DPDP Act 2023 & DPDP Rules 2025 and How to be Ready

- DPDP Act 2023 & DPDP Rules 2025 and How to be Ready
- Digital Personal Data Protection Act FAQ

DPDP Act 2023 & DPDP Rules 2025 and How to be Ready

> You can read the information below in over 15 languages! Simply use the translation tool in the top-left corner of the screen to select your preferred language, including □□□□□□□, □□□□□, □□□□□□□, □□□□□□, □□□□□, □□□□□□, □□□□□, □□□□□□□□, □□□□□□, □□□□□, □□□□□□, □□□□□□□□□□, □□□□□, □□□□□□, and اُردُو.

Table of Contents

- Why DPDPA is relevant for NPOs
- Coverage
- Definitions
- Obligation of Data Fiduciary
- Rights & Duties of Data Principal
- Legitimate uses and Exemptions/exceptions
- Penalties
- Being Ready (Compliance checklist)

Why DPDP Act is relevant for NPOs

- NPOs collect, store and process personal data for programming/service delivery, research, advocacy and donor reporting.

- Sources from which data collected: Beneficiary, Donor, Employee
- Examples of data collected by NGOs: Name, Address, Contact no, Age, ID proof, Photograph, Profession, Caste and Religion, Health or Income data etc
- Source of personal data: surveys, beneficiary records, meeting/workshop records
- The DPDP Act 2023 is a foundational data privacy law and provides a framework for the processing of digital personal data. This framework covers:
  1. Notice & lawful consent
  2. Purpose limitation
  3. Collection limitation/data minimization
  4. Retention limitation
  5. Data security
  6. Grievance redressal
  7. Accountability

Coverage of DPDP Act (DPDPA) & Implementation Schedule

Applicability

1. when Personal Data is collected online from Data Principals, and
2. when Personal Data is collected offline (non digital) and subsequently transferred to a digital form.

The Act also covers processing personal data outside of India if that processing is related to profiling people in India or offering goods and services to data principals in India.

Not Applicable

1. Personal data for personal or domestic purpose
2. Personal data made public e.g. blogging

Implementation Timelines

- DPDP Act notified in Aug 2023 and DPDP Rules notified in Nov 2025
- DPB and definition clauses effective from Nov 2025
- Registration and obligations of Consent Managers — Nov 2026
- Full implementation from May 2027

Definitions

- **Personal Data:** Any information about an individual who can be identified by or in relation to such data (Eg. name, age, address, email address, Aadhaar number, contact details, financial & medical data, biometric details, digital identifiers).
- **Digital Personal Data:** Personal Data in a digital format
- **Data Principal:** The individual to whom the personal data belongs, which includes the parents or legal guardians if the person is a child (less than 18 years of age) or person with disability. This Act is for personal data of individuals only.
- **Data Fiduciary:** Any person who alone or in collaboration with others determines the purpose and means (what data, security, retention) of processing Personal data. NPOs assume role of data fiduciaries.
- **Data Processor:** Any person who processes personal data on behalf of a Data Fiduciary under a valid contract, e.g., payroll, research agencies/data scientists, CRM service provider
- **Significant Data Fiduciary:** Central Government define SDF considering factors such as quantity and sensitivity of processed Personal Data, potential risks to the rights of Data Principals, the possible impact on India's sovereignty and integrity, risks to electoral democracy, state security and maintenance of public order. These include digital payment & fintech players, social media platforms, healthcare aggregators, insurance companies, telecommunication and ISP etc. They need to conduct periodic data protection impact assessment and audit.
- **Data Protection Board of India:** A statutory body to enforce compliance, adjudicate violations and impose penalties. The Board will operate digitally and shall have the power to conduct inquiries, issue directions, and ensure protection of rights of Data Principals.
- **Processing:** means a wholly/partly automated operation performed on digital personal data and includes operations such as collection, recording, organising, structuring, storage, adaptation, retrieval, use, alignment or combination, indexing, sharing,

disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction. Meaning is very wide.

