Future of Privacy Forum Asia-Pacific
9 Straits View #06-07
Marina One West Tower
018937 Singapore

5 March 2025

Ministry of Electronics and Information Technology (Government of India)
Electronics Niketan, 6
CGO Complex,
Lodhi Road
New Delhi - 110003

To the Minister and all staff concerned,

Draft Digital Personal Data Protection Rules, 2025

The Future of Privacy Forum (**FPF**) is grateful for the opportunity to provide comments on the Ministry of Electronics and Information Technology (**MeitY**)'s draft Digital Personal Data Protection Rules, 2025 (dated 3 January 2025) (**DPDP Rules**).

About FPF

FPF is a global non-profit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies. FPF brings together industry, academics, consumer advocates, and other thought leaders to explore the challenges posed by technological innovation and develop privacy protections, ethical norms, and workable business practices.

Comments from FPF

FPF's comments on the Draft Guide are set out in **Annex A** for your kind consideration. We have also submitted a shorter version of our comments through the MyGov portal.

We welcome the opportunity for future engagement with MeitY on the DPDP Rules. If you have any questions on, or responses, to any of the comments set out in Annex A, or if we may be of any further assistance in the development of the DPDP Rules, please do not hesitate to contact Josh Lee Kok Thong (jlee@fpf.org) and Dominic Paulger (dpaulger@fpf.org). Thank you.

Yours sincerely,

Josh Lee Kok Thong
Managing Director for Asia-Pacific
Future of Privacy Forum

(enc.)

Annex A: Comments

FPF is committed to supporting the development of India's data protection ecosystem. We welcome efforts of MeitY and the Government of India to develop the DPDP Rules to provide much-needed guidance on the implementation of the Digital Personal Data Protection Act, 2023 (**DPDPA**). Nevertheless, we note that several aspects of the DPDP Rules could benefit from further clarification. To this end, we highlight our main recommendations below:

1. Replace the mandatory minimum security measures in Rule 6 with a more flexible, principles-based approach.
2. Adjust the DPDP Rules' approach to data breach notifications to avoid potential downstream operational issues.
3. Provide greater detail to operationalize Verifiable Parental Consent (**VPC**) under Rule 10 effectively.
4. Clarify the scope and implementation of the exemptions in Rule 11 and the Fourth Schedule relating to processing children's data.
5. Clarify the criteria and methodology for designation of Significant Data Fiduciaries (**SDFs**), and guidance on SDFs' obligations under Rule 12.
6. Provide greater clarity on the procedure for the exercise of Data Principals' rights under the DPDPA.
7. Provide greater clarification for cross-border data transfer mechanisms in Rules 12(4) and 14.
8. Expressly empower the Data Protection Board of India (**Board**) to issue interpretative guidance on the DPDPA.

We hope that MeitY and the Government of India will find these recommendations useful in respect of further development of the DPDP Rules. FPF would be happy to engage in further consultations or discussions, and provide further support and assistance, wherever it may be helpful.

1. Replace the mandatory minimum security measures in Rule 6 with a more flexible, principles-based approach.

FPF appreciates the policy intent to establish clear security standards through Rule 6 of the draft DPDP Rules. We wish to propose, however, that MeitY adopts a "principles-based" approach to Rule 6 — specifically, one that specifies reasonable security expectations and the need to implement appropriate measures at a high level, but avoids prescribing the adoption of any specific measures in a blanket manner, irrespective of other factors (such as the size and type of the Data Fiduciary, or the nature of the personal data being processed).

Such an approach is a common practice among data protection regulators globally, including in the following jurisdictions:

- **Brazil:** Article 46 of the General Data Protection Law (**LGPD**) requires controllers and processors (collectively, "data processing agents") of personal data to adopt security, technical and administrative measures able to protect personal data from unauthorized accesses and accidental or unlawful situations of destruction, loss, alteration, communication or any type of improper or unlawful processing. Brazil's national data protection authority (**ANPD**) has released a guide on information security for small data processing agents[1] which recommends many of the measures recommended under Rule 6 of the

[1] https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-vf.pdf

draft DPDP Rules as good practices for complying with Article 46 of the LGPD, but does not make these practices mandatory. The guide also clarifies that the ANPD expects larger data processing agents to comply with international best practices for information security but again, does not mandate the adoption of any specific practices.

