March, 2025

# National Level Public Policy Document

# Commentary on the Draft Digital Personal Data Protection Rules, 2025


National Law University, Jodhpur

*An initiative by the* ***Centre for Law and Technology***

# CONTRIBUTORS

**Prof. (Dr.) Harpreet Kaur**
*Vice Chancellor*
*&*
*Chief Patron*
*Centre for Law and Technology,*
*National Law University, Jodhpur*

**Prof. (Dr.) Shilohu Rao**
*Professor of Law*
*&*
*Director*
*Centre for Law and Technology,*
*National Law University Jodhpur*

## Student Contributors

Ms. Harshita Gupta (IV Year)
Mr. Y. Leela Krishna Reddy (III Year)
Mr. Kush Taparia (II Year)
Mr. Atharv Dwiwedi (II Year)
Mr. Ram Sumant (II Year)
Mr Arav Tiwari (II Year)
Mr. Vibhuti Shyam (II Year)
Mr. Ansh Arora (II Year)
Ms. Manishka Baweja (II Year)
Ms. Sunidhi Khabya (II Year)
Ms. Harshita Logre (II Year)
Ms. Suhana Gandhi (II Year)
Mr. Udit Jain (II Year)
Ms. Sarah Singh (II Year)

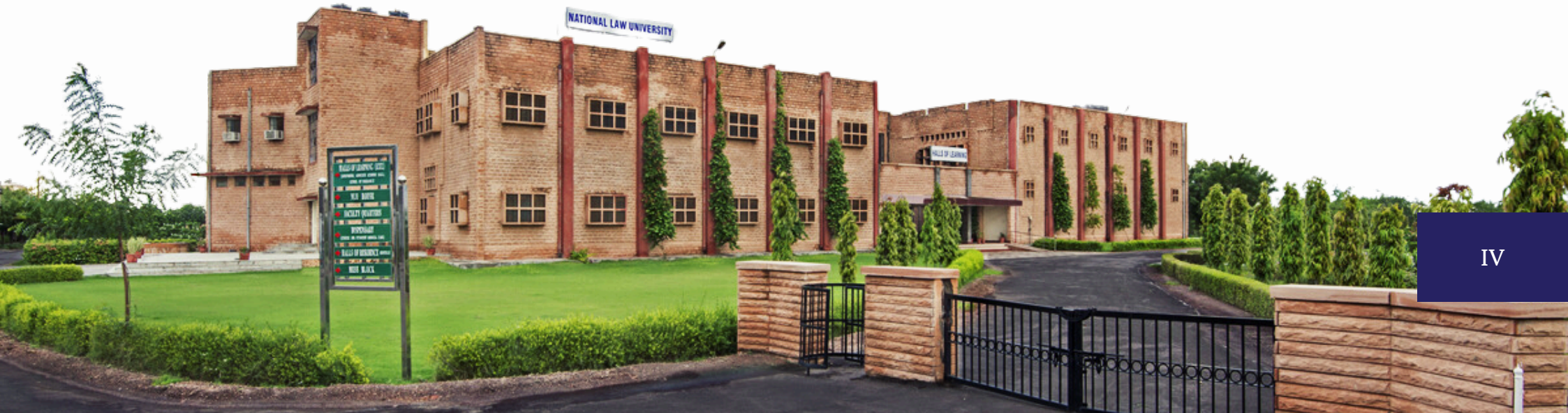
# TABLE OF CONTENTS

About National Law University, Jodhpur.....IV
About Centre for Law and Technology.....V
About Working of the Report.....VI-VII
Table of Suggestions.....1
Legal Evaluation Matrix..... 61

# ABOUT NATIONAL LAW UNIVERSITY JODHPUR

National Law University Jodhpur (NLUJ) is one of India's leading Law Schools situated at the vibrant and colourful city of Jodhpur, Rajasthan. NLUJ has constantly been ranked as one of the top law schools in India. Since its establishment in 1999, NLUJ has endeavoured to produce exceptional lawyers and legal scholars aimed at pushing and challenging the existing boundaries of knowledge.

