

## **THE DPDP ACT 2023: CRITICAL INSIGHTS INTO ITS LEGAL FRAMEWORK AND PRACTICAL IMPACT**

**Amrita Jha<sup>1\*</sup>**

Research Scholar, Gujarat National  
Law University, Gandhinagar, Gujarat,  
India  
E-mail: [amritajha93@gmail.com](mailto:amritajha93@gmail.com)

### **Abstract:**

The DPDP Act 2023 seeks to meet the objective of the fundamental right of privacy and data protection. This paper provides a comprehensive analysis of the making of the DPDP Act 2023, tracing its emergence from legislative proposals to its enactment. This paper critically analyses the key provisions of the Act, including the principles of legitimate use and consent. Through the critical examination, the effectiveness of the newly enacted Act in providing the remedy to e-commerce consumers in case of violation of their privacy rights is tested. Further, the paper highlights the limitations and offers recommendations for enhancing the effectiveness and enhancing data protection in the digital marketplace.

### **Keywords**

DPDP, fundamental rights, data protection, privacy, e-commerce

### **1. Introduction**

The e-commerce sector is data-driven, therefore, protecting consumer privacy is a challenging strive in India's e-commerce setting. Safeguarding and protecting consumer's personal data while using their data for business purposes is a tightrope walk that e-commerce companies and policymakers must undertake. Therefore, it is vital to delve deep into the potent and aptness of the laws dealing with the protection of consumer privacy in the digital age. India has taken decades to enact a specific law on personal data protection, especially when the developed countries have already framed their laws on data protection and are now at the revolutionary stage, India is at the evolution stage.

The DPDP Act 2023 is part of the broader national strategy to prepare India in advance to fulfill the needs of the digital world by providing an exemplary legal paradigm to usher the needful. The DPDP Act 2023 seeks to meet the objective of the fundamental right of privacy and data protection as well as to meet all of the reasonable and fair requirements that are lawful and required for the innovative system to grow.

### **2. The Making of the DPDP Act 2023**

The DPDP Act 2023 is not the first version of India's data protection law. After the Supreme Court's decision in the Puttaswamy case, in which the right to privacy is declared as a fundamental right, multiple attempts to enact a comprehensive and specific data protection law were made by the legislatures. On 3 August 2023, the Government introduced a new version of DPDP in the Lok Sabha, and on 11 August 2023, the efforts of the Indian legislators culminated after receiving the assent of the President that solidified DPDP Bill 2023 into an Act. The DPDP Act 2023 does not contain a transitional period between the enactment to its entry into force, rather, it empowers the Government to decide the date on which different

sections of the Act will come into force. To supplement the DPDP Act 2023, the Rules will be notified by the Central Government on 26 specified subjects. The DPDP Bill 2023 was the fifth and final version of India's draft data protection law. Before this, in November 2022, the DPDP Bill 2022 was introduced by replacing the old Personal Data Protection Bill 2021 (PDP Bill 2021). The DPDP Bill 2022 was introduced to safeguard the fundamental rights and freedom of natural persons and, in particular, their right to privacy with respect to the processing of their personal data. Following the path of EU GDPR, through the DPDP Bill 2022, the Indian legislatures have made a deliberate attempt to bring holistic national legislation on digital privacy rights, which is underpinned by seven national privacy principles. However, the DPDP Bill 2022 was criticized for multiple reasons, including being a leaner version compared to its erstwhile versions. As compared to the GDPR, the principles mentioned under the DPDP Bill 2022 were not very elaborative in nature. Also, contrary to its predecessor, i.e., the PDP Bill, the DPDP Bill 2022 did not categorize the data on the basis of the sensitivity of the information, and for all kinds of personal data, uniform security measure was provided. In addition to that, the concept of deemed consent was highly criticized. This Bill was also criticized for taking away all the data protection rights that the earlier version provided and coming up with a weaker version of the previous versions of the data protection law.

