The Indian Journal for Research in Law and Management
Open Access Law Journal – Copyright © 2026
Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

DPDP ACT 2023 AND ITS IMPLICATIONS ON THE BANKING SECTOR

Lakshmi P Nath

INTRODUCTION

India did not have a standalone legal framework to protect digital personal data until 2023. In the year 2023, the Digital Personal Data Protection Act [DPDP Act][1] was passed which provides a comprehensive legal framework for data privacy, empowering citizens to have a control over their personal data.

This stems from the landmark 2017 Supreme Court judgement in the case *Puttuswamy v. UoI* [(2017) 10 SCC 2]. The Supreme Court held that right to privacy is a fundamental right under the ambit of Article 21.

Up until the implementation of the DPDP Act, India relied on the limited data protection guidelines under the IT Act 2000, which was found to be insufficient to cater to the needs of the modern digital economy.

SCOPE AND APPLICABILITY

The Act exclusively deals with digital personal data within India, where the personal data is either:

[1] https://www.indiacode.nic.in/bitstream/123456789/22037/1/a2023-22.pdf

- Collected in a digital form or,
- Collected in a non digitized form and subsequently converted into digital form.

The DPDP Act has extra territorial application where in it applies to foreign entities supplying goods and services within the territory of India and process personal data in connection to such activities.

IMPLEMENTATION

The DPDP Act was enacted in the year 2023. However its implementation has been phased out into 3 stages.

PHASE I : Certain provisions of this Act such as setting up of a Data Protection Board was being made effective immediately after its enactment.

PHASE II : Provisions relating to consent managers are to be implemented with 12 months from the date of notification (ie: Nov 13, 2026)

PHASE III : Other substantive provisions of the DPDP Act are to be made effective within 10 months from the date of notification (ie; May 13, 2027).

KEY PROVISIONS OF THE DPDP ACT

DEFINITIONS

The DPDP Act 2023, provides a comprehensive and broad definitions under Section 2 of the Act.

- **DATA**

By virtue of Section 2 (h) “data” means a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human beings or by automated means.[2]

- **DIGITAL PERSONAL DATA**

[2] Digital Personal Data Protection Act, 2023, § 2(h), No. 22, Acts of Parliament, 2023 (India).

Section 2 (n) defines digital personal data as any personal data in digital form.[3]

- **PERSONAL DATA**

The DPDP Act defines 'personal data' broadly to include any data about an individual who is identifiable by or in relation to such data.

- **PERSON**

By virtue of Section 2(s), person included an

- Individual
- HUF
- A company
- Firm
- Association of persons/ body of individuals
- State
- Artificial juristic person

DATA FIDUCIARY

By virtue of Section 2 (i), a Data Fiduciary is an entity that determines the purpose and means of processing personal data. They bear the primary legal responsibility for safeguarding user data. It is therefore clear from the above definition that a person can be identified as a "data fiduciary" only if such person "***determines***" both, the purpose and means of processing personal data.[4]

---

[3] Digital Personal Data Protection Act, 2023, § 2(n), No.22, Acts of Parliament, 2023 (India)

[4] https://www.azbpartners.com/bank/data-fiduciary-versus-data-processor-an-identity-crisis/

Data fiduciaries must engage processors through valid contracts, ensure data deletion and cessation of processing upon consent withdrawal, and implement strict security measures. Fiduciaries remain accountable for processors' actions, including compliance with confidentiality, breach management, and restrictions on cross-border data transfers.[5]

OBLIGATIONS OF DATA FIDUCIARY

GROUNDS FOR PROCESSING PERSONAL DATA

By virtue of Section 4, a person may process the personal data of a Data Principal only in accordance with the provisions of this Act and for a lawful purpose,

(a) for which the Data Principal has given her consent; or

(b) for certain legitimate uses.[6]

NOTICE

Where a request is made to the Data Principal for obtaining consent, the Data Fiduciary shall give a notice informing them about:

- the personal data and the purpose for which it is to be processed.
- manner in which she may exercise her rights
- the manner in which she can make a complaint to the Board

CONSENT

The consent given by the Data Principal shall be free, specific, informed, unconditional and unambiguous with a clear affirmative action and shall signify an agreement to the processing of her personal data. The request for consent shall be presented to the Data Principal in clear

[5] https://media.licdn.com/dms/document/media/v2/D561FAQFGn_kBLqDINA/feedshare-document-url-metadata-scrapper-pdf/B56Zi7m4FjHMA0-/0/1755494192145?e=1785506400&v=beta&t=JN6I_mlF5eSCaXZe7sahGsinN2LyHoJQAc_IOkWGbMs

[6] Digital Personal Data Protection Act, 2023, § 4 No.22, Acts of Parliament, 2023 (India)

and plain language and the details of the Data Protection Officer shall also be provided along with the same.

