

Digital Personal Data Protection Act, 2023 (DPDPA 2023)

Ravi Jugalkishor Vyas

LLM Student (Business Law)

Bhagubai Changu Thakur College of Law, New Panvel

Abstract:

Digital Personal Data Protection Act, 2023 (“DPDPA 2023”) and the Digital Personal Data Protection Rules, 2025 (“DPDPA Rules 2025”) it is applied by India at rank of 137th Country to enact a data protection Law. it is force by 13th May 2027. The DPDP Act, 2023 is dedicated to protecting Digital footprint & geographies serving Indian users. Rights of individuals to protect personal data and the need of organization to process data for lawful, necessary purposes only. The DPDP Act, 2023 is applied to Digital form, Digitized data, Withing India & Outside India. It is not applicable on personal or domestic use & publicly made available data. The enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act) marks a significant development in India’s data protection framework, establishing a legal regime for the processing of digital personal data while safeguarding individual privacy rights. The Act seeks to strengthen accountability among Data Fiduciaries, including internet companies, mobile applications, and businesses that collect, store, and process personal data. By introducing obligations relating to lawful data processing, consent, transparency, security, and accountability, the legislation aims to balance the legitimate interests of data-processing entities with the fundamental right to privacy of individuals. This paper examines the significance of the DPDP Act, 2023, with particular emphasis on its role in strengthening data protection, promoting responsible data governance, and addressing emerging privacy concerns in India’s rapidly evolving digital ecosystem.

Keyword: DPDP Act,2023., Data Protection, Article 21(Right to Privacy) – Puttaswami judgment, B.N. Shrikrishna Committee, Data Fiduciary, penalty 10K to 250Cr Risk, Applied withing India & Outside India, 13th May 2027.

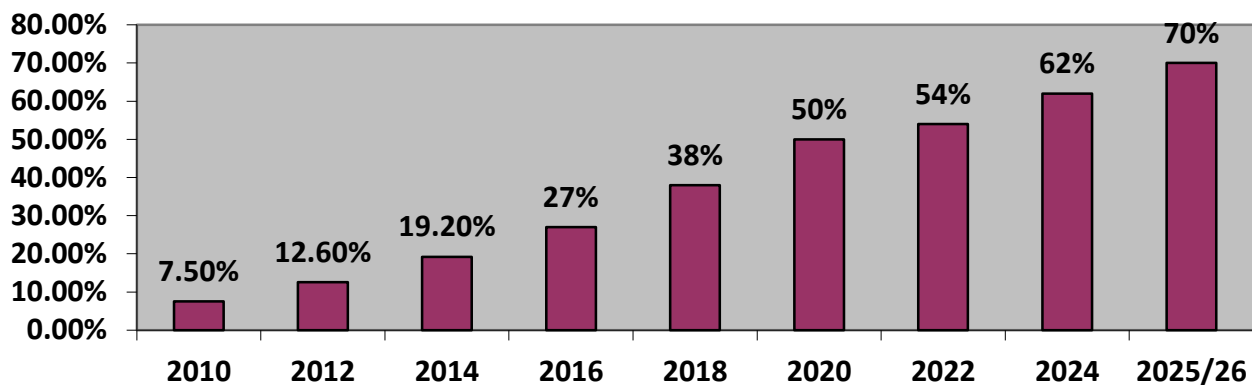
Background:

- 1) 2011 : Justice AP Shah Committee recommended Privacy legislation
- 2) 2017 : (The Right to Privacy) Supreme Court justice KS Puttaswami vs union of India recognized privacy as a fundamental right
- 3) 2018 : (The Shrikrishna Committee) Justice B.N. Shrikrishna release initial draft of the Personal Data Protection Bill.
- 4) 2019 : (The PDP Bill 2019) the Government Introduced the Personal Data Protection (PDP) bill in parliament, which was refer to a Joint Parliament Committee (JPC).
- 5) 2021 : (JPC Recommendation) the JPC submitted reports with the recommendation and proposed expanding the Bill cover non personal data as well, leading the government to withdraw the 2019 bill entirely.