NLUJ is known for its rigorous academic curriculum and its commitment to providing students with a comprehensive education in the field of law. The faculty consists of experienced legal scholars, and the university is equipped with state-of-the-art facilities and resources to support student learning and research. In addition to its academic programs, NLUJ is also known for it strong commitment to social justice and human rights, and for its focus on practical skills training.



# ABOUT CENTRE FOR LAW AND TECHNOLOGY

The rapid advancement of technology has created an urgent need for legal frameworks that can address the novel challenges arising from innovations like artificial intelligence, big data, and cybersecurity. Centre for Law and Technology have emerged to fill this critical gap, recognizing that traditional legal approaches are often insufficient to navigate these complexities. The Centre aims to foster interdisciplinary research, bringing together legal scholars, technologists, and policymakers to explore the intersection of law and technology.

Our work encompasses a wide range of activities, including:

- Conducting in-depth research on emerging legal issues, such as data privacy regulations, the ethical implications of AI, and the legal aspects of online platforms.
- Engaging in policy advocacy and providing expert advice to government agencies and organizations on the development of sound technology policies.
- Facilitating dialogue and collaboration between stakeholders from various sectors, including academia, industry, and civil society, to promote informed and balanced approaches to technology governance.

CLT

CENTRE FOR LAW
AND TECHNOLOGY

NATIONAL LAW UNIVERSITY, JODHPUR

# ABOUT THE WORKING OF THE REPORT

This report presents recommendations to the Ministry of Electronics and Information Technology on the Draft Digital Personal Data Protection Rules, 2025. The report is based on opinions that have been gathered through an expert survey wherein the Rules were assessed on a number of parameters identified through the following documents:

1. A.P Shah Committee Report
2. Justice B.N. Srikrishna Committee Report
3. Law Commission Reports
4. Justice K.S. Puttaswamy and Another v. Union of India
5. Joint Parliamentary Committee Report on Draft Data Protection Bill, 2019

The principles so identified have been used as parameters to asses the Draft Digital Personal Data Protection Rules, 2025. A score sheet relevant to each sector/relevant stakeholders with appropriate parameters for assessment was prepared, and an expert survey via telephone was conducted.

Experts from the respective fields were asked to evaluate the rules on a scale of 7-1, wherein:

# ABOUT THE WORKING OF THE REPORT

| | |
|---|---|
| **7** | **Excellent compliance with the parameters** |
| **5-6** | **Good compliance with the parameters** |
| **4 or below** | **Poor Compliance with the parameters** |

Additionally, experts were also asked to provide any justifications or rationale behind their scores.

After the completion of the telephonic interview, these parameters were matched with the relevant rules. For example, Rule A has parameters no. 1, 3, 5, 8, and 9 relevant. Then, the average of scores for parameters no. 1, 3, 5, 8, and 9 was taken and placed before Rule A. This process has been adopted for each Rule in the Draft Digital Personal Data Protection Rules, 2025. Subsequently, if the Rule A has received a score of 7, then no recommendations have been made.

In case Rule A, received a score less than 7, certain issues have been identified based on the justifications/rationale of the experts and recommendations/ suggestions have been drafted by the student contributors.

