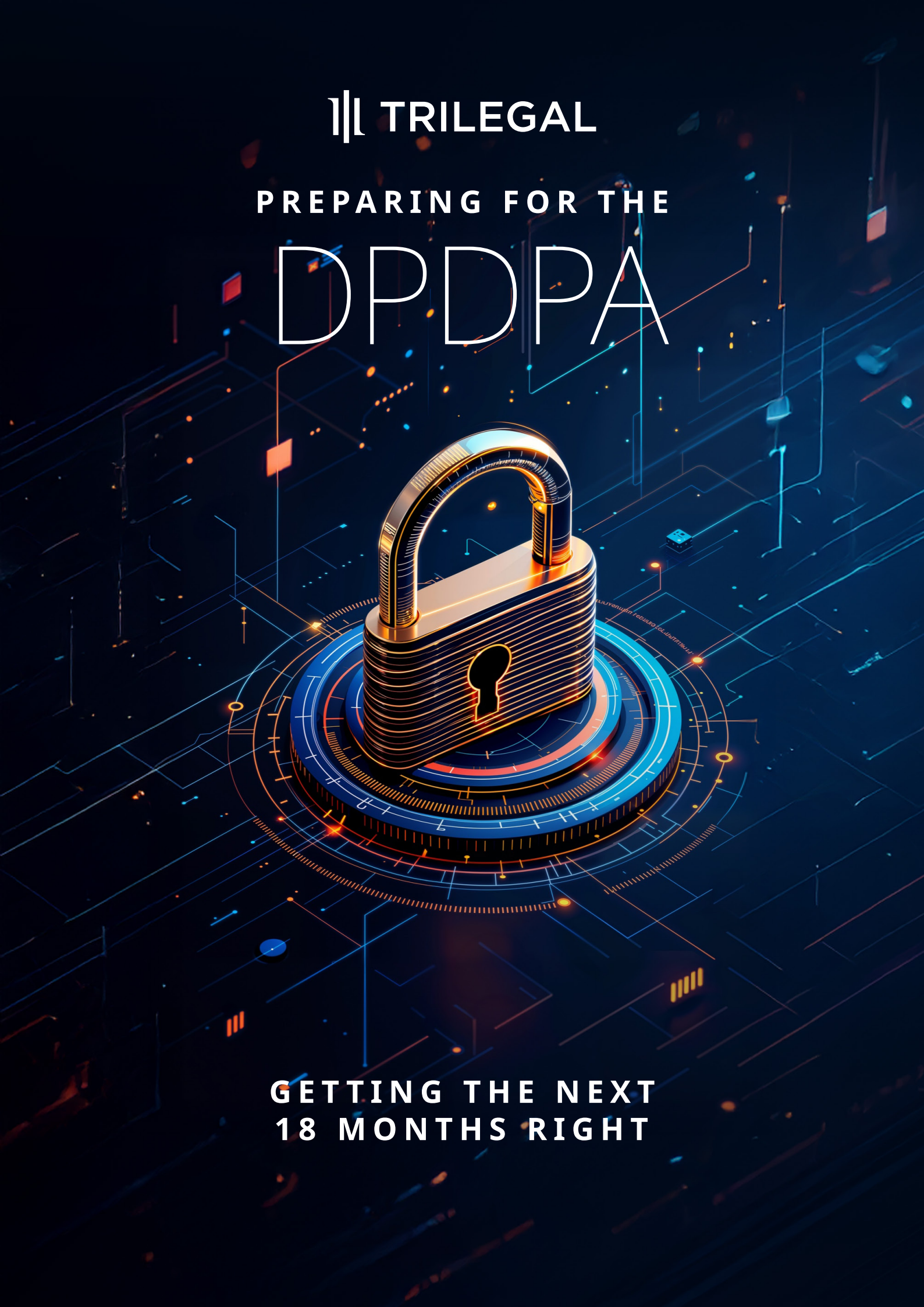
TRILEGAL

PREPARING FOR THE DPDPA



GETTING THE NEXT 18 MONTHS RIGHT

CONTRIBUTORS — Partners: Rahul Matthan, Nikhil Narendran, Jyotsna Jayaram, Jaideep Reddy, Jishnu Sanyal; **Counsel:** Thomas J. Vallianeth; **Senior Associates:** Anjana Ravi, Madhav Tampi, Akshaya Parthasarathy, Kuruvila Jacob, Prabal De, Sanah Javed, Janak Pradhan; **Associates**: Muskaan Wadhwa, Amala G., Yashaswini Hareesh, Divya Govindan, Afifa Sultan, Radhika Sikri, Adithi Holla

Introduction

On 13 November 2025, the Ministry of Electronics and Information Technology (**MeitY**) notified the implementation timelines for the Digital Personal Data Protection Act, 2023 (**DPDPA**) and published the final version of the Digital Personal Data Protection Rules, 2025 (**Rules**).