However, after the Puttaswamy judgment, the Personal Data Protection Bill 2018 was the first legislative attempt to enact a comprehensive data protection law in India under the Chairmanship of former Supreme Court Justice Shri B N Srikrishna. The Bill recognizes privacy as a fundamental and basic right. The basic advantage of the Bill was the emphasis on 'informed user consent' for the processing of personal data and the enshrined 'right to be forgotten' and 'right to access' to the data principal. It also segregated data into personal and sensitive data. Further, it weighs and balances the digital economy and, at the same time, safeguards the data of the individual. The Bill lays down stringent provisions penalizing public and private sectors both for any contravention of the law. However, despite all the affords, the Bill has fallen short on various aspects: data privacy law was not equally applicable to the government and private actors, and it falls short of laying guidelines for data security standards for data fiduciaries, which may cause an increase in the cost of the company, the scope of the government's accountability when the personal data is processed without consent is not defined, fear of addition costs for storage of at least one copy of personal data on a server or data center located in India, the cost of withdrawing consent is put on the data principal.<sup>1</sup> It was also criticized for diluting the scope and intent of the Bill with its confused and vague wordings.

As a result, the Personal Data Protection Bill introduced by the B N Srikrishna Committee in 2018 has undergone several amendments and recommendations since its introduction. Later on, the PDP Bill 2019 was introduced to protect the right to privacy of internet users/data principals. The Bill was based on the recommendations of the Expert Committee report, which examined issues related to the protection of personal data and proposed a Draft Personal Data Protection Bill 2018.<sup>2</sup> It proposed a legal framework for data processing, usage, data flow, and cross-border transfer. It also proposed to establish a Data Protection Authority of India to fix the data processor's accountability and to provide the remedy in case of unauthorized and

<sup>1</sup> Anghrija Chakraborty, Ashima Obhan, and Amar K Sundram, *Data Protection Laws Demystified* (OakBridge Publishing Pvt Ltd 2020) 160.

<sup>2</sup> Anurag Vaishnav, 'The Personal Data Protection Bill, 2019: How It Differs from the Draft Bill' (*PRS Legislative Research*, 27 December 2019) <<https://prsindia.org/theprsblog/personal-data-protection-bill-2019-how-it-differs-draft-bill>>.

harmful processing of data. To create a collective culture that fosters a free and fair digital economy, the PDP Bill 2019 was drafted. Through the PDP Bill 2019, the data processor's duty was restricted to processing the data in a fair and reasonable manner, but dissent was received from the various factions of the society. As a result, the PDP Bill 2019 and, by extension, the 2021 Bill were withdrawn by the Government, citing the need for a more comprehensive legal framework.

After extensive delay and discussions, the DPDP Act 2023 has been enacted. The DPDP Act 2023 governs how the data will be collected, processed, shared, and deleted and lays down compliance expectations, such as obtaining consent, legitimate use, giving notice, response to access requests, and data breach notification, on the data fiduciary and additional obligations on significant data fiduciaries to conduct periodic data protection impact assessment, periodic audit, etc and appoint a Data Protection Officer (DPO), an independent data auditor. All the data intermediaries like e-commerce companies, banks, big tech, insurance companies, or other social media or internet giants have to follow these obligations and have to strictly protect the personal data of users, failing any of the obligations or requirements or misuse of data runs the risk of penalties that may extend up to Rs 250 crore for a single violation and even blocking of the platform in case of severe and repeated violations. In addition to that, the rights and duties of the data principal are also provided under the Act. The Act further strengthens the law through its data protection principles and provides a legal framework to set up a secure data protection regime in India. The DPDP Act 2023 has a significant impact on various sectors, including the e-commerce sector. The e-commerce regime is data-driven and has plenty of data or personal information of its users/consumers. The subsequent sections of this chapter analyze the provisions of the DPDP Act 2023 to test the aptness and potentness of this legislation.

### **3. Basic Protection Under the DPDP Act 2023: A Demystification**

The DPDP Act 2023 requires that personal data must be processed for lawful purposes. For processing to be lawful, personal data should be processed on the basis of the data principal's consent or for certain legitimate uses laid down by law. The lawful purpose is broadly defined under the DPDP Act 2023, which states that lawful purpose means any purpose which is not expressly forbidden by law. The criteria for the lawful processing that is mentioned under the Act is 'consent' or 'certain legitimate uses'.<sup>3</sup>

#### **3.1 Consent**

Consent can be called the heart and soul of the whole DPDP Act 2023. According to the DPDP Act 2023, consent should be proclaimed in a lawful manner. To be proclaimed in a lawful manner, the data principal's consent should be free, explicit, informed, unconditional, and unambiguous with clear affirmative action. It should also signify that the data principal agrees to the processing of her personal data for a specified purpose and be restricted to such personal data only that is required for such specified purpose.<sup>4</sup> In addition to that, the request for consent should be in plain and clear language, with the option to access that in English or any other language specified in the Eighth Schedule of the Indian Constitution. India boasts many languages, and each has its nuances. One of the characteristics of an effective data protection law is unambiguous communication with its users/consumers to ensure their informed decisions about their data. Linguistic diversity demands a commitment from e-commerce

---

<sup>3</sup> See section 2(d) of the Digital Personal Data Protection Act, 2023. "Certain legitimate uses" means the uses referred to in section 7.