- 6) 2022 : (The Shift to DPDP) the ministry of electronics and information technology released a simplify draft with title Digital Personal Data Protection Bill 2022
- 7) July 2023 : (Cabinet Approval) after the public feedback, the union cabinet approved the revised Digital Personal Data Protection Bill 2023.
- 8) August 2023 : The will Introduced in the Lok Sabha on the 3rd August 2023, Passed on 7th August 2023. By Rajya Sabha passed on 9th August 2023 and received presidential assent on 11th August 2023.
- 9) 2023 : Official become Law Digital Personal Data Protection Act, 2023
- 10) 2025 : (Operationalization via DPDP Act rules) The Government released and notified the implementation rule to Operationalize compliance, set up the Data Protection Board.

1. Introduction:

Internet (Digital) Users in india



In 2011 the evolution of India's data protection regime is closely associated with the government's growing emphasis on establishing a comprehensive digital governance ecosystem. A significant milestone in this development was the introduction of the Aadhaar biometric identification programme in 2010, which involved the extensive collection and management of citizens' personal and biometric information. In 2011, the Parliamentary Standing Committee on Finance, while examining the Aadhaar initiative, drew attention to the absence of a dedicated and comprehensive legal framework for data protection. The Committee highlighted the potential dangers of collecting and maintaining large volumes of citizens' information without sufficient statutory safeguards, thereby underscoring the urgent need for effective mechanisms to protect personal data and privacy. (3)

as well as social media was gradually growing in India like Facebook were emerging. Due to social media in India day by day rapidly increased an internet user, and the personal data was easy to access for any unlawful activity. Considering the situation, the Justice AP Shah committee 1st time recommended for Privacy legislation and digital personal data protection rules and same 2017 passed one judgment on basis of article 21 (Right to privacy) at Supreme Court justice KS Puttaswami vs union of India recognized

privacy as a fundamental right. It enacted in 2023 after it was passed by Rajya Sabha and India's 137th Country to enact a data protection Law and it will impose from 13th May 2027.

The right to privacy is an important fundamental human right recognized under international human rights law. It is protected by major international instruments such as the Universal Declaration of Human Rights, 1948 (UDHR), the International Covenant on Civil and Political Rights, 1966 (ICCPR), the International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, and the Convention on the Rights of the Child, 1989. The right to privacy is also recognized in various other international and regional human rights treaties. International and regional human rights courts and bodies have recognized privacy as an important right that protects an individual's personal life, dignity and freedom (4).

The government provides different provisions for data protection, including Data Fiduciary, Significant Data Fiduciary, Data Principal, Data Localization, and Data Sovereignty. A Significant Data Fiduciary is an organization or government body that handles a large amount of personal data and may have a significant impact on data privacy. A Data Principal is the individual to whom the personal data relates.

Data Localization refers to storing or processing data within a particular country as required by its laws. Data Sovereignty means that data stored or collected within a country is subject to the laws and regulations of that country. For example, if a foreign company collects and processes personal data in India, it may be required to comply with applicable Indian data-protection laws.

The Indian government collects and stores large amounts of data through agencies and initiatives such as UIDAI, the Census of India, MGNREGA, the Income Tax Department, Digital India, and the Smart Cities Mission. Big data is also widely used by private companies, including online travel agencies, e-commerce platforms, and telecom companies. Although big data provides many benefits, it also creates concerns about privacy, data security, access control, and data ownership. These concerns are greater in public-private partnership projects, where private organizations may collect and process large amounts of personal data. Therefore, there is a need to examine how Indian laws protect personal data and privacy and how they address the challenges created by the growing use of big data. (5)

2. Scope and Applicability:

DPDPA, 2023 at a glance by industry as follows;

- 1) BFSI: Customer KYC, transaction data, account aggregator flows, align with RBI.
- 2) Healthcare: Sensitive health data, telemedicine, hospital records, specific consent for clinical use.
- 3) Ed-Tech: Minors below 18; tracking & behavioural monitoring banned, verifiable parental consent.
- 4) E-Commerce: above 2cr users triggers 3 years retention rule; vendor sharing, processor contract
- 5) Telecom: Subscriber data, CDRs; processor relationships for billing, ensure processors cease on opt-out.
- 6) IT: often the processor for clients; cross-border flows, localisation readiness.

