Comments on the Draft Digital Personal Data Protection Rules

March 2025

V | D H | Centre for Legal Policy

This submission is an independent, non-commissioned piece of work by the Vidhi Centre for Legal Policy, an independent think-tank doing legal research to help make better laws and improve governance for the public good.

Authors

Nirmalya Chaudhuri, Research Fellow, Applied Law and Technology Research, Vidhi Centre for Legal Policy.

Shehnaz Ahmed, Lead, Applied Law and Technology Research, Vidhi Centre for Legal Policy.

Vrinda Pareek, Senior Resident Fellow, Applied Law and Technology Research, Vidhi Centre for Legal Policy.

Kahaan Mehta, Research Fellow, Applied Law and Technology Research, Vidhi Centre for Legal Policy.

Contributors

The authors are grateful to the following for their contributions to specific issues / provisions of this submission.

Damini Ghosh, Lead, Disability Inclusion and Access, Vidhi Centre for Legal Policy.

Rahul Bajaj, Senior Associate Fellow, Disability Rights, Vidhi Centre for Legal Policy,

Varsha Banta, Senior Resident Fellow, Corporate Law and Financial Regulation, Vidhi Centre for Legal Policy.

Neha Lodha, Senior Resident Fellow, Corporate Law and Financial Regulation, Vidhi Centre for Legal Policy.

Arhat Chhabra, Research Fellow, Corporate Law and Financial Regulation, Vidhi Centre for Legal Policy).

Yashaswini Basu, Outreach Lead, Nyaaya, Vidhi Centre for Legal Policy.

Debargha Roy, Research Fellow, Research Director's Office, Vidhi Centre for Legal Policy.

The authors would also like to thank Samrudh Shirolkar (Intern, Vidhi Centre for Legal Policy) for his research assistance during his internship with Vidhi.

Errors in the paper, if any, are the sole responsibility of the authors.

The copyright in this work vests with the Vidhi Centre for Legal Policy. For any clarifications/ queries in relation to this submission, please email Nirmalya Chaudhuri, Research Fellow, ALTR, at nirmalya.chaudhuri@vidhilegalpolicy.in.

DRAFT DIGITAL PERSONAL DATA PROTECTION RULES | KEY ISSUES

The Vidhi Centre for Legal Policy submitted its comments on the Draft Digital Personal Data Protection Rules, 2025 ("**Draft Rules**")[1] to the Ministry of Electronics and Information Technology ("**MeitY**"), Government of India. The submission analyses the Draft Rules along with the corresponding Schedules and identifies key legal and implementation issues. For each issue identified, the submission offers targeted recommendations aimed at strengthening the Draft Rules for better clarity and ensuring consistency with constitutional principles, the parent statute (i.e. the Digital Personal Data Protection Act, 2023 ("**DPDP Act**")[2], and global best practices.

While the detailed rule-wise breakdown of issues and recommendations is provided in Table A, a brief overview of key issues (emanating from the DPDP Act and the Draft Rules) identified in the submission is provided below.

1. Anonymisation Standards

Anonymisation is a commonly used practice that involves removing identifiers from personal data to reduce the risk of re-identification of the data principal. The DPDP Act and the Draft Rules are currently silent on whether anonymised data falls outside the purview of the legislation. Further, neither the DPDP Act nor the Draft Rules define anonymisation or envisage any legal standards for anonymisation. This assumes significance given the growing evidence that it may be possible to identify individuals from datasets that appear anonymised, particularly when combined with other datasets.[3] In the absence of clear definitions and standards for anonymisation, data fiduciaries may apply inconsistent or insufficient anonymisation standards raising privacy concerns. The risk of re-identification from such anonymised datasets is heightened with technological advancements that enable sophisticated data linkage techniques. Notably, the Personal Data Protection Bill 2018 ("**PDP Bill 2018**") recommended by the Committee of Experts under the Chairmanship of Justice B.N. Srikrishna ("**Expert Committee**")[4] constituted by MeitY defined anonymisation as an "irreversible process of transforming or converting personal data to a form in which a data principal cannot be identified, meeting the standards specified by the Authority".[5] The PDP Bill 2018 expressly excluded anonymised data from the ambit of the data protection law[6] and empowered the proposed Data Protection Authority of India to issue standards for anonymisation.[7] The General Data Protection Regulation in the European Union ("**EU**"), in Recital 26, categorically states that it does not apply to anonymised data.[8] Similarly, the data protection authorities in Singapore[9] and Australia[10] have published advisory guidance on the

