edgeGRC

Guide India

India DPDP: organisation readiness guide

What the Digital Personal Data Protection Act, 2023 and the DPDP Rules, 2025 expect from organisations, and how to prepare a programme before the main obligations apply.

Last reviewed: 27 November 2026

General information only. Not legal advice, a legal opinion or a certification of compliance.

1 At a glance

India's Digital Personal Data Protection Act, 2023 (the DPDP Act) sets the rules for processing digital personal data. The Digital Personal Data Protection Rules, 2025 (the DPDP Rules), notified in November 2025, fill in the operational detail and bring the Act into force in phases.

Phase	What applies
On notification (November 2025)	Definitions and the provisions that set up the Data Protection Board of India and how it works.
12 months after notification	The framework for registering Consent Managers.
18 months after notification (May 2027)	The substantive obligations for organisations: notices, consent, security safeguards, breach reporting, retention and erasure, children's data, rights of individuals, Significant Data Fiduciary duties and the Board's penalty powers.

Check the exact dates

Commentators cite slightly different notification dates. Rely on the Gazette notification of the DPDP Rules (G.S.R. 846(E)) and MeitY's releases for the exact commencement of each provision.

2 Who the law applies to

The Act applies to the processing of **digital personal data** within India, whether it was collected in digital form or collected offline and later digitised. It also applies to processing outside India when it is connected with offering goods or services to individuals in India.

It does not apply to personal data processed by an individual for purely personal or domestic purposes, or to personal data that the individual concerned (or someone under a legal obligation) has made publicly available.

Key roles

Role	Meaning
Data Principal	The individual the personal data relates to. For a child, this includes the parent or lawful guardian; for a person with a disability, their lawful guardian.
Data Fiduciary	The organisation that decides the purpose and means of processing. Most obligations sit here.
Data Processor	An organisation that processes personal data on behalf of a Data Fiduciary, under a valid contract.

Role	Meaning
Significant Data Fiduciary (SDF)	A Data Fiduciary, or class of them, that the Government designates based on factors such as the volume and sensitivity of data and the risk to individuals. SDFs carry additional obligations.
Consent Manager	An entity registered with the Board that lets individuals give, manage, review and withdraw consent through an accessible platform.
Data Protection Board of India	The body that inquires into breaches of the Act, directs remedial measures and imposes penalties.

3 Grounds for processing

Personal data may be processed only for a lawful purpose and on one of two grounds:

- **Consent.** Consent must be free, specific, informed, unconditional and unambiguous, given by a clear affirmative action, and limited to the personal data necessary for the specified purpose. It must be as easy to withdraw as it was to give. After withdrawal, processing must stop within a reasonable time, unless another legal ground applies.
- **Certain legitimate uses.** The Act lists specific situations where consent is not needed. Examples include data an individual voluntarily provides for a specified purpose without indicating objection, compliance with a law or court order, responding to medical emergencies, and certain employment-related purposes.

Notices

When consent is the ground, the request for consent must come with a notice. The notice should stand on its own and be clear and plain. Under the Rules, it should at least:

- give an itemised description of the personal data and the specified purpose, and describe the goods, services or uses it enables;
- explain how consent can be withdrawn, with the process comparable in ease to giving consent;
- explain how individuals can exercise their rights and how they can complain to the Board.

Individuals can ask for the notice in English or in any language listed in the Eighth Schedule to the Constitution.

4 Children and persons with disabilities

Under the Act, a **child is anyone under 18**. Before processing a child's personal data, a Data Fiduciary must obtain **verifiable consent** of the parent or lawful guardian. The Rules describe how a Data Fiduciary can check that the person consenting is an identifiable adult. The same applies to a person with a disability who has a lawful guardian.

Data Fiduciaries must not process children's data in ways likely to cause a detrimental effect on a child's well-being. They also must not undertake tracking, behavioural monitoring or targeted advertising

directed at children. The Rules set out limited classes of Data Fiduciaries and purposes that are exempt from some of these conditions.

5 Rights and duties of individuals

Right	What it involves
Access to information	A summary of the personal data being processed and the processing activities, and the identities of other Data Fiduciaries and Processors it has been shared with.
Correction and erasure	Correction, completion, updating and erasure of personal data, subject to legal retention requirements.
Grievance redressal	A readily available way to raise grievances with the Data Fiduciary, which must be used before approaching the Board.
Nomination	Nominating another person to exercise these rights in the event of death or incapacity.

Data Fiduciaries must publish how individuals can make these requests and set a response period. Under the Rules, grievances must be answered within a reasonable period, not exceeding 90 days. Individuals also have duties under the Act, for example not to file false or frivolous grievances.

6 Security safeguards and breach reporting

A Data Fiduciary must protect personal data in its possession or control, including data processed by its Processors, through reasonable security safeguards. The Rules describe minimum measures, including:

- appropriate data security measures such as encryption, obfuscation, masking or virtual tokens;
- access control over computer resources;
- visibility of access through logs, monitoring and review, so unauthorised access can be detected and investigated;
- measures for continued processing after a compromise, such as backups;
- retaining logs and related personal data for **one year** for detection and investigation, unless another law requires otherwise;
- contracts with Processors that require reasonable security safeguards.