The Act has a wide scope and can apply even outside India when a foreign entity provides goods or services to Data Principals in India. Thus, foreign organizations processing the personal data of individuals in India may also have to follow the Act. The Act applies to both digital data and data that was originally collected in physical form but later converted into digital form. However, it does not apply to personal data used by individuals for personal or domestic purposes, or data that has been made publicly available by the Data Principal or as required by law. (6)

3. Type of Data:

- 1) Personal Data: Personal data means any information that can identify a person, such as a name, mobile number, email address, identification number, or other details. The Act applies to personal data that is collected in digital form. It also applies when data is first collected in physical form and later converted into digital form.
- 2) children's data: The Act provides special protection for the personal data of children. Organizations processing children's data must follow additional requirements and cannot process such data in a way that may harm the child.
- 3) sensitive personal data: The DPDP Act does not create a separate category of sensitive personal data, unlike some earlier data-protection laws and proposals in India. The Act also does not generally apply to personal data processed by an individual for personal or domestic purposes. For eg. Army records, ISRO's data, Govt. Data, etc
Further, certain personal data that has been made publicly available by the Data Principal or is required to be made public under law is excluded from the scope of the Act in specified situations. Thus, the DPDP Act mainly focuses on digital personal data, children's data, and responsible processing of personal information, while providing individuals with greater control over their personal data and placing duties on organizations that process such data.

4. Consent:

The DPDP Act, 2023, requires Data Fiduciaries to obtain verifiable consent from a parent or lawful guardian before processing the personal data of children and persons with disabilities who are unable to provide legally valid consent, as applicable. It also places restrictions on processing activities that may adversely affect a child's well-being and prohibits behavioral monitoring and targeted advertising directed at children, subject to statutory exemptions. The DPDP Rules, 2025, further clarify the manner in which parental or guardian consent is to be verified and specify certain circumstances in which the consent requirement may be relaxed. These exemptions cover limited purposes, such as the provision of healthcare, educational activities, childcare services, and measures intended to ensure children's safety, subject to the conditions prescribed under the Rules. However, such exemptions are purpose-specific and do not provide a general waiver of the obligations imposed on Data Fiduciaries under the Act.

Section 9(4) permits exemptions from both parental consent under Section 9(1) and the restrictions on tracking, behavioral monitoring and targeted advertising under Section 9(3). However, the exemption does not extend to Section 9(2), which prohibits processing likely to cause a detrimental effect on a child's well-being. (7)

- ✓ Child protection duties – Processing as necessary for legal functions

- ✓ Email account creation – Limited to account creation and email use
- ✓ Real time location tracking – Only for child safety and security
- ✓ Blocking harmful content – Only to prevent access to detrimental information
- ✓ Child verification – Only as necessary for confirmation.

5. Responsibility of Data Fiduciary:

DPDP Act obligation on the Data Fiduciary.

- 1) Lawful Purpose: Data fiduciary whichever is data collected by the data principle that use only for legislate purpose, they cannot use for a thing which is prohibited in india. They only use our data for that purpose only for that which they have collected.
- 2) Data retain: Data fiduciary store data till 3 years from the date of collect or till the completed the purpose of collecting data. After that the fiduciary data will delete and before deleting the fiduciary must be inform to principle regarding the deleting of data
- 3) Data Breach: Data fiduciary have responsibility to inform the data principle that data was hack, or any cyber hack same as well as inform to Data Committee board for safety side
- 4) Processing: a data principle can ask to data fiduciary for the process of the data, can it they are sold that data to anyone
- 5) Data protection Impact assessment (only for Significant D.F.): under this Data fiduciary must be know about the assessment there have no harm to Environment & Social

Rights of citizens (8):

- 1) Right to information: Individually will have the right to seek more information on how their data is processed, and the data fiduciary will make this information available in a clear and understandable way
- 2) Data Correction, update or erase: Individually shall have the right to correct inaccurate or incomplete data and erase data that is no longer require for processing.
- 3) Right to Nominate: a data which is with the Data Fiduciary, I can choose the nominee who will access size all the rights over of data principle in case of death or incapability.
- 4) Right to grievance: A person shall have the right to use readily available mean of registering a grievance with a data fiduciary.

6. Breach Notification or Appeal:

The Data Protection Board will be introduced for Monitoring to the progress of this DPDP Act, to give direction to all Data Fiduciary regarding the compliance of the Act. The board introduce with 1 chairman & 2 other Person (retired supreme court / high court judge) appointed by Government of India with 2 years tenure.

The Act defines a personal data breach as any unauthorized or accidental compromise of personal data's confidentiality, integrity, or availability, and requires Data Fiduciaries to promptly notify the Board and affected individuals with details for timely protective action. The Rules build on this by mandating that Data Fiduciaries notify the board and the affected data principals without any delay on becoming aware of a data breach. Further, they have to submit a detailed report to the Board within 72 hours.