[1] Draft Digital Personal Data Protection Rules, 2025 https://www.meity.gov.in/writereaddata/files/259889.pdf accessed 4 April 2025.
[2] Digital Personal Data Protection Act, 2023 https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf accessed 4 April 2025.
[3] Jules Polonetsky, Omer Tene and Kelsey Finch, 'Shades of Gray: Seeing the Full Spectrum of Practical Data De-identification' 56(3) Santa Clara Law Review 596, 605; P Schwartz and D Solove, 'The PII Problem: Privacy and a new Concept of Personally Identifiable Information' (2011) 86 NYU Law Review 1814.
[4] 'Committee of Experts under the Chairmanship of Justice B.N. Srikrishna' https://prsindia.org/files/bills_acts/bills_parliament/2019/Committee%20Report%20on%20Draft%20Personal%20Data%20Protection%20Bill,%202018_0.pdf accessed 8 April 2025.
[5] Personal Data Protection Bill, 2023, s. 3(3), https://prsindia.org/files/bills_acts/bills_parliament/1970/Draft%20Personal%20Data%20Protection%20Bill,%202018%20Draft%20Text.pdf accessed 8 April 2025.
[6] Personal Data Protection Bill, 2023, s. 2(3).
[7] Personal Data Protection Bill, 2023, s. 61(6).
[8] General Data Protection Regulation, Recital 26.
[9] Personal Data Protection Commission, 'Guide to Basic Anonymisation' https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/advisory-guidelines/guide-to-basic-anonymisation-(updated-24-july-2024).pdf accessed 24 February 2025.
[10] Office of the Australian Information Commission, 'De-Identification and the Privacy Act' https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-

standards of anonymisation that are to be adopted by data fiduciaries based on a risk analysis. Legal clarity on anonymisation is important for several reasons. First, it ensures meaningful protection of data principals from the risk of re-identification. Second, it provides legal certainty for data fiduciaries in adopting appropriate anonymisation techniques. Third, it helps prevent the misuse of weak anonymisation techniques by entities seeking to remain outside the ambit of the DPDP Act.

2. Regulatory Challenges in Effective Implementation of the DPDP Act

The DPDP Act does not confer regulatory powers on the Data Protection Board of India ("**Board**") to issue regulations or directions. This presents a significant challenge for the effective implementation of the DPDP Act, particularly in a rapidly evolving area such as data protection. It is neither feasible nor efficient to expect the Central Government to prescribe rules for every operational detail. For instance, the absence of such regulatory power could hinder the development of crucial frameworks and standards on anonymisation techniques, mechanisms to be adopted for verifying parental consent for the processing of children's personal data, the data protection standards and "assurance frameworks" to be adopted by Consent Managers, etc. The Draft Rules' omission to address such issues may lead to legal uncertainty about the implementation of several critical provisions. In many Indian regulatory frameworks, sectoral regulators are empowered to issue subordinate legislation or guidance to address evolving implementation issues. Similar approaches are also followed internationally. In the EU[11] and Singapore,[12] the respective data protection authorities have been empowered to issue binding guidelines as well as advisory guidance. In the absence of any statutory provision regarding such regulatory powers, it will be necessary to explore alternative mechanisms (such as non-binding guidance or FAQs) to respond to implementation issues that are raised by different stakeholders.

3. Independence and Autonomy of the Board

The DPDP Act envisages that "the Board shall function as an independent body". In order to do so, the Board needs to be structurally, functionally and financially independent from executive interference. This is particularly important given that the Board may need to address complaints against the Government (as a data fiduciary). In this regard, certain provisions in the Draft Rules, such as heightened executive control in the appointment of the Chairperson and members of the Board, subjecting employees of the Board to Civil Service (Conduct) Rules, 1964, and the lack of a designated fund or financial provision for the functioning of the Board, raises questions as to the perceived independence and autonomy of the Board. Therefore, to fulfil the spirit of the DPDP Act, and ensure effective grievance redressal for data principals, appropriate amendments may be made in the Draft Rules to ensure the structural, administrative and financial independence of the Board.

4. Verifiable Consent of Parents and Guardians

The DPDP Act mandates verifiable parental or guardian consent, as the case may be, for the processing of personal data of minors and persons with disabilities ("**PwDs**"). The Draft Rules, in their current form, do not adequately verify whether the person purporting to be the parent of the child is indeed the parent. Further, there is a lack of clarity on the virtual tokens envisaged under Rule 10 and the "due diligence" measures to be adopted to verify guardianship. In addition, there are concerns that the two different mechanisms adopted for verification of the parent in the Draft

information/de-identification-and-the-privacy-act#:~:text=De%2Didentification%20is%20a%20risk,likelihood%20of%20re%2Didentification). accessed 24 February 2025.

[11] General Data Protection Regulation, art. 57 https://gdpr-info.eu/art-57-gdpr/ accessed 4 April 2025.

[12] Personal Data Protection Act, 2012, art. 6 https://sso.agc.gov.sg/Act/PDPA2012?ProvIds=P12-#pr6- accessed 4 April 2025.

