice. Information Technology for Development, 27(1), 50-66.

needs to be reported to the Supervisory Authority unless there is a negligible chance of risk to the data subject[26].

Data Processors

Both GDPR and the PDP have provisions in place regarding the employment of data processors. Under GDPR, only compliant data processors can be employed by data controllers. The eligibility of a particular data processor is determined either through adherence to an approved code of conduct or through certification.

A data processor would need clearance from the data controller before employing another data processor.

In the PDP, it is specified that data fiduciaries can employ a data processor using a valid contract. The contractual requirement for a data processor is a lot more relaxed than mentioned in GDPR, where data processors must furnish sufficient guarantees of their adherence to GDPR before they can be contracted. The PDP also does not require DPAs to specify standard contractual clauses between data controllers and processors, whereas GDPR allocates the European Commission with the authority to recommend such clauses[27].

Data Storage

GDPR mentions that data must be stored in an identifiable form for a certain length of time. Any extension in the storage period would be under certain exceptions. These exceptions include the use of the data for scientific, statistical, historical, or public interest purposes. Under the PDP, data can only be stored for the period required for it to satisfy its purpose. Once it has served its purpose, it must be expunged. Any case where the data is to be retained for a longer period requires explicit consent from the data subject under the PDP. This means that satisfying GDPR compliance requirements regarding data storage might not be a sufficient condition to remain compliant with the PDP[28].

[26] Arora, P. (2019). Decolonizing privacy studies. Television & New Media, 20(4), 366-378.
[27] González, F., Yu, Y., Figueroa, A., López, C., & Aragon, C. (2019, May). Global reactions to the cambridge analytica scandal: A cross-language social media study. In Companion Proceedings of the 2019 world wide web conference (pp. 799-806).
[28] Naavi. (2020). Personal Data Protection Act of India (PDPA 2020): Be Aware, Be Ready and Be Compliant. India: Notion Press.

Penalties and Grievance Redressal

Under GDPR, data controllers and processors are required to assist the DPO when it comes to matters of grievance redressal. The data subjects can also directly contact the DPO to freely exercise their rights as mentioned in GDPR. In specific cases, data subjects also have the recourse of to seek legal remedies by directly approaching the Supervisory Authority. Upon failure to comply with these obligations, GDPR also recommends fines amounting to up to 10 million Euros applicable to the data controller, monitoring body, and certification authority.

Under the PDP, data fiduciaries are tasked with maintaining appropriate grievance redressal mechanisms. The data subject can raise a concern with the assigned officer, in which case the grievance must be satisfactorily addressed within a maximum period of 30 days. An appellate tribunal can handle grievances arising from the orders of adjudicating officers. In specific cases, the PDP recommends financial penalties of up to Rs.15 Crores[29]. The bill also defines significant data fiduciaries eligible to pay up to Rs.1 Crore and other entities eligible to pay up to Rs.25 Lakh in case no specific penalties are assigned.

The time limit imposed by the PDP for grievance redressal is a major point of difference from GDPR. The financial penalties recommended also vary quite significantly. Also, the appellate process is only available to the data principal under GDPR, whereas any person can appeal to the tribunal under PDP.

Automated Decisions

In cases where personal harm can ensue from an automated decision-making process, GDPR has clear and stringent provisions. While large-scale profiling is said to require thorough assessment under the PDP, the bill does not allocate any rights to individuals to object to automated profiling, with only children being exempt. The GDPR covers this ground much more thoroughly, mandating that data subjects can object to automated profiling for direct marketing[30]. GDPR also mandates that this right to object be conveyed to the data subject as clear and distinct information.

[29] Kumar, R., Goyal, G. (2016). The Right to Privacy in India: Concept and Evolution. United Kingdom: Partridge Publishing India.
[30] Matthan, R. (2018). Privacy 3.0: Unlocking Our Data-Driven Future. India: HarperCollins Publishers India.

V. CONCLUSION

The investigation of data protection law in India in connection to the General Data Protection Regulation (GDPR) indicates a varied legal environment that is impacted by the changing needs of the digital world. This is the conclusion of the examination. The General Data Protection Regulation (GDPR) has laid the groundwork for a groundbreaking framework that has raised the standard for data protection by putting a substantial focus on individual rights, transparency, and strong enforcement mechanisms. This has resulted in the raising of the bar for data protection. In contrast, the Digital Personal Data Protection Act (DPDPA) of India represents a significant step forward in the field of comprehensive data protection. This law was developed to particularly meet the unique needs and challenges that are experienced by the nation.

A complete examination of numerous areas of these laws has been undertaken. These aspects include geographical jurisdiction, definitions, legal reasons for data processing, data subjects' rights, obligations of data processors, and procedures for enforcement. Both the General Data Protection Regulation (GDPR) and the Data Protection Directive for Police and Criminal Justice Authorities (DPDPA) exhibit distinct characteristics, such as differences in their scope and stated obligations, but both frameworks demonstrate a shared dedication to safeguarding the personal data of persons. One such example of this shared dedication is that both frameworks demonstrate a shared dedication to protecting individuals' health information. The research that was conducted was able to shed light on the role of contextual factors in affecting the development of data privacy laws.

The outlook on the protection of data that is reflected in India's Data Protection and Privacy Act (DPDPA) has been influenced by the diversity of India's socioeconomic conditions, as well as the country's aspiration to position itself as a worldwide leader in the digital economy. The General Data Protection Regulation (GDPR), which was developed for the highly linked market in the European Union, puts a focus on the alignment of legislation and the implementation of harsh repercussions for failing to conform to its standards. This was done to protect personal data.

The tremendous progress that has been achieved via the implementation of the DPDPA is evidence of India's continued attempts to resolve the issues connected with managing

innovation, economic growth, and the protection of individual privacy. These efforts may be viewed in the context of the previous sentence. In contrast to the rigorous standard that was established by the General Data Protection Regulation (GDPR), the data protection environment in India is marked by a greater degree of adaptability and pragmatism in its approach. Both the General Data Protection Regulation (GDPR) and the Data Protection and Privacy Directive for the Public Administration (DPDPA) are ongoing efforts, which means that they are susceptible to future modifications and enhancements. This is important to keep in mind within the context of this dynamic and ever-changing domain, as it is important to acknowledge that the GDPR and the DPDPA are both ongoing endeavours.

Within the context of the digital ecosystem, the effective adoption and implementation of these measures will play an essential part in ensuring the protection of personal data and the cultivation of trust. In addition, because of the worldwide character of data flows, it is necessary to place a high priority on the implementation of uniform data protection standards as well as international cooperation.

This comparative study is a valuable resource that may be used by policymakers, legal practitioners, organizations, and individuals who are interested in better comprehending the intricate web of data privacy regulations. The purpose of this article is to give an examination of the similarities and differences between the General Data Protection Regulation (GDPR) and the Data Protection Directive for Police and Criminal Justice Authorities (DPDPA), which is the acronym for both of those pieces of legislation.

This research contributes to the ongoing conversation taking place all around the globe on data privacy by analysing these two different systems. The facts and insights that are offered here are intended to serve as important knowledge that will guide future developments and upgrades in data privacy laws across a variety of countries. The goal of data protection should agree with the larger goal of developing a digital culture in which innovation and privacy may coexist in a way that is mutually advantageous to both parties.

****