# DECODING THE DIGITAL PERSONAL DATA PROTECTION RULES, 2025 AND ITS IMPLICATIONS

JANUARY 13, 2025

RACHANA RAUTRAY
*Anagram Partners*

**rachana.r@anagrampartners.in**

## Introduction

With the release of the draft Digital Personal Data Protection Rules ("**Rules**") under the Digital Personal Data Protection Act, 2023 ("**DPDPA**") on January 3, 2025, a near complete picture to the evolving data privacy landscape is now in sight. We examine the proposed Rules to identify its impact on technology business agnostic of its scale and irrespective of the staggered implementation contemplated for these Rules.

The Rules prescribe *inter alia* the terms of data processing, storage and erasure, breach notification and heightened compliance for '*significant data fiduciaries*'. These compliances would continue to apply to any processing (unless such processing is exempted), of digital personal data (collected digitally or subsequently digitized) of an individual within India, or outside India in connection with any activity related to offering goods or services to data principals in India (the DPDPA read with its Rules is referred as '*Indian Data Privacy Legislation*').

## The Consent Conundrum

Indian Data Privacy Legislation requires the data principal's consent to be obtained for any purpose of processing. The Rules elucidate that a notice for consent has to be '*presented and understandable independently of any other information made available by the data fiduciary*'. The notice should also include *inter alia* a fair account of details necessary for the consent sought, and a communication link or other means that facilitates (i) withdrawing consent as easily as providing it; and (ii) exercise of data principal rights such as access to details of other data fiduciaries with whom data has been shared, erasure of personal data or grievance redressal.

Flexibility in seeking consent arises in two scenarios:

*Processing is for legitimate use:* No consent being required for identified events, such as processing for a specific purpose that the data principal has 'voluntarily provided' her personal data, and has not indicated a lack of consent; or

*Prospective processing:* Notice for consent must be sent as soon as reasonably practicable, and processing can continue until consent is not withdrawn.

The Rules remain silent on how a data fiduciary or processor would need to facilitate the exercise of a data principal's rights when consent notice is not required.

*If you have any questions regarding the matters discussed in this publication, please contact the attorney(s) listed above or call your regular contact at Anagram.*

### *Industry Takeaway*

Considering consent is tied to purpose and the spectrum of exemptions, an enterprise should revisit the following:

- objectives for which it seeks personal data;
- the UI/UX design to streamline seeking consent for each purpose;
- identify when its user would likely
  - voluntarily provide personal data;
  - fall within the bucket of 'exempted processing'; or
  - seek withdrawal of consent vis-vis prospective processing; and
- once processing objectives and volume is identified, taking the decision to engage a consent manager or tokenization service providers, to ease compliance.

## Verifiable Consent for Minors or Persons with Disability

DPDPA mandates for verifiable consent to be obtained from parents/ guardians of minors or persons with disabilities and restricts processing that could have detrimental effect on the well-being of a child. It also restricts tracking, behavioral monitoring and targeted advertising to children, and employing due diligence in verifying the identity of the parent/guardian, though the standards for this due diligence are unclear.

While flexibility to determine the manner of verification of parental/guardian consent is afforded, reference must be made either upon:

- details of identity and age available with the data fiduciary; or
- details voluntarily provided, or virtual tokens issued by a government agency or a digital locker service provider.

### *Exemptions?*

Exemptions to seeking consent for personal data of minors or persons with disability, are available to:

- mental health establishments, (such as private or public institutions either wholly or partly meant for mental illness), clinical establishments or professionals, for provision of health services;
- educational institutions, to track and undertake behavioral monitoring for educational activities or in the safety of children enrolled by educational institution;
- enterprises offering creche or day care centers, to track or undertake behavioral monitoring for safety of children;
- data fiduciaries engaged by educational institutions, creche or child care centers for their safety, such as course of their travel; and
- any data fiduciary for minor data if such data is required to *inter alia* (a)

create user accounts where communication is limited to email; (b) ensure that information having detrimental effect on minors is not available; or (c) exercise of any power, function or duties in the interest of a child under any law in force.