<sup>4</sup> Section 6(1) of the Digital Personal Data Protection Act, 2023.

companies to multilingual communication or translation facilities to make consumers aware of their rights and the data protection practices of the e-commerce companies. Apart from that, the consent will be only for minimum data, which is required for service, and if the data fiduciary wants to collect more data for advertisement or any other purposes, then that data fiduciary has to take the consent of the data principal for that purpose as well. It can be said that the consent given by the data principal should be purpose-specific, and every time a new purpose is added or if the purpose changes, then it is the duty of the data fiduciary to inform that and accordingly take the consent of the data principal. Many times, e-commerce companies unwittingly take consent from consumers for more personal data than required. The DPDP Act 2023 clearly spells out that even if consent is unwittingly given, purpose limitation will apply. Purpose limitation prevents misuse of data. It further allows the data principal to give, review, manage, and revoke her consent given to the data fiduciary through the ‘consent manager’,<sup>5</sup> who shall be registered with the Board. The consent manager is a new class of licensed intermediaries who can be used by consumers or individuals as a single point of contact to assist in the legal aspects of the consent. Under the Act, the consent manager is accountable to the data principals and acts on their behalf. To give more emphasis on consent, the DPDP Act 2023 imposes the obligation on the data fiduciary to accompany or precede the consent request with notice.

However, if the consent is given by the data principal before the date of commencement of the DPDP Act 2023, then in that case, it is the duty of the data fiduciary to give the notice to the data principal as soon as it is reasonably practicable. Unless and until the data principal withdraws her consent to process her personal data, the data fiduciary may continue to process her personal data. With the purpose of including all the sections of the country, the DPDP Act 2023 makes it mandatory to give the data principal the option to access the contents of the notice in English or any other language listed in the Eighth Schedule to the Constitution of India.

### **3.2 Certain Legitimate Uses**

In addition to consent, the other criteria for the lawful processing of personal data are the legitimate uses prescribed under this Act. Section 7 of the DPDP Act 2023 provides an exhaustive list of the legitimate uses for which the data fiduciary may process the data principal’s personal data. These are:

- (a) Any specified purpose for which the data principal has voluntarily provided her personal data to the data fiduciary without any express prohibition on the use of her personal data.
- (b) For the State and any of its instrumentalities for the purpose of providing or issuing subsidy, benefit, service, certificate, license, or permit, subject to the condition that for availing these facilities, (i) the data principal has previously given her consent for the processing of her personal data by the State or any of its instrumentalities, or (ii) such personal data is available in the digital form or digitized from a non-digital form, which is maintained by the State or any of its instrumentalities and is notified by the Central Government. However, processing should not compromise on the standards followed for processing of such policy or under any law for the time being in force for the governance of personal data.
- (c) For the performance by the State or any of its instrumentalities of any function under any law for the time being in force in India or for the sovereignty and integrity of India or security of the State.

---

<sup>5</sup> Section 6(7) of the Digital Personal Data Protection Act, 2023.

- (d) To fulfil the obligation under any law that is in force in India on any person to disclose the information to the State or any of its instrumentalities, subject to the condition that the processing should be lawful.
- (e) To fulfil the compliance of any judgment or decree, or order issued under any law for the time being in force in India, or any judgment or order relating to the claims of a contractual or civil nature under any law for the time being in force outside India.
- (f) For responding to the medical emergence involving a threat to the life or immediate threat to the health of the data principal or any other individual.
- (g) For the purpose of taking measures to provide medical treatment or health services to any individual during the time of epidemic, outbreak of disease, or any other threat to public health.
- (h) For the purpose of taking measures to ensure the safety of, or to provide assistance or services to, any individual during any disaster or any breakdown of public order.
- (i) For the purpose of employment or related matters to safeguard the employer from loss or liability, such as prevention of corporate espionage, maintenance of confidentiality of trade secrets, intellectual property, classified information, or provision of any service or benefit sought by a data principal who is an employee.

