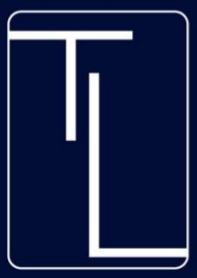
# PRIMER: DIGITAL PERSONAL DATA PROTECTION ACT AND RULES



TRACE
LAW
PARTNERS

C O N T E N T S

## 1. BACKGROUND

- The Digital Personal Data Protection Act, 2023[1] ("Act") and Digital Personal Data Protection Rules, 2025[2] ("Rules") are a response to the need for a comprehensive data protection framework in India. In 2017, the Supreme Court of India recognized the right to privacy as a part of the fundamental right to life and personal liberty, setting into motion the process of drawing up a data protection framework.[3] From there on, several iterations of a draft framework were drawn up by various committees culminating in the final Act and Rules introduced by the Ministry of Electronics and Information Technology ("MEITY").

- In August 2023, the Act, which provided the framework for processing of "personal data", was passed in the Indian parliament. However, much of the prescriptive guidance for operationalizing the Act was left to be fleshed out in the Rules. A draft version of the Rules was released in January 2025 for consultation. Based on feedback, MEITY notified the final version of the Rules and the implementation timeline of the Act and the Rules on 14th November 2025. The final version of the Rules remains largely the same as the draft version circulated earlier this year.

**Implementation Timeline**

| Immediately | 12 months, by 13th November 2026 | 18 months, by 13th May 2027[4] |
|---|---|---|
| Provisions relating to the Data Protection Board ("DPB") | Provisions related to registration and obligations of consent managers commence | Most substantive obligations under the Act, such as notice and consent, security obligations, breach reporting obligations, transfer restrictions, etc. |

- In the meantime, Section 43A of the Information Technology Act, 2000 ("IT Act") and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011[5] will continue to apply.

[1] Available here: Digital Personal Data Protection Act, 2023.
[2] Available here: Digital Personal Data Protection Rules, 2025.
[3] Justice K.S. Puttaswamy & Anr. vs. Union of India & Ors., (2017) 10 SCC 1
[4] See Annexure B for our quick guide on what to do in these 18 months to build for compliance
[5] Available here: Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

**Key Terms**

- The Act applies to digital personal data and broadly defines "personal data" as any data about an individual who is identifiable by or in relation to such data.[6] It does not apply to offline data, unless such data is subsequently digitized.

This definition not only covers commonly understood types of personal data such as name, address, etc., but may also cover identifiers such as IP addresses, user preferences (if these can be used by themselves or when used with other information to identify an individual). Therefore, organisations must carefully examine the types of data they collect to understand if obligations under the Act apply.

- "Processing" is defined as a wholly or partly automated operation or set of operations performed on digital personal data, and includes operations such as collection, recording, organisation, structuring, storage, adaptation, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction.[7]

- Data Fiduciary ("DF") is defined as any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data.[8]

Multiple entities may act as data fiduciaries, if they jointly decide why and how the personal data is processed. In such case, both data fiduciaries must ensure compliance with the law.

- Significant Data Fiduciary ("SDF") is defined as a data fiduciary, or a class of data fiduciaries which are notified by the Central Government basis factors such as the volume and sensitivity of data processed, risk to DP rights, impact on sovereignty and integrity of India, risk to electoral democracy, security of State, and public order.[9]

The Government has not notified SDFs yet. These may include entities that carry out high volume personal data processing, as well as entities that process personal data in sensitive sectors such as healthcare or finance.

[6] Section 2(t), Digital Personal Data Protection Act, 2023.
[7] Section 2(x), Digital Personal Data Protection Act, 2023.
[8] Section 2(i), Digital Personal Data Protection Act, 2023.
[9] Section 10, Digital Personal Data Protection Act, 2023.

- Data Principal ("DP") is an individual to whom the personal data relates. If such an individual is (a) A child, it includes the parents or lawful guardian of such child; (b) A person with disability ("PwD"), it includes her lawful guardian, acting on her behalf. [10] In case of a child or PwD, their rights may be exercised by their parent/guardian.

- Data Processor is any person who processes personal data on behalf of a DF.[11]

The classification of an entity as a Data Processor is based on the substance of the processing functions it undertakes, and not merely on the nomenclature assigned to it under the contract between the Data Fiduciary and the vendor. The distinction is significant because the Act places compliance obligations solely on Data Fiduciaries. Hence, entities processing personal data must determine whether they are substantively acting in a fiduciary or processor capacity.

## 2. APPLICABILITY

**Territorial applicability**

The Act applies to processing of digital personal data (a) in India, or (b) outside of India for the purpose of offering goods or services to DPs in India.

The Act applies to foreign data fiduciaries located outside of India, targeting Indian data principals in terms of both offering goods and services, as well as advertising them to DPs in India. Further, the application of the Act is not limited to data of Indian residents/citizens but also to processing of personal data of a foreign nationals in India. However, if the processing of personal data of foreign nationals is pursuant to an outsourcing agreement, most substantive obligations under the Act do not apply (See the discussion on Outsourcing Exemption below).

**Exemptions**

The Act does not apply to personal data:

(a) shared publicly by the DP;

(b) made public by any other person legally required to do so;

(c) processed by an individual for any personal or domestic purpose;

[10] Section 2(j), Digital Personal Data Protection Act, 2023.
[11] Section 2(k), Digital Personal Data Protection Act, 2023.

