International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

# The Digital Personal Data Protection Bill 2022 in Contrast with the EU General Data Protection Regulation: A Comparative Analysis

**Adv. Ashwini Kumar**

Data Protection Lawyer & Privacy Professional

**Abstract**

The European Union's General Data Protection Regulation (GDPR) is considered to be the most comprehensive & strong privacy and data protection law in the world, which doesn't only regulate within the territory of EU but also has an extra-territorial effect. GDPR has influenced privacy & data protection legislation of many nations. India is ready with the draft Digital Personal Data Protection Bill, 2022 (DPDP Bill) which is the latest in a series of draft legislations presented and removed since mid-2018. In this article we discuss the key differences between the GDPR & DPDP Bill by analysing the different approaches and methods prescribed in both the legislations to understand their scope & applicability, concerned parties, classification of personal data, legal basis for data processing, children's rights, reporting breach, cross-border data transfer, penalties, etc. In conclusion, we can say that the GDPR is relatively more detailed in its instructions, whereas the DPDP Bill establishes certain fundamental concepts.The DPDP Bill offers a glimpse of hope for balancing the interests of data subjects while acknowledging the practical challenges that businesses may encounter.

**Keywords:** DPDP Bill, GDPR, Data Protection Law, Privacy Law

## I. Introduction

The European Union's General Data Protection Regulation (GDPR) is considered to be the most comprehensive & strong privacy and data protection law in the world. It was drafted on 14$^{th}$April, 2016 and was passed by the European Union on 25$^{th}$ May, 2018. Though it is drafted by the EU but it imposes obligations on all the organizations around the globe, which process the data of EU residents. Non-compliance with theprivacy and security standards of the GDPR by anorganization results into imposition of heavy fine by the Data Protection Authorities (DPAs) on the organization. [1] The GDPR has had a significant impact on the development of data privacy legislation in many countries. For instance, the Personal Data Protection Act (PDPA) in Thailand and the General Personal Data Protection Law (LGPD) in Brazil have both been influenced by the GDPR. In fact, over 130 countries have established their own data privacy laws to protect the rights of their citizens till now. [2]On November 18, 2022, India's Ministry of Electronics and Information Technology (MeitY) released the draft Digital Personal Data Protection Bill, 2022 (DPDP Bill) and requested input from relevant stakeholders. The bill is the latest in a series of draft legislations presented and removed by the Ministry in the Indian Parliament and for public consultation since mid-2018, with the goal of introducing a comprehensive data protection regime in India. Surprisingly, the DPDP Bill comes only a few months after MeitY withdrew its predecessor, the Personal Data Protection Bill, 2019 (PDP Bill), in August 2022, following

the Joint Parliamentary Committee's proposal of over 80 amendments and multiple recommendations. [3]

The present article discusses the differences between the long-awaited draft Digital Personal Data Protection Bill, 2022 (DPDP Bill) & European Union's General Data Protection Regulation (GDPR), which is also sometimes referred to as the constitution for data protection laws.

## II. Scope&Applicability

Material Scope - In terms of the material scope, the GDPR applies to the processing of personal data, whether wholly or partially, through automated means or non-automated means that are part of a filing system or intended to be part of a filing system. However, there are certain exemptions to this rule, such as processing of personal data in an activity outside the scope of Union law, personal or household activities carried out by natural persons, data processing by competent authorities (i.e., public or government authorities) for the purpose of preventing, investigating, detecting or prosecuting criminal offenses or executing criminal penalties, and data processing by member states while carrying out activities that fall under Chapter 2 of Title V of the TEU (Treaty on European Union).[4,5]On the other hand The DPDP Bill is applicable to the processing of digital personal data within India's borders, specifically data collected from Data Principals online, as well as offline data that has been digitized. However, certain types of data processing are exempt from the provisions of this Act, such as non-automated processing of personal data, offline personal data, personal data processed by an individual for personal or domestic purposes, and personal data contained in records that have existed for at least 100 years. [6,7]

Territorial Scope - GDPR applies to the processing of personal data by a controller or processor established in the Union, regardless of whether the processing occurs in the Union or not. It also applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, provided that the processing relates to the offering of goods or services to such data subjects in the Union, or the monitoring of their behaviour within the Union. Furthermore, this regulation applies to the processing of personal data by a controller not established in the Union but located in a place where Member State law applies under public international law, regardless of whether the data is stored in physical or digital form. [4,5]The DPDP Bill 2022 will have jurisdiction over the processing of digital personal data within India's borders as well as the processing of digital personal data outside of India if it involves profiling (analysing or predicting the behaviour, characteristics, or interests of a data principal) or offering goods or services to data principals within India's borders. [6,7]