***Industry Takeaway***

*Pharma and Education:* Exemptions vis-vis minor data can be leveraged along with exemptions available under the DPDPA for research, to offer goods and services for minors with limited privacy hurdles.

*Gaming and Social Media:* These industries are poised to grapple with this interpretation of 'detrimental effect' in the initial years of implementation of Indian Privacy Legislation. This is until such time that the government procures market data pursuant to its power to protect the interests of a child or under the garb of seeking information to identify significant data fiduciaries ("**SDFs**") as stipulated under the Rules.

## To Purge or Not to Purge?

The Rules set strict timelines for certain data fiduciaries (excluding significant ones) to erase personal data once the processing purpose is fulfilled, in addition to undertaking such erasure at a data principal's request.

E-commerce entities and social media intermediaries having at least 20 million registered users in India and intermediaries enabling users to access one or more online games with at least 5 million registered users in India, are required to erase personal data 3 years from the "*date the data principal last approached the data fiduciary for the performance of specified purpose or exercise of her rights, or commencement of DPDPA, whichever is latest*". These entities meeting the prescribed registered user thresholds are referred to as "*Specified Intermediaries*".

***Exemptions?***

The following circumstances would permit continued storage of personal data by Specified Intermediaries:

- compliance with law;
- enabling access to user account or virtual tokens that may be used to get money, goods or services;
- at least hours prior to the prescribed timeline, the data principal has logged into its user account or "*otherwise initiates contact with the data fiduciary for the performance of the specified purpose or exercise of rights*".

***Industry Takeaway***

- Specified Intermediaries will need to track their registered user base in India to balance their compliance requirements across all jurisdictions of operations.
- User engagement may need to be rethought, to identify which actions or inactions is sufficient to demonstrate "*contact with the data fiduciary has been made vis-vis performance of a specified purpose*".

***Illustration***

To deliver goods, a user may store their home address with an e-commerce entity. The purpose would be linked to such a delivery and therefore, unless the user deactivates the platform entirely, such entity will continue to store such data. Despite a user ceasing its engagement, storage of their home address enables the platform to retain delivery partners for relevant locations.

To ensure the extension of the erasure timeline, such e-commerce entity would need to assess whether the user browsing its catalogue of products/services is sufficient to demonstrate contact as envisaged under the Rules.

**Scope of the right of the Government to 'call for information'**

The Rules fall short of defining concrete fetters on the right of the Government to call for "*information*" from data fiduciaries such as prescribing the nature of information that can be sought. It merely specifies that the request will set a timeframe for providing information and prevent disclosure of such request being made, if the Government deems it prejudicial to the country's interests.

***Industry Takeaway***

Close ties between data storage versus data purging, is likely to result in litigations on whether disclosure of "*information*" under DPDPA breaches upon confidentiality rights that the data fiduciary may seek to exercise.

**Data Breach Notifications**

Distinct from the 6-hour timeline prescribed by the Indian Computer Emergency Response Team ("***CERT-In***"), data fiduciaries are required to ("***Notification Obligations***"):

- intimate data principals and the Data Protection Board ("***Board***"), "*without delay*" of any personal data breaches on becoming aware of such breach;
- deliver to the Board, within 72 hours or such longer period as granted by the Board, updated details of the breach, measures adopted to mitigate the same, findings of the cause, and a report regarding intimations provided to data principals.

Failure to meet Notification Obligations can result in monetary fines extending upto INR 2000 Million. Similar to the Notification Obligation, the Rules require enterprises to:

- identify appropriate security measures that ensure access controls for computer resources, log monitoring and review, continued processing despite a data breach;
- deploy detection tools for unauthorized access; and
- retain logs of personal data for 1 year unless other timelines are prescribed in law.

Failure to deploy these measures could attract penalties up to INR 2500 Million.