The Act also does not apply to following processing activities:

(a) by the government for specific purposes such as in the interest of sovereignty and integrity of India, security of the state, friendly relations with foreign states, subject to compliance with prescribed conditions.

(b) necessary for research, archiving or statistical purposes if personal data is not used to make decision about a DP and subject to standards prescribed under the Rules.

**Non-applicability of certain provisions**

With respect to personal data shared publicly, it is unclear if social media profiles with privacy settings will qualify for this exemption. The standards prescribed for the research/government use exemption are similar to obligations that would otherwise apply to processing like lawful processing, purpose limitation, security safeguards, necessary measures to ensure the completeness and accuracy of personal data, etc. Hence, although the Act and Rules state these activities are exempted; in order to avail of the exemption, these activities are in effect subject to compliances.

It is unclear if personal data used for instance, to train and fine-tune AI models, would be covered under the research exemption, since these are exploratory processes involving disruptive technology. On the one hand, it may be argued that model training involves technical research for innovation, whilst on the other hand it may be argued that if it is product-driven processing for commercial products, it may fall outside the exemption.

Certain processing activities are exempt from most substantive provisions of the Act including the requirement to obtain consent, provide notice, etc.[12] These include:

(a) Processing activities necessary to enforce legal rights or claims;

(b) Processing by courts or quasi-judicial bodies;

(c) Processing in the interest of investigations or prosecution of offences;

(d) Outsourcing exemption: Processing data of DPs located outside India, pursuant to a contract with any Indian and foreign person;

[12] Section 17(1), Digital Personal Data Protection Act, 2023.

(e) Processing necessary for mergers, amalgamations, demergers, transfer of undertaking, etc., approved by a court or tribunal;

(f) Financial institutions processing persons' personal data to evaluate their financial information, assets and liabilities if such person has defaulted on loans, subject to certain conditions.

**Government's power to exempt applicability**

The government can:

(a) exempt DFs or class of DFs like start-ups from certain obligations (notice, data accuracy, data retention, SDF obligations and rights of DPs) based on the volume and nature of data they process.

(b) declare that any provision of the Act will not apply to certain DFs or classes of DFs for notified periods, within the first five years from the commencement of the Act (i.e., before November 13, 2030).

(c) Provide exemptions in relation to handling of children's data.

**ASSESS IF THE ACT APPLIES TO YOUR ORGANISATION:**

- Does your organisation store/access/use/collect personal data belonging to individuals located in India – for instance, customer information, employee data, data of customers of B2B clients?
- When processing such personal data, does your organisation independently determine the purpose and means of processing, or is it acting solely on behalf of a client under a contractual mandate?
- Where personal data of foreign nationals is processed within India, is such processing undertaken pursuant to an outsourcing or service arrangement?
- If you are a foreign organisation processing personal data of individuals located in India, is the processing connected to the offering of goods or services to such individuals?

## 3. GROUNDS FOR PROCESSING

Personal data can only be processed for a lawful purpose either based on consent or in relation to one of the specified legitimate uses.

Data fiduciaries may also evaluate whether any exemptions under the Act apply to processing activities.

## 4. CONSENT AND NOTICE

If processing is consent based, then the request for consent must be accompanied or preceded by a notice to the DP.

**Substance of Notice**

Contents of a notice must include:

(a) Information about personal data collected and the purpose for the same and a fair account of information necessary to give specific and informed consent. This must include:
- an itemised description of personal data
- the specified purpose of and specific description of goods/services, or uses to be provided through such processing;

(b) Information about the manner to exercise her rights under the Act including withdrawal of consent, and manner of exercise of other rights.

(c) Contact details of a Data Protection Officer, where applicable, or any other person authorised to respond to communications;

(d) Information about the manner to make a complaint to the DPB.

(e) Communication link to access the website/app or both of the DF.

**Form of Notice**

(a) Notice must be given to the DP in English or any language in the Eighth Schedule of the Indian Constitution.[13]

(b) It must be given in a clear and plain language.

[13] These include: (1) Assamese, (2) Bengali, (3) Gujarati, (4) Hindi, (5) Kannada, (6) Kashmiri, (7) Konkani, (8) Malayalam, (9) Manipuri, (10) Marathi, (11) Nepali, (12) Oriya, (13) Punjabi, (14) Sanskrit, (15) Sindhi, (16) Tamil, (17) Telugu, (18) Urdu (19) Bodo, (20) Santhali, (21) Maithili and (22) Dogri.

(c) It must be presented and understandable independently of any other information shared by the DF.

A question arises as to whether fresh notice is required **every** time personal data is collected. If the purpose of data collection changes, or additional datasets are collected. If the same dataset is collected on an ongoing basis for a notified purpose, a new notice may not be necessary.

**Notice Requirements for Legacy Data**

Where a DF has been processing personal data based on consent since before the Act's implementation, a fresh notice including the aforementioned information must be given as soon as reasonably practicable. Any such past processing activities can be continued by the DF until consent is withdrawn by the DP.

For past processing, the Act & the Rules do not specify a timeline for what may be considered "reasonably practicable" to provide fresh notices. Further, if personal data was not processed based on consent, then DFs must take consent or determine if their activities fall under any other lawful ground for processing.

