Images are generated using AI for academic purpose

www.ynzgroup.co.in

ENTER DPDP ACT & RULES: INDIA'S GLOBAL TRUST TOOLS

WEDNESDAY WISDOM

03.12.2025

© COPYRIGHT YNZ GROUP

India's comprehensive digital data privacy law **Digital Personal Data Protection Act, 2023 ("DPDP Act)** was passed in August 2023 but did not come into effect until 13th November 2025. With the notification of the **Digital Personal Data Protection Rules, 2025 on 13th November 2025, ("Rules")** the DPDP Act has formally come into force, establishing the first complete personal data protection framework in India. However, the actual implementation of the DPDP Act will decide the law's effectiveness in practice.

This article explores the core statutory framework, rights and obligations it creates, the enforcement body and the practical compliance implication, particularly for technology companies and businesses in e-commerce sector.

WHAT COMPANIES NEED TO KNOW AS INDIA'S DPDP ACT AND RULES TAKE EFFECT IN PHASES?

DPDP Act will only be applicable to processing of personal data in digital form or in non-digital form and digitised subsequently.

The DPDP Act and Rules now repeals section 43A of Information Technology Act, 2000 and The Information Technology (reasonable Security Practices And Procedures And Sensitive Personal Data Or Information) Rules, 2011 ("SPDI Rules"). However, since the implementation of the DPDP Act is being carried out in a phased manner, the provisions of the IT Act, 2000 and the SPDI Rules will continue to remain in force until the corresponding provisions of the DPDP Act are fully notified and implemented.

[1]The article reflects the general work of the author on the date of publication and the views expressed are personal. No reader should act on any statement contained herein without seeking detailed professional advice.

© COPYRIGHT YNZ GROUP

WHAT IS THE TIMELINE FOR THE DIGITAL PERSONAL DATA PROTECTION (DPDP) ACT, 2023 TO BE FULLY IMPLEMENTED, INCLUDING THE NOTIFICATION OF ITS RULES AND THE COMMENCEMENT OF ALL OPERATIONAL PROVISIONS?

The DPDP Act and Rules will be implemented phase wise in three phases.

First Phase: The provisions related to definitions and appointment of chairman for Data Protection Board under DPDP Rules are in force effective **13th November 2025** which means that the Data Protection Board, the primary body to deal with data protection related complaints will be formed and established before the other provisions of the DPDP Act comes into force.

Second Phase: After One (1) year from the Rules coming into force i.e., 13th November 2026, the provisions related to Consent Manager will come into force.

Third Phase: After 18 months on **13th May 2027**, all other provisions related to rights and obligations of Data Principal and Data Fiduciary and Data Processor will come into force.

WHAT DOES CONSENT MANAGER MEAN AND WHO CAN BE REGISTERED AS CONSENT MANAGER?

The DPDP Act introduces the concept of a **Consent Manager**, an entity required to be registered with Data Protection Board. For a company to qualify as a Consent Manager, it is required to be company incorporated and registered in India and shall have worth of not less than two crores rupees and must demonstrate adequate technical, operational, and financial capacity.

Consent Manager will be tasked with providing an interoperable platform for Data Principals to centrally grant, review, manage, or withdraw consent for the use of their personal data across different data fiduciaries, including banks, insurers, and online platforms. Consequently, individuals will be able to control how their information is accessed without having to approach each organisation separately.

WHAT ARE THE OBLIGATIONS OF A CONSENT MANAGER?

Consent Manager will have the following important obligations to:

© COPYRIGHT YNZ GROUP

- Enable users to give, manage, review, or withdraw consent for personal data processing. Personal data shared through the platform remains unreadable to the Consent Manager.
- Maintain clear records of all consent activities, accompanying notices, and data sharing with Data Fiduciaries. Records must be accessible to users, in machine-readable format, and retained for at least seven years.
- Maintain a website or app as the primary means of offering their services.
- Maintain **effective audit mechanisms** to monitor technical and organizational controls.

