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

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 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