**Requirements of consent**

(a) Consent must be:

- free, i.e., voluntarily and not through coercion, etc.
- specific, i.e., with the purpose of processing clearly specified
- informed, i.e., with the DP being informed of all necessary information with respect to processing
- unconditional, i.e., not dependant on provision of the service. To illustrate, a platform mandating collecting and sharing of location data with their partner platform for the DP to access the platform.
- Unambiguous, i.e., clearly provided and not implied.

(b) Consent must be supported by a clear affirmative action, i.e., through opt in.

(c) Consent-based processing must ensure that personal data is processed for only specified purposes and only such personal data that is necessary to process for the specified purpose is collected.

(d) A DP must be provided with a right to withdraw her consent at any time and with relative ease as providing the consent.

(e) If consent is withdrawn, a DF and its processors must stop processing the personal data of such DP unless otherwise required to be retained by any law.

(f) A DF must be able to prove that its processing activities were undertaken based on consent by the DP. The Business Requirement Document for Consent Management under the Act released by MEITY provided examples for logging consent by way of metadata like timestamp, session ID, consent method, user ID.

Since the Act requires specific consent, organisations must obtain itemised consent for each purpose. Bundled consent (i.e., single consent for loans, insurance, investments) would be invalid under the Act. Additionally, collecting personal data unrelated to the purpose, even with consent is likely to be invalid. Hence, ad-supported platforms must be able to justify the necessity of processing data for delivery of the key service.

A question arises whether obtaining consent for a general category (such as insurance) would suffice, or product-specific consent is required for sub-categories (such as health insurance, and life insurance). While the Act and Rules don't specify, ideally if the nature of the product differs significantly, fresh consent would be required.

## 5. CERTAIN LEGITIMATE USES

Apart from consent-based processing, a DF can process personal data based on certain legitimate uses. These include:

- Processing based on voluntarily provided personal data for a specified purpose only to the extent the data fiduciary does not indicate that she does not consent to use of her personal data for such purposes.

While broadly worded, the scope of this ground does not appear to be open-ended. The examples in the Act (e.g., providing a phone number to receive an invoice) suggest that the Government intended this ground to cover narrow, immediate, transactional contexts, and not broad, ongoing processing.

- Processing for fulfilling any legal obligation to disclose information to the government.

The scope of this ground is limited to purpose of disclosing information to the government under a legal obligation.

- Processing for compliance with any judgement, decree or order passed under any Indian laws or relating to contractual or civil claims.
- Processing to respond to medical emergencies involving a threat to life or any immediate threat to the health of the DP or any other individual.
- Processing for medical services during an epidemic, outbreak or other threats to public health.
- Processing for safety during a disaster or breakdown of public order.

The healthcare industry has been evaluating whether they may avail of the above health related grounds. However, these grounds are narrowly drawn to include only emergencies, epidemics, and providing safety disasters and do not cover ongoing processing for healthcare related purposes.

- Processing for the purposes of employment or safeguarding the employer from loss or liability like prevention of corporate espionage, maintenance of confidentiality of trade secrets, intellectual property, classified information or provision of a service or benefit to the DP who is an employee.

The term “purposes of employment” is not defined in the Act and may give rise to interpretational considerations for organisations. For instance, businesses should assess whether their pre-employment workflows (e.g., interviews, shortlisting, background checks) fall within this ground or require separate consent. Similarly, employers should evaluate how this ground applies to processing of information relating to employee dependants, the cross-border transfer of employee data for HR operations, and disclosures to third-party service providers such as insurers or payroll processors. These issues will need to be carefully aligned with the organisation’s data governance framework.

## 6. ENGAGEMENT OF DATA PROCESSORS

A DF is primarily responsible for complying with the obligations under the Act even if it engages a Data Processor for processing data on its behalf. Such engagement for processing data must only be under a valid contract.

DFs should ensure that contracts with Data Processors are watertight, including clear protocols for breach intimation, transfer restrictions and implementation of security safeguards. Therefore, organisations must review their existing vendor contracts to pass down such obligations.

**QUESTIONS TO CONSIDER READINESS:**

- Does the organisation's service providers process personal data strictly in accordance with the organisation's documented instructions, or do they exercise any independent control?
- Has your organisation entered into agreements with all service providers who have access to personal data of your customers/employees?
- What obligations have been passed down to such vendors?
- Do you have visibility on whether vendors engage sub-processors, and if so, what obligations are passed down to such sub-processors?
- Does your organisation carry out diligence to ensure that processors have the organisational capacity to comply with obligations?
- Does your contractual arrangement with processors enable appropriate oversight

## 7. BREACH INTIMATION

"Personal data breach" is defined *as 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 personal data.*

There is no materiality threshold for intimating breach. Breaches will need to be reported regardless of the impact on DPs. This may cause fatigue and desensitization with DPs.

In case of a personal data breach, a DF must intimate the DPB and every affected DP in the following form and manner:

**Intimation to the DP**

(a) *When and how to notify:* The DF must notify the DP "without delay" after becoming aware of the breach, using the Data Principal's account or any registered mode of communication.

