

Demystifying Digital Personal Data Protection (DPDP) Act, 2023

Published on: 1st December 2025

Published by: Proton Technosoft (OPC) Private Limited

Applicability of this Act:

- Personal data in Digital or Digitized form
- Processing of Digital Personal data within India
- Processing of Digital Personal data outside of India, for services or goods provided to Data Principals within India

Rights of Data Principal:

- Access to self-personal data information.
- Correction and erasure of personal data.
- Grievance redressal.
- Nominate other Data Principal.

Duties of Data Principal:

- Do not impersonate identity of another Person
- Do not suppress material information to Data Fiduciary
- Do not register false grievance with Data Fiduciary

Prescribed Penalties:**₹ 250 Cr.**

Data Fiduciary:

- fails to safeguard digital personal data
- did not notify Data Protection Board and/or Data Principal for Data Breach
- fails to protect child related information safeguards

₹ 50 Cr.

Breach of any other provision of DPDP Act

₹ 10K

Data Principal fails to follow prescribed duties

Obligations of Data Fiduciary:**CONSENT:**

- Obtain consent from Data Principal for related Data Processing
- Provide option to Data Principal for revoking their earlier provided consent
- Disclose Data Principal's rights and process for related complaints before collection of Digital Personal Data
- Communicate the consent status to Data Processor within a reasonable time for their action

GRIEVANCE ADDRESSAL:

- Provide details of Data Protection Office (DPO) or another responsible person to address Data Principal's concerns – if any
- Grievance redressal system should be established.

PURPOSE, SAFEGUARD AND LAWFULNESS:

- Use the collected Digital Personal Data for Lawful purpose
- Ensure data's completeness, accuracy and consistency
- Ensure safeguards to protect digital personal data breach
- Data breach notification should be shared with Board and Data Principal's affected
- Retain Digital Personal Data until requested by Data Principal for erasure, and/or till required for providing services and/or goods to Data Principal and/or as prescribed by law.
- Do not undertake tracking or behavioral monitoring of children or targeted advertisement.

Additional Obligations of Significant Data Fiduciary:

- Appoint Data Protection Officer (DPO) in India
- Appoint Independent Data Auditor
- Periodic Data Protection Impact Assessment (DPIA)
- Periodic Audit against DPDP Act



Person?

Individual
Hindu Undivided Family (HUF)
Body of Individuals

The State
Artificial Juristic Person
A Company
A Firm

**Personal Data?**

Any data about an individual who is identifiable by or in relation to such data

**Data Fiduciary?**

Any person who alone or in conjunction with other person determines the purpose & means of processing of personal data.

**Digital Personal Data?**

Personal Data in Digital Form.

**Significant Data Fiduciary?**

Indian Central Govt. notified Data Fiduciary based on volume & sensitivity and risk to personal data processed, etc.

**Lawful Processing?**

Freely given, Informed, Unambiguous, verifiable consent for processing Children's digital personal data.

**Data Processor?**

Any person who processes personal data on behalf of a Data Fiduciary

**User Account?**

Online account registered with Data Fiduciary with which Data Principal can access services.

**Lawful Guardian?**

Guardian who is appointed by a court of law, or by a designated authority or by a local level committee



D e f i n i t i o n

(Rule #3) Notice Given By Data Fiduciary To Data Principal

Effective: 12 May 2027

- Independent in clear and plain language
- Include itemized description
- Give communication link to exercise their rights under the Act
- In English or any of the 22 languages specified in the Eighth Schedule of Indian Constitution

(Rule #4) Registration And Obligations Of Consent Manager

Effective: 12 Nov 2026

- Fulfills the condition for registration with Data Protection Board (DPB)
- Adhere to the conditions and obligations set-out in DPDP Act

(Rule #5) Processing Of Personal Data By State And Its Instrumentalities

Effective: 12 May 2027

The Government and its Instrumentalities (government bodies, agencies, and entities that execute its functions) are permitted to process a Data Principal's personal data when it is necessary for providing them with official government offerings.

