DPDP Compliance Is No Longer Optional: What Every Business and Organisation Needs to Know Before the 2027 Deadline

India's data-protection regime has now moved from legislation to implementation. The Digital Personal Data Protection Act, 2023 ("DPDP Act"), together with the Digital Personal Data Protection Rules, 2025 ("DPDP Rules"), creates a comprehensive compliance framework for organisations that collect, store, use, share or otherwise process digital personal data.

DPDP compliance is not limited to technology companies, large corporations or online platforms. Any company, LLP, partnership firm, startup, hospital, school, educational institution, e-commerce business, service provider, employer, professional organisation or other entity processing digital personal data may fall within the framework, subject to the statutory exemptions.

This includes something as routine as maintaining customer names and mobile numbers in software, storing employee records electronically, collecting Aadhaar or PAN copies, maintaining subscriber databases, using CRM tools, operating websites or mobile applications, recording CCTV footage digitally, or sharing personal data with payroll processors, cloud service providers or other vendors.

The Act applies to digital personal data processed within India, including data initially collected in physical form and subsequently digitised. It may also apply to processing outside India where such processing relates to the offering of goods or services to individuals in India.

What is the compliance deadline?

This is perhaps the most important question for businesses today.

The Central Government notified the phased commencement of the DPDP Act and the final DPDP Rules in November 2025. While certain institutional and procedural provisions have already come into force, the principal substantive obligations relating to collection, consent, notices, security, data breaches, children's data, rights of individuals and general obligations of Data Fiduciaries are scheduled to come into force eighteen months from publication of the notification.

Accordingly, the broad implementation timeline is:

14 November 2025: Certain preliminary, institutional and procedural provisions came into force.

14 November 2026: The provisions relating principally to registration of Consent Managers become operational.

14 May 2027: The principal compliance obligations under the DPDP framework become enforceable.

Thus, 14 May 2027 is the critical compliance date for most organisations.

However, businesses should not treat this as a reason to wait until 2027. Effective compliance requires identification of data flows, review of existing consent mechanisms, preparation of privacy notices, vendor-contract restructuring, establishment of grievance mechanisms, retention policies, security safeguards and breach-response procedures. For organisations holding substantial volumes of customer, employee, subscriber or user data, this exercise can take several months.

What does a business actually have to do?

Compliance is not achieved merely by uploading a privacy policy on a website. The organisation must examine the entire lifecycle of personal data from collection to deletion.

A practical DPDP compliance exercise should ordinarily cover the following areas:

1. Data Mapping and Data Inventory

An organisation should first identify:

- What personal data it collects;
- From whom it is collected;
- Why it is collected;
- Where it is stored;
- Who has access to it;
- With whom it is shared;
- How long it is retained; and
- Whether it is transferred outside India.

Without a proper data inventory, meaningful compliance is practically impossible.

2. Identify the Legal Basis for Processing

Personal data cannot simply be collected because it may be useful in the future. Processing must be for a lawful purpose and ordinarily based upon either valid consent or one of the recognised legitimate uses under the Act. Consent must be free, specific, informed, unconditional and unambiguous, involving clear affirmative action. Further, withdrawing consent must be as easy as giving it.

3. Issue Clear Privacy Notices

Before or along with seeking consent, the Data Principal must be adequately informed about the personal data being collected, the purpose of processing, the manner in which rights may be exercised and the grievance mechanism.

The DPDP Rules require notices to be clear, understandable and capable of being read independently of other information. The notice must contain an itemised description of the personal data involved and specify the purpose for which it will be processed.

Therefore, organisations should review:

- Website privacy policies;
- Mobile-app privacy notices;
- Customer onboarding forms;
- Employee privacy notices;
- Consent forms;
- Cookie mechanisms;
- Vendor and channel-partner forms; and
- Existing customer databases collected before implementation.

4. Maintain Reasonable Security Safeguards

A major component of compliance is actual data security. Depending upon the circumstances, organisations may have to implement measures such as encryption, masking, access controls, activity logs, monitoring systems, backups, incident-response procedures and contractual safeguards with Data Processors.

The Rules specifically contemplate technical and organisational measures, control over access to computer resources, logging and monitoring, backup arrangements and appropriate provisions in contracts entered into with Data Processors.