(b) *Manner of notification:* The intimation must be concise, clear, and in plain language. It must describe the nature, extent, and timing of the breach, the relevant and likely consequences, the measures taken in response, the steps the DP can take for their safety, and the contact details of the person designated to address queries.

**Intimation to the DPB**

The reporting is at two levels:

(a) *Immediate reporting* - The DF must report the breach to the DPB "without delay," providing a description of the breach, including its nature, extent, timing, location, and likely impact.

(b) *Within seventy-two hours* of becoming aware of the breach (or within an extended period permitted upon request), the DF must submit updated information, including relevant facts, circumstances, and reasons for breach, measures implemented and proposed, findings regarding the person who caused the breach, futuristic measures taken for prevention, and a report on the intimations given to the DPs.

- Stakeholders had pushed back on the timeline for intimation given that 72 hours were provided for "additional information", meaning a much shorter timeline for "without delay" related intimation. However, the reporting timelines remain unchanged in the Rules.
- Certain parallel breach-reporting requirements apply under other laws for example, reporting to CERT-In within six hours of becoming aware of a "cyber security incident" and reporting to sectoral regulators such as RBI, SEBI. Data Fiduciaries will therefore need to establish clear standard operating procedures to ensure timely compliance across all frameworks and must ensure that their data-processing agreements impose corresponding obligations on processors.
- Breaches occurring prior to the breach reporting provisions under the DPDP Act coming into effect (i.e., before May 14th, 2027) are not required to be reported. However, CERT-In reporting may be required.
- It is also unclear whether separate data fiduciaries will have to intimate data breaches, or a single notification jointly made to the DPB would suffice.

**QUESTIONS TO ASSESS READINESS:**

- Does your organisation have SOPs in place to ensure timely reporting to all relevant regulators/authorities?
- Are your service providers obligated to notify you of breaches within a strict and defined timeline that allows you to meet statutory reporting obligations?

## 8. DATA ERASURE

### General obligations

A DF must by itself and through its Data Processor erase personal data upon withdrawal of consent or when the specified purpose is no longer being served, whichever is earlier, subject to the one-year retention requirement discussed below, and unless otherwise required under any law.

A specified purpose is deemed to be no longer served if the DP does not approach the DF for:

(a) its performance by initiating contact with the DF in person or online, or
(b) to exercise any rights in such regard, for a prescribed period of time.

Specific time periods have been prescribed only for three categories of data fiduciaries:

- E-commerce entities having at least 2 crore registered users in India;
- Online gaming intermediaries having not less than 50 lakh registered users in India;
- Social media intermediaries having at least 2 crore registered users in India.

If the specified purpose is no longer being served, such categories of data fiduciaries may retain the personal data for a period of three years, from the latest of the following:

- The date on which the DP last approached the DF for the performance of the specified purpose;
- The date on which the DP last exercised any of her rights under the Act; or
- The date of commencement of the Rules, 2025.

Such DFs may retain personal data beyond this period for the purposes of enabling the DP access to her user account or any virtual token which may be used to get money, goods or services. They must also retain it beyond this period if required under applicable law.

For other data fiduciaries, apart from the three categories of data fiduciaries, there is no prescribed maximum retention period. Such data fiduciaries would need to erase data by determining the exhaustion of the specified purpose, unless the data fiduciary withdraws consent or requests deletion.

Forty-eight hours before erasing personal data, such DFs are required to inform the DP of the erasure, which may be halted if –

(a) she logs into her user account,
(b) initiates contact with the DF for the performance of the specified purpose, or
(c) exercises her rights relating to the processing.

**One year retention requirement**

All DFs are required to retain personal data and associated traffic data and other logs of processing for a minimum period of one year in case the government wants to use the data:

(a) in the interest of sovereignty, integrity, or security of India,
(b) to perform any function under law,

(c) to disclose information under law, or

(d) to assess if a DF is an SDF.

**QUESTIONS TO ASSESS READINESS:**

- Has the specified purpose been documented? Is the purpose still being actively served?
- Do you fall within the class of data fiduciaries subject to statutory maximum retention periods?
- Is retention required for any legal obligation?
- Are your data systems (including CRM, HRMS, cloud storage, backups, SaaS tools, and legacy databases) technically capable of isolating, deleting, or rendering personal data irretrievable upon request?
- Has all personal data been mapped to confirm where personal data resides to ensure that deletion is operationally feasible across all systems?
- Is data subject to erasure stored across multiple systems, vendors and backups?

## 9. PROCESSING OF PERSONAL DATA OF CHILDREN

A DF must obtain verifiable parental consent before processing any personal data of a child (i.e., a person below the age of 18 years).

**How to obtain verifiable parental consent**

DFs are required to adopt appropriate technical and organisational measures to ensure that:

(a) Verifiable consent of the parent is obtained and

(b) Due diligence is observed for checking that the individual identifying herself as the parent is an adult who is identifiable, if required, by referring to the details available with the DF about the adult or by way of voluntary information provided by the adult or through a virtual token mapped to such information issued by an authorised entity.

To begin with, data fiduciaries may need to implement measures at the time of customer onboarding to determine if the customer is a child to assess the manner in which consent must be taken.

There is no requirement to ascertain if there exists an actual relationship between the user and the supposed parent. The compliance relies upon the self-identification of the user as a child or by its parent.

