The Dialogue®
INFORM ENGAGE IDEATE

Preliminary Analysis

DRAFT DIGITAL PERSONAL DATA PROTECTION RULES, 2025

January, 2025

→

Preliminary Analysis

DRAFT DIGITAL PERSONAL DATA PROTECTION RULES, 2025

Authors: Kamesh Shekar and Vaishnavi Sharma

Designer: Shivam Kulshrestha

The Dialogue is a public policy think tank with a vision to drive a progressive narrative in India's policy discourse. Founded in 2017, we believe in facilitating well-researched policy debates at various levels to help develop a more informed citizenry, on areas around technology and development issues. The Dialogue has been ranked as the world's Top 10 think tanks to watch out for, by the Think Tank and Civil Societies Programme (TTCSP), University of Pennsylvania in their 2020 and 2021 rankings.

For more information
Visit thedialogue.co

Suggested Citation
Shekar, K. & Sharma, V. (January 2025) *Preliminary Analysis - Draft Digital Personal Data Protection Rules, 2025*. The Dialogue

Catalogue No
TD/PDG/PA/0125/01

Publication Date
January 6, 2025

Disclaimer
This document presents a preliminary analysis of the draft rules under the Digital Personal Data Protection (DPDP) Act, 2023 does not necessarily constitute as the position of The Dialogue. It is intended solely to provide an initial overview of key provisions and potential areas of impact. A comprehensive analysis with stated recommendations will be prepared for submission to MeitY.

Contents

1. Introduction

Intrinsic to India's long-drawn transition towards chartering a privacy-safe environment, the Ministry of Electronics and Information Technology (MeitY), Government of India, enacted the Digital Personal Data Protection Act, 2023 (DPDPA 2023) during the monsoon session of the Parliament, on 11th August 2023. The Act sets obligations for Data Fiduciaries and Significant Data Fiduciaries, provides safeguards for children's data, vest rights in individuals, allows cross-border data transfers, outlines exemptions from the Act as well and provides contour of the Data Protection Board (DPB), financial penalties, and grievance management system.

In continuation of the enactment, MeitY published the Draft Digital Personal Data Protection Rules, 2025 (DPDP Rules, 2025), which fleshes out the sections of the Act and provides directions toward operationalising the provisions. While this is a step in the right direction, as we move forward, some rules require further deliberation to ensure that we have a data protection regulation that balances state interest, business development, and consumer protection.

Towards that objective, this preliminary analysis document explores the key legal and policy provisions enumerated in the rules while discussing the potential impact of such provisions on individuals and businesses. As follows, the documents deliberated on some of the key provisions within DPDP Rules 2025, which would impact the ecosystem as we move towards operationalisation.

2. Analysis of the Draft Rules

2.1. Short Title and Commencement

About the Rule: Rule 1 of the DPDP Rules 2025 provides that rules about data fiduciaries and consent managers will become effective on a specified date prescribed by the central government. However, the rules governing the Data Protection Board and Appellate Tribunal will take effect immediately from the date of notification of the DPDP Rules 2025.

Implication of the Rule: This is a step in the right direction, as industry players, including emerging start-ups and MSMEs, will require time for transition. However, as the date of commencement of the rules is yet to be suggested, the government needs to consider the practical realities of the ecosystem so that sufficient transition time is accounted for. Moreover, Rule 1 signals a promising direction towards implementation, as establishing the Data Protection Board will commence as soon as the DPDP Rules 2025 are notified. This early activation will help lay the groundwork for enforcement and direction for operationalisation.

2.2 Notice given by Data Fiduciary to Data Principal

About the Rule: Rule 3 on notice to seek the data principal's consent provides direction on how notice must be given. The rule also elaborates on the necessary details to be provided by data fiduciaries to data principals so that they can make informed decisions based on their consent.

Implications of the Rule: The rules governing notice aim to enhance clarity by ensuring that specific provisions are presented in a manner that is comprehensible and independent of any additional information. The term "presented" could be interpreted to encompass visual representations, such as infographics, which may improve accessibility and comprehension.

The requirement for an itemised description of the personal data requested and associated goods and services will clarify things for Data Principals. Further, the Rule mirrors the provisions of the Act by explicitly stipulating that withdrawing consent should be as straightforward as granting it. This could significantly mitigate the risks associated with "dark patterns" or the deliberate obfuscation of consent-withdrawal mechanisms.