The scope of applicability of the GDPR is much wider than the DPDP Bill as the GDPR covers not only digitally stored data but also physically stored data into its ambit. [8]

## III. Concerned Parties

The GDPR uses the term "Data Subject" to refer to the natural person whose data is being processed, while the DPDP Bill uses the term "Data Principal" to refer to the same. The "Data Controller" is the entity that collects the data of the data subjects and decides the purposes and means of processing personal data in both laws. However, the DPDP Bill uses the term "Data Fiduciary" to refer to the Data Controller. In both laws, the entity that processes the data on behalf of the Data Controller/Data

Fiduciary is called the Data Processor. Although the terminology may differ, the definitions and concepts of the terms remain similar. [9]

## IV. Data Fiduciaries Categorisation

The DPDP Bill 2022 designates certain data fiduciaries as "significant data fiduciaries," on which the Bill imposes additional compliance responsibilities. These obligations include appointing a resident data protection officer to handle complaints, hiring an independent data auditor, conducting Data Protection Impact Assessments (DPIAs), and complying with any other prescribed compliance requirements. The categorisation of data fiduciaries will depend on factors such as the sensitivity and volume of personal data they process, the potential harm to the data principal, the possible impact on India's sovereignty and integrity, the threat to democratic elections, the safety of the State, public order, and any other relevant factors considered necessary. [10] There is no such classification or categorisation of data controller in the GDPR.

## V. Classification of Personal Data

Special categories of personal data are defined under the GDPR as a specific subset of personal data, which includes data relating to an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, genetic or biometric data processed for identification purposes, sex life, and sexual orientation. These types of personal data have different compliance requirements compared to other types of personal data. Specifically, special categories of personal data require a unique legal basis for their processing. [5] On the other hand, the DPDP Bill covers a wider range of personal data and does not differentiate it into sensitive or critical personal data. Therefore, there are no specific compliance requirements for different types of personal data under the Bill. Instead, the Bill requires implementing reasonable security measures for personal data protection. [11]

## VI. Legal Justification for Processing Personal Data

The GDPR has six legal bases for processing personal data, which include consent, performance of a contract, legitimate interest, vital interest, legal requirement, and public interest. [5] In comparison, the DPDP Bill has seven legal bases, which include consent, legal obligation, medical emergency, providing medical/health services, protecting individual safety during disasters, employment purposes, and reasonable purposes as specified by regulations. While some of these bases are similar to the GDPR's, such as consent and legal obligation, the DPDP Bill includes unique bases such as medical emergency and reasonable purposes.[7,8]Although these reasonable purposes are similar to the GDPR's "legitimate interest" basis, they are limited to purposes that are specified by regulation and are not very comprehensive. Additionally, the bases for health and safety or employment, which are separately defined in the DPDP Bill, are already covered by the GDPR's legitimate interest or public interest bases.

## VII. Deemed Consent

Both the GDPR and the DPDP Bill provide additional grounds for processing personal data in addition to consent. However, a notable difference between the two is that the DPDP Bill recognizes that a data principal is considered to have given “Deemed Consent” for processing when they voluntarily provide personal data to a data fiduciary, and it is reasonable to expect that they would do so. The Bill provides

an example to illustrate this provision: if someone shares their name and mobile number with a restaurant to reserve a table, they are deemed to have given consent to the collection of their name and mobile number by the restaurant (as the data fiduciary) for the purpose of confirming the reservation. [12]

**VIII. Consent Managers**

The GDPR and the DPDP Bill both acknowledge the importance of individual consent as a legal basis for processing personal data. However, the DPDP Bill introduces a new concept of "consent managers," which are data fiduciaries designated to collect and manage the consent of data principals. This will allow individuals to easily give, review, manage, and withdraw their consent through a transparent and interoperable platform. All consent managers will need to be registered with the Data Protection Board (the Board) in accordance with prescribed technical, operational, financial, and other conditions. [13]

**IX. Data Portability Right**

The DPDP Bill diverges from the GDPR by not including a provision for data principals to have the right to data portability. Although the Personal Data Protection Bill, 2019 had included such a provision, the current version of the Bill does not. [12]

**X. Protection of Children's Rights& Age of Majority**

A notable contrast exists in the age of majority as defined by the GDPR and the DPDP Bill. The GDPR considers individuals under the age of 16 as children (although some EU member states may lower this age to 13 years). On the other hand, the DPDP Bill defines children as individuals who have not yet turned 18 years old. [12]

