Document Date: 4 March 2025

## Recommendations on the Digital Personal Data Protection Rules, 2025

Submitted to the MEITY, Government of India.

Authors:

1. Prabhat Mishra, Doctoral Scholar, Centre for the Study of Law and Governance, Jawaharlal Nehru University, New Delhi and
2. Dr. Nupur Chowdhury, Centre for the Study of Law and Governance, Jawaharlal Nehru University, New Delhi

Email for further communication: prabhat0104@gmail.com

### Introduction

Section 40, subsections (1) and (2), of the Digital Personal Data Protection Act, 2023 (hereafter, 'the Act') empower the Central Government to make rules consistent with the provisions of the Act by notification, In light of this, the Digital Personal Data Protection Rules, 2025 (DPDP Rules) provide the operational framework for implementing the Digital Personal Data Protection Act, 2023 (DPDP Act). We sincerely appreciate the call for public consultation by the Ministry of Electronics and Information Technology (MeitY) and hope that our recommendations will contribute to assessing the coherence, legality, and effectiveness of the Rules, ensuring they align with the statutory provisions of the DPDP Act.

We have reviewed the DPDP Rules with reference to two aspects. First, whether the rules align with the substantive rights and institutional structures as provided under the DPDP Act? Second, whether the rules conform with principles of good governance in terms of clarity, coherence and effectiveness of implementation strategies.

**Themes in the recommendations**

Our recommendations below revolve around five interconnected themes:

1. Legal Compliance with the DPDP Act
2. Rights of Data Principals
3. Overall Institutional Framework
4. Government Exceptions
5. AI Governance

Our analysis finds that while the Rules mostly align with the Act, although specific provisions either exceed the Act's scope or lack necessary clarity. Further, the Rules fall squarely short in addressing the rights of data principals and liabilities of data fiduciaries. Additionally, in examining whether the proposed institutional framework sufficiently supports data protection governance in India, we find a lack of explicit mention of impact of AI-tools on privacy, thereby making it less effective in confronting contemporary realities. Strengthening these aspects will align India's data protection framework with global best practices and ensure a truly forward-looking, robust yet balanced, privacy-preserving regulatory regime in India.

---

**Rule-wise Recommendations:**

**Rule 1**: While staggered implementation of the rules is practical, more clarity is needed regarding the timeline of implementation of rules 3 to 15 and rules 21 and 22. Ample time should be given to all stakeholders to comply with the full implementation of the Act.

**Rule 2**: The Act defines consent manager as "*a person registered with the Board, who acts as a single point of contact to enable a Data Principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform*". We recommended that the roles and responsibilities of consent managers be more explicitly defined. Specifically, clarity is required, whether the data principals are now required to exercise their rights only through consent managers.

**Rule 3**: Subsection (b)(ii) states the requirement for data fiduciaries' notice to provide "*a fair account of the details necessary*" in clear and plain language. The phrase is highly ambiguous and can lead to various interpretations. Moreover, the notice is stipulated "*at the minimum*" to contain "*specified purpose*". These terms are also open to interpretation. We recommend that the Rules, in accordance with Section 6 of the Act which states "*The consent given by the Data Principal shall be free, specific, informed, unconditional and unambiguous with a clear affirmative action, and shall signify an agreement to the processing of her personal data for the specified purpose and be limited to such personal data as is necessary for such specified purpose*", should provide a standardised notice format as an annexure for the fiduciaries to comply.
We propose that an item wise affidavit listing the rights of the data principals should be separately and periodically sent to Data Principals by the Data Fiduciary informing them of their rights under the Act.

**Rule 4**: Section 6, subsection (7) of the Act states the intermediary nature of consent managers as follows: "*The Data Principal may give, manage, review or withdraw her consent to the Data Fiduciary through a Consent Manager*." Subsection (8) establishes a fiduciary relationship between the Consent Manager and Data Principal as follows: "*Consent Manager shall be accountable to the Data Principal and shall act on her behalf in such manner and subject to such obligations as may be prescribed*." However, nowhere is the purpose for consent made clear. Moreover, the term "accountability", which does not have a legal basis, is used in several places. The proper legal term is "liability", and it should be clearly stated whether Data Fiduciaries or Consent Managers bear liability for consent violations. In tandem, the procedure for making a complaint against Consent Managers should be explicitly stated as well.

Point 8, Part B of the First Schedule, Obligations of Consent Manager, states that "*The Consent Manager shall act in a fiduciary capacity in relation to the Data Principal*". There is potential conflict of interest in the Consent Manager's role as a data fiduciary as well as an intermediary. Point 3 states that the Consent Manager shall maintain a record of notices, requests for consents, consents given, denied or withdrawn while Point 2 dictates that the records kept by the Consent Manager shall not be readable by it. It is not possible for the Consent Manager to maintain records on its platform and be unable to read them.