2.3. Registration and Obligations of Consent Manager

About the Rule: Rule 4, along with the First Schedule, sets the consent managers' obligations, registration mechanism, and accountability mechanism. As per DPDPA 2023, a Consent Manager is a person registered with the Data Protection Board who acts as a single point of contact for the Data Principal to give, manage, review, and withdraw their consent through an accessible,

transparent, and interoperable platform. It is not legally binding for Data Fiduciaries to onboard a consent manager to fulfil the consent requirements of the legislation; however, having a consent manager would aid in streamlining their processes around consent management.

Implications of the Rule: The rules outline several conditions for registration and impose broadly defined obligations under the Act. However, the precise nature and scope of consent managers are ambiguous. It is unclear what incentive a consent manager will get to pursue such consent management. Moreover, since, according to the Rules, data fiduciaries are to be onboarded onto consent manager platforms (this process is similar to the AA framework where Banks have to be onboarded as well), this may present issues as it may fall upon consent managers now to 'onboard' data fiduciaries. However, unless data fiduciaries are incentivised to participate, they may lack the motivation to undergo the onboarding process, particularly if they are already meeting their obligations under the Act.

Further, taking the example of AAs, the process of onboarding AAs is fairly technical and legally extensive. However, techno-legal guidance outlines how this would happen. Generally, the Rules do not provide such guidance for consent managers.

Besides, it is less clear whether a single consent manager will oversee all personal data in all sectors (e.g., health, finance, social media) or whether sector-specific consent managers will be established, similar to the Account Aggregator model[1]. When sector-agnostic consent managers make economic sense, however, having a sector-specific consent manager would aid in complying with DPDPA 2023 and sectoral requirements.

2.4. Standards of processing for the State and its instrumentalities for purposes exempted under the Act

About the Rule: Rule 5, along with the Second Schedule, establishes minimum standards for data processing under Section 7 (b) of the DPDPA 2023.[2]

Implications of the Rule: This rule specifically addresses exemptions granted to the state and its instrumentalities for purposes such as the provision of subsidies, benefits, services, certificates, licenses, or permits (e.g., driving licenses, welfare schemes) and does not encompass other relevant exemptions outlined under Section 7 of DPDPA 2023. Further, it provides for substantive standards and does not refer to techno-legal procedures for exactly implementing the section.

A critical concern arises regarding whether data collected and processed under other provisions, such as the "Certain Legitimate Uses" outlined in Section 7 of the DPDPA 2023, can be utilised by the government without restrictions. The issues with Section 7 include: (i) the term "instrumentalities" remains undefined and ambiguous, and (ii) the sub-sections to Section 7 of DPDPA 2023 are vague, allowing for broad and discretionary interpretation. While legitimate

1. The Account Aggregators (AAs), though provided for and established well before the enactment of the DPDP Act, 2023, are essentially a type of "consent managers" which are meant to facilitate the interoperability of financial information between the key stakeholders, keeping the customer at the forefront. AAs and other stakeholders in the framework are bound by the relevant directions of the RBI. See RBI Master Directions, https://rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=10598.
2. Section 7 (b) of the Act provides that a DF (specifically, the State and any of its instrumentalities) may process the data of a DPs for subsidy, benefit, service, certificate, licence or permit as prescribed, if (i) she has previously consented, or (i) when such data resides with the State and any of its instrumentalities in digital or non-digital form.

objectives may underpin these provisions, it is unclear what specific circumstances would necessitate such data processing beyond the stated purposes. For instance, if other laws, such as those related to criminal investigations, require certain information for investigative or other purposes, consent would not be necessary under these exemptions, nor would there be any standards mandated on the State or its "instrumentalities."

2.5. Reasonable security safeguards

About the Rule: Rule 6 mandates data fiduciaries to operationalise reasonable security safeguards at the technical and organisational levels. The rule suggests data fiduciaries take appropriate data security measures such as encryption, masking of data, etc. Besides, it also mandates having necessary mechanisms to monitor, view, and audit data flow and control access. While the listed security safeguards are minimum requirements, data fiduciaries may need additional security safeguards based on the nature, volume and type of data processed.