- **Consent Manager:** A person registered with Data Protection Board of India that serves as a neutral point of contact to facilitate Data Principal to give, manage, review and withdraw consent. CM platform that is accessible, transparent, secure and interoperable. Not mandatory if compliance can be handled in-house.
- **Data Protection Officer (DPO):** An employee of an SDF organization that ensures internal compliance with the Act and serves as the designated point of contact for Data Principals and the Data Protection Board. Significant Data Fiduciaries must mandatorily appoint a DPO. POC intimation to CERT-In.
- **Personal Data Breach:** Any unauthorised or accidental access, disclosure, alteration, loss or destruction of personal Data that compromises its confidentiality, integrity, or availability.

2 Key Parts of Data Privacy Law i.e. DPDPA

1. **Privacy Notice:** by Data Fiduciary to data principal. The notice should provide information about data collection i.e. type of data being collected, for lawful purpose, access to data (user rights), process for withdrawing consent, procedure for grievance redressal, details of DPO/POC and how to file a complaint with the Data Protection Board. Language of notice (English or 22 languages in Eighth Schedule)
2. **Verifiable Consent:** by data principal to Data Fiduciary. Consent for collecting and processing data for specific lawful purpose should be free, specific, informed, unconditional and clear affirmative action (demonstrable), revocable.

Content of Notice

The notice should contain:

- Itemized notice: details what data and purpose for which personal data is collected

- Uses enabled by processing personal data
- A disclaimer on data protection and a description of measures taken to safeguard the data
- User rights and process to withdraw consent
- Details of grievance redressal mechanisms, including whom to contact and within what timelines
- The process to file a complaint with the Data Protection Board in case of unresolved grievances or misuse of data
- The website/app link/alternate means (such as physical address or phone number) through which Data Principal can withdraw consent and exercise rights i.e. accessing, correcting, or erasing data.

Obligation of Data Fiduciary

- Process personal data of DP for lawful purpose (not illegal), legitimate use and after consent of DP
- Clear notice — what data, why and for how long. Onus of proving notice and consent in a proceeding is on DF.
- Accurate and complete personal information of data principal — processed by data fiduciary or data processor on its behalf or shared with another data fiduciary
- Security of personal data to prevent data breach — access control to authorized persons, logs and monitoring system, backup and recovery, confidentiality, integrity and availability of personal data, appropriate contracts with external data processor. Stiff penalty to ensure safety for data breach (upto Rs.250 cr)
- Notify data breach: Data fiduciary notify to concerned Data Principals immediately and DPB (72 hours) regarding breach, consequences, measures to mitigate the risk, safety measures by data principal to handle the breach and contact details of data fiduciary. DPO/POC also inform Indian Computer Emergency Response Team (CERT-In website)
- Delete (erase) data no longer required (purpose limitation) or erase in case of withdrawal of consent whichever is earlier: Notice of erasure to Data Principal 48 hours before erasing the data. Processing logs, consent records retained for 1 year post erasure. Ensure data erasure if provided to Data Processor
- Erasure for e-commerce entity (2 crore users), gaming intermediary (50 lakhs users) and social media entity (2 cr users) — 3 years from day last approached or commencement of

DPDP Rules whichever is latest

- Publish contact details of DPO or person who answers to DP: to address issues relating to processing of Data Principal's personal data.
- Establish Grievance redressal mechanism on website and resolve within 90 days from complaint
- Cross border transfer permitted unless the geography restricted by Govt

Children's data / data of PWD

Verifiable consent through identified parent/lawful guardian.

- Not process data that causes harm to well being of child
- No tracking or behavioral monitoring of children (with exceptions), targeted advertising to children.
- Failure to report breach or non compliance with children data has stiff penalty

Rights & Duties of Data Principal

Rights

- Right to access information about personal data from Data Fiduciary (to be provided within 7 days): summary of personal data being processed, any third party with whom data shared and any other information regarding personal data under any law
- Right to withdraw consent for collection and processing of data, only prospectively
- Right to correction and erasure of personal data: Data Principal can approach Data Fiduciary to (a) correct incorrect/inaccurate data (b) complete incomplete data (c) update personal data (d) erase data unless retention required by law
- Right to nominate in case of death/incapacity of Data Principal
- Right to grievance redressal: first with Data Fiduciary and then with Data Protection Board

Duties

furnish only verifiably authentic information, not to impersonate another person while providing personal data for a specified purpose, not to register a false or frivolous grievance or complaint with a data fiduciary or the DPB etc. For any breach in such duties, the data principals may be penalized up to INR 10,000.

