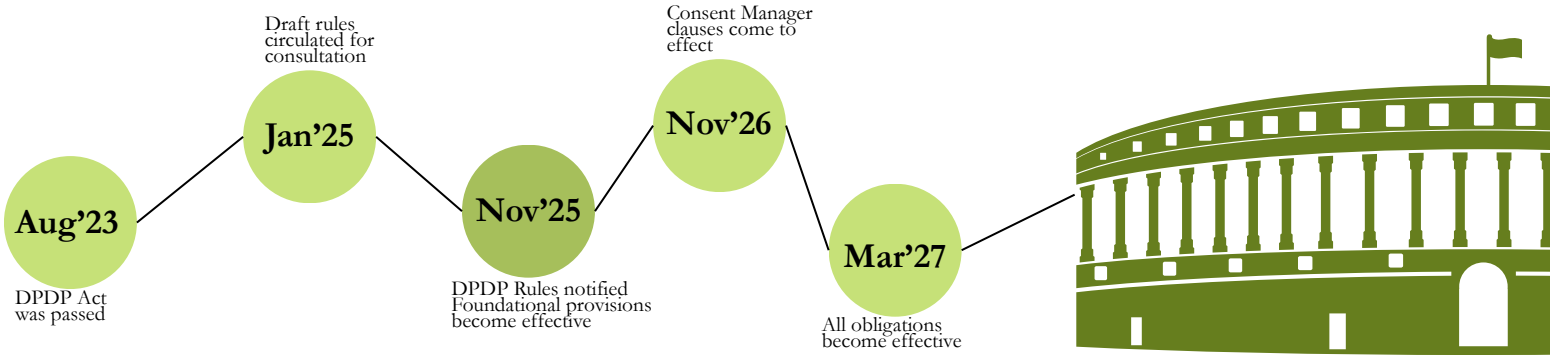
KRIA LAW

India's Privacy Regime

& its impact on International Businesses

Focuses on Digital Personal Data Protection Act, 2023 & its Rules 2025



India now joins the growing global cohort of jurisdictions with comprehensive privacy laws. The DPDP Act passed in Aug 2023, became operational with the notification of the Rules in Nov 2025. The Act further introduces an **18-month** compliance runway for organisations to transition into full conformity.

Our earlier writeup available here explores what these developments mean for local businesses. This current note would focus on how the Indian Data Protection Regime impacts international businesses.

Does DPDPA apply to Foreign business?

The Act can apply even to businesses outside of India if you:

- Have a Branch, or office in India
- Hire workforce/ employees in India
- Offer platforms or apps targetted to or accessed by users in India
- Offer goods or services to individuals located in India
- Engage with Vendors in India who may process personal data
- Host cloud storage infrastructure in India

Exception: Outsourcing processing to India

If your business outsources any processing activities to India, and the data to be so processed only corresponds to persons outside of India, then large number of obligations under DPDPA such as assisting data subject rights, having vendor contracts, storage limitation, cross boarder transfer restrictions, breach notification, etc do not apply

What forms of data processing does the Act cover?

The DPDPA applies to:

- **Digital personal data**
  Any personal data collected, processed, or stored digitally.
- **Digitised personal data**
  Offline data that has been **subsequently** digitised.

The DPDPA does not apply to:

- **Personal data for domestic use**
  Data used for personal or domestic use falls outside of the scope of the act.
- **Publicly available personal data**
  If lawfully made available by the individual or a public authority.

What sets the DPDPA apart from global privacy laws?

For international businesses, the DPDPA is both familiar enough to align with existing global frameworks and different enough to require India-specific compliance adjustments.

1. Data Fiduciary, not Data Controller

Under the DPDPA, the entity that determines the purpose and means of processing is called a Data Fiduciary (DF), rather than a "Data Controller" as seen in global laws like the GDPR. This is more than just a change in terminology. By choosing the term *fiduciary*, the Act signifies that such entities carry a higher degree of responsibility toward individuals and must act with fairness, transparency and care. The label reinforces that Data Fiduciaries are accountable for how personal data is collected, used, shared and protected, and must ensure that their processing activities do not harm or disadvantage the Data Principal.

2. Processor obligations arise only from contract

Unlike Data Fiduciaries, Data Processors under the DPDPA have no direct statutory obligations toward individuals. Their responsibilities arise only through the contract they sign with the Data Fiduciary. In other words, it is the Data Fiduciary that remains fully accountable for compliance, oversight and safeguarding personal data, while the Processor's duties are limited to what the contract requires them to do—nothing more, nothing less. This structure reinforces that the ultimate responsibility for lawful and secure processing stays with the Data Fiduciary.

3. Risk-Tiered Compliance

The DPDPA distinguishes between ordinary Data Fiduciaries and Significant Data Fiduciaries (SDFs), i.e, entities whose processing activities present higher risks. Government may designate organisations as SDF, based on factors such as the volume or sensitivity of data processed, risks to individuals' rights, or potential impact on electoral democracy. This is similar in intent to the GDPR's concept of high-risk processing, but DPDPA's approach is far more explicit and structured. SDFs may be required to appoint a Data Protection Officer, undergo independent data audits, and conduct Data Protection Impact Assessments annually, while ordinary businesses are subject to a much lighter compliance burden.