- **Singapore:** Section 24 of the Personal Data Protection Act (**PDPA**) requires organizations to "protect personal data … by making reasonable security arrangements to prevent – (a) unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; and (b) the loss of any storage medium or device on which personal data is stored." Singapore's Advisory Guidelines on Key Concepts in the PDPA[2] further clarify that "[t]here is no 'one size fits all' solution for organisations to comply with the Protection Obligation [in Section 24 of the PDPA]. Each organisation should consider adopting security arrangements that are reasonable and appropriate in the circumstances …"

- **South Africa:** Section 19 of the Protection of Personal Information Act (**POPIA**) requires parties to secure the integrity and confidentiality of personal information in their possession or under their control by taking "appropriate, reasonable technical and organisational measures to prevent (a) loss of, damage to or unauthorised destruction of personal information; and (b) unlawful access to or processing of personal information." The provision outlines several mandatory reasonable measures at a high level and requires parties to have "due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations."

In our view, it is important to provide organizations flexibility to identify and implement appropriate measures based on factors specific to their operations. These factors may include the nature of data processed, technological capabilities, implementation costs, and evolving industry standards. Indeed, adopting a fixed framework to security measures could pose several implementation challenges.

- **First**, a rigid, one-size-fits-all approach may inadvertently burden Data Fiduciaries, especially small and medium enterprises that may lack the technical expertise to implement advanced security controls, potentially discouraging compliance. Conversely, the prescribed measures may be insufficient for organizations handling sensitive personal data or operating complex data protection requirements. In prescribing as such, such organizations may be lulled into a false sense of security – believing that simply following such measures would be enough to protect personal data under their care regardless of their operational context.

- **Second**, stipulating fixed security measures could cause downstream regulatory issues, as there may be challenges and delays in updating the DPDP Rules to keep pace with technological, regulatory, business, or other developments.

In light of the above, we therefore respectfully recommend avoiding prescribing any specific security measures and instead, ensuring that the DPDP Rules provide a flexible and risk-based framework to securing personal data. Such a framework can be supplemented by sector-specific guidelines to account for variations in organizational size, technical capacity, data processing activities, and other considerations, such as best practices of the industry. This would also provide MeitY with regulatory flexibility to adjust enforcement efforts according to regulatory, industry, technological and national imperatives.

---

2 https://www.pdpc.gov.sg/guidelines-and-consultation/2020/03/advisory-guidelines-on-key-concepts-in-the-personal-data-protection-act

2. Adjust the DPDP Rules' approach to data breach notifications to avoid potential downstream operational issues.

Rule 7 of the draft DPDP Rules requires Data Fiduciaries, upon discovering a personal data breach, to promptly provide affected Data Principals with information about the breach details, potential consequences, mitigation measures, and contact information.

Rule 7 also requires Data Fiduciaries to report basic details to the Board immediately on discovering the breach, and within 72 hours, to follow up with comprehensive information about the circumstances of the breach, remediation actions taken, and confirmation that affected individuals were notified.

Several aspects of Rule 7 could create downstream operational challenges that undermine their effectiveness.

First, organizations may find it challenging to provide such comprehensive information immediately upon becoming aware of the breach as in practice, this level of detail is rarely available in the early stages of a data breach. Organizations typically need time to investigate the incident's scope, understand its impact, and develop appropriate remediation strategies. Hence, premature notification requirements may result in incomplete or inaccurate information being shared with Data Principals, potentially causing unnecessary alarm or preventing them from taking appropriate protective measures. Further, requiring organizations to disclose implemented security measures during an active incident, as mandated by Rule 7(c), could inadvertently assist malicious actors and compromise ongoing remediation efforts.