5. Prepare a Personal Data Breach Response Mechanism

A data breach cannot be dealt with casually after it occurs. Organisations should have a documented incident-response plan identifying who will investigate, contain, document and report a breach.

Under the notified Rules, an affected Data Principal must be informed without delay in the prescribed manner. The Data Protection Board must also be informed without delay, followed by detailed information ordinarily within 72 hours of the organisation becoming aware of the breach, unless additional time is permitted.

6. Create a Mechanism to Honour Individual Rights

Individuals have statutory rights concerning their personal data, including rights relating to access, correction, completion, updating, erasure, grievance redressal and nomination.

Businesses should therefore establish an internal procedure for receiving, verifying, tracking and responding to such requests within the applicable framework.

7. Review Data Retention and Deletion Practices

The principle should no longer be to retain personal data indefinitely merely because storage is inexpensive. Organisations need to determine when the purpose of processing has been fulfilled and whether there is any independent legal requirement justifying continued retention.

A proper Data Retention and Deletion Policy should reconcile the DPDP framework with requirements under taxation laws, company law, employment law, sector-specific regulations and other applicable statutes.

8. Review Vendor and Data Processor Agreements

A company may outsource processing, but not its responsibility. Payroll agencies, cloud-hosting providers, CRM vendors, call centres, software providers, marketing agencies and numerous other service providers may process personal data on behalf of an organisation.

Contracts with such vendors should therefore address security obligations, confidentiality, breach reporting, permitted use of data, subcontracting, retention and deletion, audit rights and cooperation in responding to Data Principal requests.

9. Children's Personal Data Requires Special Attention

Processing the personal data of children attracts additional obligations, including requirements relating to verifiable parental consent, subject to the statutory framework and notified exemptions.

Businesses operating in education, gaming, healthcare, social media, entertainment and child-focused services should undertake a particularly careful assessment. Breaches of children's-data obligations can attract substantial monetary penalties.

What are the penalties for non-compliance?

The financial consequences can be significant.

The statutory Schedule presently provides for penalties including:

Nature of breach	Maximum monetary penalty
Failure to take reasonable security safeguards to prevent a personal data breach	₹250 crore
Failure to notify the Board or affected Data Principal of a personal data breach	₹200 crore
Breach of obligations concerning children	₹200 crore
Breach of additional obligations applicable to a Significant Data Fiduciary	₹150 crore
Breach of other provisions of the Act or Rules	₹50 crore

The amount of penalty is not automatically imposed at the maximum level. The Board is required to consider factors including the nature, gravity and duration of the breach, the type of personal data involved, repetition, gains or losses arising from the breach, mitigation measures and proportionality. Nevertheless, the potential exposure clearly demonstrates that data protection can no longer be treated merely as an IT-department issue. It is now a matter of legal compliance, corporate governance and enterprise risk management.

The right time to act is now

The principal compliance deadline may be 14 May 2027, but an organisation cannot realistically become compliant overnight. The process may involve coordination among management, legal teams, HR, IT, cybersecurity personnel, marketing departments and external vendors.

The prudent starting point is a DPDP gap assessment followed by a phased compliance programme covering data mapping, notices and consent, internal policies, Data Principal rights, vendor contracts, cybersecurity safeguards, retention and deletion protocols, and breach management.

Our team at Utkrishtha Law Offices has been working on the legal and practical aspects of DPDP compliance and

assisting entities in understanding their data-processing activities, identifying compliance gaps and developing organisation-specific documentation and implementation frameworks. The objective is not merely to prepare standard-form policies, but to align actual business processes with the requirements of the law.

The DPDP regime fundamentally changes the manner in which organisations must view personal data. Data may be a business asset, but it is now equally a legal responsibility. The entities that begin preparing early will not only reduce regulatory exposure but will also be better positioned to demonstrate accountability and earn the trust of customers, employees and stakeholders.

This article is intended solely for general information and awareness and does not constitute solicitation or legal advice for any specific factual situation.

Contact us at:-

Mr. Himanshu Dhawan, Advocate
Mr. Shubham Jain, Advocate-on-Record, Supreme Court of India

Contact@utkrishthalaw.com
Ph- +91-9999309222;
+91-8750021607

www.utkrishthalaw.com