Together, the DPDPA and the Rules set out the framework that applies to the processing of all types of personal data. It will impact all businesses that process personal data regardless of their privacy footprint. Within an organisation, it will apply to the breadth of a business' internal and external processes, such as HR, marketing and sales, R&D, procurement, and accounting.

The DPDPA has been notified in a staggered manner – with organisations being given an extended timeline to evaluate their systems and align with the substantive provisions of the law.

Implementation

In 18 months (May 2027) - Organisations must comply with the substantive provisions of the DPDPA. Until then, the existing regime under the Information Technology Act, 2000, and the rules framed under it will continue to apply.

In 12 months (November 2026) - Provisions relating to consent managers will come into force, giving them a 6-month head start to set up their businesses before the substantive obligations under the DPDPA kick in.

With immediate effect - Provisions dealing with the administrative machinery of the DPDPA are already in force. These will only have a meaningful impact once the rest of the DPDPA is implemented.

If you are an organisation that processes personal data, the next 18 months present a critical transition period as you will need to analyse your existing data protection practices and assess implications under the upcoming regime. If you are looking to understand how to approach this transition period, this update provides an overview of some of the key action items.

A. Assess the applicability of the DPDPA

ACTION ITEMS: To assess if the DPDPA applies to you

- Identify all activities that involve personal data processing – i.e., what personal data is processed, how much, and for what purposes, and create an inventory of personal data. This inventory should span both external functions (e.g., sales, marketing, customer support, procurement) and internal business functions (e.g., HR, accounting, IT).
- Confirm if the processing takes place in India, or outside India.
- Evaluate the applicability of any exemptions or exclusions provided under the DPDPA to your organisation's processing activities. For instance, if you are processing personal data as part of cross border outsourcing activities you are exempted from most requirements under the DPDPA.

Whether the DPDPA applies to you depends on several factors:

- ***Type of data/activity:***
  The DPDPA governs the processing of digital personal data[1] regardless of sensitivity. A wide range of activities, such as collection, sharing, storage, indexing, use, alignment or combination of data can constitute 'processing' of such data.

- ***Where you carry out the processing:***
  The DPDPA is applicable if: (i) the personal data is processed within India, or (ii) the personal data is processed outside India, in connection with any activity related to offering goods or services to Data Principals within India.

- ***Your role:***
  The DPDPA applies directly to you only if you are a Data Fiduciary – i.e., if you determine the purpose and means for which personal data is processed by you or on your behalf. If you only process personal data on a third-party's behalf pursuant to their instructions, you are a Data Processor and the DPDPA does not directly apply to you. However, the Data Fiduciary for whom you are processing the data may impose contractual requirements on you.

- ***Certain exemptions:***
  In some cases, you may be exempt from (i) the DPDPA entirely, e.g., where personal data has been made publicly available by the Data Principal, or for research, archival or statistical purposes (subject to other conditions), or (ii) most of the requirements under the DPDPA, e.g., if an organisation in India processes the personal data of Data Principals outside India pursuant to a contract with an overseas entity, or to enforce a legal right.

1 'Digital personal data' refers to any data in digital form, by or in relation to which, an individual, called a Data Principal, may be identified.

B. Establish a legal basis for processing personal data

ACTION ITEMS: To identify the legal bases for processing personal data

- Review your existing personal data inventory and the purposes for such processing.
- Identify the personal data processing activities presently being carried out on the basis of a Data Principal's consent.
- For legacy datasets processed based on consent, assess incremental DPDPA compliances.
- For new datasets, or existing datasets processed for new purposes, put in place DPDPA compliant privacy notices and consent mechanisms.
- Alternatively, assess if a 'legitimate use' ground is more suitable to cover your data processing activities. For instance, in relation to your employees, you may be able to rely on the legitimate use ground for employment-related purposes and need not collect consent from such employees.