Second, there may be operational difficulties if Data Fiduciaries are required to report "any personal data breach" (emphasis added). By this provision, Data Fiduciaries would technically be required to report to Data Principals and the Board all data breaches, even if (for instance) only a single individual's data was involved. This creates several operational difficulties:

- requiring every instance of a data breach to be reported could result in affected Data Principals and the Board being overwhelmed by significant numbers of reported breaches;

- there may be enforcement difficulties for the Board in ensuring that all data breaches are reported; and

- Data Fiduciaries may be disincentivized from reporting due to the significant reporting obligations for even small-scale data breaches.

For this reason, other jurisdictions often set reporting thresholds, where organizations are required to report data breaches only when the data breach crosses a threshold of severity:

- **Brazil:** Under Regulation CD/ANPD 15/2024, issued pursuant to the LGPD, breaches must be reported only if they significantly affect Data Principals' interests and fundamental rights and involve any of the following: sensitive personal data, data related to children, adolescents, or the elderly, financial data, data used for system authentication (e.g., login credentials, tokens, or passwords), data protected by legal, judicial, or professional confidentiality obligations, or large-scale data.

- **Singapore:** Section 26 of the PDPA only requires organizations to report "notifiable data breaches", which are defined as data breaches that (a) result "in, or is likely to result in, significant harm to an affected individual; or (b) (are), or (are) likely to be, of a significant scale."

Respectfully, MeitY may therefore wish to consider implementing such a threshold to avoid operational and compliance difficulties for Data Fiduciaries reporting data breaches.

To address these concerns, we recommend that Rule 7 be amended to:

- Establish a tiered notification system where organizations inform the Board first (for instance, "without undue delay" or "without unreasonable delay"), and affected individuals only after gathering sufficient information (for instance, by establishing a fixed amount of days that satisfy the policy objectives sought);

- Include a notification threshold for data breaches that cross a certain threshold of severity;

- Provide clear criteria for extension requests; and

- Consider releasing a template for breach notifications to the Board and affected Data Principals.

These changes, if adopted, would help avoid potential downstream implementation issues with the data breach notification segment of the DPDP Rules, and ensure a more effective breach response and notification processes.

3. Provide greater detail to operationalize Verifiable Parental Consent (VPC) under Rule 10 effectively.

We welcome Rule 10 of the DPDP Rules for seeking to provide greater clarity on the VPC mechanisms for processing children's personal data under the DPDPA. However, several aspects of this Rule may benefit from further elaboration to ensure consistent implementation and avoid unintended barriers to digital participation.

Rule 10 establishes two verification pathways: (a) relying on "reliable" existing user data for parents who are registered with the Data Fiduciary, or (b) requiring government-issued identity verification for non-registered parents. We note, however, that there are presently no clear criteria for determining when identity and age details should be considered "reliable". This ambiguity could lead to potential compliance challenges and inconsistent implementation across different Data Fiduciaries. We therefore respectfully recommend amending Rule 10 to provide clearer guidance or criteria for determining when Data Fiduciaries can rely on existing identity and age verification details.

Further, Rule 10 at present does not appear to address situations where the specified verification methods are unavailable or inaccessible, such as when government-entrusted entities experience system outages, or when parents lack the required documentation. Additionally, the prescribed verification methods may create unintended barriers to digital participation for families who cannot easily meet the specified verification requirements.

Rule 10's requirement for Data Fiduciaries to implement "appropriate technical and organizational measures" would also benefit from greater specificity about expected standards or assessment criteria. The existing provision could result in widely varying implementation approaches and make it difficult for organizations to determine whether their measures meet regulatory requirements. In this regard, we invite MeitY and the Government of India to review FPF's comprehensive research on verification methods under the US Children's Online Privacy Protection Act (**COPPA**) for insights on practical implementation approaches that balance security with accessibility.[3] While COPPA does not mandate any particular approach, the US Federal Trade Commission maintains a list of approved VPC methods, and an organization is able to use any method as long