**Restrictions in relation to personal data of children**

(a) A DF must not carry out any processing which may have any detrimental effect on a child.

(b) A DF must not undertake tracking or behavioural monitoring of children or target advertisement towards children.

(c) A DF is exempted from the requirement to obtain verifiable parental consent and restrictions on tracking/behavioural monitoring/targeted advertising if:

- *By class:* Processing is undertaken by a clinical establishment, mental health establishment, healthcare professional, allied healthcare professional, educational institution, creche or child day care centre, transportation service provider for educational institutions, creche or child care centre. Processing by such DFs is allowed for limited and narrow purposes of safety, education and health, during specific activities. For instance, processing by transportation service providers may only process such data during the course of children's travel to and from their educational institutions.

- *By purpose:* Processing is undertaken to:
  - exercise power, or performance a function in the interest of a child under any law,
  - for issuing benefit, licence or certificate under law or using public funds, where they have previously consented, or is available in any State database/register notified by the Central Government.
  - for creating a user account for communication by email,
  - for tracking the real-time location of a child,
  - for ensuring that any detrimental information, service or advertisement is not accessible to a child, or to confirm that that the DP is not a child.
  - Processing for such purposes is restricted to the extent it is necessary to perform the function or carry out the purpose.

The DPDPA and Rules are not clear on whether fresh consent is required when a child attains majority. It is likely that fresh consent would be required when this takes place, since the child becomes a data principal in their own right.

The restrictions on tracking or behavioural monitoring of children or targeting advertisements towards children are some of the most restrictive measures under the Act, creating operational uncertainties for ad-supported platforms and child-related services. Despite heavy industry feedback against these provisions when the draft Rules were introduced, they were retained. These prohibitions in effect appear to restrict any personalisation of services towards children, resulting in information or advertisements unrelated to the children's interest possibly being served to children.

**QUESTIONS TO ASSESS READINESS:**

- Do you have tools to determine if a customer whose personal data is being collected is an adult or a child?
- Do you have tools to track when a child becomes an adult, i.e., crosses 18?
- Do your systems prevent behavioural monitoring, tracking, targeted advertising, or profiling of children, as prohibited under the DPDPA?
- Are the relevant teams sensitised of the prohibitions on behavioural monitoring, tracking, targeted advertising, or profiling of children?

## 10. PROCESSING OF DATA OF PERSONS WITH DISABILITIES

A DF must obtain verifiable consent of the lawful guardian before processing any personal data of a PwD.

A person with disability is defined as a person who:

(a) has a long-term physical, mental, intellectual, or sensory impairment that, when combined with various barriers, prevents them from fully and equally participating in society. Even when they receive proper and adequate support, they still cannot make legally binding decisions.

(b) A person who has autism, cerebral palsy, intellectual disability (mental retardation), or any combination of two or more of these conditions. This also includes people with severe multiple disabilities. Even with proper and adequate support, they are unable to make legally binding decisions.

Hence, all disabled persons are not subject to these provisions. Only disabled persons that are unable to make legally binding decisions are covered. It is unclear how data fiduciaries will make this determination.

In this regard, the DF must undertake due diligence to verify that such guardian is appointed by a court of law or by a designated authority, or by a local level committee under the applicable guardianship law.

There are two applicable law governing appointment of guardians, i.e., the Rights of Persons with Disabilities Act, 2016, ("RPWD Act"), and the National Trust for the Welfare of Persons with Autism, Cerebral Palsy, Mental Retardation and Multiple Disabilities Act, 1999 ("NT Act").

The RPWD Act provides for the appointment of limited guardians by district courts or designated authorities notified by State Governments. Each State has enacted legislation providing for the appointment of guardians, such as Delhi under the Delhi Rights of Persons with Disabilities Rules, 2018, which enables district courts to appoint limited guardians to take legally binding decisions on behalf of the person with disability.

The NT Act provides for appointment of guardians by way of an application made to local level committees by (1) parents or relatives of persons with disability, or (2) by registered organisations. These committees subsequently confirm appointment upon determination of such applications.

However, there is significant overlap in scope of applicability between the NT Act and the RPWD Act, hence it is not clear which mechanism applies to certain disabilities, such as cerebral palsy, which is arguably covered under both. Additionally, it is unclear whether data fiduciaries would have the ability to undertake such sophisticated due diligence to make such determinations. This may result in data fiduciaries that are unable to comply with these provisions to cease offering their services to disabled persons, which defeats the purpose of Government initiatives to *increase* technical inclusivity of disabled persons.

**QUESTIONS TO CONSIDER READINESS:**

- Do you have tools to determine if a customer whose personal data is being collected is a person with disability as defined under the Act?
- Do you have the tools to determine if their guardian has been validly appointed under the RPWD Act and/or the NT Act?

## 11. RIGHTS OF DPs

A DF has to provide the following rights to its DPs:

i. If processing has been done based on consent or voluntary consent:
   (a) Right to withdraw consent;
   (b) upon a request, provide a summary of personal data being processed, identities of all DFs and Data Processors with whom personal data has been shared and the description of such data, and any other information relating to such processing.
   (c) Means to request correction, completion, updating and erasure of personal data.

ii. A DF must provide a right to nominate any other individual to exercise the rights of the DP under the Act in the event of death or incapacity.

iii. Right to grievance redressal: A DF must establish a grievance redressal mechanism for its DPs. The DF must respond to grievances within 90 days. If a DP is unsatisfied with the DF's resolution of its grievance, it may appeal to the DPB. A DP has to exhaust the opportunity of redressing her grievance under this mechanism before approaching the DPB.

iv. Publish on its website/app or both and on any correspondence with the DP the information of the means to make a request to exercise rights under the Act and any other information to identify the user such as mobile number, email address customer identification file number, customer acquisition form number etc.