**(The evaluation matrix has been attached as an annexure to this Report)*

**Feedback/comments on the draft 'Digital Personal Data Protection Rules, 2025 submitted to the Ministry of Electronics and Information Technology (MeitY). Government of India.**

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| 1. | **Draft Rule 1: Short Title and Commencement** | No Comments |
| 2. | **Draft Rule 2: Definitions** | **Issues Identified-**<br>While the rule defines key terms, it lacks forward-looking definitions *(e.g., "algorithmic transparency", and "non-personal data").*<br>**Score: 5* out of 7 (max)**<br>**Proposed Suggestions-**<br>1. To ensure the DPDP Rules remain comprehensive and relevant, we suggest including definitions for 'algorithmic |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| | | transparency,' 'non-personal data'. These additions would enhance clarity and future-proof the legislation<br><br>2. The definitions provided in Rule 2 provide a solid foundation for the rules. To further enhance clarity and adaptability to emerging technologies, we respectfully suggest considering the inclusion of terms such as 'algorithmic transparency,' and 'non-personal data'. These additions could strengthen the Rules' alignment with global best practices and future-proof the legal framework.<br><br>***Note:** The aggregate score obtained from the expert rating is based on the legal alignment principles adopted from Law Commission Reports, Justice Puttaswamy Judgement, Justice Srikrishna Committee Report and JPC recommendations. National Law University, Jodhpur reserves the right to revise the |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| | | scores as per further research and evaluation. |
| 3 | **Draft Rule 3: Notice for Personal Data Processing** | **<u>Issues Identified-</u>**<br>1. The requirement that the notice should be "understandable independently" [Rule 3(a)] lacks clarity on whether this applies to all data principles (including those with<br>disabilities) or ones with limited digital literacy.<br>2. Requires notices but lacks multilingual support and clear presentation guidelines. |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| | | **Score- 4.9* out of 7 (max)**<br><br>**Proposed Suggestions**<br><br>1. We recommend clarifying the accessibility standards for notices to ensure inclusivity for all Data Principles, including those with disabilities and limited digital literacy. Providing guidelines on clear language and formatting would be beneficial. Encouraging multilingual notices and offering translated templates could further enhance accessibility.<br><br>Rule 3 provides a clear framework for notices to Data Principles, ensuring they are standalone and comprehensible. To further strengthen this provision and align it with principles of inclusivity, such as those in the UNCRPD and RPwD Act, 2016, we suggest clarifying that 'understandable independently' encompasses all Data Principles, including those with |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| | | disabilities or limited digital literacy. Additionally, incorporating guidelines on accessibility standards and a sample notice format in the Schedule could enhance implementation. We also recommend considering multilingual notices, such as in English and the state's official language, to broaden reach and ensure equitable access.<br><br>***Note:** The aggregate score obtained from the expert rating is based on the legal alignment principles adopted from Law Commission Reports, Justice Puttaswamy Judgement, Justice Srikrishna Committee Report and JPC recommendations. National Law University, Jodhpur reserves the right to revise the scores as per further research and evaluation. |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| 4 | **Draft Rule 4: Consent Requirements** | **Issues Identified-**<br>1. In Part A of 1st schedule, point 1 uses the term 'sufficient capacity' – Clarity is required on the connotation of the term.<br>b) Part A of the 1st Schedule, Point 3 uses the phrase 'financial conditions and general character should be sound'.<br>c) Can a data principal assess the Consent Manager given that an objective criterion has not been prescribed?<br>d) Schedule I, Part A, Point 6 states that "members of the senior board of the consent manager should have general reputation and record of fairness." Clarity and objective assessment criteria should be provided for the benefit of the data principles and data fiduciaries.<br>e) Can taking the consent manager route create a situation |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| | | wherein a data principal may have to avail the services of various consent managers since not all can have a tie-up with all the data fiduciaries?<br>f) The mechanism gives huge control to the consent Manager over the interests of the data principles since the volume of data stored with them is huge.<br>g) How does the Ministry plan to implement the rule in India without affecting the interests of all, given the unequal internet access among people and lack of technical know-how in matters about privacy?