[3] https://fpf.org/verifiable-parental-consent-the-state-of-play/

as it is “reasonably designed in light of available technology to ensure that the person giving the consent is the child’s parent.”[4]

We therefore recommend revising Rule 10 of the DPDP Rules to:

- Establish clear criteria for determining when identity and age verification details should be considered “reliable” under Rule 10;
- Specify contingency procedures for situations where primary verification methods (such as government-issued identity verification) are unavailable or inaccessible;
- Create alternative verification pathways for families who cannot meet the currently specified verification requirements;
- Define concrete standards and assessment criteria for the “appropriate technical and organizational measures” that Data Fiduciaries must implement;
- Provide detailed guidance on acceptable verification methods, drawing from international best practices such as those developed under COPPA; and
- Implement a framework for assessing and approving alternative verification methods when primary methods prove inadequate.

4. Clarify the scope and implementation of the exemptions in Rule 11 and the Fourth Schedule relating to processing children’s data.

We welcome the clarity provided in Rule 11 and the Fourth Schedule regarding exemptions to children’s data processing obligations in the DPDPA. However, several aspects of these provisions could benefit from further refinement to ensure that they achieve their intended purpose without compromising children’s data.

First, the scope and conditions of the exemptions may present operational concerns. While the Fourth Schedule attempts to restrict exemptions through the qualification that “processing is restricted to the extent necessary,” this standard lacks a clear definition and scope, which would complicate enforcement efforts. For healthcare providers and educational institutions in particular, the current language could permit expansive data processing. For example, the exemption allowing educational institutions to conduct “tracking and behavioral monitoring” for educational activities or safety purposes could lead to overcollection of student data, presenting significant increased privacy and security risks.[5]

Second, the breadth of the exemptions in Part B of the Fourth Schedule (**Part B exemptions**) could raise concerns that they are too expansive. While the Rule includes qualifying language restricting processing to what is “necessary,” the absence of additional guidance on interpreting the exemptions and the standard of what is “necessary” could lead to inconsistent application and potential abuse.

Similarly, DPDP Rules may benefit from guidance as to the boundaries of what constitutes processing “necessary” for protecting a child’s health or supporting treatment plans. To the extent possible, such guidance

[4] https://www.ftc.gov/business-guidance/privacy-security/verifiable-parental-consent-childrens-online-privacy-rule
[5] See, for example, https://timesofindia.indiatimes.com/technology/tech-news/cyber-attacks-surge-in-education-institutions-across-country-8000-weekly-incidents-reported-report/articleshow/113779911.cms

should align with existing rules, regulations, and guidance issued by the National Medical Commission and other relevant bodies.

The exemption for email account creation could also benefit from clarification as to why this specific use case warrants an exception and how it differs from other account creation scenarios.

To ensure the exemptions serve their intended purpose while maintaining robust protection for children's privacy rights, we therefore recommend:

- Establishing clear criteria for determining when processing is "restricted to the extent necessary";
- Developing specific limitations and safeguards for each category of exempt Data Fiduciary;
- Creating detailed guidance on interpreting and applying the Part B exemptions;
- Implementing monitoring and enforcement mechanisms for exemption compliance;
- Clarifying the interaction between consent requirements and processing exemptions;
- Providing specific examples of permitted and prohibited processing under each exemption;
- Establishing oversight mechanisms to prevent misuse of exemptions; and
- Adding explicit safeguards against potential overreach in educational and healthcare contexts.

In the alternative, MeitY could adopt a less prescriptive approach by amending the language on exemptions for processing children's data only to processing that is done in the "best interests of the child." This phrasing would align with Article 3 of the UN Convention on the Rights of the Child, to which India is a signatory. Such a restriction may also help prevent organizations from engaging in excessive data processing beyond the intended scope of the exemption.

5. Clarify the criteria and methodology for designation of Significant Data Fiduciaries (SDF), and guidance on SDFs' obligations under Rule 12.