Rules will result in a competitive advantage for those data fiduciaries that already possess the requisite details of the parent. On a broader scale, there is a need to ensure that the "guardian" whose verifiable consent needs to be obtained, aligns with the concept of "guardian" under the Right of Persons with Disabilities Act, 2016, and that the verifiable consent requirements should not be blindly extended to all PwDs if they are able to take legally binding decisions on their own or with adequate and appropriate support.

5. Standards for Processing Personal Data for Research Purposes

The DPDP Act provides an exemption for processing of personal data for research, archiving and statistical purposes if the personal data is not used to take any decision specific to a data principal and if such processing complies with certain standards prescribed in the Draft Rules. These standards appear to be overly broad and general, thus providing data fiduciaries with a large degree of discretion. Notably, the same standards are also applicable to the processing of personal data by the State to provide a subsidy, benefit, service, certificate, license or permit. Government processing is typically linked to public interest or legal obligations while research exemptions could potentially be invoked by private entities. These uses carry distinct privacy risks and therefore warrant more tailored standards. A review of other jurisdictions also shows that the research exemption is subject to heightened standards. In the EU[13] and South Africa,[14] this exemption can only be invoked when the research cannot be effectively carried out using anonymised data, and the results of such research are required to be published in a manner that does not lead to re-identification of the data principal. Further, in South Africa, the research exemption is only applicable when research is carried out in the public interest.[15] To strengthen accountability and prevent misuse of the research exemption, Table A highlights the need to impose additional standards for research.

6. Concerns over Standards for Processing of Personal Data by the State

The DPDP Act allows the State to process personal data without the consent of data principals for certain legitimate uses, namely, provision of a benefit, subsidy, service, certificate, license or permit to the data principal. However, the DPDP Act and the Draft Rules allow such processing to be subject to either a law or a policy, which can potentially be read as a dilution of the judgment of the Supreme Court in *Puttaswamy I*[16] and *II*[17]. In these cases, the Supreme Court held that an action by the State which results in a restriction of the right to privacy must be authorised by a law. Further, although certain standards for such processing by the State, as mandated under the DPDP Act, are listed in the Second Schedule of the Draft Rules, the standards do not specifically lay down security standards, retention periods, accountability of the person processing personal data, etc. Such vagueness in the Draft Rules is not sufficient to address privacy concerns around the processing of personal data without data principals' consent. This necessitates appropriate amendments in the Draft Rules to protect the rights of data principals. In addition, for certain purposes of processing by the State, such as processing in the interests of the sovereignty of India or security of the State, no standards have been laid down in the Draft Rules. Further, the Draft Rules empower the Central Government to call for information from the Board or any data fiduciary for a range of purposes, including "sovereignty and integrity of India" and "security of the State", which may not be strictly in consonance with the "purposes of the Act" and may be viewed as excessive delegation.

[13] General Data Protection Regulation, art. 89.
[14] Protection of Personal Information Act, 2013, s. 15 https://popia.co.za/ accessed 8 April 2025.
[15] Protection of Personal Information Act, 2013, s. 27.
[16] *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.
[17] *K.S. Puttaswamy v. Union of India*, (2019) 1 SCC 1.

7. Assessing the Impact of the Digital First Approach of the Board

The DPDP Act and the Draft Rules mandate the Board to function as a digital office, with all its proceedings, including receipt of complaints, being conducted online. Complete reliance on a digital approach may raise issues of access, since data principals in remote areas or without access to the requisite technology or its knowledge, may be excluded from the right to approach the Board. This can exacerbate the digital divide in India and affect the rights of data principals. To address this concern, it is important to provide alternative means for approaching the Board and conducting the proceedings of the Board, so that the redressal of grievances of data principals is not hampered, irrespective of their access to digital technology.