<br>h) Specifies consent requirements but makes withdrawal cumbersome.<br>**Score- 5.4* out of 7 (max)**<br>**Proposed Suggestions-** |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| | | a) We suggest clarifying the meaning of 'sufficient capacity' and providing specific criteria for evaluating Consent Managers. This would ensure transparency and fairness in the consent process. Additionally, addressing potential challenges associated with the Consent Manager mechanism, such as unequal internet access and data protection safeguards, would be beneficial.<br><br>Rule 4 and the First Schedule establish a robust framework for Consent Managers. To enhance transparency, we suggest providing specific, objective criteria for terms like 'sufficient capacity' and 'sound financial conditions and general character' in the Schedule. This would empower Data Principles to assess Consent Managers effectively. Additionally, while the ease of consent withdrawal is addressed, introducing a one-click withdrawal option and user education tools, such as videos, could further simplify the process and align with global |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| | | standards like GDPR Article 7, enhancing user trust and accessibility.<br><br>***Note:** The aggregate score obtained from the expert rating is based on the legal alignment principles adopted from Law Commission Reports, Justice Puttaswamy Judgement, Justice Srikrishna Committee Report and JPC recommendations. National Law University, Jodhpur reserves the right to revise the scores as per further research and evaluation. |
| 5. | **Draft Rule 5: Processing for provision or issue of subsidy, benefit, service, certificate, license or permit by State and its instrumentalities** | **Issues Identified-**<br><br>1. The rules 5(3)(a) and 5(3)(b) permit broad State data processing for subsidies and services but lack specificity, bypassing necessity and proportionality safeguards.<br>2. Lack of explicit guidelines on accountability for misuse of data or data breaches<br>3. There are no clear limitations on how much data is |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| | | collected or how long it is retained, increasing risks of function creep.<br><br>The rule permits the State and its instrumentalities to process personal data without obtaining fresh consent from Data Principles which raises concerns regarding the potential for indefinite data retention and the lack of explicit limitations on data usage.<br><br>**Score- 3.67* out of 7 (max)**<br><br>**Proposed Suggestions-**<br><br>1. To ensure responsible data handling by the state, we recommend incorporating clear guidelines on data retention limits, accountability measures for data misuse, and the necessity of obtaining fresh consent from Data Principles. These safeguards would promote transparency and trust in government data processing activities. |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| | | Rule 5 enables State processing for essential services, supported by standards in Schedule II. To further align with the Justice Puttaswamy Judgement's emphasis on necessity and proportionality, we recommend refining the provision with explicit legal remedies and penalties for data misuse by State entities. Defining precise, purpose-specific limitations could also enhance clarity, ensuring data collection remains proportionate and transparent, thus strengthening public trust.<br><br>***Note:** The aggregate score obtained from the expert rating is based on the legal alignment principles adopted from Law Commission Reports, Justice Puttaswamy Judgement, Justice Srikrishna Committee Report and JPC recommendations. National Law University, Jodhpur reserves the right to revise the scores as per further research and evaluation. |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| 6. | **Draft Rule 6: Reasonable security safeguards** | **<u>Issues Identified-</u>**<br>1. The rules use the term 'Appropriate Data Security Measures' and "Reasonable Measures", without giving a clear and precise definition for the same.<br>2. Rule 6(f) does not provide the definition of what constitutes as an appropriate provision in the contract entered into between such Data Fiduciary and such a Data Processor for taking reasonable security safeguards.<br>3. Rule 6(g) does not define appropriate technical and organizational measures to ensure effective observance of security safeguards.<br>4. There is an absence of sector-specific security provisions, like Finance or Healthcare might require stricter safeguards. |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| | | **Score- 4.75* out of 7 (max)**<br><br>**Proposed Suggestions-**<br><br>1. Rule 6 provides a strong foundation for security safeguards with examples like encryption and access controls. To enhance its effectiveness, we suggest further defining 'appropriate' and 'reasonable' measures with reference to globally recognized standards, such as those in GDPR Article.