FPF recognizes the Government of India's policy objective of introducing enhanced obligations for entities that process large volumes of personal data. However, the current draft DPDP Rules could provide greater clarity and specificity regarding the designation of SDFs beyond the high-level criteria set out in Section 10 of the DPDPA to ensure legal certainty and create a foreseeable regulatory environment that fosters innovation.

Additionally, it would be beneficial for the DPDP Rules to provide greater clarity on how SDFs should comply with Rule 12 of the DPDP Rules. In particular:

- Rule 12(1) requires SDFs to undertake a Data Protection Impact Assessment (**DPIA**) and an audit every twelve months "to ensure effective observance of the provisions of this Act and the rules made thereunder." However, it is not the periodicity of a DPIA that achieves its goals, but the fact that it is performed whenever processing operations are novel and complex and may result in harms to the rights of Data Principles, and throughout the lifecycle of processing operations, when they are significantly modified in means and scope. Prevention of harms to Data Fiduciaries and more effective resource

allocation would be better achieved if this Rule is not mandated for every 12 months, but every time a processing activity is significantly modified or novel and complex processing activities are proposed.

- Rule 12(2) requires the person carrying out the DPIA and audit to furnish the Board with a report containing "significant observations." This rule is likely to result in significant bandwidth pressure on the resources of the Board, with no immediate benefit for Data Principals. Instead, we recommend that the Rule requires SDFs to maintain an internal record of the DPIAs and audits which should be made available to the Board upon request, at any time.

- Lastly, Rule 12(3) requires SDFs to verify that algorithmic software used for processing personal data is not likely to pose a risk to the rights of Data Principals. This Rule would benefit from clarification of whether the rights being referred to are those under the DPDPA or those guaranteed by the Constitution of India. Additionally, as algorithms are commonplace in all current technologies and most of them are innocuous, the Rule would better achieve its policy goals if it would focus on algorithms that result in automated decisions concerning a Data Principal.

We therefore recommend four targeted amendments to Rule 12:

- Modifying Rule 12(1) to require SDFs to undertake DPIAs when processing activities are significantly modified or when novel and complex processing is proposed, rather than on a 12-month schedule;

- Amending Rule 12(2) to require SDFs to make internal records of DPIAs and audits available to the Board upon request, rather than requiring automatic submission of reports;

- Specifying in Rule 12(3) which rights are being referenced (i.e., whether those in the DPDPA, or the Constitution); and

- Narrowing the scope of Rule 12(3) to focus specifically on algorithms resulting in automated decisions concerning Data Principals, rather than all algorithmic software.

6. Provide greater clarity on the procedure for the exercise of Data Principals' rights under the DPDPA.

The draft DPDP Rules aim to enable Data Principals to exercise their rights under the DPDPA. For this goal to be achieved, we recommend the following clarifications:

- **Maximum timelines for responding to Data Principals' requests:** While Rule 13(3) mentions that Data Fiduciaries and Consent Managers must publish the period under their grievance redressal system for responding to grievances, and implement measures to ensure that they respond within that period, these provisions do not specify a timeframe within which these parties should respond to Data Principals on their requests for exercising rights. By contrast, Singapore's Personal Data Protection Regulations 2021 (which are Singapore's equivalent of the DPDP Rules) provides a timeframe notification mechanism. In particular, it states that if an organization is unable to respond to an individual on their data subject request within 30 days, the organization must, within that time, inform the individual the time by which they will respond to their request.

- **Nominee rights**: Rule 13(4) mentions the right of a Data Principal to nominate an individual to exercise their rights. In this regard, it may be helpful for the DPDP Rules to provide clarity on the process for nomination, the scope of the nominee's powers, and how the nominee's identity and authority will be verified.

To improve this, we recommend that the final version of the DPDP Rules should establish specific response timelines for Data Fiduciaries to respond to requests from Data Principals. Additionally, it would also be helpful to:

- Permit Data Fiduciaries to provide Data Principals with a timeframe within which they will be able to respond to the Data Principal on their requests, should they justifiably not be able to respond within the original stipulated timeframe; and

- Allow Data Fiduciaries to request additional verification information, when reasonable doubt exists about the requestor's identity.