As a Data Fiduciary, you must have a legal basis to process personal data, i.e., the circumstances under which you are permitted under law to process personal data. The only two legal bases are – the Data Principal's consent or if the activity of processing falls under certain 'legitimate uses.'

a. Notice and Consent

- *Notice:* To rely on the consent of the individual to process their data, you must provide them with a notice while, or before, requesting their consent. The notice must contain details required for an individual to provide consent, such as the personal data being collected, the purpose of collection, and information on grievance redressal and availing of data subject rights. To help enable an individual to understand the notice, you must provide the individual the option to access translated copies of the notice in regional language as well.

- *Consent:* Consent that you obtain must be provided through an affirmative action only for specific purposes and to the extent necessary for such purpose. If consent was obtained for processing before the DPDPA's 'notice and consent' provisions took effect, you can continue processing such personal data until the Data Principal withdraws their consent. However, you must provide such Data Principal a DPDPA compliant privacy notice. To process personal data of children or persons with disability who have a legal guardian, you must obtain verifiable consent of a parent or legal guardian (see ***Section C*** for further details).

- *Withdrawal of consent:* An individual must be able to withdraw their consent at any time and with the same ease with which it was provided.

b. Legitimate use

- You can process personal data for certain limited 'legitimate uses' without an individual's consent.
- One example is processing for the purposes of employment. This would allow you to process the personal data of your employees for purposes that are linked to their employment, such as payroll, benefits, and performance management.
- Other legitimate uses recognised under the DPDPA include processing of data: (i) voluntarily provided by the data principal, (ii) to meet statutory disclosure requirements, (iii) for medical emergencies where there is an imminent threat to the life or health of the Data Principal, and (iv) by the State or its instrumentalities in relation to their sovereign functions.

C. Additional measures for children and persons with disabilities

ACTION ITEMS

- You must implement processes to obtain verifiable consent from parents or lawful guardians before processing personal data of children or persons with disabilities.
- You must review your products and processing activities to eliminate tracking, behavioral monitoring, and targeted advertising aimed at children.
- You must ensure that no processing activity has a detrimental effect on a child's well-being.

As a Data Fiduciary, you must obtain verifiable consent from a parent or lawful guardian of a person with disability to ensure that anyone claiming to be a parent or lawful guardian is an identifiable adult. For a parent, this can be verified either through (i) reliable age and identity information already available with the data fiduciary, (ii) information voluntarily provided, or (iii) a virtual token linked to such details. For a lawful guardian, you must verify that the guardian is appointed by the appropriate authority or a court under the law applicable to guardianship.

You are also prohibited from engaging in any processing that is detrimental to a child's well-being and tracking, monitoring the behaviour of, or directing targeted advertisements at children.

The Rules, however, exempt specific types of Data Fiduciaries, like educational institutions and clinical establishments, and also exempt processing for certain purposes, such as real-time child location tracking, from (i) the requirement of obtaining verifiable parental consent, and (ii) the restriction on tracking, behavioural monitoring of, or targeting advertisements at children.

D. Ascertain how long you require personal data

ACTION ITEMS

- You must establish purpose-based retention timelines. Personal data must be deleted when consent is withdrawn. Certain classes of entities have prescribed retention requirements.
- You must retain personal data, traffic data, and processing logs for at least one year

The DPDPA requires you to retain personal data only for as long as it is necessary for the specified purpose, or for compliance with the law. Once consent is withdrawn or the purpose is no longer served, you must, after retaining the personal data and associated traffic data and processing logs for at least one year, delete the data, unless further retention is required under any other law. You must also ensure the same action is taken by your Data Processor.

The Rules prescribe specific retention requirements for certain entities that meet specified user thresholds, such as e-commerce entities and social media intermediaries with at least two crore users in India, and online gaming intermediaries with at least fifty lakh users in India. If you qualify as such an entity, you must delete data after three years of user inactivity, except to the extent personal data is required to enable account access, or the use of a virtual token. You must also give the Data Principal forty-eight hours' notice before deletion. The requirement to retain the personal data and associated traffic data and processing logs for a minimum of one year also applies in such cases.

E. Assess if you have reasonable data security practices

ACTION ITEMS

- To the extent not already in place, you must implement security measures (e.g., access controls, access management or data back-ups) commensurate to the nature of your data processing activities.