#### **4. Allocation of Responsibilities**

The primary responsibility and liability for complying with the provisions of the DPDP Act 2023 is assigned to the data fiduciary. The Act also assigns certain duties to the significant data fiduciary in a situation where the central government notifies any data fiduciary as a significant data fiduciary. The Act empowers the data fiduciary to enlist another entity or individual as a data processor to process personal data on her behalf. However, the ultimate responsibility is of the data fiduciary to comply with the provisions of the DPDP Act 2023 for the processing undertaken by it or on its behalf by a data processor, and the ultimate duty to ensure compliance is upon the data fiduciary as a data processor is mere a delegate of the data fiduciary. Unlike the majority of international laws on data protection, the DPDP Act 2023 imposes duties on the data principals as well.

#### **5. Rights of Data Principal**

One of the objects of the enactment of the DPDP Act 2023 is to recognize the rights of the data principals related to the processing of personal data. Under the DPDP Act 2023, the primary responsibility is on the data fiduciary to accommodate the rights of data principals. Even if the responsibility can be shifted to another entity, i.e. the data processor, through a contract, the data fiduciary cannot escape the responsibility to ensure the rights of data principals. The rights that are recognized under the DPDP Act 2023 are:

- i. Right to information via notice: The data principal has the right to information via the notice, which means the data fiduciary is obliged to give the data principal information relating to the personal data collected and the basis for the processing of personal data, the information about the manner to withdraw the consent and grievance redressal, and information about the manner in which the complaint can be made to the Board by the data principal.<sup>6</sup>
- ii. Right to rectification: The data principal has the right to correct, complete, update, and erase her personal data.<sup>7</sup>

<sup>6</sup> Section 5(2) of the Digital Personal Data Protection Act, 2023.

<sup>7</sup> Section 12(2) of the Digital Personal Data Protection Act, 2023.

- iii. Right to withdraw consent: The data principal has the right to revoke consent for the processing of her personal data.<sup>8</sup>
- iv. Right to erasure: Withdrawal right brings with it the right to erasure<sup>9</sup>. However, this right is not absolute to the extent that the data fiduciary can retain the data where it is absolutely necessary in relation to the purpose the data was collected for and where it is necessary for the compliance of the law. This right to erasure is subject to the time limit that will be prescribed later on, and if, during that prescribed time period, the data principal does not exercise her right, then that right shall no longer be served.<sup>10</sup> However, in all such cases, the data fiduciary shall have to ensure that adequate safeguards are in place. Therefore, the data principal has the right to request the erasure of personal data, and the erasure may also be required automatically when consent is withdrawn or when the specified purpose for which the data was provided is no longer required.
- v. Right to access: Subject to section 11(2)<sup>11</sup>, the data principal has the right to access information related to her personal data, information such as a summary of the processed personal data, identities of all the data fiduciaries and data processors with whom the data principal personal data has been shared, what purpose it is being processed for, along with the details of the shared data, and any other information related to the personal data which the Act may prescribe.<sup>12</sup> Pursuant to this right, data principal has the right to get access to their personal data. The rule can define the list of information that a data principal can request from the fiduciary. If the data principal makes the request by electronic means, the information should be provided in a commonly used electronic format unless the data principal requests otherwise. Organisations have the right to ask for specific directions on what the requesters are asking for if this is not clear. A reasonable time limit with a further extension on reasonable grounds, such as the complexities, number of requests, and significant volume of work, etc should be provided.
- vi. Right of grievance redressal: The data principal has the right to readily available means of grievance redressal, which will be provided by the data fiduciary or consent manager. This right can be exercised by the data principal in respect of the rights provided to the data principal or the obligations imposed on the data fiduciary or consent manager.
- vii. Right to nominate: The data principal has the right to nominate any other individual to exercise the rights of the data principal in the event of death or incapacity of the data principal.

## 6. Conclusion

India is witnessing explosive growth in data production, which is estimated to be doubling substantially. The refining of these data involves challenges and risks. The absence of comprehensive data protection law had negative effects on driving innovation, cross-border trade, and consumer trust. Undoubtedly, with the enactment of the DPDP Act 2023, India strides boldly toward a progressive data protection regime. The DPDP Act 2023 is applauded for being easy to read, understandable, compliance-friendly, and has a pragmatic approach that makes it easy to implement at scale. It is a principle-based law rather than a prescriptive law. It is digital by design implementation, and local language has been given importance under the

<sup>8</sup> Section 6(4) of the Digital Personal Data Protection Act, 2023.