<br><br>2. This could provide Data Fiduciaries with clearer guidance and ensure robust protection aligned with international best practices.<br><br>3. We suggest providing clear and measurable definitions for terms like 'Appropriate Data Security Measures' and 'Reasonable Measures.' This would ensure greater consistency and effectiveness in implementing security |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| | | safeguards. Additionally, considering sector-specific security requirements could enhance protection for sensitive data in sectors like finance and healthcare.<br><br>***Note:** The aggregate score obtained from the expert rating is based on the legal alignment principles adopted from Law Commission Reports, Justice Puttaswamy Judgement, Justice Srikrishna Committee Report and JPC recommendations. National Law University, Jodhpur reserves the right to revise the scores as per further research and evaluation. |
| 7. | **Draft Rule 7: Intimation of personal data breach** | **Issues Identified-** Mandates breach reporting but has unclear timelines and conflicts with IT Act,2000/IT Rules & directives/CERT-In rules.<br><br>**Score- 4* out of 7 (max)**<br><br>**Proposed Suggestions-** |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| | | 1. Differentiate timelines based on breach severity and align with IT Act,2000/IT Rules/CERT-In rule requirements. To ensure timely and effective breach reporting, we recommend clarifying the timelines for reporting data breaches, considering the severity of the breach and ensuring consistency with existing CERT-In requirements.<br>**2.** Rule 7 establishes a robust breach notification framework, consistent with GDPR Article 33's 72-hour timeline. To enhance clarity and operational feasibility, we suggest refining the timeline to account for breach severity—e.g., immediate reporting for high-impact breaches and 72 hours for others. Additionally, harmonizing with CERT-In's 6-hour reporting requirement could streamline compliance for Data Fiduciaries, ensuring consistency across India's regulatory landscape while upholding the Explanatory Note's emphasis on prompt action. |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| | | ***Note:** The aggregate score obtained from the expert rating is based on the legal alignment principles adopted from Law Commission Reports, Justice Puttaswamy Judgement, Justice Srikrishna Committee Report and JPC recommendations. National Law University, Jodhpur reserves the right to revise the scores as per further research and evaluation. |
| 8. | **Draft Rule 8: Time period for specified purpose to be deemed as no longer being served** | **Issues Identified-**<br>1. The exemption allowing for data retention for compliance with the law from the general obligation for purpose limitation is unclear and may be potentially misused. It grants excessive discretionary power to the authorities<br>**Score 3.67* out of 7 (max)**<br>**Proposed Suggestions-**<br>1. Rule 8 provides a practical framework for data retention |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| | | to meet legal obligations, as noted in the Explanatory Note. To align further with the Justice Puttaswamy Judgement and GDPR Article 5, we suggest refining the scope of the 'legal compliance' exemption. Introducing specific criteria or periodic reviews—akin to Singapore PDPA's documentation requirements—could prevent unintended retention, ensuring fiduciaries uphold purpose limitation while maintaining accountability<br>2. We suggest clarifying the scope of the exemption for data retention based on legal compliance. This clarification would help prevent potential misuse and ensure that data erasure obligations are upheld.<br>3. It is recommended to strengthen accountability measures, ensuring that fiduciaries cannot circumvent erasure obligations by vague references to legal compliance. |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| | | ***Note:** The aggregate score obtained from the expert rating is based on the legal alignment principles adopted from Law Commission Reports, Justice Puttaswamy Judgement, Justice Srikrishna Committee Report and JPC recommendations. National Law University, Jodhpur reserves the right to revise the scores as per further research and evaluation. |