Personal data breaches

On becoming aware of a personal data breach, the Data Fiduciary must:

1. **Inform each affected individual without delay**, in plain language. Explain what happened, the likely consequences, the mitigation measures taken, the safety steps the individual can take, and who to contact.
2. **Inform the Board without delay** with an initial description of the breach.

3 **Send the Board a detailed report within 72 hours** of becoming aware, or a longer period if the Board allows it on request. It should cover the facts, the cause, the mitigation, any findings about the person responsible, the remedial measures and the reports sent to individuals.

7 Retention and erasure

Personal data must be erased when the individual withdraws consent or when the specified purpose is no longer being served, whichever is earlier, unless a law requires it to be kept. A Data Processor must also erase data the Data Fiduciary made available to it.

- For certain large classes of Data Fiduciaries listed in the Rules, the purpose is treated as no longer served if the individual has not engaged with them for a set period. These are e-commerce entities, online gaming intermediaries and social media intermediaries above specified user thresholds, and the period is generally three years.
- Under the Rules, individuals must generally be told at least **48 hours before** their data is erased on this basis, so they can log in or otherwise engage.

8 Significant Data Fiduciaries

If your organisation is designated as an SDF, the following additional obligations apply:

- appoint a **Data Protection Officer** based in India, who represents the SDF and answers to its board or similar governing body;
- appoint an **independent data auditor**;
- carry out a **Data Protection Impact Assessment and an audit** periodically (once every twelve months under the Rules) and report significant observations to the Board;
- exercise due diligence that algorithmic software used to process personal data does not pose a risk to individuals' rights;
- follow any measures the Government specifies, which may restrict certain personal data from leaving India.

9 Transfers outside India

The Act generally permits transfers outside India. The Government may restrict transfers to countries or territories it notifies. The Rules allow the Government to set requirements for making personal data available to foreign States or their agencies. Sector-specific laws that impose stricter localisation continue to apply.

10 Penalties

The Board can impose monetary penalties after an inquiry, taking into account factors such as the nature, gravity and duration of the breach. The maximum amounts in the Schedule to the Act are:

Breach	Penalty up to
Failure to take reasonable security safeguards to prevent a personal data breach	₹250 crore
Failure to notify the Board or affected individuals of a personal data breach	₹200 crore
Breach of additional obligations relating to children	₹200 crore
Breach of additional obligations of a Significant Data Fiduciary	₹150 crore
Breach of any other provision of the Act or Rules	₹50 crore
Breach of duties by an individual (Data Principal)	₹10,000

11 Readiness checklist

A practical order of work for the period before the main obligations apply:

Governance

- [ ] Name an accountable owner for DPDP compliance and agree how decisions reach senior management.
- [ ] Assess whether your organisation could be designated a Significant Data Fiduciary, and plan for a DPO, an independent auditor and annual assessments if so.
- [ ] Set a budget and timeline that ends before the 18-month deadline, with time for testing.

Know your data

- [ ] Build a record of each processing activity: the personal data, purpose, ground (consent or legitimate use), systems, Processors, transfers and retention.
- [ ] Identify children's data and data of persons with disabilities, and how age or guardianship is established.
- [ ] List every Data Processor and review contracts for security and erasure terms.

Notices, consent and rights

- [ ] Rewrite notices to meet the Rules: itemised data, specified purpose, how to withdraw, how to exercise rights and complain.
- [ ] Make withdrawal as easy as giving consent, and make sure withdrawal stops processing in practice.
- [ ] Publish the contact route for rights requests and grievances, and set internal response targets within the 90-day limit.

Security, breach and retention

- [ ] Map the minimum security measures in the Rules to your current controls, and close gaps (for example, logging and one-year log retention).

- [ ] Update the incident response plan for notifying individuals without delay and the Board within 72 hours, and rehearse it.
- [ ] Set retention periods per purpose, with an erasure process and the 48-hour advance notice where it applies.

Evidence

- [ ] Keep evidence of each decision: assessments, approvals, policies, training and test results, so you can show the Board what you did and why.

12 Official sources

- The Digital Personal Data Protection Act, 2023: Ministry of Electronics and Information Technology (MeitY), meity.gov.in
- The Digital Personal Data Protection Rules, 2025, G.S.R. 846(E): Gazette of India, egazette.gov.in, and MeitY
- Press Information Bureau release on the notification of the DPDP Rules (November 2025): pib.gov.in

---

About this guide

This guide summarises publicly available legislation and regulator guidance in our own words, as of the review date above. Laws, rules and regulator guidance change; always check the current official text and obtain advice appropriate to your organisation's circumstances.

EdgeGRC and Cyber Intelligence Private Limited is an Indian technology company focused on developing software platforms for enterprise privacy management and AI governance. Questions about this guide: **info@edgegrc.com** · edgegrc.com