Implications of the Rule: This rule is a step in the right direction, clarifying the minimum security and safeguards requirements to be met while not prescribing any specific standards to be followed. However, the government must suggest technical frameworks and benchmark some international standards for technical measures like encryption, obfuscation, masking, and using virtual tokens mapped to personal information. Similarly, the government could provide some direction towards constituting access control measures and log retention. In addition to technical measures, it would be essential to benchmark some of the organisational measures suggested under Rule 6(1)(g).

2.6. Intimation of Personal Data Breach

About The Rule: The Rule clarifies the timeline and procedure for notifying a personal data breach to both data principals and the Data Protection Board (DPB) as prescribed in the DPDPA 2023. Rule 7(1) and Rule 7(1)(a) mandate data fiduciaries to report the data breach to the data principal and DPB immediately without any delay, while additional 7(2)(b) mandates data fiduciaries to provide a detailed report on the breach to the board within 72 hours.

Implications of the Rule: This rule significantly impacts Data Fiduciaries, necessitating a proactive approach to data security and breach management. The requirement to promptly report breaches ensures that Data Fiduciaries remain vigilant and responsive to potential data security threats. For Data Principals, this rule offers greater transparency and reassurance that their data is handled responsibly.

While the rules provide that data breaches must be notified to both data principals and the board without delay, the lack of a threshold for breach notifications and a timeline range could confuse the data fiduciaries and overburden regulatory bodies with minor incidents.

In addition to reporting an incident to the Data Protection Board, the data fiduciaries may have to report the incident to CERT-IN, sectoral regulators (if required), and other appropriate bodies within different timelines. For instance, under Rule 2 of CERT-IN Directive 2022, the data fiduciaries must report a data breach within 6 hours of noticing the incident. However, as we move forward, it would be essential to streamline the breach notification timeline to bring uniformity while avoiding hurdles to businesses and confusion.

Moreover, providing definitional clarity on subjective terminologies like “without delay” is essential to mitigate confusion and clarify the timelines for reporting the breach. Similarly, provisioning for flexibility in timelines for providing detailed data breach reports (as per Rule 7(1)(b)) is beneficial. However, the criteria for extensions need to be clearly defined to ensure transparency and uniformity.

2.7. Time period for specified purpose to be deemed as no longer being served

About The Rule: Rule 8 of DPDP Rules 2024 lays out specificities in terms of erasing data when the specified purpose for which the data is collected is done, and its retention is not necessary for compliance with any law for the time being in force.

Implication of The Rule: While it is a step in the right direction, there is less clarity in terms of why this rule only applies to specific classes of data fiduciaries listed under the Third Schedule, including (a) E-commerce entity having not less than two crores registered Indian users, (b) online gaming intermediary having not less than fifty lakh Indian registered users, (c) social media intermediary having not less than two crore registered Indian users.

2.8. Verifiable consent for the processing of personal data of a child or of a person with a disability who has a lawful guardian

About the Rule: Rule 10 discusses the due diligence to be followed by data fiduciaries when obtaining verifiable consent from parents and lawful guardians to process the personal data of children and persons with disabilities, respectively. Moreover, Rule 10(1)(b) layout means that data fiduciaries can generate a virtual token to identify the parent of a child.

Implications of the Rule: As provisioned in the DPDPA 2023, the verifiable consent process requires:

a. Identifying and segregating everyone who uses digital services based on age, i.e., below and above 18.
b. Followed by identifying and verifying the parent of an individual under 18.
c. Finally, parent consent must be collected, and a mechanism must be established through which data fiduciaries can verify the process (a,b,c) and demonstrate compliance with section 9(1) of DPDPA 2023.

Rule 10 laid out procedures for step (b), where data fiduciaries can verify identity and age details of parents using existing reliable data that they hold of parents or through using virtual tokens mapped to identity and age details issued by government-authorised entities like digital locker service providers. However, there is less clarity on how to proceed with (a) and (c). This would be difficult to implement in the digital setup, as it is difficult to ascertain whether a user is a minor. These issues may enable minors, such as a 16-year-old, to misrepresent their age (e.g., claiming to be 21 years old) and circumvent the requirements intended to protect them.

Moreover, the rules fail to prescribe specific verification methods besides digital locker systems. Whether phone calls, video meetings, signed forms, financial information, or other approaches will suffice to establish a parent or guardian's identity remains unclear. This ambiguity raises concerns about the adequacy and reliability of the verification process.