There are no prescriptive procedures for appointing nominees, providing grievance redressal mechanisms etc., thereby providing flexibility to establish procedures and mechanism suitable to the business model. DFs will be required to set up mechanisms and designate a point of contact to enable the DPs to exercise their rights and inform the DPs of the same through its website/app.

**QUESTIONS TO ASSESS READINESS:**

- What rights is your organisation required to provide to DPs and how are these implemented?
- Do you have necessary infrastructure to enable DPs to enforce their rights?
- Are your internal teams (IT, product, HR, customer support) trained on how to recognise, escalate, and fulfil rights requests?

## 12. REASONABLE SECURITY SAFEGUARDS

A DF must implement technical and organisational measures to comply with the Act and Rules and must protect the data in its possession and in possession of its DPs by implementing reasonable security safeguards to prevent a data breach. This must include, at the minimum:

(a) Data security measures such as encryption, obfuscation, masking, use of virtual tokens;
(b) Access control measures;
(c) Visibility measures relating to access of personal data through appropriate logs, monitoring and review;
(d) Business continuity measures in the event of compromise of personal data such as by way of data-backups;
(e) Log and personal data retention for one year for detection and prevention of a compromise event.
(f) Inclusion of security requirements in data processing contracts.

**QUESTIONS TO ASSESS READINESS:**

- What safeguards does the organisation implement and are they adequate to meet the minimum requirements under the Rules?
- Do your contracts with data processors contain adequate measures to ensure they are implementing security measures?

## 13. DATA ACCURACY

When a DF processes personal data to make a decision affecting a DP or discloses it to another DF, the DF must ensure that the data is complete, accurate, and consistent.

## 14. SIGNIFICANT DATA FIDUCIARIES

A DF may be categorised as a Significant Data Fiduciary ("SDF") based on factors such as volume and sensitivity of personal data, risk to the rights of DPs, potential impact on the sovereignty and integrity of India, risk to electoral democracy, security of the state, and public order.

Apart from the general obligations, an SDF has to comply with certain additional obligations such as:

(a) Appoint an India-based Data Protection officer to represent the SDF and serve as the point of contact for redressing DPs grievances.
(b) Appoint an independent data auditor to undertake data audits to evaluate compliance.
(c) Undertake periodic audits, and Data Protection Impact Assessments ("DPIAs") to assess the risks to the rights of the DPs every twelve months.
(d) Submit a report to the DPB containing observations in the DPIA and audit.
(e) Ensure that personal data and traffic data is not transferred outside India if recommended by the committee constituted by the Central Government for this purpose.[14]
(f) Ensure that technical measures like algorithmic software adopted for hosting, storing, or sharing of personal data does not pose a risk to the rights of the DPs.

[14] This committee will include officials from the Ministry of Electronics and Technology and may include officials from other Ministries or Department of the Central Government

SDFs have not been notified as yet, however will be notified post 14th May, 2027 (i.e., after the enabling provisions for notification come into effect).

SDFs that have global operations may be subject to localisation obligations to localize personal data and traffic data in India basis the committee's recommendations. In such cases, they would need to ensure their infrastructure supports such retention in India.

There are also certain ambiguities in the implementation of the requirements in relation to DPIAs. For instance, the Rules suggest that the SDFs must carry out DPIA's every 12 months. However, typically DPIAs are carried out in advance of only high-risk processing activities. This suggests that DPIAs must be carried out even if there is no change in processing activity, or no additional processing activity. It is also unclear whether the DPIA may be carried out internally, or by an independent person.

## 15. CROSS-BORDER TRANSFERS

A DF must not process personal data in such counties or territories as notified by the government. The government has not specified any restricted countries yet.

Any personal data transfer to any foreign state or entity under the control of such state must comply with any restrictions specified by the government by general or special order. An Indian law which imposes additional restrictions on data transfers outside India will take precedence over the Act.

SDFs may also be required to ensure that personal data and traffic data is not transferred outside India if recommended by the committee constituted by the Central Government for this purpose.[15]

A data fiduciary must ensure that any cross-border transfer to a data processor is carried out under contract. Additionally, it must ensure that personal data is not further transferred to a black-listed country by the data processor or any sub-processor.

It is unclear if data directly collected by foreign DFs or Data Processors of Indian residents will be considered as a 'transfer', thereby attracting restrictions.

[15] This committee will include officials from the Ministry of Electronics and Technology and may include officials from other Ministries or Department of the Central Government

## 16. CONSENT MANAGERS

A novel mechanism has been introduced for DPs to provide, manage, review, or withdraw their consent through consent managers. It acts as an intermediary between the data fiduciary and DPs. They are also required to act in a fiduciary capacity toward DPs.

These entities will have to be registered with the DPB and can be held accountable to the DPs. They are also required to provide access to records and grievance redressal mechanisms to DPs, and can be penalised for non-compliance. Consent managers must be data blind, i.e., they cannot access contents of the data accessed through their platforms.