Limit of the fine is finalized at the time of introducing of Act is till 10K on Data Principle and up to 250 Cr on Data Fiduciary. If anyone is not satisfied with the result of Board, they can approach to TD SAT (Telecom Dispute Settlement Aplt Tribunal) it is introduced in 1992 with TRAI Act (Telecom Regulatory Authority of India).

Fine under Section 33:

Sr. No	Type of Violation	Maximum Penalty
1	Failure to take reasonable security safeguard	Upto Rs. 250cr
2	Failure to notify Board or affected Principals of a breach	Upto Rs.200cr
3	Breach of additional obligations relating to children's data	Upto Rs.200cr
4	Failure of SDF to meet additional obligations	Upto Rs.150cr
5	Breach of duties of the data principal	Upto Rs. 10,000/-
6	Breach of any voluntary undertaking accepted by the Board	Upto Max applicable to that breach
7	Breach of any other provision of the Act or the rules	Upto Rs. 50cr

Exemptions:

That the state machinery is the biggest data fiduciary in this country, state machinery means all the Central Government, State Government, All the municipalities and Local authority Body as well (Panchayat). Data principles gave the anyone can erase the data when they required but there have exemption for Government of India. The Data Personal Data Protection Act is not applicable on Government of India. Government use all personal data without any permission or rights for any specific research

7. Legal & Practical Challenges:

- 1) No Victim Compensation:** No provision for individuals received no damages for privacy breaches. While the act introduces massive financial penalties for data fiduciaries, all fined amounts are credited directly to the **Consolidated Fund of India**. Legal experts at the MNLU Mumbai Law review point out that the law fundamentally lacks a mechanism for restorative justice. Individuals whose privacy is compromised or who suffer financial loss from a leak cannot claim damages or financial restitution under this framework
- 2) Independence:** The Data Protection Board of India (DPBI) is heavily reliant on the central government, critics from the hindu argue that because the government controls the appointment terms, salaries, and removal processes of DPBI members, the board lacks the structural autonomy envisioned by the original **Justice B.N. Srikrishna Committee**. Since the government is one of the largest data aggregators in the country, an executive board may struggle to impartially adjudicate data breaches involving public agencies.
- 3) Publicly Available Data:** the act does not apply to personal data that a user has made publicly available. Constitutional research from the National Law School Forum warns that this creates an unregulated environment for tech companies to scrape public profiles for AI training. It creates an

artificial legal hierarchy between public and private data that ignores how modern data analytics can weaponize public data.

- 4) **Burden on Small Enterprises:** Implementing advance cybersecurity protocols, setting up mandatory breach-reporting infrastructure, and hiring **Data Protection Officers(DPOs)** requires heavy technological and financial investment. Legal clinics like the Lloyd law College Research Blog note that while multinational corporations can easily pivot, India's booming startup and MSME sectors face steep compliance costs that could inadvertently stifle operational growth and localization.
- 5) **Cross-Border Transfers:** Negative list model allows transfers globally unless the Central Government explicitly bans or blacklists a country. the criteria for blacklisting countries remain unspecified, global tech firms, cloud providers, and fintech sectors are left in regulatory limbo, complicating long-term international data architecture strategy.

References:

1. Digital Personal Data Protection Act, 2023 (DPDPA, 2023)
2. Digital Personal Data Protection Rules, 2025 (DPDPA Rules 2025)
3. Fifteenth Lok Sabha, Standing Committee on Finance, "The National Identification Authority of India Bill, 2010" (Forty Second Report, 2011-2012)
<https://elibrary.sansad.in/server/api/core/bitstreams/f8632892-bd58-4606-833c-b1b4a2be0d0b/view>
4. An International Legal Framework for Data Protection: Issues and Prospects by Christopher Kuner :: SSRN <https://ssrn.com/abstract=1443802>
5. Dhiraj R. Duraiswami, Privacy and Data Protection in India - Journal of Law & Cyber Warfare -166, (2017)
6. Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023
7. <https://indiacode.ecourtsindia.com/rules/digital-personal-data-protection-dpdp-rules-2025-fe07b131/>
8. https://www.ey.com/en_in/insights/cybersecurity/decoding-the-digital-personal-data-protection-act-2023