7. Provide greater clarification for cross-border data transfer mechanisms in Rules 12(4) and 14.

We respectfully believe that greater clarity on Rules 12(4) and 14 would be helpful to show how they interact with Section 16 of the DPDPA.

We understand that Section 16 of the DPDPA empowers the Central Government to restrict transfers of personal data to specific *jurisdictions*. As presently phrased, however, Rules 12(4) and 14 appear to be intended to establish new mechanisms that regulate the transfer of personal data out of India. This is because Section 16 does not appear to extend to restrictions for *specific kinds of personal data* (Rule 12(4)) or transfers of personal data to *specific persons or entities* (Rule 14). Section 16 of the DPDPA also does not make reference to the kind of committee envisioned in Rule 12(4).

Given the centrality of cross-border data transfers to India's digital economy and for India's businesses to provide goods and services and compete abroad, we recommend that further consideration be given to the implications of Rules 12(4) and 14. In particular, for SDFs, the requirement under Rule 12(4) to process certain categories of data exclusively within India could disrupt business operations, increase compliance costs, and limit access to global resources and expertise. Absent further regulatory guidance, the potential reach of Rule 14 could also create business uncertainty and impact business confidence.

While FPF fully appreciates that MeitY and the Central Government has legitimate policy interests in establishing the data transfer mechanisms in Rules 12(4) and 14, we respectfully believe that these interests can be realized in ways that do not disproportionately impact India's competitiveness and status as a key node in the global digital economy. We therefore recommend that Rules 12(4) and 14 be augmented by:

- Making an express clarification of their legal basis within the DPDPA (whether under Section 16 or otherwise);

- Establishing clear criteria for determining when transfer restrictions may be imposed – in particular, ensuring that such restrictions, when imposed, are: (a) limited to specific and legitimate policy objectives; (b) proportionately scoped to achieving those objectives; (c) based on clear and published criteria; (d) as far as operationally possible, subject to stakeholder consultation prior to implementation; and (e) accompanied by reasonable and feasible transition periods;

- Providing mechanisms for businesses to seek exceptions when necessary;

- Providing, whether within the DPDP Rules or otherwise, guidelines for implementation and enforcement; and

- Ensuring alignment with India's international trade commitments and digital economy objectives.

These suggested recommendations can help provide needed clarity while preserving the government's ability to protect national interests through targeted, proportionate measures.

8. Expressly empower the Data Protection Board of India (Board) to issue interpretative guidance on the DPDPA.

We welcome the detailed provisions in the draft DPDP Rules regarding the establishment and functioning of the Board, particularly the clear framework for appointment procedures, operational protocols, and decision-making processes outlined in Rules 16 to 19. A well-functioning Board would be crucial for effective oversight of privacy regulations, serving as the primary institution responsible for monitoring compliance, investigating violations, and enforcing penalties when necessary.

Nevertheless, we note that the draft DPDP Rules are silent on whether the Board (or some other body) will serve an advisory function. A common feature of data protection authorities (**DPAs**) in most jurisdictions tracked by FPF is their role in raising awareness and providing guidance.[6] This role is particularly valuable during the early stages of implementation, where DPAs serve a useful function in helping industry organizations understand their obligations and implement appropriate compliance measures, especially in response to advancements in technology or the emergence of new business models.

Further, given that it will take time for a body of case law to develop through the Board's interpretation of the DPDPA, we invite MeitY to consider explicitly empowering the Board, or another suitable body, to issue DPDPA-related guidance. This would provide much-needed clarity to organizations and promote consistent interpretation of the DPDPA's requirements across different sectors and use cases.

[6] See FPF's report mapping the regulatory approaches and strategies of key data protection authorities in the APAC region: https://fpf.org/blog/regulatory-strategies-of-data-protection-authorities-in-the-asia-pacific-region-2024-and-beyond/