On the other hand, there is no classification of "sensitive personal data". All digital personal data is treated equally under the law

4. Introducing Consent Managers

One of the most distinguishable features of the Act is the concept of Consent Managers, introduced as part of India's efforts to build a secure and trusted digital environment. Consent Managers are neutral, interoperable platforms through which individuals can give, manage, or withdraw consent. Under the DPDPA, a Consent Manager can be any person or entity registered with the Data Protection Board, and under the Draft Rules, such an entity must be incorporated in India and meet prescribed technical, organisational, and governance requirements. No comparable mechanism exists under the GDPR, California's CCPA, Brazil LGPD or Singapore PDPA.

5. Cross-Border Transfers: Allowed-by-default

The DPDPA adopts an "allow unless restricted" model for cross-border data transfers, permitting transfers to all countries except those specifically blacklisted by the Indian government. This approach is the reverse of the GDPR's "prohibit unless adequate" or safeguard-based framework, which relies on adequacy decisions and mechanisms like SCCs or BCRs. In effect, while the GDPR maintains whitelists, the DPDPA operates on a blacklist system, making cross-border transfers significantly easier for businesses to operationalise.

What are the key obligations under the law?

GENERAL OBLIGATIONS - an overview

Purpose Limitation:
Collect only for specific, lawful purposes

Consent Requirements:
A Consent must be
- Explicit (no pre-checked boxes)
- Informed (notice must precede consent)
- Purpose-specific
- Unbundled (separate from T&C acceptance)
- Revocable at any time with ease
- Logged digitally
- Be given and managed by using a consent manager

Exceptions: voluntary deemed consent, employment, law enforcement, etc

Data Minimisation:
Avoid excessive or irrelevant data collection

Data Retention:
Retain personal data only for as long as it is necessary to fulfill the specified purpose for which it was collected.

Retain all personal data used in processing, traffic data, and processing logs for at least 1 year from the date of processing to enable breach investigation, audits, and regulatory review unless another law requires longer time period of retention

When purpose is served → the data must be erased, unless a legal obligation requires retention. (ex. Tax returns, audits, legal dispute, regulatory matters, etc)

Large Industry Players
Certain categories of organisations (e-commerce, social media intermediaries, gaming intermediaries, online platforms with large user bases) have to
- defined deletion timelines based on inactivity, typically 3 years of non-engagement.
- give 48 hours' notice to the individuals before deleting the data.

Grievance Handling
- Appoint a Grievance Officer (DPO if applicable)
- Enable complaint filing
- Publish in website and/or app:
    - Business contact information for grievance redressal (email/phone number)
    - how to exercise the rights of individuals (such as right to access, erasure, amend, nominate)
    - particulars required (username, identifier, etc) if any)
- Provide resolution within 90 days for individual's requests

Notice Requirements:
Provide a clear, accessible Privacy Notice before collection.

The notice must:
-be separate, simple, easy to understand
-include itemized description of personal data
-explain what data you collect. and why
-explain how to withdraw consent, exercise rights or complain to board
-be given even for data collected before enforcement of the act (legacy data)

Accuracy:
Ensure data remains correct and updated

Data Security:
Reasonable technical & organisational measures.

Implement measures to prevent Data Breach
- Secure data through encryption, obfuscation, masking or the use of virtual tokens;
- access control measures
- Logging and monitoring of data access and processing activity
- Data backups and continuity measures
- Contractual safeguards with processors
technical and organisational processes that ensure safeguards are consistently implemented

Accountability
Adopt internal governance measures, audits, and compliance checks.

Vendor Contracts
Ensure all agreements with Data Processors (vendors/service providers) include mandatory DPDP-aligned safeguards.

International Transfers
- Government may blacklist certain countries to which data should not be transferred.
- As of Nov 2025 → No blocked countries announced.
- International Transfers must meet any conditions under government order, if any.

CIRCUMSTANTIAL OBLIGATIONS

...in case of a Data Breach

Breach Notification

To Individuals:

- Timeline - Upon becoming aware of the breach
- Contents -
  - Description of breach (nature, extent and the timing of its occurrence)
  - relevent consequences
  - mitigating measures implemented
  - safety measures to be taken by individual; and
  - business contact information of the organisation's representative to address queries

To Board:

Initial Notification

- Timeline - Without delay upon becoming aware of the breach
- Contents - Description of breach (nature, extent and the timing of its occurrence, location & likely impact)

Detailed Notification

- Timeline - Within 72 hours
- Contents
  - updated and detailed description;
  - the broad facts, circumstances and reasons leading to the breach;
  - mitigation measures implemented or proposed;
  - any findings regarding the person causing the breach;
  - remedial measures to prevent recurrence; and
  - a report on notice to affected individuals.