(Rule #6) Reasonable Security Safeguards

Effective: 12 May 2027

- Data Fiduciary should take reasonable security safeguards for preventing personal data breach.
- Use of encryption, masking, hashing, virtual tokens, backup, BCP, access control, logging and monitoring are some examples.
- Contractual provisions with Data Processor for safeguard of Digital Personal Data
- Retention of Logs and Digital Personal Data for minimum of 1 year.

(Rule #7) Intimation Of Personal Data Breach

Effective: 12 May 2027

- In case of Digital Personal Data Breach Data Fiduciary should:
 - intimate the Data Principal and DPB about the same with description of breach, relevant consequences, measures implemented, and business contact information.
 - intimate the Data Protection Board (DPB) within 72 hours of their awareness of breach.



(Rule #8) Concrete, Mandatory Data Retention Timeline

Effective: 12 May 2027

- **Mandatory Erasure:** If the Data Principal has not engaged with Data Fiduciary within the **three (3) year** period, the data must be erased. *This is applicable on certain set of Data Fiduciary as mentioned in the note.*
- **Exclusions:** The three-year limit does not apply to data that is necessary for:
 - Enabling the Data Principal to access their user account.
 - Enabling access to any virtual tokens (e.g., in-game currency, loyalty points) issued by or on behalf of the Fiduciary.
 - Compliance with any other law
- At least **48 hours** before the three-year period is complete and the erasure process begins, the Data Fiduciary must inform the Data Principal.
- Retain Digital Personal Data, Transaction Logs and other relevant data for a minimum of **one (1) year** period or as required under applicable law(s).

Note: Large E-Commerce Entities (≥ 2 Crore registered users), Large Online Gaming Intermediaries (≥ 50 lakh registered users) and Large Social Media Intermediaries (≥ 2 Crore registered users)

(Rule #9) Contact information of person to answer questions about processing Effective: 12 May 2027

- Data Fiduciary should include contact details of Data Protection officer (DPO) and Data Principal rights on their Website, Application, and in communication to Data Principal.

(Rule #10) Verifiable consent for processing of personal data of child

Effective: 12 May 2027

- Parent's age (age ≥ 18 years) and identity verification is mandated for processing of Child's Digital Personal Data.
- Verifiable consent of Parent to be obtained before processing of Child's Digital Personal Data.

(Rule #11) Verifiable consent for processing of personal data of person with disability with Guardian

Effective: 12 May 2027

- Verifiable consent from lawful guardian of person with disability should be obtained.

Note: Disability covers for long term physical, mental, intellectual or sensory impairment, autism, cerebral palsy, mental retardation or a combination of any two or more of such conditions.



(Rule #12) Exemptions to processing of personal data of child

Effective: 12 May 2027

Clinical establishments, Mental health Institutions, Healthcare and Allied Professionals, Educational Institutions, and Childcare or Caregiving Establishments are exempted from obtaining **Verifiable Parental Consent**, and **Prohibitions on Tracking and Targeted Advertisements**, if they are processing the Child's digital personal data for:

- Healthcare and Treatment
- Education and Learning
- Caregiving Functions
- Real-time Location
- Safety Monitoring

(Rule #13) Additional obligations of Significant Data Fiduciary

Effective: 12 May 2027

- Once in every Twelve (12) months, carry out Data Privacy Impact Assessment (DPIA) and Audit w.r.t DPDP Act 2023 and DPDP Rules 2025.
- Carry out Due Diligence review for algorithmic software used for processing of Digital Personal Data.
- Personal data elements as notified by Central Government, should not be processed outside the territory of India.

(Rule #14) Rights of Data Principals

Effective: 12 May 2027

- Data Fiduciary must prominently publish on their website or application the **specific means** (email, web form, etc.) and **specific identifiers** (username, customer ID, etc.) for Data Principal to submit a request.
- Grievance addressal must be completed within **Ninety (90) days** of the complaint.

(Rule #15) Transfer of personal data outside the territory of India

Effective: 12 May 2027

- Personal data processed by a Data Fiduciary may be transferred outside the territory of India.