According to Article 8 of the GDPR, there are additional requirements when obtaining consent from children who are either under the age of 16 or the age specified by their respective EU member state. The law specifies that when offering information society services directly to a child, processing their personal data is only legal if the child is at least 16 years old. If the child is below this age, processing their data is only lawful if the parent/guardian has given consent or authorized it. It is important to note that significant automated decisions should not be made regarding these children as per the law.[5]Under DPDP BillData fiduciaries must confirm the age of a child and obtain permission from a parent or guardian before processing any personal information related to the child (someone under 18 years old). The primary responsibility when processing personal data is to ensure that the rights of children are safeguardedand decisions made are in the child's best interests.[7]

**XI. Appointment of a Representative**

Controllers and/or processors who are not based in the EU but handle the personal information of EU citizens or are subject to the GDPR must designate a representative in the EU. This requirement does not apply if the processing of data is occasional and does not involve significant handling of sensitive data. [5] In contrast, the DPDP Bill does not mandate such a requirement.

**XII. Appointment of a Data Protection Officer (DPO)**

According to the GDPR, a Data Protection Officer (DPO) is only necessary if the primary activity of the controller/processor involves either (a) routinely and systematically monitoring data subjects on a large

scale, or (b) processing large amounts of sensitive data. The DPO must be sufficiently independent and skilled and have the ability to report to top management. Although outsourcing DPOs is allowed, it is recommended that they be located in the EU. [5] On the other hand, the DPDP Bill requires all significant data fiduciaries to appoint a DPO who will represent them before authorities. Additionally, the DPO must be based in India. [6]

**XIII. Data Protection Impact Assessment (DPIA)**

The GDPR mandates that controllers perform a Data Protection Impact Assessment (DPIA) for (a) extensive and systematic profiling, (b) processing sensitive data on a large scale, (c) systematically monitoring a publicly accessible area on a large scale, and other high-risk activities. When such risks cannot be mitigated, the controller must consult with the DPA before processing the data. [5] On the other hand, DPDP Bill mandates that significant data fiduciaries conduct a Data Protection Impact Assessment (DPIA) as prescribed by the bill for evaluation of the relevant Significant Data Fiduciary's processing of personal data, the risks or harm associated thereto, and the management thereof. [3]

**XIV. Breach Notification&Reporting of Personal Data Breaches**

There is a significant difference between the Bill and the GDPR regarding the notification threshold for personal data breaches to authorities and affected individuals.The GDPR follows a risk-based approach for notifying personal data breaches to authorities, whereas the Bill does not specify any such threshold.[12] According to the GDPR, personal data breaches likely to pose a risk to the rights and freedoms of data subjects must be reported to authorities. Additionally, personal data breaches must be communicated to affected data subjects only when such breaches are likely to result in a high risk to their rights and freedoms. [5] However, the Bill does not provide any specific criteria for notifying personal data breaches to the Board and affected data principals (similar to data subjects under the GDPR).[8] Regarding data breaches suffered by data processors, the GDPR requires only the concerned data controller to be notified. If the breach meets the necessary threshold set out under the GDPR, the data controller is responsible for reporting it to the authority.In contrast to the GDPR, both the data fiduciaries and data processors under the Bill are obligated to report personal data breaches to the Board and affected data principals in all cases. [12]

**XV. International or Cross-BorderTransfer of Personal Data**

The DPDP Bill appears to have a simpler process for transferring personal data to other countries. According to the Bill, personal data may be transferred to countries that have been pre-approved by the government based on certain factors. The government may also set conditions for such transfers at a later stage, although it is unclear what these conditions will be.In contrast, the GDPR provides several methods for transferring personal data, including an adequacy decision and various safeguards such as legally binding instruments between public authorities, Binding Corporate Rules, Standard Contractual Clauses adopted by the European Commission, approved codes of conduct, and certification mechanisms. [12]

**XVI. Penalties**

One of the key differences between the DPDP Bill and the GDPR is the approach to penalties for violations. The DPDP Bill allows for the imposition of financial penalties of up to INR 500 crore

(approximately €59 million) for each instance of non-compliance, depending on the type of contravention. Various factors, such as the severity, length, and nature of non-compliance, the type of personal data involved, or the recurrence of non-compliance, may be considered in determining the amount of the penalties.[8] On the other hand the GDPR lays out a number of penalties for non-compliance, which could involve fines of up to €20 million or 4% of the total worldwide annual revenue of the previous financial year, whichever is greater. These fines are applicable for a range of GDPR violations such as neglecting to obtain consent for data processing, failure to inform the supervisory authority and those affected by a data breach, or neglecting to appoint a Data Protection Officer (DPO) where required. The exact fine amount will be determined based on the severity, duration, and nature of the violation, as well as the level of cooperation provided by the organization to the supervisory authority. [5]Another difference is that under the GDPR, data subjects can file compensation claims in court and use mechanisms such as class action lawsuits, which lacks in the DPDP Bill.