TABLE A | RULE-WISE COMMENTS

Sr. No.	Rule	Key Issues and Recommendations
1.	Rule 3: Notice given by Data Fiduciary to Data Principal	1. Section 5 of the DPDP Act mandates that the consent notice includes information about personal data, the purpose for processing, manner of exercising the data principals' rights under the DPDP Act and the manner of making a complaint to the Board. Rule 3 prescribes the format of the notice. Rule 3 only requires a communication link to be mentioned in the notice to enable the data principal to exercise her rights, withdraw consent and make a complaint to the Board. It does not specify how such information should form part of the consent notice. Rule 3 may be amended to require the consent notice to explicitly mention the process for a data principal to exercise her rights under the DPDP Act and make a complaint to the Board in addition to the communication link. The actual procedure can continue to be implemented through the link. 2. Rule 3 may be amended to clarify that the specifications in this rule apply both to consent sought after the enactment of the DPDP Act (Section5(1)), as well as consent given by data principals before the coming into force of the DPDP Act (Section 5(2)). For this purpose, in Rule 3(b)(ii), the phrases "to be provided" and "to be enabled" may be replaced with "to be provided, or that have been provided" and "to be enabled, or that have been enabled" respectively. 3. Rule 3 may be amended to state that a data fiduciary cannot deny services to a data principal for not giving fresh consent under section 5(2) if the data principal had already consented to the processing before the DPDP Act came into force, unless the data principal has withdrawn her consent. 4. In line with jurisdictions like the United Kingdom (UK) and Singapore, to ensure effective implementation of the DPDP Act, the Board may issue guidance or a baseline format of notice, use of audio-visual means etc., which may inform consent notices given by data fiduciaries. Please refer to the submission on Rule 18, relating to the need for the Board to be conferred with powers to issue guidance.
2.	Rule 4 read with First Schedule: Registration and obligations of Consent Manager	1. Rule 4, read with the First Schedule, lays down the conditions of registration of consent managers, along with their obligations. Under the DPDP Act, only consent managers registered with the Board can manage consent of data principals. Existing entities managing consent will have to separately register under the DPDP Act. However, the DPDP Act and the Draft Rules lack a transition mechanism for existing consent managers, both regulated (such as account aggregators) and unregulated. It is not clear if existing consent

		managers can operate without registration. Rule 4 may be amended to allow existing consent managers (such as account aggregators) to continue their operations for 6 months after the commencement of the DPDP Act, unless they register with the Board, or their application is rejected. 2. Regulators often charge a small fee for registrations / issuing licenses to regulated entities. The Draft Rules must clarify whether the Board will charge fees for the registration of consent managers. If yes, the Draft Rules must further clarify to which fund such fees will be credited. 3. Consent managers are envisaged as separate interfaces for onboarding both data fiduciaries and data principals. However, requiring users to register separately with a consent manager and data fiduciaries may impact user convenience. To encourage the uptake of consent managers, the interface should prioritise ease of use and seamless integration. Users may prefer a common consent manager for multiple registered data fiduciaries. A business case for consent management also needs to be established. 4. Rule 4(5) may be amended to provide that in addition to existing grounds for suspension and cancellation of registration of consent managers, non-compliance with directions of the Board under Rule 4(4) may be a ground for suspension and cancellation under Rule 4(5). 5. Clause 9, Part A, First Schedule empowers the Board to issue data protection standards and assurance frameworks for consent managers. As the DPDP Act does not empower the Board to issue any subordinate legislation, the Schedule may be amended to clarify the nature of such standards / frameworks. 6. First Schedule, Part B, Clause 13 may be amended to state that if the Board does not approve the consent managers' change in control within a specified period, then the approval will be deemed to have been granted. 7. The phrase "transferee data fiduciary" in Clause 3(c), Part B, First Schedule, may be substituted with "transferee data fiduciary registered with the Consent Manager". 8. Clause 12, Part B, First Schedule requires submission of audit reports periodically. The term periodically may be interpreted differently. This clause may be amended to put a specific timeline for submission of reports under this clause. 9. "Reasonable security safeguards" for CMs under Clause 7, Part B, First Schedule may be defined in order to avoid ambiguity.
3.	Rule 5 read with the Second Schedule: Processing for provision or issue of subsidy, benefit,	1. Rule 5, read with the Second Schedule, deals with the grounds and standards for processing personal data by the State without the consent of the data principal, when such processing is necessary for providing a subsidy, benefit, service, certificate, license or permit by the State and its instrumentalities. Section 7(b) of the DPDP Act read with this Rule appears to dilute the