As a Data Fiduciary, the Rules require you to implement at least the following security safeguards to ensure that any personal data that you process is protected from breach:

- Measures to ensure data security (e.g., encryption), access control (e.g., role-based access) and monitoring (e.g., access logs), and business continuity and disaster recovery (e.g., data back-ups).

- Technical and organisational measures to effectively operationalise security safeguards (e.g., personnel training and standard operating procedures).
- Appropriate provisions in contracts with Data Processors (see ***Section I*** below).
- Retaining access logs and personal data for one year, unless other laws require otherwise.

F. Setup mechanisms to enable Data Principal rights

ACTION ITEMS

- Tailor a framework that enables Data Principals to exercise their rights.
- Implement necessary measures to address grievances within the prescribed timeline.

Data Principals have the right to (i) access a summary of their personal data processed, (ii) correct and erase their personal data, (iii) nominate individuals to exercise rights on their behalf, and (iv) seek grievance redressal.

To enable these rights for your Data Principals, you must:

- ***Publish the information required to enable rights:***
  Publish a clear and accessible framework that allows Data Principals to exercise their rights.

- ***Set up systems and processes:***
  Set up systems and processes that enable Data Principal rights, once a request is made.

- ***Establish a mechanism for grievance redressal:***
  You must establish and publicise a grievance redressal mechanism and ensure that it is able to respond to grievances within a timeline not exceeding ninety days.

G. Setup processes for monitoring and reporting personal data breaches

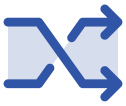
ACTION ITEMS: To the extent not already in place, you must:

- Designate persons to whom a breach may be reported.
- Set up standard operating procedures to be followed in the event of a real or suspected breach.
- Incorporate contractual obligations on Data Processors to implement similar measures.

On becoming aware of any personal data breach[2], you must inform each affected individual and the Data Protection Board of India (**Board**).[3] The intimation to the affected individual should:

- describe the nature, extent, timing and consequences of the breach,
- mention measures implemented to mitigate the risk and safety measures the individual may take to protect their interests, and
- mention contact details of a person who can respond to their queries.

As soon as you become aware of the data breach, you must inform the Board of the nature, extent, timing, location and likely impact of the breach. You should subsequently update the Board with additional details, such as the broad facts relating to the events leading up to the breach, findings regarding the perpetrator, remedial measures and the intimations given to the affected individuals.



H. Cross-border transfer restrictions

ACTION ITEMS: To the extent not already in place, you must:

- Review and update contractual safeguards and data transfer provisions in customer and vendor agreements once the government issues conditions for outbound transfers.
- Account for any data localisation requirements that may apply to Significant Data Fiduciaries for categories of personal data identified by the central government.

The DPDPA and the Rules do not generally restrict cross-border transfers of personal data, but empower the central government to:

- blacklist territories to which personal data cannot be transferred; and
- specify conditions that will apply to any outbound transfers from India.

Significant Data Fiduciaries are also subject to a data localisation requirement for certain types of data, as set out in ***Section J*** below.

2 'Personal data breach' refers to any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data that compromises the confidentiality, integrity or availability of the data.

3 The Data Protection Board of India is a body corporate established by the central government and is responsible for enforcing the DPDPA.

I. Identify and establish controls over your Data Processors

ACTION ITEMS

- You must put in place a contract with every Data Processor that captures the relevant obligations mandated under the DPDPA and the Rules.

As a Data Fiduciary, you remain accountable for any processing of personal data undertaken on your behalf by a Data Processor. Accordingly, you must (i) establish robust contractual controls for their processing activities, and (ii) review existing data processing agreement templates to ensure that they align with the framework under the DPDPA and the Rules.

For instance, your contract with your Data Processor must require them to implement prescribed reasonable security safeguards. These include practices covered in ***Section E*** above, and terms to ensure they apply these safeguards consistently and protect the personal data they process on your behalf. You should also require the Data Processor to assist with your compliance obligations, such as responding to Data Principal requests and promptly reporting personal data breaches.

J. Measures for Significant Data Fiduciaries

ACTION ITEMS

- If you are designated as a Significant Data Fiduciary, you must appoint an India-based data protection officer, undertake periodic impact assessments and audits, and adhere to data localisation measures.

Under the DPDPA, certain Data Fiduciaries or classes of Data Fiduciaries may be designated as Significant Data Fiduciaries (**SDF**) by the central government based on factors such as volume and sensitivity of personal data processed, risk to Data Principal rights, security of the State and risk to electoral democracy. Notifications designating SDFs are awaited.