Legitimate Uses Without Consent

- Data Principal voluntarily provided personal data to a Data Fiduciary and has not conveyed non-consent for its utilisation.
- To state to provide or issue any subsidy, benefit, service, certificate, license, or permit where:
  - The Data Principal has already consented to such processing, or
  - The data is available in a government-maintained and notified database, either in digital form or digitised from a physical source.
- For the State or its agencies to perform any legal function for sovereignty, integrity, or security of the country.
- To comply with legal obligation requiring disclosure of Personal Data to the State or its agencies.
- To comply with a judgment, decree, or order, whether issued by an Indian court or related to civil or contractual claims from a foreign legal system.
- To respond to a medical emergency, where there is a threat to the life or health of the Data Principal or others.
- To provide medical treatment or health services during public health emergencies, such as disease outbreaks or epidemics.
- To assist/protect individuals during disasters or situations of public disorder as defined under the Disaster Management Act, 2005.
- For purpose of employment or safeguarding employer from loss or liability i.e. preventing corporate espionage, protecting trade secrets, intellectual property, classified information or service or benefit desired by DP (employee). Non employment related processing is not legitimate use.

Exemptions/Exceptions

- Act not to apply for processing of data for research, archiving or statistical purpose as per standards in Rules
  Standards: purpose limitation only, de-identify data, ensure data security and Govt guidelines
- Verifiable parental consent exception for DF in case of children:
  1. Clinics, hospitals, mental health centres and healthcare/allied healthcare professionals for ensuring health protection
  2. Educational institutions, creche, child day care centre for tracking and behavioral monitoring for educational purpose or safety of children
  3. DF for transport of children in educational institution, crèche or day-care centre for tracking location to ensure safety

Penalties

Levied for offences under DPDP by DPB considering: nature, gravity and duration of breach, type of personal data affected, repetitive nature of breach, realized gain or avoided loss due to breach etc.

- Security safeguards & data breach: upto Rs.250 cr
- Children personal data breach: upto Rs.200 cr
- Failure to notify DPB of data breach: upto Rs.150 cr
- General non compliance with Act & Rules: upto Rs.50 cr

No compensation to Data Principal if personal data gets compromised.

NGO Compliance Checklist

- Prepare policy on data privacy
- Map all personal data collected — beneficiaries, donors, volunteers, staff
- Prepare privacy notice and consent form in plain, local-language text
- Use technology to handle access, correction, and erasure requests from DP
- Identify a contact person for grievances and data protection queries
- Review contracts with vendors (payment gateways, CRMs, cloud hosts)
- Put basic security measures in place: access control, backups, encryption

- Prepare a data breach response plan with reporting timelines as per DPDP
- Train staff who handle personal data — compliance, program, finance

Digital Personal Data Protection Act FAQ

Contents

01	DPDPA Basics & Definitions	9 questions
02	Consent & Notice Requirements	7 questions
03	Rights of Data Principals	3 questions
04	Penalties & Enforcement	3 questions
05	Significant Data Fiduciaries	3 questions
06	Children’s Data Protection	3 questions
07	Data Breach & Security	2 questions
08	Cross-Border Data Transfer	2 questions
09	Data Retention & Erasure	3 questions
10	Data Protection Board of India	2 questions
11	Exemptions & Special Provisions	2 questions

12	Practical Scenarios	6 questions

01 Digital Personal Data Protection Act (DPDPA) Basics & Definitions

Q1 What is Digital Personal Data Protection Act 2023?