Note: The primary focus is on data access by foreign governments and their agents. The Central Government ensures that when data is transferred abroad, it is not unduly exposed to foreign governmental access or control without meeting specific Indian requirements.



(Rule #16) Exemption from Act for research, archiving or statistical purposes

Effective: 12 May 2027

- Provisions of DPDP Act does not apply to processing of digital personal data necessary for research, archiving or statistical purposes if:
 - Processing is done in lawful manner
 - Personal data is retained till required
 - Reasonable security safeguards are taken to protect it
 - Consent has been obtained by the Data Principal

(Rule #23) Calling for information from Fiduciary or intermediary

Effective: 12 May 2027

- The Central Government can ask Data Fiduciaries/Intermediaries to provide specific information for lawful purposes, including but not limited to protecting national sovereignty and integrity.



The DPDP Act is India's first comprehensive law for protecting digital personal data, mandating that Data Fiduciaries (entities processing data) can only process personal data for a lawful purpose after obtaining free, specific, informed, and unambiguous consent from the Data Principal (the individual). It also grants individuals rights, including the right to access, correct, or erase their personal data.

It imposes clear obligations on Data Fiduciaries, such as ensuring data accuracy, implementing reasonable security safeguards, and promptly notifying the Data Protection Board of India (DPBI) and affected individuals in case of a data breach. The DPBI is established as the regulatory authority to enforce the Act and impose significant penalties for non-compliance (up to ₹250 crores).

The Act and its Rules are being implemented in a structured, phased manner over 18 months to allow organizations time to adapt:

Phase 1 (Immediate - Nov 2025)

Establishment of the Data Protection Board of India (DPBI) and operationalization of initial definitions and administrative provisions.



Phase 2 (12 Months - Nov 2026)

Requirements for Consent Managers (entities to help individuals manage their permissions) and their registration/oversight become active.



Phase 3 (18 Months - May 2027)

Full operational compliance deadline for all core requirements, including consent notices, breach reporting, security, retention, and data principal rights management.



Reference for content:

1. DPDP Act 2023: <https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf>
2. DPDP Rules 2025: https://dpdpa.com/DPDP_Rules_2025_English_only.pdf





AUDIT

WHAT NEED BE DONE?

01

Data Privacy Assessment

Cover DPDP Act, CCPA, GDPR and other relevant data privacy regulatory compliance assessment.

02

Third Party Risk Management

Enhance your Risk discovery and addressal beyond organizational boundaries by covering qualified Third Parties into your Risk management program.

03

Data Flow Review

Data flow reviews allows organization to visually determine the areas of control coverage and where focus needs to improve,

04

Control Implementation Assistance

Project managing the control implementation ensure efficient control roll-out with reduced overlaps and consistent enforcement.

05

Internal Audit

Carry out Internal Audit related to DPDP Act and Rules to ensure compliance adherence to legal requirement.

06

Business Continuity Framework Implementation

Implement Business Continuity framework for ensuring availability of personal data and systems in secure and lawful manner.

07

Training and Awareness

Make your workforce more aware on Personal data protection through structure and tailor made training programs to meet the intent, purpose and process of your organization.

08

Cloud Security Assessment

Cloud security assessment to determine personal data processing, hosting & transmission; and mapping existing controls to DPDP Act/ Rules, and other Privacy regulations.

09

Application Risk Assessment

Application security Risk assessment allows for determining applicable Risks on personal data through the usage and exposure from Application Architecture standpoint.

10

Privacy Framework Development

Develop Privacy Framework related Policies, Processes and Procedures to ensure consistent roll-out of controls and to improve compliance posture on applicable regulations.

11

Control Maturity Review

Carry out thorough Control Maturity Review to assess the strength of controls in protecting the Personal Data against data breaches, and other eventualities.

12

Zero Trust Architecture Review and Implementation

Implement and Review (existing implementation) on Zero Trust architecture, demonstrating due diligence in protecting personal data.

Contact Us:

Parnika

+91 9555473700
parnika@protonts.in

Paras

+91 9036358082
paras@protonts.in