<sup>9</sup>Section 8(7)(a) r/w section 12(1) and (3) of the Digital Personal Data Protection Act, 2023.

<sup>10</sup> Sec 8(8) of the Digital Personal Data Protection Act, 2023.

<sup>11</sup> Section 10(1)(a) and (b) of the Digital Personal Data Protection Act, 2023 do not apply in the cases where data is shared with such data fiduciary who is authorised under the law for the purpose of prevention or detection, or investigation of offences or cyber incidents, or for prosecution or punishment of offences.

<sup>12</sup> Section 11(1) of the Digital Personal Data Protection Act, 2023.

Act.

However, the law lacks in many areas. It boldly discarded or diluted the concepts that, up until now, enabled prior iterations of the draft laws to posit a differential approach to data protection premised, in part, on categorizing personal data based on sensitivity and harms associated with certain kinds of processing. In addition to that, a punitive penalty structure which was required to show a key deterrent under the law and an open-ended compensation scheme that marked prior draughts of India's data protection law has been replaced by sleeker, leaner provisions, raising concerns about whether the lite approach to data protection is, in fact, the right approach.

Therefore, the path forward demands much more effort. The Act has hidden within itself numerous complex provisions as the DPDP Act 2023 is not complete in itself, and the essential operative parts will be followed in the subordinate legislations or rules that are believed to be introduced in the near future. The DPDP Act 2023 left 26 subjects to be regulated by the rules, and these rules will influence the efficacy of India's data protection law. It hinders the effectiveness of the DPDP Act in providing comprehensive legislation for the protection of consumer privacy in the digital world. The following are the significant regulatory gaps in the DPDP Act 2023:

- The manner in which an entity collecting data seeks consent and provides notice is left open to future guidelines or rules.
- The DPDP Act makes the consent manager accountable to the data principal, but the extent of that accountability and the obligations of the consent manager towards the data principal are not specified and are left to the rules. Unless and until the rules are prescribed, the role of the consent manager remains unclear.
- The technical, operational, financial, and other prerequisites for the registration of the consent manager with the Board as well as the manner of registration, are not provided in the DPDP Act 2023.
- The form and manner of notifying the data principal and Board in the event of a personal data breach has been left to the rules.
- The time period and the limitations for certain circumstances, such as responding to a grievance mentioned in the DPDP Act 2023, will be prescribed in accordance with the requirements of various sectors or different classes of data fiduciaries and purposes.
- The manner of publishing the business contact information of the DPO will be notified by rules.
- The manner of obtaining verifiable parental consent before processing any personal data of a child or a person with a disability who has a lawful guardian will be notified by the rule.
- The future rule will determine which classes of data fiduciaries or purposes and conditions are exempted from the requirement of obtaining verifiable parental consent and restrictions on tracking or behavioural monitoring or targeting advertisements for a child or a person with a disability having a lawful guardian.
- The details related to the obligation of significant data fiduciary related to periodic data protection impact assessment and any other measures, if required, shall be notified by rules.
- The law related to data principal's right to access information about personal data is also reserved for future rules and regulations.
- Similarly, the manner of exercising the data principal's right of erasure of personal data will be notified later.
- The DPDP Act 2023 does not define exemptions from the checks imposed by data protection laws like blanket exemptions given to the Government. In order to get the exemptions provided under the Act for research, archiving, or statistical purposes, the conditional standards will be notified by the rules or regulations.
- The manner of appointment of the chairperson, other members, officers, and employees of the Data Protection Board of India and their salary, allowances, other terms and conditions

of service, as well as the procedure of conducting business of the Board shall be notified by rules.

Thus, it can be concluded that the DPDP Act 2023 has created a data protection framework that provides principles that should be followed and the protection that has to be given. However, over and above the basic principles, obligations, and rights, there is a need for sectoral regulations. Consequently, the DPDP Act 2023 can be characterized as a horizontal law that, in general, applies to all sectors. However, the DPDP Act 2023 needs to be supplemented with vertical rules and regulations because certain sectors, such as e-commerce, have their individual requirements. However, if supplemented with the right rules and regulations for e-commerce, then, in the digital kaleidoscope, this law can be a harmonious symphony to re-engineer the data privacy regime of India.