DRN Legal

INDIA'S DPDP (DIGITAL PERSONAL DATA PROTECTION) ACT -

What It Means For Your Business

The **DPDP Act** is India's new data privacy law that governs how organizations must collect, use, share, store, and process **digital personal data.**

If your business handles customer, employee, or vendor data, it is likely that the DPDP Act applies to you, irrespective of industry, size, or whether you are based in India or global.

Why It Matters:

The DPDP Act requires businesses to redesign their data operations, onboarding journeys, marketing and HR workflows, vendor contracts, and internal governance practices.

Statutory Foundation

Governing Law:

- The Digital Personal Data Protection Act, 2023
- The Digital Personal Data Protection Rules, 2025

Enforcement Timeline:

Going live in phases

Fully operational by May 2027

Discussions are ongoing to fast-track enforcement

Regulator:

Data Protection Board of India – empowered to oversee compliance, conduct inquiries and impose penalties.

Business impact:

Regulatory exposure increases progressively as more obligations become enforceable. Monetary penalties can extend up to INR 250 Crores (~USD 27.6 Million) per violation.

Key Concepts Every Business Must Know

Personal Data:
Any data that can identify an individual directly or indirectly.

Digital Personal Data:
Personal data in digital form (including offline data later digitised).

Data Principal:
The individual whose personal data is processed.

Data Fiduciary:
Entity deciding why and how personal data is processed – this may be your business.

Data Processor:
Processes personal data on behalf of a data fiduciary – this may be your vendors or sub-contractors.

Processing:
Any wholly or partly automated operation performed on digital personal data – this includes any collection, recording, organisation, adaptation, retrieval, indexing, storage, sharing, use, restriction, deletion etc carried out by your business.

Does The DPDP Act Apply To You?

DPDP Act applies if

- Your business processes digital personal data **in India.**
- You process digital personal data **outside India** *in connection with offering goods or services to individuals in India.*

What does not matter

- Physical presence in India.
- Cloud location or geography of server.

Exclusions:

- Processing for personal/domestic purpose.
- Publicly available data.

When Your Business May Process Personal Data (Legal Basis For Processing)

- Personal data can only be processed for a **lawful purpose**

AND

- The processing meets any of the following grounds
  - The data principal provides consent.
  - It is for a permissible legitimate use permitted under the DPDP Act.

Consent must be:

- Free
- Specific
- Informed
- Unconditional
- Unambiguous
- Based on a clear affirmative action
- Easily withdrawable

What Your Business Needs To Disclose (Notice Requirements)

A **clear notice** must be provided before or at the time of collecting personal data detailing:

- What data is being collected
- Why it is collected
- Data principal's rights
- Grievance redressal method

The notice must be **accessible in multiple Indian languages.**

This means updating the external and internal facing privacy notices for your business.

Legitimate Uses And Statutory Exemptions

Your business may process personal data without consent in the context of:

- Voluntary provision by the data principal
- Processing of data of non Indian individuals in certain scenarios
- Prevention, detection, investigation or prosecution of any offence
- Court-approved mergers, demergers, compromise, amalgamation etc
- Enforcing legal rights or claims
- Research, archiving or statistical purposes
- Financial investigation on loan default
- Medical emergencies, public health situations, disasters
- Permissible employment-related purposes

What Your Business Must Do To Prioritise DPDP Act Compliance

Documentation Changes

- Update your privacy governance framework – data protection policy, processing notice, data retention policy, data sharing policy for vendor arrangements.
- Prepare formats for consent requests, withdrawal, exercise of rights and grievances.
- Update your vendor contracts.
- Prepare detailed data processing agreements.
- Conduct enterprise-wide data mapping to identify what personal data you collect, where it flows, who accesses it, and which of your vendors process it.
- Create and maintain record of processing activities (ROPA).

Process Changes

Create workflows to

- Send consent requests and obtain consent before the collection of personal data.
- Maintain consent records.
- Track retention schedule and delete personal data upon expiry of relevant period.

Implement processes for:

- Data breach reporting.
- Testing of protocols and controls.
- Audit of compliance status.
- Periodic training.

System Changes

- Establish systems for:
  - Consent withdrawal.
  - Exercise of rights by data principals.
  - Grievance redressal mechanism.
- Strengthen security controls.

