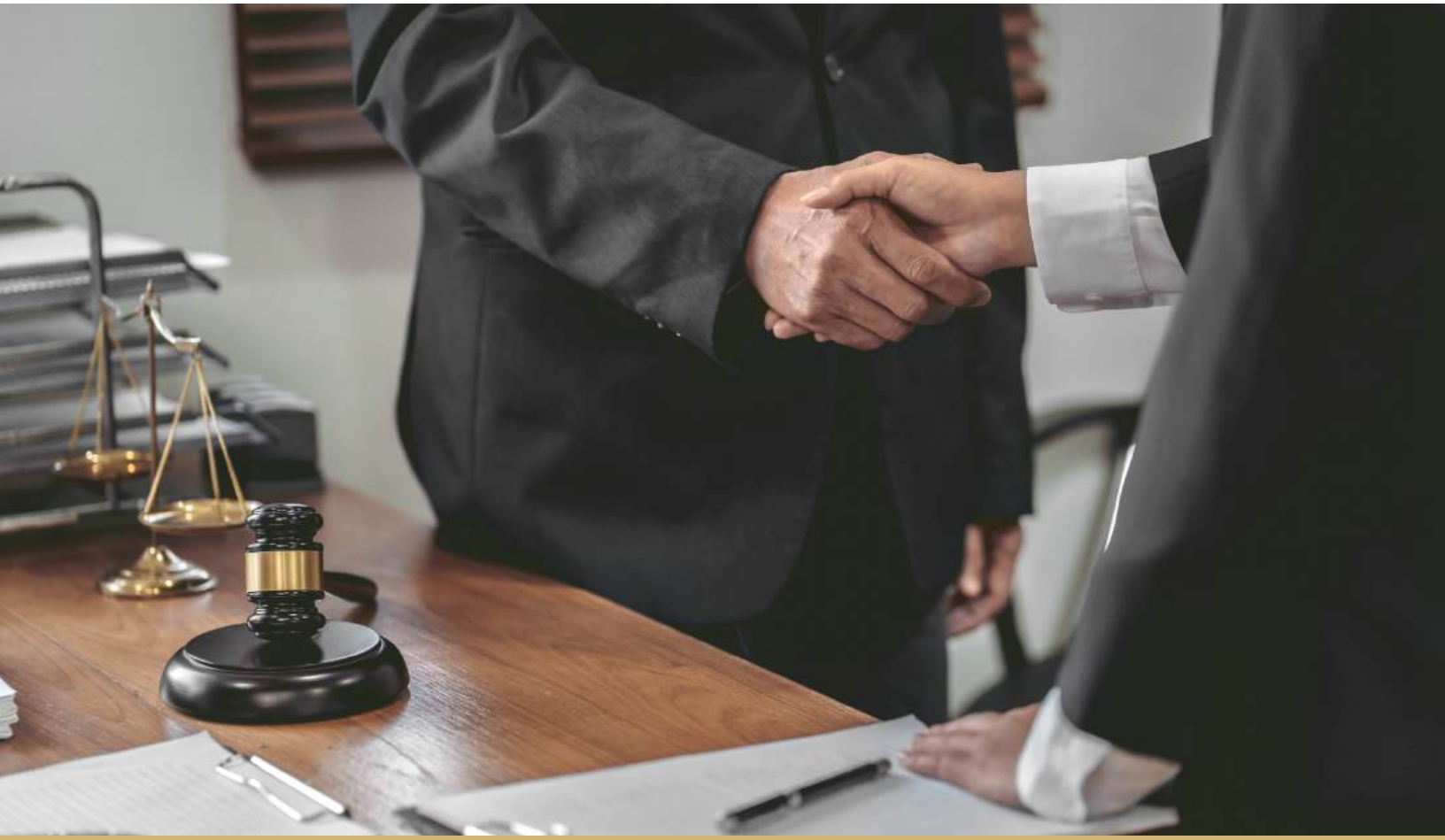
TG
LAW OFFICES

Key Questions Businesses Are Asking About

Digital Personal Data Protection Act & Rules

This is relevant to *every business* that processes / handles *personal data*.



When Does This Apply To You?

Act Enacted

Digital Personal Data Protection Act 2023 (DPDP / DPDPA) received Presidential assent on 11 August 2023.

Rules Notified

DPDP Rules 2025 were notified in November 2025. Operational obligations are now defined.

Phased Rollout Begins

An 18-month compliance timeline is underway. Businesses should begin **gap assessments** & consent **framework design** now.

Full Compliance Due

All obligations expected to be in force by approximately **May 2027**. Penalties up to **INR 250 crore per breach** apply from that date.

The Cost Of Non-Compliance

The penalties for failing to comply with the Act range from INR 10,000 to INR 200 crore, with a maximum cap of INR 250 crore.