Finally, point 7 mentions that "*The Consent Manager shall take reasonable security safeguards to prevent personal data breach*". We recommend that the required cybersecurity protocols be explicitly mentioned or atleast reference should be made to best practices of the industry, as Rule 6 does in the case of Data Fiduciary, lest the Consent Manager's platform should turn out to be the weakest link in data breaches. Overall, Rule 4, read with the First Schedule needs streamlining with the motive of making rules and responsibilities clearer through the lens of liability.

**Rule 5**: Provisions are made in this rule to grant the State widespread exceptions as per Section 7 of the Act. We recommend that mandatory processing of data by the State and its instrumentalities should come with a no-harm principle to ensure the Rights of Data Principals. Heightened security protocols and adequate judicial oversight should be explicitly established for mandatory processing.

Having said that, the inability of the State to process data should not be used as a reason for denial of any subsidy, benefit, service, certificate, licence or permit, either. In other words, the State is liable to correct processing of data. Point (d) in the Second Schedule calls for "making reasonable efforts to ensure the accuracy of personal data", which is wholly inadequate and should be reconsidered.

We recommend that a similar standard for the State should be specified as set for Significant Data Fiduciaries in Rule 12 (4) to *"observe due diligence to verify that algorithmic software deployed by it for hosting, display, uploading, modification, publishing, transmission, storage, updating or sharing of personal data processed by it are not likely to pose a risk to the rights of Data Principals."*

**Rule 6**: Neither the Act nor the Rules define the term "reasonable security safeguards". Further, there is no provision for auditing by a third party of such safeguards. The issue of data security is a trenchant one, but various jurisdictions have come up with holistic views on reasonable administrative, technical, and physical data security practices to protect personal data's confidentiality, integrity, and accessibility, like Title 16 of US Code of Federal Regulations[1]. In accordance with the best practices worldwide, the case for instituting sector-specific cybersecurity guidelines may also be explored.

We recommend that terms like "reasonable safeguards" and "appropriate measures" should be avoided as they do not convey meaning in the modern cybersecurity parlance. Instead, international technical standards and security protocols should be explicitly mentioned. We also recommend that annual security audits and cybersecurity certifications should be conducted by a competent third party.

**Rule 7**: A standard format for breach notifications to both Data Principals and the Data Protection Boards is recommended. Further, we recommend annual self-reported transparency assessments of Data Fiduciaries.

**Rule 8**: The Rule, read with the Third Schedule makes distinctions between different classes of Data Fiduciaries and stipulates the time periods for erasure of user data. However, "date on which the Data Principal last approached the Data Fiduciary" is vague and could be understood differently by the parties, for example, as the date on which contact is made with the Data Protection Officer by the user, or the date on which user request is processed by the fiduciary. Therefore, the cut-off date should be explicitly mentioned and uniformly applied.

**Rule 9**: Companies routinely ignore user queries or make information obscure on their websites and apps, as anyone who has tried and failed to deactivate their account on a social media website can attest. Therefore, the requirement to "prominently publish" information of the person responsible for answering questions about processing is not enough. We recommend that such information should be included in the binder of rights proposed above as well as made available on request over email.

**Rule 10**: We agree that it is important to have special provisions for processing of personal data of children or persons with disabilities. However, the issue requires balancing several considerations. The Rules make parents or guardians Data Principals on behalf of the children or persons with disabilities, which may have adverse impacts on their rights and autonomy as

[1] https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314

well. A child may have disagreements with their parents with respect to online activities or a person with disabilities may find it a violation of their autonomy to disclose their activities to their guardians. What of the cases when a child chooses to lie about their age or a child without parents or legal guardians?

Part A of the Fourth Schedule provides exceptions for Data Fiduciaries that are clinical establishments, mental health establishments, healthcare professionals, allied healthcare professionals, educational institutions, crèches, child day care centres, or engaged by an educational institution, crèche or childcare centre for transport of children enrolled with such institution, crèche or centre. The conditions for exceptions are explicitly defined, however, at S.No. 3, column of conditions, we recommend that the word "or" between a) and b) should be replaced with "and".

**Rule 12**: Subsection 3 reads, "*A Significant Data Fiduciary shall observe due diligence to verify that algorithmic software deployed by it for hosting, display, uploading, modification, publishing, transmission, storage, updating or sharing of personal data processed by it are not likely to pose a risk to the rights of Data Principals*." Algorithms are the core building blocks of programming; every software is algorithmic. An algorithm is just a step-by-step recipe of instructions for a computer. The term "algorithmic software" refers to everything and nothing. It should either be substituted with names of specific software or "AI models", or "AI-driven decision-making", if that was the intended meaning. Further, it is not clear how the connection between such software and personal data would be proven since it is difficult to pinpoint which algorithmic processes are "likely to pose a risk".

More significantly, this points to a general shortcoming of the Rules taken in their totality. The rise of AI models has driven innovation and transformed industries in the past few years. In parallel, there has been a well-documented rise of harms related to AI-based surveillance, profiling, scams, malicious targeting, and so on. The Act as well as the Rules are silent on this issue. We recommend that this potential gap should be addressed by formulating provisions that specifically ensure Data Principals' rights with respect to AI tools and products as well as provide a right to explanation and grievance redressal.