..if you process Children's data

When you are processing data of children or persons with disabilities who cannot give consent on their own. In such cases you must

- Obtain Verifiable Consent from parent/guardian
- Conduct due diligence to check that the person giving consent is truly the parent(and an adult) / guardian. This can be done using reliable identity details, or a virtual token (e.g., via Digital Locker) to verify the adult's identity and age.

- No behavioural monitoring, tracking, or targeted advertising directed at the child.
- Stronger security measures have to be put in place to protect the child's personal data.

Exemptions apply to certain forms of processing in a limited manner such as healthcare providers, educational institutions, childcare centres, processing for providing benefits, services, certificates, or licenses under law, creating a user account via email, Restricting access to child-sensitive content.

However, all organisations should put in place reasonable safeguards when handling child data.

What happens when you do not comply

The Data Protection Board of India (DPB) is the regulatory authority created under the DPDP Act. It is responsible for enforcing the law, and can conduct inquiries, order urgent blocking of platform, require mitigation measures, or impose penalties

*approximate value based on conversation rate as of 05/Dec/2025

up to ~28 million* (up to INR 250 crores)

Failure to take reasonable security safeguards to prevent data breach

up to ~22 million* (up to INR 200 Crores)

Failure to report data breach (or) failure to protect Children's data.

up to ~17 million* (up to INR 150 Crores)

Failure in fulfilling duties of Significant data fiduciary

up to ~6 million* (up to INR 50 Crores)

Failure in respect of fulfilling any other obligation under this Law.

What should foregin businesses be doing to prepare for DPDPA Compliance?

Initial action

1 Assess Applicability

Confirm which activities and transactions fall within scope of DPDPA and map the data flows

2 Determine adoption Strategy

Whether to integrate India into global data governance or separate it.

3 Localize Notice & Consent

Adapt existing global notices to reflect DPDPA requirements

Implementation

4 Review vendor contracts

Enter into appropriate agreements with processors to meet DPDPA's requirements

5 Set-up Greivance Redressal

Form a Greivance Redressal mechanism and publish its details

6 Align Security measures

Confirm that technical and organisational measures meet or exceed DPDPA requirements

7 Breach Response Protocols

Ensure procedures are adapted for DPDPA breach response - notification timelines and contents

8 Fulfil situational obligations

Ensure addition obligations that apply to children's data processing or SDF(if applicable) are complied.

9 Retention & Deletion

Set up measures for 1 year retention requirements and deletion when no longer needed

Ongoing Compliance

10 Train Employees and members

Educate workfoce on compliance with the data protection requirements

11 Periodic Due Diligence

Carry out vendor assessments, evaluate internal processes, and review breach response protocols.

12 Track regulatory updates

Keep track of regulatory developments and update policies and practices accordingly.

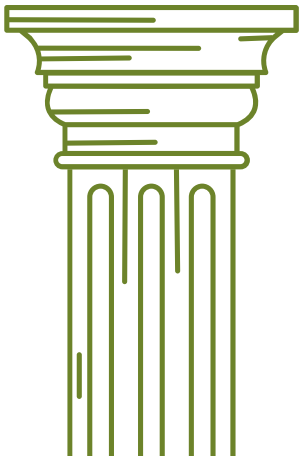
About KRIA LAW

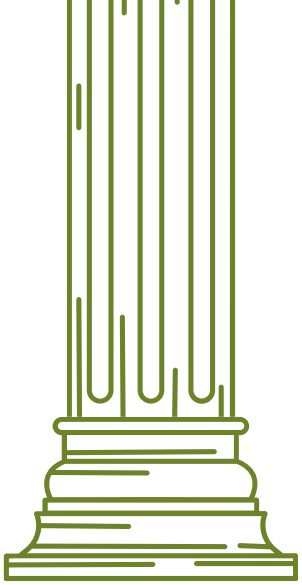
KRIA Law is a full-service law firm headquartered in Chennai, India.

We focus on providing "KRIAtive" and innovative solutions to our clients through a holistic approach combining our experience and expertise in various practice areas that includes intellectual property, data protection, information technology, litigation & dispute resolution, commercial, taxation, competition and anti-trust and general civil disputes. KRIA Law provides a wide range of legal, regulatory, and advisory services to its clients.

With strong working relationships with firms across all major cities in India and in over 150 countries globally and access to network of high-quality experienced lawyers, we are positioned to service our client's needs across India and the world in all fields of law.

- Patents
- Trademarks
- Copyrights
- Industrial Designs
- Commercial Litigation
- Dispute Resolution
- Commercial Contracts
- Data Protection
- Technology Laws





KRIA Law's assistance in Data Protection

- Legal Advise on compliance requirements under the law
- Sessions to relevant stakeholders sensitizing compliance requirements
- Assistance in performing GAP assessments
- Training employees and stakeholders on DPDPA
- Drafting Policies and Privacy Notices
- Drafting, Review or vetting of Agreements or terms and conditions with customers, employees, vendors, and other stakeholders.
- Assistance in setting up Grievance Redressal Committees