Sl. No.	Breach of provisions of this Act or rules made thereunder	Penalty (INR)
1	Breach in observing the obligation of Data Fiduciary to take reasonable security safeguards to prevent personal data breach under sub-section (5) of section 8	May extend to two hundred and fifty crore rupees
2	Breach in observing the obligation to give the Board or affected Data Principal notice of a personal data breach under sub-section (6) of section 8	May extend to two hundred crore rupees
3	Breach in observance of additional obligations in relation to children under section 9	May extend to two hundred crore rupees
4	Breach in observance of additional obligations of Significant Data Fiduciary under section 10	May extend to one hundred and fifty crore rupees
5	Breach in observance of the duties under section 15	May extend to ten thousand rupees
6	Breach of any term of voluntary undertaking accepted by the Board under section 32	Up to the extent applicable for the breach in respect of which the proceedings under section 28 were instituted
7	Breach of any other provision of this Act or the rules made thereunder	May extend to fifty crore rupees

Part 1 : Consent & Lawful Processing

1. Consent Must Be Specific

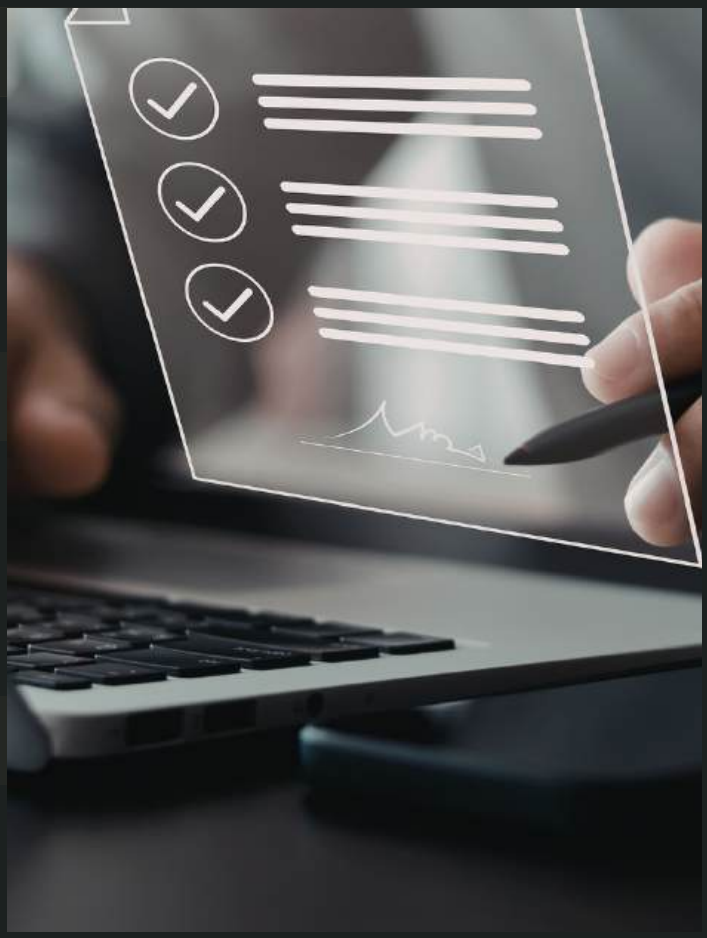
Consent is only valid for the specified purpose it was collected for. Blanket consent is not lawful under the Act.

2. Notice Must Precede Consent

Before seeking consent for any new purpose, a clear notice identifying the data being processed and the purpose must be provided.

3. Fresh Consent For New Purposes

If a new feature involves processing data for a different purpose, fresh consent must be obtained.



Q.

We are launching a digital app. What kind of consent should we take from users at onboarding?

A.

Consent must be free, specific, informed, unconditional, and unambiguous, and limited to what is necessary for the stated purpose.

At onboarding, seek consent only for account creation. For additional features, such as personalised recommendations, marketing, professional services, seek separate consent with a fresh notice at the point the user opts in. Bundled or blanket consent may not be not valid under the Act.

Q.

Do we need fresh consent every time a user accesses a new feature or service?

A.

Fresh consent, with a fresh notice is required whenever a new feature involves processing personal data for a purpose not specified at the time of the original consent. An updated notice alone does not substitute for fresh consent. If the new feature does not introduce a new purpose, no fresh consent is required, though notices must remain accurate.

Q.

Multiple parties handle our data. How do we determine who is the Data Fiduciary and who is the Data Processor?

A.

The Data Fiduciary is the entity that determines the purpose and means of processing. A Data Processor processes data on behalf of a Fiduciary.

The test is actual decision-making authority, not how contracts label the parties. If your organisation decides what data is collected and why, it is the Fiduciary and remains responsible for compliance even when a third-party vendor carries out the processing on its behalf.