Additional conditions apply if you are:

- Processing personal data of children or persons with disabilities.
- Designated as significant data fiduciary.

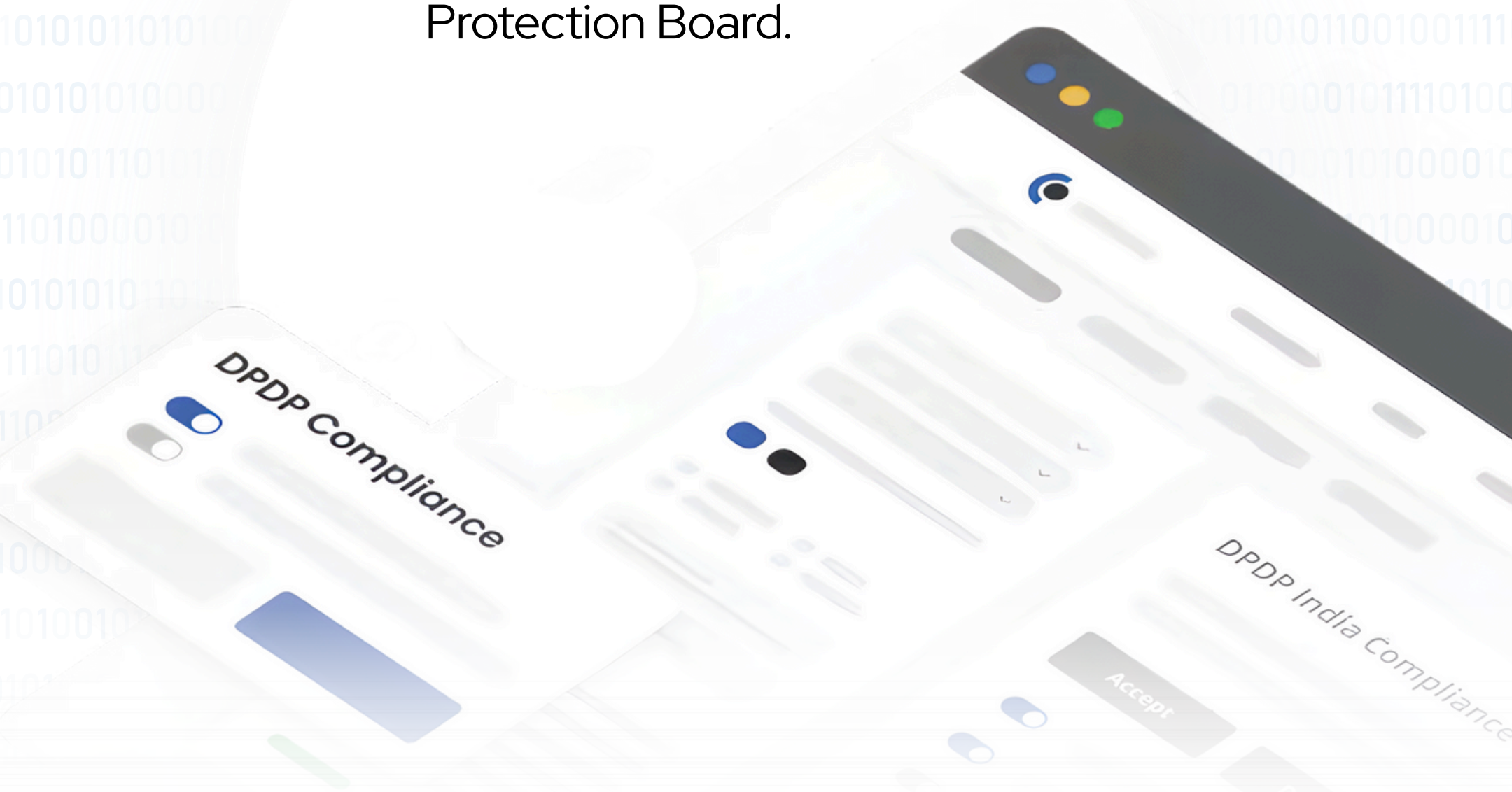
DRN Legal

BOTTOMLINE

DPDP COMPLIANCE MATTERS

If breached, it can attract:

- Significant monetary penalties.
- Reputational and contractual risk.
- Regulatory scrutiny by the Data Protection Board.



For more details, get in touch:

deepthi.rajeev@drnlegal.com