## XVII. Duties of data principals

The DPDP Bill imposes some obligations for data principals, which is quite noteworthy. According to the Bill, data principals are required to refrain from filing any unfounded or trivial complaints against data fiduciaries and are instructed to provide genuine and verified information. Failure to comply with these duties may lead to financial penalties on data principals, which can go up to INR 10,000 (approximately € 116 million). In contrast, there is no equivalent requirement for data subjects under the GDPR. [12]

## XVII. Conclusion

Both the GDPR & the DPDP Bill adopt different approaches and methods, as explained the article. The GDPR is relatively more detailed in its instructions, whereas the DPDP Bill establishes certain fundamental concepts. The DPDP Bill offers a glimpse of hope for balancing the interests of data subjects while acknowledging the practical challenges that businesses may encounter. It has received considerable attention from all stakeholders, and it remains to be seen how it will be ultimately implemented.

## References

1. Wolford, B. (2018) What is GDPR, the EU's new data protection law?, GDPR.eu. Available at: https://gdpr.eu/what-is-gdpr/ (Accessed: April 14, 2023).
2. Mathi, S. et al. (2022) The genesis and evolution of India's data protection and privacy regime, MediaNama. Available at: https://www.medianama.com/2022/12/223-genesis-evolution-india-data-protection-regime-views/ (Accessed: April 14, 2023).
3. Hanspal, A. (2023) Analysis of the Digital Personal Data Protection Bill, 2022, Ahlawat & Associates. Available at: https://www.mondaq.com/india/data-protection/1267190/analysis-of-the-digital-personal-data-protection-bill-2022 (Accessed: April 14, 2023).
4. Art. 2 GDPR – material scope - general data protection Regulation (GDPR) (no date) General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu/art-2-gdpr/ (Accessed: April 14, 2023).

5. Kuner, C., Bygrave, L. A. and Docksey, C. (2020) The EU general data protection regulation (GDPR) the EU general data protection regulation (GDPR): A commentary. Edited by C. Kuner et al. London, England: Oxford University Press.
6. The Digital Personal Data Protection Bill, 2022.
7. Draft digital personal data protection bill, 2022 (no date) PRS Legislative Research. Available at: https://prsindia.org/billtrack/draft-the-digital-personal-data-protection-bill-2022 (Accessed: April 14, 2023).
8. Nagpal, N. and Bareja, A. (2023) Key features and issues in The Digital Personal Data Protection Bill, 2022, Bar and Bench - Indian Legal news. Available at: https://www.barandbench.com/law-firms/view-point/key-features-and-issues-in-the-digital-personal-data-protection-bill-2022 (Accessed: April 14, 2023).
9. Sinha, A. C. E. by (no date) GDPR and India, Cis-india.org. Available at: https://cis-india.org/internet-governance/files/gdpr-and-india (Accessed: April 14, 2023).
10. [10] Sanzgiri, V. (2022) DPDP Bill 2022: What are the new responsibilities for data fiduciaries?,MediaNama. Available at: https://www.medianama.com/2022/11/223-dpdp-bill-2022-data-fiduciaries-responsibilities/ (Accessed: April 14, 2023).
11. Verma, V. (2023) Privacy Watch: Digital Personal Data Protection Bill, 2022 seeks to secure individuals' rights, Net.in. Available at: https://tele.net.in/privacy-watch-digital-personal-data-protection-bill-2022-seeks-to-secure-individuals-rights/ (Accessed: April 16, 2023).
12. India: Comparing the digital personal data protection bill, 2022 and the GDPR (2023) DataGuidance. Available at: https://www.dataguidance.com/opinion/india-comparing-digital-personal-data-protection-0 (Accessed: April 17, 2023).
13. Mathi, S. et al. (2022) What's missing from the Consent Manager framework in the Data Protection Bill, 2022, MediaNama. Available at: https://www.medianama.com/2022/12/223-dpdp-bill-2022-consent-manager-views/ (Accessed: April 17, 2023).