| 9. | **Draft Rule 9: Contact information of person to answer questions about processing** | **Issues Identified-**<br>1. The qualifications required for appointing a person as the Data protection officer (DPO) along with the roles and responsibilities attached to the office have not been properly delineated. The scope of functions of the DPO needs to be clarified and a uniform framework must be established for their appointment in both large-scale as well as small-scale data fiduciaries.<br>The definition of Data Protection Officer needs to be clarified. |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| | | Currently, the definition states that an officer appointed by a Significant Data Fiduciary is a data protection officer, raising the question of whether data fiduciaries need to appoint a data protection officer as well.<br><br>**Score- 4.4* out of 7 (max)**<br><br>**Proposed Suggestions-**<br>1. Rule 9 advances transparency by ensuring Data Principles can contact a designated person, as emphasized in the Explanatory Note. To strengthen this provision, we suggest specifying whether this individual must be a Data Protection Officer (DPO) and outlining basic qualifications, drawing from Brazil LGPD Article 41's flexible approach. While Singapore PDPA mandates DPOs universally, GDPR Articles 37-39 adopt a risk-based model. We recommend considering a tiered requirement— |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| | | mandatory DPOs for high-risk processing and trained contact persons for others—to balance compliance with practicality.<br><br>We recommend clarifying the qualifications, roles, and responsibilities of DPOs. Standardizing the DPO appointment process and ensuring their independence would enhance data protection oversight.<br><br>***Note:** The aggregate score obtained from the expert rating is based on the legal alignment principles adopted from Law Commission Reports, Justice Puttaswamy Judgement, Justice Srikrishna Committee Report and JPC recommendations. National Law University reserves the right to revise the scores as per further research and evaluation. |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| 10 | **Draft Rule 10: Verifiable consent for processing of personal data of child or of person with disability who has lawful guardian** | **Issues Identified-**<br>1. What constitutes verifiable consent is not clarified and no standard process for verifiable consent is provided, leaving room for inconsistent practices across platforms.<br>2. The Rules must specify the number of times parental consent is required while accessing the internet or other digital platforms. Are the parents required to give a one-time consent for accessing a website/digital platform or a fresh consent is required every time.<br>3. No clear parameters or guidelines have been provided on what constitutes due diligence.<br>4. Over reliance on Digital Locker services, with no clarity on alternatives if the parent or guardian does not use or have access to Digital Locker. |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| | | 5. No clarity on the liability when someone falsely claims to be a parent or lawful guardian — it is unclear whether the data fiduciary or the individual will be held responsible.<br>6. The rule treats all data in the same manner without distinguishing between sensitive and non-sensitive data.<br>7. There is a need to define the age of a "child" or "minor" to determine how a person shall be treated under the rules. This is because different platforms have different thresholds for age of consent. While the rule explicitly defines adulthood as beginning at the age of 18, it does not provide a clear definition of childhood across different platforms. Additionally, it does not clarify how this definition aligns with platforms where the age of digital consent varies, leading to potential inconsistencies in how minors are categorized and protected online. |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| | | 8. No clarification on whether the rule applies equally to all digital services, including education, healthcare, and social media platforms.<br>9. The provision presumes incapacity of persons with disabilities (PwDs) to provide independent consent, thereby mandating consent from a legal guardian, which equates adult PwDs with minors. This presumption undermines the legal capacity and autonomy of PwDs to make independent decisions regarding the processing of their personal data.<br>10. The rule lacks clarity on the practical implementation of obtaining guardian consent for PwDs, creating ambiguity in its application.<br>11. There are no specific guidelines or procedural safeguards prescribed for digital platforms on the manner in which guardian consent must be verified for PwDs. |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| | | 12. The provision fails to address the consequences if a guardian refuses consent, thereby potentially denying PwDs access to essential digital services such as online banking, e- commerce platforms, or healthcare services.<br>13. While the rule relating to verifiable parental consent for children includes detailed illustrations explaining the process in various scenarios, no corresponding illustrations or examples are provided for the process of obtaining guardian consent for PwDs, leading to practical uncertainty.