The Digital Personal Data Protection Act, 2023 is India's comprehensive data protection legislation that governs the processing of digital personal data. It establishes a legal framework for data collection, storage, and processing while empowering individuals with rights over their personal data.

KEY FEATURES

- Applies to digital personal data of an individual processed within India
- Has extra-territorial application for processing related to offering goods/services to Indian individuals
- Establishes the Data Protection Board of India for enforcement
- Prescribes penalties up to ₹250 crore for non-compliance

Q2 What is Personal Data under DPDPA?

Under Section 2(t), "Personal Data" (PD) means any data about an individual who is identifiable by or in relation to such data.

EXAMPLES INCLUDE

- Name, Aadhaar number, PAN, passport
- Email address, phone number, address
- Biometric data (fingerprints, facial recognition)
- Financial data (bank accounts, transactions)
- Health records and medical history
- Online identifiers (IP address, device ID)

> **NOTE** Unlike General Data Protection Regulation (GDPR), DPDPA does not have a separate category for "sensitive personal data" - all personal data is treated similarly.

Q3 What is a Data Fiduciary?

A Data Fiduciary (Section 2(i)) is any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data.

In simple terms: If your organization decides **WHY** and **HOW** personal data is collected and used, you are a Data Fiduciary.

> **EXAMPLE** An e-commerce company collecting customer data for order fulfillment is a Data Fiduciary. The cloud provider hosting that data is a Data Processor.

Q4 What are the key obligations of Data Fiduciaries under DPDPA?

All obligations under DPDPA and its consequent liability lie with the Data Fiduciary. In addition to the core obligation of ensuring that processing is only for lawful purposes with a valid Processing Bases, some of the other key obligations for Data Fiduciaries include:

- engaging Data Processors only through a valid contract;
- ensuring the accuracy, completeness, and consistency of PD processed where PD is likely to be used for making a decision concerning the Data Principal or where PD is disclosed to another Data Fiduciary;
- implementing appropriate technical and organizational measures for processing of PD in compliance with DPDPA;
- implementing reasonable security measures for preventing Personal Data Breach;
- notifying the DPB and Data Principals in case of a Personal Data Breach;
- erasing PD and causing engaged Data Processors to erase PD processed by them for the Data Fiduciary, upon withdrawal of consent if consent is the Processing Basis, or once the processing purposes are achieved, whichever is earlier, except where extended retention period is necessary for compliance with applicable law.

Q5 What is a Data Principal?

A Data Principal (Section 2(j)) is the individual to whom the personal data relates. Simply put: If it's YOUR data, YOU are the Data Principal.

SPECIAL PROVISIONS

- For children (under 18): Parent/lawful guardian acts as Data Principal
- For persons with disabilities with lawful guardian: The guardian acts as Data Principal

Q6 What is a Data Processor?

A Data Processor (Section 2(k)) is any person who processes personal data on behalf of a Data Fiduciary.

KEY DIFFERENCES FROM DATA FIDUCIARY

- Follows instructions from Data Fiduciary
- Does not determine purpose or means of processing
- Has contractual liability, not direct DPDPA liability

> **EXAMPLES** Cloud service providers, payroll processing companies, CRM service providers, data analytics vendors.

Q7 What does ‘Processing’ of personal data mean?

Under Section 2(x), "Processing" means any automated operation on digital personal data, including:

- Collection and recording
- Organisation and structuring
- Storage and adaptation
- Retrieval and use
- Sharing and disclosure
- Restriction and erasure

> **IMPORTANT** Even viewing personal data on a screen constitutes "processing" - the definition is extremely broad.

Q8 Is processing of publicly available PD regulated under DPDPA?

DPDPA excludes from coverage completely, all PD that is:

- made publicly available (such as through public profiles) by the data principal, or
- becomes public through the operation of law (such as public government records)

While this is the broadest public data exception globally, it does not mean that all “publicly available” PD stands unregulated. Before relying on “public” data, it may be advisable to make sure that the PD is indeed public and meets one of the two tests above.