The high age threshold of 18 further complicates compliance, as individuals close to this age are unlikely to seek or desire parental supervision for using digital technologies. Moreover, there is less clarity regarding how the children's data would be handled once they become adults.

Children without any parents or lawfully appointed guardians are, in effect, excluded from the process of obtaining variable consent. However, to recognise a guardian, the rules must carefully enquire into the understanding of definitions of guardians from other relevant legislations such as The Guardians and Wards Act, 1890, etc.

Furthermore, the requirement for parental or guardian consent raises an additional issue: The adults might lack the technological literacy needed to provide well-informed and meaningful consent. The requirement for obtaining verifiable parental consent for every instance of data processing can also contribute to consent fatigue, as parents may become overwhelmed by the frequency and volume of consent requests. The could affect the validity of consent obtained, and may heighten risks for children, contrary to the intent of Section 9 of the DPDPA 2023.

2.9. Exemptions from certain obligations applicable to the processing of personal data of a child

About the Rule: Rule 11 provides that the class of data fiduciaries listed under Part A of Schedule VI will be exempt from Section 9(1) to Section 9(3) of DPDPA 2023. The rules also exempt specific purposes from compliance with Section 9(1) to Section 9(3) of DPDPA 2023, including observing due diligence with Rule 10.

Implications of the Rule: The suggested exemptions are narrow and only include education institutions, creches, child day care centres, mental health establishments, allied healthcare professionals, and clinical establishments. Exemptions must be expanded to digital service providers who add value to children's cognitive development and are for the best interests of the child, provided terminologies like "cognitive development" are defined.[3] Therefore, Rule 11 must also outline the procedure and parameters through which classes of data fiduciaries can seek

[3] Note, section 9(2) of the Act and the Rule in question already employ the term "well-being" without defining it, and do not refer to comparable legal standards established in relevant jurisprudence such as "best interests of the child."

exemptions from processing children's personal data for specific purposes.

Moreover, while the DPDPA 2023 prohibits targeted advertising directed at children, contextual advertising, or advertising based on the content of the page, is still possible and may be appropriate. Note that some data fiduciaries may rely on advertising to offer their products or services for free. However, aspects of contextual advertising are not discussed in Rule 11 along with Part B of the Fourth Schedule.

2.10. Additional obligations of Significant Data Fiduciary

About the Rule: Rule 12 provides additional obligations for the Significant Data Fiduciaries, including conducting a data protection impact assessment and audit every twelve months. The Rule 12(3) mandates due diligence on algorithmic software deployed.

Along with Section 10(1)(c)(iii) of DPDPA 2023, where the central government could suggest additional obligations for significant data fiduciaries, Rule 12(4) provisions for potential data localisation measures for significant data fiduciaries, where a class of personal data suggested by the committee formed by the central government would be restricted from flowing outside the country.

Implications of the Rule: Restrictions on cross-border data transfer would be disproportionate, as data security is agnostic to location. Various existing and upcoming sectoral regulations also mandate data localisation.

Some of the regulations which mandate data localisation are (a) Reserve Bank of India's 2018 circular titled "Storage of Payment System Data", which mandates conditional data localisation mandate, where end-to-end data relating to payment systems must be stored in India while it can be processed outside the territory of India brought back to India within 24 hours, (b) Amended Unified Access License agreement of Ministry of Communications and IT mandates telecom service providers to store and process subscribers information locally, (c) IRDAI's Outsourcing of Activities by Indian Insurers Regulation, 2017 mandates localisation of payholders' account details; in case of cross-border transfer the insurer must ensure easy regulatory access and oversight by the Authority. Besides, IRDAI's Maintenance of Insurance Records Regulation, 2015 mandates organisations to store insurance data within India's territory.

With these differences in regulations and guidelines, it is technically impossible to process data by segregating it according to the difference in mandates. This would cause operational concerns for businesses, especially for the data processors and cloud service providers, as they must reprogram their systems. Also, aggregating data of individuals across the globe is essential for better insights; however, when certain data sets are restricted from flows across the border, this might hamper the businesses' data processing capabilities.