This provision also allows the Data Principal to withdraw her consent and in such cases the Data Fiduciary must ensure that both the data fiduciary and its processors cease processing the data within a reasonable time unless legally required to continue.

LEGITIMATE USES

Section 7 of the Act lays down certain conditions under which the personal data of the Data Principal can be processed. The following are the conditions[7]:

- for the specified purpose for which the Data Principal has voluntarily provided her personal data to the Data Fiduciary.
- for the State and any of its instrumentalities to provide or issue any subsidy, benefit, service, certificate, licence or permit to the Data Principal, provided the consent of that personal has been obtained in prior and the data is available in digital form.
- for the performance by the State or any of its instrumentalities of any function or in the interest of sovereignty and integrity of India.
- compliance with any judgment or decree or order issued under any law for the time being in force in India
- responding to a medical emergency involving a threat to the life or immediate threat to the health of the Data Principal or any other individual;
- taking measures to provide medical treatment or health services to any individual during an epidemic, outbreak of disease
- taking measures to ensure safety of, or provide assistance or services to, any individual during any disaster, or any breakdown of public order.

[7] Digital Personal Data Protection Act, 2023, §7 No.22, Acts of Parliament, 2023 (India)

GENERAL OBLIAGTIONS

- The Data Fiduciary shall be responsible for compliance with the provisions of this Act and carry out the duties lay down in this Act.
- A Data Fiduciary may engage a Data Processor to process personal data on its behalf for any activity related to offering of goods or services to Data Principals only under a valid contract.
- The Data Fiduciary has a duty to implement appropriate technical and organisational measures to ensure effective implementation of the provisions of this Act.
- A Data Fiduciary shall protect personal data in its possession or under its control, by taking reasonable security safeguards to prevent personal data breach.
- In the event of a personal data breach, the Data Fiduciary shall give the Board and each affected Data Principal, intimation of such breach in such form and manner as may be prescribed.
- A Data Fiduciary shall publish, the contact information of a Data Protection Officer, or a person who is answerable on behalf of the Data Fiduciary.
- A Data Fiduciary shall establish an effective mechanism to redress the grievances of Data Principals.

PROCESSING OF PERSONAL DATA OF CHILDREN

Section 9 of this Act explicitly requires the Data Fiduciary to obtain the consent of the parents/guardian of the child or a person with disability before processing their personal data. Any personal data that is likely to be detrimental to the well being of the child shall not be processed by the Data Fiduciary and it also has an obligation to not undertake tracking or behavioural monitoring of children or targeted advertising directed at children.

SIGNIFICANT DATA FIDUCIARY

By virtue of Section 2 (z) of the Act, a Significant Data Fiduciary is any Data Fiduciary or class of Data Fiduciaries as may be notified by the Central Government under section 10. The Central

Government may notify any Data Fiduciary or class of Data Fiduciaries as Significant Data Fiduciary, on the basis of an assessment of such relevant factors as it may determine. The following factors are taken into consideration while determining a SDF:

- the volume and sensitivity of personal data processed
- risk to the rights of Data Principal
- potential impact on the sovereignty and integrity of India
- risk to electoral democracy
- security of the State; and
- public order

The SDF is empowered to appoint a Data Protection Officer who shall be responsible for representing the Significant Data Fiduciary under the provisions of this Act.

The SDF also appoints an independent data auditor to carry out data audit, who shall evaluate the compliance of the Significant Data Fiduciary in accordance with the provisions of this Act. They also undertake periodic Data Protection Impact Assessment and periodic audit.

DATA PRINCIPAL

Section 2 (j) lays down the definition of a Data Principle. “Data Principal” means the individual to whom the personal data relates and where such individual is[8]—

- a child, includes the parents or lawful guardian of such a child;
- a person with disability, includes her lawful guardian, acting on her behalf

The law empowers individuals with five core legal rights to control how their data is processed:

---

[8] Digital Personal Data Protection Act, 2023, §2(j) No.22, Acts of Parliament, 2023 (India)

RIGHT TO ACCESS INFORMATION ABOUT PERSONAL DATA

The Data Principal shall have the right to obtain from the Data Fiduciary any information regarding the processing of her persona data and the request for the same shall be given in the manner prescribed.[9]

The following information can be obtained from the Data Fiduciary:

- a summary of personal data which is being processed by such Data Fiduciary and the processing activities
- the identities of all other Data Fiduciaries and Data Processors with whom the personal data has been shared
- any other information related to the personal data of such Data Principal and its processing.