Q9 What is the phased implementation timelines under DPDPA

Phase 1 (13 November 2025): Immediate enforcement of definitions, the constitution and digital functioning of the Data Protection Board of India, and general institutional provisions.

Phase 2 (13 November 2026): Activation of the Consent Manager Framework and opening of Consent Manager registrations.

Phase 3 (13 May 2027): Full substantive compliance goes live, including mandatory privacy notices, affirmative consent, data fiduciary obligations, Data Principal rights, children's data protections, and Board enforcement/penalties

02 Consent & Notice Requirements

Q1 What are the requirements for valid consent under DPDPA?

Under Section 4, valid consent must be:

- **Free:** Given voluntarily without coercion
- **Specific:** Related to a particular purpose

- **Informed:** Data Principal understands what they're consenting to
- **Unconditional:** Cannot be bundled with unrelated services
- **Unambiguous:** Clear affirmative action required

> **INVALID** Pre-ticked checkboxes, buried consent in T&C, forced bundling with unrelated services.

Q2 What must be included in Notice to a Data Principal?

Under Section 6 and Rule 3, Notice must include:

- Personal data being collected
- Purpose of processing
- How to exercise Data Principal rights
- How to make complaints to Data Protection Board

Language Requirements**:** Must be in English AND any of the 22 Scheduled languages as chosen by Data Principal.

Q3 Can consent be withdrawn?

Yes, under Section 4(6)-(7):

- Data Principal may withdraw consent at any time
- Withdrawal must be as easy as giving consent
- Data Fiduciary must provide clear withdrawal mechanism
- Upon withdrawal, processing must stop and data erased (unless legally required to retain)

> **GOOD PRACTICE** One-click unsubscribe, easily accessible settings, clear instructions, no penalties for withdrawal.

Q4 What are ‘Legitimate Uses’ for which consent is not required?

Section 5 provides Legitimate Uses without explicit consent:

- Voluntary provision: Data Principal provides for specified purpose
- State functions: Subsidies, benefits, services, certificates, licenses
- Legal obligations: Compliance with judgments or laws
- Medical emergencies: Threat to life/health
- Employment: Recruitment, verification, performance (with safeguards)
- Public interest: Mergers, acquisitions, restructuring

Q5 What are the compliances for processing PD to undertake research, archiving, and statistical activities?

Processing of PD for research, archiving, and statistical purposes is exempted under the DPDPA, provided it is (i) necessary for the mentioned purposes; (ii) not used to take any decision specific to the Data Principal; and (iii) carried out as per prescribed standards.

The following standards are prescribed under Second Schedule of DPDP Rules:

- processing is carried out in a lawful manner and be limited to such PD as is necessary for the underlying purposes;
- reasonable efforts are made to ensure the completeness, accuracy, and consistency of PD processed;
- retention is limited to durations that are needed to achieve the purposes, or for compliance with applicable laws;
- reasonable security safeguards are built in to prevent Personal Data Breach including one that involves Processor’s ecosystems;
- there is allocation of responsibility and accountability on persons who are Data Fiduciaries; and
- appropriate technical and organizational measures are implemented to effectively comply with the above stipulations.

Q6 What is a Consent Manager?

Consent Manager (Section 14) is a registered entity that enables Data Principals to:

- Give consent to multiple Data Fiduciaries through one platform
- Manage, modify, or withdraw consent easily
- Track and maintain records of all consents

Requirements (Rule 4): Must be registered with Data Protection Board, interoperable, no conflict of interest, maintain technical safeguards.

> **UNIQUE TO INDIA** Similar to Account Aggregators in financial services - no direct GDPR equivalent.

Q7 Is it mandatory for all organizations to appoint a consent manager?

No, it is not mandatory for all Data Fiduciaries to appoint a consent manager.

03 Rights of Data Principals

Q1 What are the rights of Data Principal under DPDPA?

Under Section 11, Data Principals have:

- Right to Access: Know what data is being processed
- Right to Correction: Correct inaccurate data
- Right to Erasure: Request deletion of data
- Right to Grievance Redressal: Complain to Data Fiduciary
- Right to Nominate: Designate someone to act on their behalf (Section 12)

> **NOTE** Unlike GDPR, DPDPA does NOT include right to data portability.