	service, certificate, licence or permit by State and its instrumentalities	Supreme Court judgment in *KS Puttaswamy v. Union of India*, (2017) 10 SCC 1 that held that a state action impacting the right to privacy must be authorised by a law. Section 7(b) allows processing of personal data to be subject to a policy. 2. The phrases "or other authority" and "within the territory of India" in Rule 5(3)(c)(ii) are broad and vague. This may be interpreted to mean any entity within the territory of India (and not necessarily a government agency, which may have been the original intention). These phrases must either be omitted or qualified such that the authority is either (a) statutory; or (b) subject to Government oversight. Notably, the phrase "local authority" in the same clause is defined broadly in the General Clauses Act, 1897 and accordingly, reference to "other authority within the territory of India" may be omitted. 3. In the Second Schedule: (i) Clause (f) does not clarify the security measures to be adopted. Therefore, clause (f) may be amended to provide guidance on the nature of reasonable security standards. (ii) Clause (g) does not enumerate the details to be intimated to the data principal under the clause. Clause (g) may be amended to require the data fiduciary to inform the data principal about the details of the personal data being processed, the ground on which the personal data was originally processed (if applicable), the purpose for which such data is being processed, and how it aligns with the legitimate use ground under the DPDP Act, the manner of exercising her rights under the DPDP Act, and the manner of making a complaint to the Board. (iii) In clause (h), there appears to be a lack of clarity on the "accountability" of the person specified. Clause (h) may be amended to clarify the role, the mandate and the mode of accountability of the person referred to in the clause. (iv) Clause (e) may be amended to clarify that unless required to be retained for longer periods by applicable law, data will be retained till required for such uses or achieving such purposes for which the data was processed under section 7(b) and section 17(2)(b), as may be applicable. It may further be clarified that the data will be erased post this. 4. In line with standards for section 7(b), the DPDP Act may consider enumerating specific standards for processing under Section 7(c) and 7(d) to ensure that the processing of such information is not arbitrary and is compliant with the broader principles of the DPDP Act.
4.	Rule 6: Reasonable security safeguards	1. Rule 6 lays down the reasonable security standards that are required to be adopted by a data fiduciary. Since any person "processing" personal data will be a data fiduciary, imposing a uniform set of reasonable security standards for all data fiduciaries irrespective of the data being processed and the risk that it poses, may be counterproductive, creating unintended compliance

		burdens for smaller businesses. The data fiduciaries may be provided with discretion to implement "reasonable security safeguards" based on a risk-assessment, considering factors like the nature, scope, context and purposes of processing of personal data, and the risks and severity of harm that such data processing may cause, as well as prevailing sectoral needs and industry standards. Legally, this power to determine and implement such standards must be prescribed in the parent statue. 2. To ensure that such discretion is exercised reasonably, Rule 22 may empower the Central Government to call for information from any data fiduciary under Section 36 of the DPDP Act, in order to ensure that reasonable security standards are undertaken by the concerned data fiduciary in compliance with the DPDP Act and the Draft Rules. 3. The rule may clarify what kind of information should be a part of "appropriate logs" required to be maintained by Data Fiduciaries under Rule 6(1)(e). 4. The obligation on data fiduciaries to retain logs and personal data for one year, appears to be inconsistent with the obligation to erase data on withdrawal of consent by the data principal under Section 8(7) of the DPDP Act. 5. The term "virtual tokens" may be defined. The Board may have to consider issuing guidance on such tokens upon further clarity.
5.	Rule 7: Intimation of personal data breach	1. The requirement for immediate notification to data principals under Rule 7 may potentially lead to over-reporting without adequate awareness of the details of the breach. This might lead to panic as well as "notification fatigue" on the part of data principals. Data fiduciaries may be permitted to report incidents of data breach to the data principals in a phased manner, not later than 72 hours after the breach or within such longer period as the Board may allow on a request made in writing in this behalf. 2. Rule 7 may be amended to mandate that the breach report to the data principal as well as the Board should also mention the type of personal data which is the subject matter of the breach. 3. The Indian Computer Emergency Response Team (CERT-In) Direction dated April 28, 2022, mandates reporting of "cyber incidents" as defined in the Information Technology Act, 2000, within 6 hours. Similarly, Reserve Bank of India (RBI) circular dated June 2, 2016, mandates banks to report "cyber incidents" within 2 to 6 hours of their occurrence. Such sector specific data breaches may be accounted to avoid overlap. A centralised data breach reporting mechanism with a common format may be prescribed, so that all concerned regulatory authorities are intimated in case of a personal data breach. This will ensure concerted mitigation strategies and reduce compliances for businesses.
6.	Rule 8 read with the Third Schedule: Time period for specified	Rule 8, read with the Third Schedule, provides for timelines of retention of personal data by data fiduciaries. There appears to be a lack of clarity over retention timelines for data fiduciaries other than the classes mentioned in the Third