DPs must register as users on consent managers' platforms, and DFs are also simultaneously onboarded onto such platforms, enabling DPs to manage consents across DFs. Consents may be provided by the DPs both directly to DFs onboarded onto the platform, and to third-party DFs (not on the platform), through another onboarded DF that already holds their data.

**Eligibility Criteria**

Consent Managers must:

(a) Be a company incorporated in India;
(b) Have technical, operational, and financial capacity to fulfil obligations;
(c) Have a net worth of INR Two Crore or more;
(d) Have directors, key managerial personnel and senior management of general reputation and record of fairness and integrity;
(e) Undertake operations in the interest of the DPs
(f) Have sound financial condition and management
(g) Have adequate capital structure, earning prospects and likely volume of business;
(h) Ensure that the MoA and AoA contain provisions to ensure compliance with obligations under the Act and the Rules, along with policies and procedures to ensure compliance;
(i) Obtain independent certification that:
(j) its platform is in compliance with such standards and frameworks as notified by the DPB from time to time;
(k) There are appropriate technical and organizational measures to ensure compliance with such standards, and disclosure requirements for Consent Managers on their website/app.

Critically, Consent Managers cannot be foreign entities. Additionally, data fiduciaries cannot be consent managers so as to avoid conflicts of interest.

Upon meeting the eligibility criteria, applicants may apply for registration to the DPB.

Provisions related to consent managers will come into force from November 14th, 2026. Hence, entities desirous of becoming Consent Managers must ensure they meet eligibility requirements before they apply for registration by this date.

**Key Obligations**

Post registration, Consent Managers must, among others:

(a) Maintain records of consents managed, consent notices provided, and personal data shared with the relevant DF,;

(a)

(b) Fulfil access requests of DPs to access records and information shared in a machine readable format, and ensure such records are retained for 7 years or longer as may be required under law;

(c) Appoint a grievance officer and respond to grievances within a reasonable period, and at max 90 days.;

(d) Publish means to exercise rights on their website/apps;

(e) Implement reasonable security safeguards to prevent personal data breach;

(f) Avoid conflict of interest with DFs including with their promoters and key managerial personnel;

(g) Make certain disclosures on their website/app of their key managerial personnel;

(h) Audit the technical and organizational measures to ensure compliance with obligations and conditions.

Consent Managers are also restricted from transferring control of their entities without approval from the DPB, and sub-contracting or assigning their obligations.

While most obligations applicable to data fiduciaries are applicable to Consent Managers, there does not appear to be explicit obligations on Consent Managers to report data breaches, for instance.

DFs do not have to mandatorily onboard consent managers. However, if DPs desire to provide consent only through consent managers, DFs may need to accommodate such requests and calibrate their workflows accordingly.

## 17. DATA PROTECTION BOARD

- A Data protection Board or DPB has been established under the Act as the primary adjudicatory body. It has limited regulatory functions only in relation to Consent Managers. It will consist of 4 persons, including a Chairperson.

- Civil courts have been barred from entertaining suits or proceedings for any matter which falls within the ambit of the DPB. Members of the DPB will be appointed by the government.

- See Annexure B for the process of adjudication by DPB.

## 18. PENALTIES

Penalties can be imposed under the law only in case of a *significant* breach and after giving the person an opportunity to be heard. Penalties of up to INR 250 crore may be imposed by the DPB based on factors such as nature, gravity, duration of contravention, type of data affected, mitigating measures adopted, etc. These include:

(a) Lack of adequate security safeguards (up to INR 250 crore).

(b) Non-compliance with obligations relating to processing data of children (up to INR 200 crore).

(c) Contraventions relating to breach intimation (up to INR 200 crore).

(d) Non-compliance with additional obligations by SDFs (up to INR 150 crore).

(e) Any other non-compliance or residuary penalty (up to INR 50 crore).