Q2 How long does a Data Fiduciary need to respond to a data access request?

Under Rule 14, Data Fiduciaries must respond within 7 days of receiving a valid request.

The response must include:

- Summary of personal data processed

- Processing purposes
- Categories of data shared with third parties

Q3 What are the duties of Data Principals?

Under Section 13, Data Principals must:

- Provide authentic information when exercising rights
- Not file false or frivolous complaints
- Not impersonate another person while providing data
- Not suppress material information

> **PENALTY** Up to ₹10,000 for false complaints or frivolous applications.

04 Penalties & Enforcement

Q1 What are the penalties for non compliance under DPDPA?

Under Section 33 and The Schedule:

MAXIMUM PENALTY	VIOLATION
₹250 Crore	Failure to take reasonable security safeguards leading to data breach
₹200 Crore	Failure to notify Board and Data Principal of breach
₹150 Crore	Non-compliance with children's data provisions
₹50 Crore	Other violations (per instance)
₹10,000	False complaints by Data Principals

> **KEY POINT** These are maximum caps - actual penalty depends on nature, gravity, and circumstances of breach.

Q2 What factors are considered while imposing penalties?

The Board considers:

- Nature, gravity, and duration of breach
- Type of personal data affected
- Repetitive nature of breach
- Number of Data Principals affected
- Actions taken to mitigate effects
- Whether intentional or negligent
- Compliance history of the entity

Q3 Is there criminal liability under DPDPA?

No. Unlike earlier drafts (2019), DPDPA 2023 does NOT prescribe criminal penalties.

Consequences are:

- Monetary penalties only
- Directions from Data Protection Board
- Possible blocking of services in extreme cases

> **NOTE** This was a significant change from earlier drafts which included imprisonment provisions.

05 Significant Data Fiduciaries

Q1 What is a Significant Data Fiduciary?

A Significant Data Fiduciary is a Data Fiduciary notified by the Central Government based on:

- Volume and sensitivity of personal data processed
- Risk of harm to Data Principals
- Potential impact on sovereignty, public order, security

- Use of new technologies for processing

Q2 What additional obligations apply to SDFs?

Under Section 10 and Rule 13, SDFs must:

- Appoint a DPO: Based in India, point of contact for Board
- Appoint Independent Data Auditor: Evaluate compliance
- Conduct DPIA: Before high-risk processing
- Periodic Audits: Regular compliance reviews
- Maintain records: For 7 years
- Publish DPO contact: Business contact information

Q3 What is Data Protection Impact Assessment (DPIA)?

A DPIA is an assessment conducted before processing activities that may pose significant risk. It should assess:

- Nature, scope, context of processing
- Risks to Data Principal rights
- Mitigation measures
- Proportionality and necessity

> **TIP** Document DPIAs thoroughly - they're evidence of compliance and due diligence.

06 Children’s Data Protection

Q1 How does DPDPA define a “child”?

Under Section 2(f), a "Child" means an individual who has not completed **eighteen years of age**.

> **GDPR COMPARISON** GDPR defines child as under 16 (with flexibility down to 13). India's uniform 18-year threshold is more conservative.

Q2 What special protections exist for children’s data?

Under Section 9:

- Verifiable parental consent: Must obtain before processing
- No behavioral monitoring: Tracking children is prohibited
- No targeted advertising: Cannot target ads at children
- No harmful processing: Processing likely to cause detrimental effect on child's well-being is prohibited

> **PENALTY** Up to ₹150 Crore for non-compliance with children's data provisions.

Q3 Are there exemptions for children’s data processing?

Yes, Rule 12 provides exemptions from verifiable consent for:

- Healthcare services for children
- Educational institutions
- Child safety and protection services
- Other classes as notified by Government

07 Data Breach & Security

Q1 What are the data breach requirements under DPDPA?