<br>14. There is no clarity on whether the consent mechanism would apply uniformly across all categories of disabilities and degrees of severity, or how it would apply to guardians appointed under different statutory frameworks, thereby necessitating comprehensive procedural guidelines. |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| | | **Score- 3.72* out of 7 (max)**<br><br>**Proposed Suggestions-**<br><br>1. We suggest providing clear guidelines on the process of obtaining verifiable consent, including specific parameters for due diligence and addressing potential issues like false guardian claims. Clarifying the definition of a 'child' and ensuring consistency across platforms would be beneficial. Additionally, offering alternative options for consent verification beyond Digital Locker services would promote inclusivity.<br><br>Rule 10 establishes a framework for verifiable consent, supported by practical illustrations. To enhance consistency, we suggest elaborating the process with uniform methods like Aadhaar-based OTP or KYC, drawing from GDPR Article 8 and USCOPPA. Additionally, to align with UNCRPD and RPwD Act, |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| | | 2016, we recommend revising the presumption of incapacity for PwDs, requiring guardian consent only where legally mandated, thus promoting autonomy and inclusivity.<br><br>***Note:** The aggregate score obtained from the expert rating is based on the legal alignment principles adopted from Law Commission Reports, Justice Puttaswamy Judgement, Justice Srikrishna Committee Report and JPC recommendations. National Law University, Jodhpur reserves the right to revise the scores as per further research and evaluation. |
| 11. | **Draft Rule 11: Exemptions from certain obligations applicable to processing of personal data of child.** | 1. Overbroad exemptions for educational institutions allow schools to bypass parental consent and anti-tracking obligations under the guise of "educational activities" or "safety." However, these terms are vague and open to misuse, potentially enabling excessive student surveillance beyond academic purposes. |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| | | 2. Behavioral tracking risks normalizing child surveillance and could lead to profiling or data monetization by third-party edtech platforms. Similarly, healthcare exemptions permit clinical and allied workers to process children's health data without explicit safeguards like data minimization, encryption, or prohibitions on sharing with insurers or employers. The lack of parental notification further undermines transparency.<br>3. Permissive tracking by childcare centers and transport providers also raises concerns, as they can monitor children's locations without parental consent.<br>4. Continuous tracking increases the risk of data breaches, potentially exposing children to stalking or misuse, and there is no mandate to delete location data after a child leaves the institution. Public interest exemptions, such as processing data for "the exercise of powers under any |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| | | law" or "providing subsidies" are equally problematic.<br>5. Terms like "in the interests of a child" are subjective, allowing mass surveillance under welfare schemes, with government agencies potentially misusing data for profiling or predictive policing without accountability.<br>6. Another concern is the exemption for email account creation, which allows children to have email accounts without parental consent if usage is limited to communication by email. However, email accounts often require additional personal data like phone numbers or recovery emails, increasing the risk of third-party access and misuse. This exemption also violates global standards such as GDPR and COPPA, which mandate parental consent for underage users. Similarly, weak conditions for blocking harmful content raise censorship risks, as there is no clarity on who defines detrimental |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| | | content. This could lead to the over blocking of crucial resources, such as LGBTQ+ or mental health content, while enabling platforms to collect excessive data under the pretext of child safety.<br><br>**Score- 3* out of 7 (max)**<br><br>**Proposed Suggestions-**<br><br>1. We recommend reviewing the exemptions for educational and healthcare institutions to ensure they are narrowly defined and subject to appropriate safeguards. This would help prevent potential misuse of children's data and ensure greater transparency and parental control.<br><br>Rule 11 provides exemptions for educational institutions to facilitate essential functions like education and safety, which is a pragmatic approach. To align with global standards such as USCOPPA and South Korea's children's data policies, we |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| | | suggest refining the definitions of 'educational activities' and 'safety' in the Fourth Schedule. Limiting tracking to physical safety purposes—such as monitoring school premises or transport—while requiring parental consent for broader data use could enhance child privacy protections while preserving institutional flexibility.