WHO ARE DEFINED AS 'DATA PRINCIPAL', 'DATA FIDUCIARY', AND 'DATA PROCESSOR' UNDER THE DPDP ACT, AND CAN YOU ILLUSTRATE THEIR ROLES WITH A PRACTICAL EXAMPLE.

Let us understand the concepts of Data Principal, Data Fiduciary and Data Processor (also explained in our previous article- link), through a common scenario in the digital economy:

ABC Bank has outsourced loan processing work of customer to PQR Services. When Ms. LMN approaches ABC Bank, her entire file is handed over to PQR Services. In this instance, the Bank's Customer Ms. LMN, to whom the personal data relates, is a Data Principal (Owner of personal data). ABC Bank, which determines the purpose and means of data processing (e.g., providing banking services), is the Data Fiduciary. Finally, PQR, which processes this data strictly on the ABC Bank's instructions and on its behalf, is the Data Processor.

WHAT ARE THE COMPLIANCE REQUIREMENTS THAT COMPANIES/ SERVICE PROVIDERS/ E-COMMERCE ENTITIES HAVE TO FULFILL AS DATA FIDUCIARIES?

Upon final phase implementation of DPDP Rules, the companies/ service providers/ e-commerce engaged in collecting or processing of digital personal data will require to comply with following provisions of DPDP Act as Data Fiduciary

- Provide Notice specifying purpose before or at the time of collecting Digital Personal Data
- Deletion of Data after purpose is fulfilled
- To keep the collected data in secure manner
- To notify the Data Principal and Data Protection Board in the event of Personal Data breach.
- Establish systems that enable Data Principals to exercise their statutory rights, including the rights to access, correct, erase personal data, and to nominate a representative.
- Maintain an effective grievance redressal mechanism for Data Principals.

© COPYRIGHT YNZ GROUP

WHAT SPECIFIC ELEMENTS MUST A DATA FIDUCIARY INCLUDE IN A VALID NOTICE ISSUED TO A DATA PRINCIPAL AS MANDATED UNDER THE DPDP ACT AND ITS RULES?

The notice given by Data Fiduciary shall—

1. be presented in a manner that is easy to understand independently, without relying on any other information the Data Fiduciary has provided or may provide.;
2. give, in clear and plain language, a fair account of the details necessary to enable the Data Principal to give specific and informed consent for the processing of her personal data, which shall include, at the minimum,
   a. an itemised description of such personal data; and
   b. the specified purpose or purposes of, and specific description of the goods or services to be provided or uses to be enabled by, such processing; and
3. give, the particular communication link for accessing the website or app, or both, of such Data Fiduciary, and a description of other means, if any, using which such Data Principal may
   a. withdraw her consent, with the ease of doing so being comparable to that with which such consent was given;
   b. exercise her rights under the Act; and
   c. make a complaint to the Board.

WHAT IS THE MANDATORY TIMELINE FOR E-COMMERCE ENTITIES TO DELETE PERSONAL DATA UNDER THE DPDP RULES?

Data collected by Data Fiduciary engaged in e-commerce related services or online gaming intermediary[2] or social media intermediary[3] shall be deleted after period of 3 years from the date on which the Data Principal last approached the Data Fiduciary for the performance of the specified purpose or exercise of her rights, or the commencement of the Digital Personal Data Protection Rules, 2025, whichever is latest.

[2] Having not less than 50 lakhs registered users in India
[3] Having not less than 2 crore registered users in India

© COPYRIGHT YNZ GROUP

IS THERE A PRESCRIBED TIMEFRAME WITHIN WHICH A DATA FIDUCIARY MUST NOTIFY THE DATA PRINCIPAL AND THE DATA PROTECTION BOARD IN THE EVENT OF A PERSONAL DATA BREACH UNDER THE DPDP ACT?

Upon becoming aware of data breach, Data Fiduciary to its best knowledge shall promptly notify the effected Data Principal in a clear and simple manner via their registered communication channel, providing:

- A description of the breach (nature, extent, timing).
- Likely consequences relevant to the Data Principal.
- Measures taken or underway to mitigate the risk.
- Safety steps the Data Principal may take to protect their interests.
- Contact details of a responsible person who can respond on behalf of the Data Fiduciary.