Under Section 8(6) and Rule 7:

WHO TO NOTIFY

- Data Protection Board of India
- Affected Data Principals

Timeline: Within 72 hours of becoming aware of breach

Contents: Nature of breach, data affected, consequences, remediation measures, DPO contact

PENALTY Up to ₹200 Crore for failure to notify breach.

Q2 What security safeguards are required?

Under Section 8(4) and Rule 6, Data Fiduciaries must implement **reasonable security safeguards**:

TECHNICAL MEASURES

- Encryption of data at rest and in transit
- Access controls and authentication
- Regular security testing
- Incident detection systems

ORGANIZATIONAL MEASURES

- Security policies and procedures
- Employee training
- Vendor management
- Incident response plans

08 Cross-Border Data Transfer

Q1 Can personal data be transferred outside India?

Yes, with conditions. Under Section 16 and Rule 15:

- Default: Transfer permitted to all countries
- Negative list: Government may notify restricted countries
- Restricted countries: Transfer prohibited unless specific approval

GDPR COMPARISON DPDPA takes permissive approach with blacklist; GDPR takes restrictive approach with whitelist (adequacy decisions).

Q2 What is data localisation under DPDPA?

DPDPA does NOT mandate blanket data localization. However:

- Government may notify countries where transfer is restricted
- Sectoral regulations (RBI, SEBI) may require localization for specific data types
- Critical personal data localization may be prescribed separately

09 Data Retention & Erasure

Q1 With respect to retention and erasure, what are the specific stipulations under DPDPA?

PD must be erased once the specified purpose is no longer being served or upon withdrawal of consent. Retention beyond the specified period is permitted only if it is required for compliance with applicable laws, and/or necessary for dispute resolution or regulatory investigations

Q2 Is the 1-year retention period mandatory for all organizations? What happens when different retention timelines are mandated under other laws?

Rule 8(3) of DPDP Rules obligate every Data Fiduciary and its Processors to retain PD processed along with associated traffic data and processing logs for a minimum period of 1 (one) year from the date of processing for the purposes mentioned in the Seventh Schedule of DPDP Rules i.e., use by the state or any of its instrumentalities for sovereignty, security, and integrity of India, or for performance of any function under law as directed by authorized person under such law, or for aiding state’s assessment for SDF notification by MeitY. After this duration, Data Fiduciary and its Processors must erase PD and its associated details unless prolonged retention is required under applicable laws.

Hence, the 1-year retention is mandatory for all organizations. Where another applicable law (or the Third Schedule of DPDP Rules) requires longer retention, such longer period will prevail over the minimum 1 year duration.

Q3 What is the mandatory retention requirement under Third Schedule of DPDP Rules?

Section 8(7) of DPDPA obligates every Data Fiduciary to erase PD unless retention is required for compliance with applicable law, either upon withdrawal of consent by the Data Principal, or as soon as it is reasonable to assume that the specific purpose is no longer served, whichever is earlier

Elaborating on when it is reasonable to assume that the specific purpose is no longer served, Section 8(8) of DPDPA states that such assumption is viable when the Data Principal has not approached the Data Fiduciary for performance of the specific purpose and has not exercised any rights in relation to such processing for the prescribed durations as notified for different classes of Data Fiduciaries (**Disengagement Criteria**).

Rules 8(1) and (2) read with Third Schedule of DPDP Rules provide the Disengagement Criteria for certain kinds of Data Fiduciaries in relation to identified purposes and the corresponding retention period therein, after the expiry of which such Data Fiduciaries must assume disengagement and proceed with erasure by providing a 48 (forty-eight) hours' notice to the concerned Data Principal as a confirmatory exercise before deletion, unless prolonged retention is required due to other applicable law. The covered Data Fiduciaries, identified purposes, and retention periods under Third Schedule are as follows:

- Covered Data Fiduciaries are e-commerce entities and significant social media intermediaries with minimum 20 (twenty) million, and online gaming intermediaries with minimum 5 (five) million registered users in India;
- Identified purposes are for enabling the user's access to their account or to any virtual token that is issued by or on behalf of the Data Fiduciary and is stored on the platform of the covered Data Fiduciaries and can be used to get money, goods or services; and
- PD that is required for the identified purposes must be retained for 3 (three) years from the date of commencement of DPDPA or the date on which the user last reached out to the covered Data Fiduciaries for the identified purposes, whichever is latest.