***Industry Takeaway***

- As an immediate step, an enterprise should identify the nature of actions vis-vis personal data that amounts to a personal data breach. For instance, in case of '*ransomware attacks*', determining the stage such attack would result in "*unauthorized processing*", "*accidental disclosure*" or "*loss of access*", would drive the notification decision.
- Close technical and legal breach monitoring systems must be put in place to identify and guide reporting. In the initial years of implementation, guidance of reporting can be driven by the directions issued by CERT-In on April 28, 2022.
- Specified Intermediaries would need to marry the purpose of processing, data purge and retention compliances under its consent notices, such that it can meet its data logs and deletion obligations.

**Data Protection Officers vs. Point of Contact vs. Officers determining Processing Decisions**

The Rules require data fiduciaries to publish the "*business contact information*" of the person that can address queries from the data principal, in addition to India based data protection officer is such data fiduciary is classified as a significant data fiduciary ("**SDF**").

If an enterprise processes personal data for research, archiving or statistical purposes that does not result in a decision on a specific data principal, to benefit from the consent exemption, standards under Schedule 2 of the Rules must be met. This includes, processing being carried out in a lawful manner, limiting processing to "*achieve its purpose*" and ensuring accuracy of personal data. Failure to adhere to these requirements while benefiting from the consent exemption, could result in liability accruing on the "*person who alone or in conjunction with other persons determines the purpose and means of processing of personal data*".

***Industry Takeaway***

- As there are no further conditions to this requirement, any personnel within an organization can be designated to carry out such liaison functions, without requiring such individual to be a citizen of India or domiciled/based in India.
- The point of contact could wear multiple hats of grievance redressal for instance, as also required under the Consumer E-Commerce Rules, 2020.
- There is sufficient flexibility under the Rules to restrict "*business contact information*" to emails or other correspondence information that does not necessarily set out the explicit identity of such point of contact so long as access is effectively provided to a data principal in case of a privacy query.
- For research related processing, executive directors or other key management personnel may incur liability in instances where their business decisions vis-vis data analytics on behavioral patterns of its data principal sets are contrary to the stipulated processing standards.

**Impact on Significant Data Fiduciaries**

While the Rules remain silent on the entities that would be classified as SDFs, expanded compliances beyond the scope of sub-ordinate legislation have been introduced, requiring:

- due diligence measures to be in place for "*algorithmic software*" that ensures that such software does not pose a risk to a data principal; and
- personal data as well as "*traffic data*" being localized.

### *Industry Takeaway*

- It is likely that the registered users' thresholds prescribed under the data purging compliance discussed above, would drive the decision on identifying SDFs. Accordingly, apart from Specified Intermediaries, large scale technology businesses such as FinTech's having more than 20 million registered Indian users could be classified as SDFs.
- Negotiations between SDFs and their data processors are likely to be contentious, as SDFs would require data processors to entirely open up their processing practices, including proprietary software, in order to comply with the Rules.

## Hurdles for Offshore Entities

The Government has the right to issue general and special orders prescribing conditions on data transfers to any foreign state or any person or entity controlled by any agency of such a foreign state. This is in extension to the right under DPDPA where the Government can also ban cross-border data transfers to specific countries.

### *Industry Takeaway*

Presence of offshore technology businesses in India is likely to take a hit, specifically Indian data center businesses on account of the possibility of ongoing restrictions to cross-border data transfers, heightened compliances arising out of the classification as an SDF and their books being called upon by the Government in exercise of its information access rights.

## Conclusion

While these Rules fulfill their directive to establish principles rather than detail procedures as alluded to under the DPDPA, the ambiguity in interpretation can be beneficial to enterprises, provided that the Government honors the industry's autonomy in developing tailored compliance methods.

In the current climate, it is crucial for enterprises to engage with specific nuances, rather than relying on the Government to prescribe compliance in detail during the consultation process. Given the growing compliance requirements related to volume, purpose, and nature of processing, the key takeaway moving forward is that processing decisions will be intentional and guided by necessity, rather than the current practice of processing personal data indiscriminately, regardless of the purpose.



anagrampartners
Mumbai | Delhi

*Follow us for more*
/ anagrampartners.in

0101—2025