	purpose to be deemed as no longer being served	Schedule, which appears to be in dissonance with Section 8(7) of the DPDP Act. Section 8(8) of the DPDP Act mandates such time limits to be prescribed in the Draft Rules by the Central Government. Therefore, time limit for erasure may be prescribed for other classes of data fiduciaries in the Draft Rules.
7.	Rule 10 read with the Fourth Schedule: Verifiable consent for processing of personal data of child or of person with disability who has lawful guardian	1. Rule 10 deals with the obligation of data fiduciaries to obtain verifiable consent of the parent/lawful guardian for processing personal data of a child or a PwD. For this purpose, mechanisms may be set out for the data fiduciary to verify that the concerned person providing verifiable consent under Rule 10(1) is indeed the parent/lawful guardian of the child or PwD. This is because, the Rule in its present form, does not appear to verify that the person purporting to be the parent / lawful guardian of a child or a PwD is indeed the parent / lawful guardian. 2. Rule 10(1)(a) creates a competitive advantage for data fiduciaries that already possess "reliable details" of the parent under Rule 10(1)(a). It may be clarified as to how the "reliable" threshold in Rule 10(1)(a) can be satisfied, e.g. if it would involve submission of government identity documents. 3. A sub-clause may be inserted requiring verification mechanisms adopted by a data fiduciary to be proportionate to the purposes of processing and the resultant risks and harms that the data processing would likely cause. 4. "Virtual tokens" that may be used for verification should be defined. Further, the Board may be empowered to issue guidance for issuance of these "virtual tokens." 5. Provision on persons with disabilities must be delinked from the provision on children's data as it perpetuates a paternalistic view of disability. 6. Data fiduciaries and consent managers must ensure barrier-free, accessible platforms and provide reasonable accommodation to PwDs to enable free, informed, and specific consent. 7. Where PwDs are unable to take legally binding decisions despite such support, a limited guardian as per Section 14 of the Rights of Persons with Disabilities Act, 2016 ("**RPWDA**") as well as the provisions of the National Trust Act, 1999 may be appointed. It may be clarified that a 'person providing support to the PwD' under Section 13 of the RPWDA is distinct from the 'limited guardian' under Section 14 of the RPWDA and Rule 10 of the Draft Rules. Rule 10 may also provide guidance on identifying when a PwD is "unable to take legally binding decisions," such as their ability to understand, foresee consequences, or communicate decisions. 8. Protocols may be set out for obtaining verifiable consent from lawful guardians under Rule 10(2) as well as "due diligence" measures to be adopted to verify guardianship in Rule 10(2). Further, it may be clarified whether data fiduciaries can rely on "reliable details" of a lawful guardian similar to the approach taken in Rule 10(1)(a).

		9. The Board may be empowered to issue guidance for the means to be used for verification under Rule 10(1) and 10(2). 10. In point 3 in the Fourth Schedule, the phrase *"for the educational activities of such institution*" may be replaced with the phrase *"for the educational activities of the child enrolled in such institution".*
8.	Rule 11: Exemptions from certain obligations applicable to processing of personal data of child	There appears to be a lack of guidelines for implementing Section 9(5) of the DPDP Act, which allows the Central Government to prescribe a different age limit for processing of personal data of children by certain data fiduciaries if certain conditions are met. Further, there is a lack of clarity over what constitutes "verifiably safe" under the DPDP Act for processing of children's personal data. Illustrative criteria may be laid down for implementation of Section 9(5), in order to avoid excessive delegation.
9.	Rule 12: Additional obligations of Significant Data Fiduciary	1. The difference in scope of the Data Protection Impact Assessment (DPIA) and audit in Rule 12(1) is not clear. Rule 12 may be amended to clarify this. The Board may be empowered to issue guidance regarding the same. 2. Data localisation envisaged under Rule 12(4) is a substantive obligation and should have been provided in the DPDP Act. Providing for this requirement under the Draft Rules appears to go beyond the rule-making powers under Section 10(2)(c)(iii). 3. The criteria for determining which personal data requires localisation must be clearly defined. To ensure informed decision-making and minimise inconvenience, the committee may consider inputs from data fiduciaries, especially significant data fiduciaries, when developing guidelines or standards. 4. The constitution and mandate of the committee under Rule 12(4) may require clarity since its recommendations will have a bearing on the implementation of data localisation norms. The Rule may also clarify if committee recommendations are binding on the Central Government. Rule 12 may be amended to outline the composition, mandate, scope of powers and functions of the committee under Rule 12(4). 5. There appears to be a lack of clarity on the definition of "algorithmic software" under Rule 12(3), the "due diligence" measures required to be undertaken, and the risk of harm envisaged. Rule 12(3) may be amended to detail the meaning of algorithmic software and the nature of due diligence measures contemplated.
10.	Rule 13: Rights of Data Principals	1. Section 13(2) of the DPDP Act provides that a data fiduciary and consent manager must respond to grievances within such time period as may be prescribed in the rules. The Draft Rules do not set out such a timeline. Rule 13(3) does not specify an upper time limit for data fiduciaries to redress grievances, allowing them to set excessively long timelines that could undermine data principals' rights under Section 13(1) of the DPDP Act. This is particularly concerning since, under Section 13(3), data principals must