10 Data Protection Board of India

Q1 What is Data Protection Board of India (DPBI)?

The DPBI is the regulatory body established under Section 18 to enforce DPDPA.

KEY FEATURES

- Digital by design - functions as "digital office"
- Composed of Chairperson and Members
- Independent in exercising powers

POWERS

- Receive and handle complaints
- Conduct inquiries
- Impose penalties up to ₹250 crore
- Issue directions to Data Fiduciaries
- Register Consent Managers

Q2 How can Board orders be appealed?

Under Section 29:

- Appeals lie to Telecom Disputes Settlement and Appellate Tribunal (TDSAT)
- Must file within 60 days (extendable by 60 days)
- TDSAT may confirm, modify, or set aside Board's order
- Further appeal to Supreme Court on questions of law only

11 Exemptions & Special Provisions

Q1 What exemptions are available under DPDPA?

Under Section 17, exemptions include processing for:

- National security: Sovereignty, integrity, security of India
- Public order: Prevention of offenses

- Legal proceedings: Enforcement of legal rights/claims
- Research/archiving: Statistical, research purposes (with safeguards)
- Startups: Notified startups may get relaxations

Q2 What are the exclusions to scope of application of DPDPA?

Under Section 3, DPDPA does NOT apply to:

- Personal data processed by individuals for personal or domestic purposes
- Personal data made publicly available by Data Principal
- Data required by law to be made public

> **EXAMPLE** Your personal phone contacts or family photos are not covered by DPDPA.

12 Practical Scenarios

Q1 How should organisations update their privacy policies for DPDPA?

Privacy policies should be updated to include:

- Clear statement of data collected and purposes
- Data Principal rights under DPDPA
- Consent withdrawal mechanism
- Grievance redressal process
- DPO contact information (if SDF)
- Data retention periods
- Cross-border transfer information
- Complaint mechanism to Data Protection Board

Q2 What records should organisations maintain for compliance under DPDPA?

Organizations should maintain:

- Consent records: When, how, what consent was obtained
- Data inventory: What personal data is processed and why
- Data Principal requests: Access, correction, erasure requests
- Breach records: Incidents and response actions
- Vendor contracts: Data processing agreements
- Training records: Employee awareness programs
- DPIA records: For SDFs
- Audit reports: Internal and external compliance reviews

> **RETENTION** SDFs must maintain records for 7 years per Rule 13.

Q3 How does DPDPA apply to employee data?

Under Section 5(b) and Rule 22, employee data processing is a **Legitimate Use** for:

- Recruitment and onboarding
- Attendance verification
- Performance assessment
- Salary processing
- Termination procedures

Q4 What is the relationship between DPDPA and Information Technology Act 2000?

DPDPA supplements IT Act. Key interactions:

- **Section 43A (IT Act):** Compensation provisions amended
- **Section 72A (IT Act):** Breach of confidentiality provisions continue
- **IT Rules 2011 (SPDI):** Effectively superseded by DPDPA
- **Section 69A (Blocking):** Continues independently

>

KEY POINT Section 38 establishes DPDPA supplements and doesn't derogate from other laws unless explicitly stated.

Q6 Who is responsible for collecting consent when PD is collected by the Processor for the Data Fiduciary?

All obligations under DPDPA apply to Data Fiduciaries, and they are obligated to ensure that their engaged Processors remain compliant with DPDPA. Where a Data Fiduciary engages a Processor to directly collect PD from Data Principal such as collecting feedback of Data Principals through surveys and market studies, the Data Fiduciary must provide its Notice for Consent and obligate the Processor to obtain DPDPA compliant consent before collecting PD. Where Data Principal refuses to signify their consent, the Processor should not collect any PD, unless the Data Fiduciary has permitted collection on any other permissible Processing Bases.