Q.

Can we structure contracts to shift Data Fiduciary responsibility to another party?

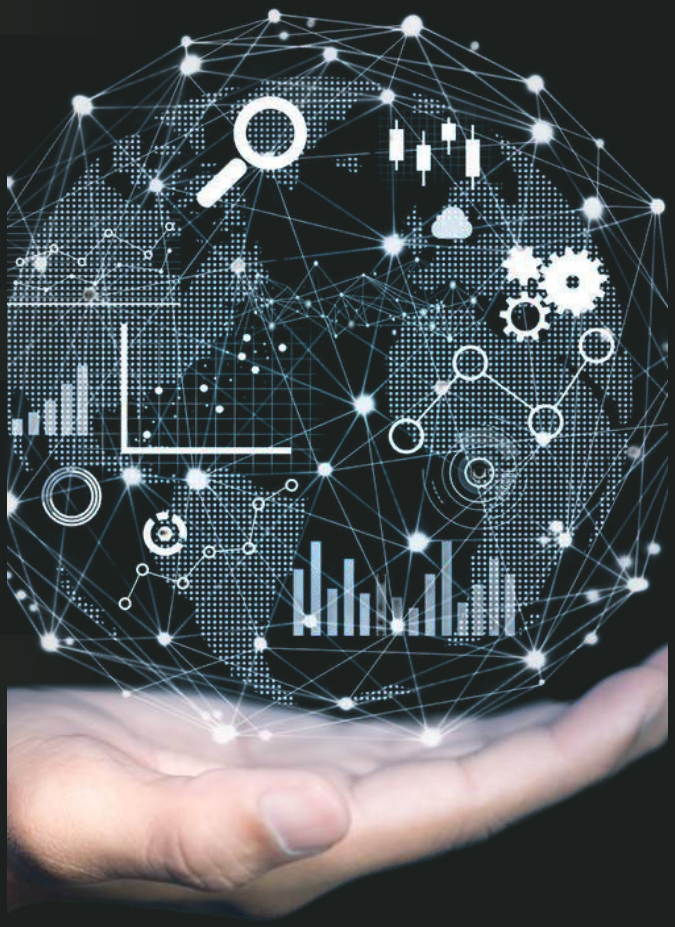
A.

No. The Act is explicit : a Data Fiduciary is responsible for DPDP obligations irrespective of any agreement to the contrary. If your organisation determines the purpose and means of processing, it is the Fiduciary, regardless of what any contract may state. Contracts can govern the relationship with a Data Processor, but they cannot override statutory responsibility or factual control.

Part 2 : Applicability & Scope

1. No Size or Sector Threshold

The Act applies to any business that processes digital personal data - regardless of size, turnover, or industry. There is no de minimis exemption.



2. B2B Is Not Exempt

B2B organisations that process employee, vendor, or client personal data are fully within scope. The Act does not distinguish by business model.

3. Extra-Territorial Reach

Foreign companies processing personal data of individuals in India, including through digital platforms and SaaS products, are bound by the Act regardless of where they are incorporated.

Q.

We are a foreign company offering digital services to users in India. What DPDP obligations apply to us?

A.

The Act applies extra-territorially to any processing of digital personal data outside India that is connected with offering goods or services to Data Principals in India. Physical presence in India is not required. Applicable obligations include: providing valid notice, obtaining consent or a recognised ground, implementing security safeguards, maintaining a grievance redressal mechanism, and complying with breach notification.

Q.

Most of our business does not involve personal data. Does the DPDP Act still apply to us?

A.

Yes. The Act applies to any processing of digital personal data, irrespective of the overall nature or scale of your business. If personal data is processed in any function, such as HR, payroll, access management, vendor management, the Act applies fully to those activities. There is no minimum threshold or de minimis exemption in the DPDP framework.

Q.

We operate multiple business lines and group entities. Can Data Fiduciary roles differ across functions?

A.

Yes. Data Fiduciary status is determined activity by activity, based on who decides the purpose and means of processing for each activity. Your organisation may be the Fiduciary for employee data processed centrally, while a separate group entity may independently be the Fiduciary for its own customer-facing services. Each entity must assess its obligations for the personal data it controls.

Pre & Post DPDP Era

Before DPDP

No single comprehensive data protection law for private sector entities in India

No stringent statutory obligation to notify individuals or a regulator of a data breach

No legal right for individuals to demand erasure or withdraw consent

After DPDP

A single, comprehensive framework, the DPDP Act 2023 applies to all sectors processing digital personal data

Mandatory breach notification to the Data Protection Board and affected individuals, without delay

Individuals (Data Principals) have statutory rights: access, correction, erasure, grievance redressal, and withdrawal of consent

Q.