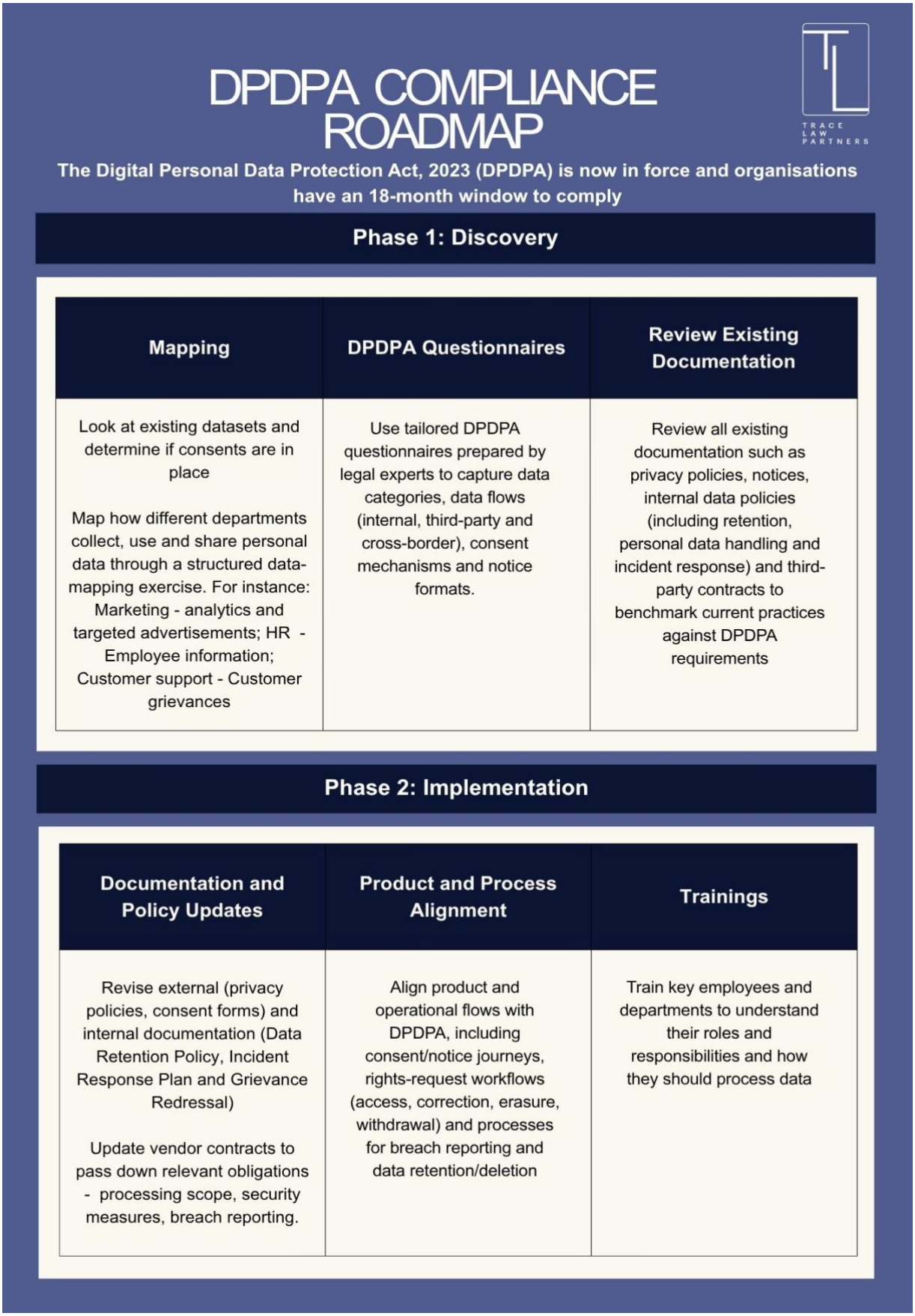
## 19. CALL FOR INFORMATION AND BLOCKING ORDERS

Where the DPB has imposed monetary penalties on a data fiduciary on two or more occasions, it may recommend to the Central Government that access to the relevant online platform be blocked in India. If the Central Government considers such blocking necessary in the interest of the general public, it may direct any Central Government agency or intermediary to block access to the platform. Prior to issuing such a direction, the Central Government shall afford the data fiduciary an opportunity to be heard.

The government is empowered under the Act and the Rules to call on the DF or intermediary to provide information for certain purposes including government use in the interest of sovereignty, integrity or security of India, or for performance of any lawful function, or for disclosure under any law, or to determine the status of the DF as an SDF. The government also has the power to require the DF or the intermediary to not disclose such furnished information to the affected DP or any other person without permission, if it affects the sovereignty, integrity or security of India.

The Act grants broad powers to the government, not limited to the DPB or any other independent regulatory body, to requisition information based on wide grounds without robust procedural safeguards raising concerns of potential misuse and overreach. The broad powers may negatively impact adequacy assessments for any transfers from European Union nations. DFs and intermediaries will need to be ready for swift responses and ensure that contracts with third parties include appropriate language for cooperation. Further, the restrictions on disclosures bring within its scope any information requested by DP while exercising their rights.

## Annexure A


DPDPA COMPLIANCE ROADMAP
TRACE LAW PARTNERS
The Digital Personal Data Protection Act, 2023 (DPDPA) is now in force and organisations have an 18-month window to comply
Phase 1: Discovery
Mapping
Look at existing datasets and determine if consents are in place
Map how different departments collect, use and share personal data through a structured data-mapping exercise. For instance: Marketing - analytics and targeted advertisements; HR - Employee information; Customer support - Customer grievances
DPDPA Questionnaires
Use tailored DPDPA questionnaires prepared by legal experts to capture data categories, data flows (internal, third-party and cross-border), consent mechanisms and notice formats.
Review Existing Documentation
Review all existing documentation such as privacy policies, notices, internal data policies (including retention, personal data handling and incident response) and third-party contracts to benchmark current practices against DPDPA requirements
Phase 2: Implementation
Documentation and Policy Updates
Revise external (privacy policies, consent forms) and internal documentation (Data Retention Policy, Incident Response Plan and Grievance Redressal)
Update vendor contracts to pass down relevant obligations - processing scope, security measures, breach reporting.
Product and Process Alignment
Align product and operational flows with DPDPA, including consent/notice journeys, rights-request workflows (access, correction, erasure, withdrawal) and processes for breach reporting and data retention/deletion
Trainings
Train key employees and departments to understand their roles and responsibilities and how they should process data

## Annexure B: Adjudication by DPB