Data Fiduciary shall also intimate the Data Protection Board about Data Breach within 72 hours.

WHAT ARE THE SPECIAL OBLIGATIONS ON DATA FIDUCIARY FOR PROCESSING PERSONAL DATA OF CHILDREN AND A PERSON WITH DISABILITY

1. For Processing Personal Data of a Child Data Fiduciary shall
   a. Obtain verifiable parental consent before processing any child's personal data.
   b. Implement appropriate technical and organisational measures to ensure that such consent is valid, verifiable, and securely recorded.
   c. Verify that the individual claiming to be the parent is an adult (i.e., 18 years or older) and is identifiable if required for compliance.
   d. Confirm identity and age of the parent through:
      i. Reliable identity and age details already available with the Data Fiduciary; or
      ii. Identity and age details voluntarily provided by the individual; or
      iii. A virtual token mapped to such details, issued by an authorised entity.
2. For Processing Personal Data of a Person with Disability
   a. Obtain verifiable consent from the lawful guardian of the person with disability before processing their personal data.
   b. Exercise due diligence to confirm the lawful authority of the guardian, verifying that the individual is legally appointed as guardian by:
      i. A court of law, or
      ii. A designated authority, or
      iii. A local-level committee under applicable guardianship laws.
   c. Ensure the verification process is documented and traceable for legal compliance.

© COPYRIGHT YNZ GROUP

WHAT IMPLICATIONS DO THE RULES HAVE FOR TECHNOLOGY COMPANIES?

The phased implementation of the DPDP Act and Rules impose substantial obligations on technology providers. Key challenges include:

Expanded Liability Exposure

Technology companies acting as Data Fiduciaries or Processors can no longer disclaim responsibility for compliance. Their operational models require to incorporate statutory duties across:

- consent workflows,
- data retention mechanisms,
- cross-border transfer protocols, and
- breach management procedures.

Contractual Reconfiguration:

Technology companies as Data Fiduciaries will need to renegotiate existing agreements with their Data Processors, or establish new ones, to ensure compliance by implementing stringent protocols for the sharing, handling, and processing of users' data.

Multiple Regulators

Technology companies, including fintechs regulated by sectoral authorities such as the Reserve Bank of India, must navigate compliance with both the DPDP Act and sector-specific regulations. Until regulators streamline their respective regulatory guidance, the technology companies may face potential overregulation, requiring dual-regulated companies to adopt a more nuanced approach to align with differing requirements for data processing.

WHAT CAN BE THE KEY STRATEGIC IMPERATIVES SUGGESTIONS/ RECOMMENDATION FOR COMPANIES?

- Investing in Privacy-Enhancing Technologies such as differential privacy, homomorphic encryption, and federated learning to enable data-driven insights while minimizing privacy risks.
- Adopting Privacy by Design and Default by integrating privacy considerations into products, processes, and system architecture from inception, supported by cross-functional privacy reviews.
- Developing robust vendor governance through due diligence, contractual safeguards, monitoring, and audit rights to ensure accountability across the entire data processing supply chain.

© COPYRIGHT YNZ GROUP

INDIA'S STEP TOWARDS GLOBAL TRUST

The coming into force of the Digital Personal Data Protection Act, 2023 and the DPDP Rules, 2025 marks a landmark moment in India's digital regulatory evolution.

By embracing strong privacy practices, businesses can enhance brand reputation, build consumer trust, and differentiate themselves in the market.

For any feedback or response on this article, the authors can be reached on darshan.mundane@ynzgroup.co.in and shravani.joshi@ynzgroup.co.in

Author: Priya Shahdeo

Priya is a Manager-Corporate Legal at YNZ Legal. By qualification she has completed her Bachelor of Arts and Bachelor of Law from Bharati Vidyapeeth Deemed University.

Co-author: Atharva Amdekar

Atharva is an Associate at YNZ Legal. By qualification he is Bachelor of Commerce and Bachelor of Law from Mumbai University

© COPYRIGHT YNZ GROUP