We are a small, B2B-focused organisation that does not deal directly with consumers. Does the DPDP Act apply to us?

A.

Yes. Applicability does not depend on whether a business operates in a B2C or B2B model. B2B organisations routinely process personal data in employment, vendor management, client engagement, and operations.

Employee personal data alone is sufficient to bring your organisation within the DPDP framework. The Act contains no B2B exemption.

Q.

We are not a Significant Data Fiduciary. Do we still need someone responsible for data protection compliance?

A.

Yes. While only Significant Data Fiduciaries (notified by the Central Government) must appoint a formally designated Data Protection Officer, every Data Fiduciary must publish contact information for a person able to respond to Data Principal queries and must establish a grievance redressal mechanism. Identifying a clear internal compliance owner is strongly advisable as a governance matter for all businesses.

Q.

We only process basic personal data, not sensitive personal data. Does the DPDP Act still apply fully?

A.

Yes. Unlike certain other frameworks, the DPDP Act does not create a separate category of sensitive personal data. All personal data is subject to the same framework of obligations- a single, uniform standard applies regardless of the nature of the data processed. There is no lower-tier of compliance available for what might be considered“basic” or non- sensitive data under other regulatory regimes.

Q.

How can DPDP compliance be aligned with business strategy and digital transformation?

A.

DPDP compliance is most effectively embedded by building data protection obligations into products, systems, and processes from the outset. This means collecting only data necessary for a specified purpose, implementing security safeguards, designing workflows that facilitate Data Principal rights, and creating consent architectures that are valid and documentable. Early integration reduces remediation costs and builds customer trust.

Q.

Our industry has unique data challenges. How should we address sector-specific risks under the DPDP framework?

A.

Different sectors face different compliance profiles. E-commerce businesses manage high-volume consent flows; healthcare entities must comply with both DPDP and sector-specific law; BFSI organisations face additional RBI and IRDAI requirements. Sector-specific regulations, such as RBI payment data localisation, operate independently of the DPDP framework and must be assessed separately. Practical measures include automated consent management, encryption, and periodic audits of processing activities.

Q.

How long can we retain personal data under the DPDP framework?

A.

Personal data must be erased as soon as it is reasonable to assume the specified purpose is no longer being served, or upon withdrawal of consent, whichever is earlier, unless another law requires retention. The Act provides a deemed-purpose standard: if a Data Principal has not engaged with the Fiduciary for a prescribed period and has not exercised rights, the purpose is deemed served. Erasure, not anonymisation is the statutory obligation.

Q.

We are launching a digital app. What kind of consent should we take from users at onboarding?

A.

Consent must be free, specific, informed, unconditional, and unambiguous, and limited to what is necessary for the stated purpose. At onboarding, seek consent only for account creation. For additional features, such as personalised recommendations, marketing, professional services, seek separate consent with a fresh notice at the point the user opts in. Bundled or blanket consent is not valid under the Act.

Responding to a Personal Data Breach

Detect & Triage

Identify the breach: **nature, extent, timing, location,** and **likely impact** on Data Principals.

Notify Data Principals

Notify each affected Data Principal without delay with: **breach description, likely consequences, mitigation steps,** and **safety measures** they should take.

Notify the Board

File **initial intimation** with the Data Protection Board without delay. **Submit detailed report within 72 hours** (Rule 7). Request extension in writing if needed.

Remediate & Report

Implement measures to **prevent recurrence**. Document findings on the responsible person. **Submit final report** on notifications sent to Data Principals.

Breach Notification - No Exceptions

THE TWO-STAGE OBLIGATION

Stage 1 - Initial Intimation: Notify the Data Protection Board WITHOUT DELAY upon becoming aware of any breach. Include nature, extent, timing, location, and likely impact.

Stage 2 - Detailed Report: Submit a comprehensive follow-up report WITHIN 72 HOURS covering facts, causes, mitigation measures, findings, and a report on notifications sent to affected Data Principals.

Important

There is no minimum harm threshold. All personal data breaches must be reported.

Cross Border Transfers & Data Localisation

1. No blanket localisation requirement. Personal data may be stored and processed abroad, subject to certain requirements.
2. Transfer restrictions apply only if the Central Government notifies specific countries.
3. Sector-specific localization rules operate independently and continue to apply.
4. Significant Data Fiduciaries may face additional restrictions on specific data categories under Rule 12(4) of the DPDP Rules 2025.
5. Security safeguards under Section 8(5) apply regardless of where data is stored or processed.
6. Monitor government notifications under the DPDP framework – transfer restrictions can be imposed by general or special order at any time.

Let's Talk.

Every matter we handle is treated with absolute discretion.

TG Law Offices

tanya@tglaw.in

+91-8390736278