		exhaust the grievance redressal mechanism before approaching the Board. Given the mandate under Section 13(2) of the DPDP Act, an upper time limit for grievance redressal by data fiduciaries may be specified. An escalation matrix within the organisational structure of the data fiduciary may be provided as a part of the grievance redressal process. 2. Rule 13 may be amended to require data fiduciaries and consent managers to provide information under this Rule in a clear, concise and accessible manner. 3. Rule 13(4) allows data principals to nominate "one or more individuals" for acting on their behalf. However, Section 14 of the DPDP Act allows data principals to nominate "any other individual" for acting on her behalf in case of death or incapacity. There appears to be a disparity in terms of the number of persons that a data principal can nominate in this regard. Rule 13(4) may be amended to substitute "one or more individuals" with "any another individual", to bring it in line with the parent DPDP Act. 4. A mechanism may be provided to ensure that the data principal can verify whether her personal data has been erased or not, upon request.
11.	Rule 14: Processing of personal data outside India	1. Section 16 empowers the Central Government to notify countries or territories outside India to which personal data transfers (by data fiduciaries) may be restricted. Rule 14 appears to deviate from this mandate. It allows the Central Government to impose restrictive "requirements" on the transfer of personal data to any country or territory outside India without having to first identify and notify specific countries/ territories as per Section 16. To rectify this, the phrase "transfer to any country or territory outside India of personal data…" may be amended to "transfer to any country or territory outside India ***notified by the Central Government under Section 16*** of personal data…" 2. Further, there appears to be a lack of clarity on the kind of specifications/restrictions that might be imposed. Guidelines may be laid down in the Draft Rules to clarify: (a) the basis on which the Central Government can notify the countries to which cross-border data transfers are not permitted or restricted; and (b) the nature and scope of restrictions that are likely to be placed on such transfer.
12.	Rule 15 read with the Second Schedule: Exemption from Act for research, archiving or statistical purposes	1. Rule 15 provides an exemption from the DPDP Act when the processing of personal data is necessary for research, archiving or statistical purposes, subject to standards mentioned in the Second Schedule. There is a need for clarity on whether the term "research" in this Rule encompasses technological research, such as training Artificial Intelligence (AI) models. Jurisdictions like the EU and Singapore adopt a broad definition of "research" that includes technological advancements. As India strives towards create an enabling environment for AI innovation, ensuring access to datasets for technological research will be crucial. However, the standards applicable to research exemption as proposed by the Draft Rules may be amended to add the following conditions:

		(a) Any person claiming a research exemption must demonstrate that access to personal data is necessary for the research and that the research cannot be effectively conducted using anonymised or aggregated datasets. (b) If research findings are published, it must be ensured that data principals whose personal data was processed cannot be identified. (c) The results of the research must not be used to make decisions affecting the individuals whose personal data was processed under this exemption. (d) Personal data must be erased once it is no longer required for research purposes. (e) The exemption should apply only if obtaining consent from data principals is impossible or would require a disproportionate effort from the data fiduciary. (f) Personal data must not be processed in a manner that causes disproportionate harm to the data principal. 2. Currently, many data fiduciaries use anonymisation techniques to process personal data for research and development. Unlike other countries and the PDP Bill 2018, the absence of a clear definition of "anonymisation" and a framework for anonymization standards under the DPDP Act creates legal uncertainties. This is particularly concerning given the broad definition of "processing" under the DPDP Act, where any automated operation on personal data (which can include anonymisation) qualifies as processing. Without clear guidance, data fiduciaries may adopt varying anonymisation techniques, potentially using them as a loophole to evade compliance with the DPDP Act. Establishing robust anonymisation standards is essential to ensure data privacy while enabling responsible research and innovation.
13.	Rule 16: Appointment of Chairperson and other Members	1. Rule 16 lays down the procedure for appointing the Chairperson and Members of the Board. Section 28 of the DPDP Act states that "the Board shall function as an independent body". Viewed in this light, there appears to be a lack of safeguards in the Draft Rules to preserve independence of the Board from executive control in the current framework. Since the Board may be called upon to regulate matters in which the Government is a party, it is imperative to ensure the independence of the Board, which isa regulatory authority, from the control of the Central Government. This can be broadly ensured through the following: (a) Independence in appointment and selection of members: Currently, the Rule provides for a 5-member Search-cum-Selection Committee for appointing the Chairperson and Members, out of which 3 members are part of the executive (Secretaries to the Government of India). The Rule may be amended to increase the number of independent / non-government members.