2.11. Processing of personal data outside India

About the Rule: Through Rule 14, the government may prescribe specific requirements to data fiduciaries, which they must follow before sharing or transferring personal data (either processed within India or outside) with foreign governments or their agencies or entities. Rule 14 does not entirely align with Section 16(1) of DPDPA 2023, which discusses processing personal data outside India. Section 16(1) only discusses restrictions on data transfer for processing outside India, while Rule 14 also discusses data processed within India's territory.

Implications of the Rule: Rule 14 grants the Government of India extra-territorial authority to regulate and impose restrictions on foreign governments or their agencies seeking access to personal data. This rule applies to data processed outside India when it is connected to businesses operating within Indian territory, or involves the personal data of Indian citizens processed within India.

While the rule does not enforce a blanket ban on cross-border data transfers, routine data flows for business or operational purposes remain unaffected. However, it empowers the government to impose restrictions or set specific requirements in cases where foreign governments, law enforcement agencies, or intelligence bodies request access to personal data.

This marks the first instance in India where a legal provision directly restricts access to a foreign state or agency. The government may invoke this rule if it determines that a foreign agency's data request poses a threat to India's national security, public order, individual privacy rights protected by Indian law, or conflicts with India's diplomatic or strategic interests.

The underlying intent of Rule 14 seems to be to determine the process of access of personal data related to India by foreign agencies. It seeks to drive oversight, checks and balances, before such data is accessed, and emphasises the need for the Indian government's alignment in cases where a foreign agency cites national security interests as the basis for access. This rule, however, may cause friction for business operations.

2.12. Exemption from the Act for research, archiving or statistical purposes

About the Rule: Rule 15 outlines the standards to be followed as prescribed under the Second Schedule while availing exemptions from the DPDPA 2023 for research, archiving and statistical purposes.

Implications of the Rule: Rule 15, along with Section 17(2)(b), provides an exemption from DPDPA 2023 for research and statistical purposes; it is unclear whether this would apply to players within the AI ecosystem, especially AI developers. An argument could be made that research includes commercial research, which could include training of datasets, but this clarity is missing from the rules.

2.13. Appointment of Chairperson and other Members

About the Rule: Rule 16 lays out the appointment procedure of the search-cum-selection committee, which could appoint the chairperson and other members.

Implications of the Rule: The proposed Data Protection Board (DPB) will be the cornerstone of India's data governance endeavours, and it will function as the independent adjudicatory authority for all relevant stakeholders - including the Government. In its present form within Rule 16, questions about its independence and capacity are raised due to the central government constituting it. This is a matter of concern as the Government may soon be one of the biggest data fiduciaries in India. Predominantly executive-driven appointments will bring into question the ability of such a board to perform as an independent arbitrator in cases involving the Government. Also, without a separate and independent board, India's chance to be considered adequate for the essential purposes of cross-border data transfers by other jurisdictions may be reduced, impacting India's position in the global digital economy.

2.14. Terms and conditions of appointment and service of officers and employees of the Board

About the Rule: Rule 20 lays out the terms and conditions for the appointment and service of officers and employees of the DPB. This aligns with Section 24 of the DPDPA 2023, which provides that the central government may prescribe terms and conditions of appointment and service of the officers and employees of the Board.

Implications of the Rule: Rule 20 is a step in the right direction as this would enhance the capacity of the Data Protection Board. As we move forward, it is essential to have a tiered structure for the office of the Data Protection Board, adopting a bottom-up approach where tasks and responsibilities are mapped and partially calibrated.

2.15. Calling for information from a Data Fiduciary or intermediary

About the Rule: Rule 22 empowers the central government, through authorised personnel, to require data fiduciaries and intermediaries to share personal information about the data principal to perform functions under Indian laws or to secure India's sovereignty, national security, integrity, etc. Besides, the rule also restricts data fiduciaries from disclosing information on such requests with data principals to maintain the confidentiality of the requests.

Implications of the Rule: Preserving national security is one of the state's key legitimate interests. However, there must be checks and balances on the state's access to personal information for law enforcement. Therefore, the rules must not deviate from *the Justice K. S. Puttaswamy v. Union of India* [2017] 10 S.C.R. 569, i.e., to balance individual interests and legitimate concerns of the state, such as national security, public order, etc.

thedialogue.co

LinkedIn | The Dialogue

Twitter | The Dialogue

Whatsapp | The Dialogue

Instagram | The Dialogue