If you are an SDF, you would be required to undertake additional compliances, including:

- appointing a data protection officer based in India;
- appointing an independent data auditor to evaluate compliance with the DPDPA;
- undertaking annual data protection impact assessments and audits from the date of designation as an SDF and furnishing reports of significant observations to the Board;
- verifying that technical measures do not pose a risk to Data Principals' rights; and
- ensuring that certain categories of personal data specified by the central government along with the associated traffic data are processed only within India.

K. Provisions for consent managers

ACTION ITEMS: If you intend to act as a consent manager:

- You must assess whether your entity meets the eligibility criteria, including the requirement for incorporation in India and the minimum net worth of two crore rupees.
- You must establish measures to avoid conflicts of interest and maintain accurate records of all consent decisions.

The DPDPA introduces the concept of a consent manager, a new type of entity registered with the Board to act as a single point of contact for Data Principals to manage their consent. If you are a consent manager, you must provide an accessible, transparent, and interoperable platform for Data Principals to give, manage, review, and withdraw their consent. Consent managers must remain data blind.

To register as a consent manager, the Rules specify certain eligibility conditions, including that you must be a company incorporated in India with a minimum net worth of two crore rupees, demonstrate sufficient technical and financial capacity, ensure your management has a general reputation, etc. Consent managers also have certain obligations under the Rules, including:

- preventing conflicts of interest with Data Fiduciaries and adopting safeguards against conflicts arising from relationships involving directors or senior management;
- maintaining a record of all consent related activities for at least seven years; and
- implementing appropriate security measures and ensuring that personal data shared through their platform remains unreadable to them.

Registration conditions and obligations of consent managers will take effect within one year (i.e., from November 2026).

There is no express clarity on the mode and manner in which Data Fiduciaries are required to integrate with consent managers; you will need to make a case-to-case assessment in this regard.

L. Engaging with the Data Protection Board of India

ACTION ITEMS

- You must establish protocols for liaising with and responding to requests from the Board.

The Board has been set up as a new regulator under the DPDPA and functions primarily as a digital office. You may have direct touchpoints with the Board in various instances, such as when reporting personal data breaches, responding to inquiries based on Data Principal complaints or government references, and engaging in proceedings. Once the substantive provisions come into force, the Board can issue binding directions, order urgent remedial steps for breaches, and impose monetary penalties. In cases of repeated non-compliance, it may also recommend blocking access to a Data Fiduciary's platform or services in India.

Conclusion: Your action plan for DPDPA compliance

While DPDPA compliance will necessitate meaningful operational change, the 18-month runway represents a clear opportunity for organisations to re-architect their data governance structures, policies, and build privacy-by-design systems. It is not just a compliance exercise but an opportunity to improve customer trust in digital products.

To prepare for the new regime and build customer trust, you should prioritise the following actions:

- Create a comprehensive inventory of all personal data you process to determine if your activities fall within the scope of the DPDPA and identify any available exemptions.
- Review every data processing activity, identify a valid legal basis (either by obtaining DPDPA-compliant consent or by relying on a specified 'legitimate use') and update your privacy notices.
- Implement a mechanism to obtain verifiable parental consent for processing data of children and persons with disabilities.
- Cease any tracking, behavioural monitoring, or processing that could be detrimental to a child's well-being.
- Establish and enforce clear, purpose-based data retention policies to ensure personal data is deleted once the specified purpose is fulfilled or consent is withdrawn, subject to any other legal retention mandates.

- Implement and document appropriate technical and organisational security measures, such as access controls and access management, to protect personal data from unauthorised access or breaches.
- Develop and operationalise clear, accessible internal procedures to effectively manage and enable Data Principals to exercise their rights.
- Create and implement a data breach response plan that includes protocols for prompt internal reporting and clear procedures for notifying the Board and affected individuals.
- Review all international data transfer arrangements and prepare to update contractual safeguards to align with government-notified restrictions.
- Ensure you have DPDPA-compliant contracts in place with all third-party Data Processors that clearly define their data protection responsibilities and obligations.
- If you are likely to be classified as an SDF, you must proactively prepare to appoint a Data Protection Officer, establish processes for conducting data protection impact assessments and periodic audits, and account for data localisation restrictions.
- If you plan to operate as a consent manager, verify that you meet all statutory eligibility criteria and establish the necessary infrastructure to manage consents transparently and without conflicts of interest.