		(b) Functional Independence: To ensure this, the Board may be empowered to set up a specialised workforce. Please also refer to the submission on Rule 20. (c) Financial Independence: Unlike other regulators like Securities and Exchange Board of India (SEBI), Telecom Regulatory Authority of India (TRAI) and Unique Identification Authority of India (UIDAI), neither the DPDP Act nor the Draft Rules provide for any designated fund for carrying out the functions of the Board, including payment of salaries and allowances to the Chairperson and other Members. This can create concerns of lack of financial independence, since the Board will be wholly dependent on the Central Government for funds. 2. Further, there should be complete separation of powers between officers who are conducting inquiry/investigation into alleged infractions of the DPDP Act and Draft Rules, and the officers adjudicating on these matters. Officers conducting the inquiry should not adjudicate on the same. It is preferable that the officers exercising adjudicatory powers have a legal background, and it may be prescribed that such officers shall belong to a certain rank. 3. To ensure accountability, the Board may also be required to publish its orders, details of consent managers registered, adjudications done under the DPDP Act and broad overview of the reports of personal data breaches, etc. on its website.
14.	Rule 18: Procedure for meetings of Board and authentication of its orders, directions and instruments	1. There appears to be a lack of clarity on the ambit of emergency powers of the Chairperson under Rule 18(6), since this power is generally not granted to Chairpersons of other regulators like SEBI, TRAI and Insurance Regulatory and Development Authority of India (IRDAI). If emergency powers are to be conferred on the Chairperson, the grounds may be clearly set out and the impact of not taking action may also be mentioned. Further, the decision taken by the Chairperson may be communicated to the other Members within 48 hours, and not 7 days as envisaged in the Rule. 2. Under the current framework in the DPDP Act and Draft Rules, the Board is conferred with only adjudicatory powers, and not regulatory powers, except a limited power to regulate and register consent managers. Unlike other sectoral regulators, the Board does not appear to have the power to issue standards or guidelines. The absence of such regulatory powers can lead to impediments in the effective implementation of the DPDP Act, especially in case of evolving issues like verifiable consent and security standards to be adopted by data fiduciaries, which would necessitate the issuing of standards. Since it is impractical for the Central Government to be expected to issue Rules to deal with such emergent situations in every case, it is proposed that the Board may be granted with powers to issue guidance and standards. Such powers should have ideally been introduced through the DPDP Act. If not feasible, power to issue guidance may be considered in the Draft Rules as long as broad principles for exercising powers are clearly outlined.

15.	Rule 19: Functioning of Board as digital office	1. Rule 19, read with Section 28 of the DPDP Act, states that the Board would be functioning as a digital office, where the receipt of complaints and conduct of proceedings would proceed digitally. In case the Board functions solely as a digital office, there could be issues of accessibility to the Board in case of absence of access to requisite technology by the parties concerned. This is especially important because Section 28 of the DPDP Act states that the Board shall function as a digital office, only "as far as practicable". Such insistence on a digital-only approach may deprive many data principals who do not have reliable digital means of pursuing their rights under the DPDP Act. The Draft Rules may recognise effective alternative means for its public-facing functions to avoid any exclusion. 2. In order to ensure adequate accessibility for PwDs, it may be provided that all content published by the Board for access to the public must be rendered in a format that is accessible to PwDs.
16.	Rule 20 read with the Fifth and Sixth Schedules: Terms and conditions of appointment and service of officers and employees of Board	Rule 20, read with the Fifth and Sixth Schedules, lists the terms and conditions of appointment of the Chairperson and Members of the Board. Authorities like the Competition Commission of India (CCI), SEBI, RBI and IRDAI are empowered to appoint persons who are not Government employees on deputation. Viewed in this light, there appears to be a lack of clarity on why the eligibility for appointment of employees of the Board is limited only to those persons on deputation from the Central or State Government, or autonomous bodies or public sector enterprises under the control of the Central and State Government. This, coupled with the fact that such employees will be bound by the Civil Service (Conduct) Rules, 1964 as applicable to Government servants, may potentially lead to concerns of lack of independence of a statutory body such as the Board. The Sixth Schedule (which relates to Rule 20) may be amended as follows: (a) In order to preserve the independence of the Board, the Civil Service (Conduct) Rules, 1964 may not be made applicable to the employees of the Board. The Board may be free to prescribe the terms and conditions of service of its employees. (b) Further, the Board may be free to appoint employees other than those who are on deputation from the Government or public sector enterprises. Further, please also refer to the submission on Rule 16 for issues relating to the independence of the Board.
17.	Rule 22 read with the Seventh Schedule: Calling for information from Data Fiduciary or intermediary	Rule 22 empowers the Central Government to call for information from the Board or any data fiduciary, for the purposes as specified in the Seventh Schedule. The power under this Rule appears to go beyond the mandate of Section 36 of the DPDP Act. This is because the powers under Section 36 are circumscribed to fulfil "the purposes of this Act", which according to the objects clause of the DPDP Act, is "to provide for the processing of digital personal data". However, the Seventh Schedule of the Draft Rules, which relates to Rule 22, extends this power for

		purposes such as “sovereignty and integrity of India or security of the State”. This appears to be a case of excessive delegation. Since the judgment of the Supreme Court in *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1, requires the enactment of a law before the right to privacy can be infringed upon, the item under serial no. 1 in the Seventh Schedule may be reconsidered and deleted. The time limit for retention of personal data by the Central Government obtained as a result of exercise of power under this Rule may be specified.