RIGHT TO CORRECTION, COMPLETION AND ERASURE

A Data Principal shall have the right to correction, completion, updating and erasure of her personal data for the processing of which she has previously given consent. A Data Fiduciary shall, upon receiving a request for correction, completion or updating from a Data Principal[10];

- correct the inaccurate or misleading personal data
- complete the incomplete personal data; and
- update the personal data

RIGHT OF GREIVANCE REDRESSAL

A Data Principal shall have the right to have readily available means of grievance redressal provided by a Data Fiduciary or Consent Manager in respect of any act or omission of such Data Fiduciary or Consent Manager regarding the performance of its obligations in relation to

[9] Digital Personal Data Protection Act, 2023, §11 No.22, Acts of Parliament, 2023 (India)

[10] Digital Personal Data Protection Act, 2023, §12 No.22, Acts of Parliament, 2023 (India)

her personal data. Before approaching the Board, the Data Principal shall have exhausted the opportunity of grievance redressal under the data fiduciary.

RIGHT TO NOMINATE

A Data Principal shall have the right to nominate, any other individual, who shall, in the event of death or incapacity of the Data Principal, exercise the rights of the Data Principal.[11] The expression "incapacity" means inability to exercise the rights of the Data Principal under the provisions of this Act or the rules made thereunder due to unsoundness of mind or infirmity of body.

DATA PROTECTION BOARD

The Data Protection Board of India (DPBI) is an independent adjudicatory body established under the DPDP Act 2023. Headquartered in New Delhi, it functions as a digital-first tribunal tasked with handling complaints, investigating personal data breaches, and enforcing India's data privacy regulations. Section 18 of the Act empowers the Central Government to setup Data Protection Board of India (DPBI).

The Board shall have the following salient features:

- a body corporate by the name aforesaid,
- perpetual succession and
- has a common seal,
- power to acquire, hold and dispose of property, both movable and immovable
- right to sue or be sued.

[11] Digital Personal Data Protection Act, 2023, §14 No.22, Acts of Parliament, 2023 (India)

COMPOSITION

The Board comprises of a Chairperson and other members as notified by the Central Government. The Central Govt. appoints the Chairperson and other members having specialised knowledge in or practical experience in the fields of data governance, administration or implementation of laws.

The Chairperson and members holds office for a period of 2 years and can also be re elected.

POWERS AND FUNCTIONS OF THE BOARD

The Board is expected to discharge the following powers and functions:

- direct any urgent remedial or mitigation measures in the event of a personal data breach, and to inquire into such personal data breach and impose penalty as provided in this Act
- inquire into breach and impose penalty as provided in this Act upon a complaint by the Data Principal or Data Fiduciary
- upon a complaint made by a Data Principal in respect of a breach in observance by a Consent Manager of its obligations in relation to her personal data, to inquire into such breach and impose penalty as provided in this Act
- issue such directions to such person, who shall be bound to comply with the same for the effective discharge of its functions under the provisions of this Act.

BANKS AS A DATA FIDUCIARY

The DPDP Rules 2025 introduces banks as a data fiduciary. Banks and other financial institutions are custodians of highly sensitive customer details such as KYC details, transaction history, credit histories etc. In the last one decade, most of these operations have been digitalised and with more digitalisation vulnerability to cyber and financial fraud increases.

The introduction of DPDP mandates on data minimisation, consent management, lawful processing, cross-border transfers, and breach response obligation, serving as an armour against financial fraud and data leaks.

Introduction of the DPDP Act in the finance sector has brought notable changes like:

Consent and Privacy Notice

Banks are made to redesign their digital onboarding to capture explicit, unbundled consent with clear multilingual privacy notices, ensuring customers understand how their data will be used.

Lawful processing of financial data

Every use of personal data like offers, underwriting, fraud detection, etc. must be tied to a lawful ground of processing. Shadow or silent data processing is prohibited, requiring stricter governance in analytics.

Data minimisation

Banks must collect only the minimum necessary data, rationalise fields, and delete records once the purpose or statutory retention period ends

Customer rights and grievance redressal

Customers gain enforceable rights to access, correct, erase, and withdraw consent. Banks must provide structured, time-bound mechanisms across branches, mobile apps or apps, and CRM systems, with seamless updates across interconnected platforms.

Third part accountability

Breaches must be reported to the Data Protection Board and affected customers within 72 hours. Banks remain accountable for breaches by outsourced making vendor risk management critical.

CONCLUSION

The DPDP Act 2023 marks a transformative shift in in India's data governance framework. Given the sensitive nature and large volume of customer data handled by banks, compliance with the Act is essential not only to meet regulatory obligations but also to safeguard customer rights. A strong data governance and privacy network will therefore be critical for banks in the evolving digital economy.