<br><br>***Note:** The aggregate score obtained from the expert rating is based on the legal alignment principles adopted from Law Commission Reports, Justice Puttaswamy Judgement, Justice Srikrishna Committee Report and JPC recommendations. National Law University, Jodhpur reserves the right to revise the scores as per further research and evaluation. |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| 12. | **Draft Rule 12: Additional obligations of Significant Data Fiduciary** | **Issues Identified-**<br>1. Lack of clarity with regard to "audit"- the provision for audit lacks specification as to the entity which shall be conducting the audit and DPIA for the SDF.<br>This could lead to potential conflicts of interest, opening a loophole for SDFs to undergo audits via favorable firms and by-pass genuine reports.<br>2. Overreach and excessive surveillance- the power to decide what data is to be restricted to storage within India is vested only with the government and there are no established guidelines for the same. This could lead to three potential roadblocks that hinder legislative intent-<br>a. This could lead to massive surveillance. If the government mandates local storage for sensitive data, access to such data would be left without essential |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| | | safeguards.<br>b. Strict Data localization also affects foreign investment.<br>c. Hinders the prospects and ease of doing business for Indian companies that rely on global data protection services.<br>Lack of Remedial/ Redressal Mechanisms- While the rule mandates compliance, it does not specify penalties for violations. There is no grievance redressal mechanism for victims of data mishandling. No compensation is being given to the data principles in case of any breach.<br>**Score- 4* out of 7 (max)**<br>**Proposed Suggestions-**<br>1. Rule 12 establishes vital obligations for Significant Data |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| | | Fiduciaries, including audits to ensure compliance. To strengthen this framework, we suggest specifying that audits be conducted by independent, certified auditors listed in a government-notified register. This would enhance impartiality and trust, aligning with accountability principles in the OECD Privacy Guidelines and GDPR Article 39, ensuring robust oversight of SDFs.<br>2. We suggest clarifying the audit process for Significant Data Fiduciaries, ensuring the independence of auditors and establishing a clear threshold for data localization requirements. This would enhance transparency and accountability in data handling practices.<br>3. A more comprehensive, analytical and reliable threshold for what constitutes "high-risk" data, based on which it will be subjected to Localized storage. Additionally, a provision for judicial oversight for cases where the government |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| | | mandates localized storage.<br><br>***Note:** The aggregate score obtained from the expert rating is based on the legal alignment principles adopted from Law Commission Reports, Justice Puttaswamy Judgement, Justice Srikrishna Committee Report and JPC recommendations. National Law University, Jodhpur reserves the right to revise the scores as per further research and evaluation. |
| 13. | **Draft Rule 13: Rights of Data Principles** | **Issues Identified-** Includes user rights but has complex processes and unclear remedies.<br><br>**Score- 4* out of 7 (max)**<br><br>**Proposed Suggestions-**<br><br>1. We recommend simplifying the process for Data Principles to exercise their rights, potentially through a centralized portal. Defining clear compensation mechanisms for data |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| | | misuse would further strengthen data protection. Outlining clear compensation mechanisms for violations would boost accountability and user confidence, making the framework more accessible and enforceable<br>2. Rule 13 strengthens Data Principles' rights, a cornerstone of data protection. To enhance its effectiveness, streamlining the exercise of these rights through a centralized portal, drawing insight from GDPR Articles 12-22 and the Singapore PDPA.<br>Scope of the Rule 13(2) can be broadened by adding the right to correct the data along with access and erasure.<br>***Note:** The aggregate score obtained from the expert rating is based on the legal alignment principles adopted from Law Commission Reports, Justice Puttaswamy Judgement, Justice Srikrishna Committee Report and JPC recommendations. |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| | | National Law University, Jodhpur reserves the right to revise the scores as per further research and evaluation. |
| 14. | **Draft Rule 14: Processing of personal data outside India** | **<u>Issues Identified-</u>**<br>1. There is no assessment framework to evaluate the adequacy of recipient countries' data protection regimes, potentially enabling arbitrary restrictions or permissiveness. This contradicts the OECD Privacy Guidelines (para 8 and 9) and Puttaswamy's proportionality test, which require legitimate, necessary, and narrowly tailored data restrictions.<br>2. The rule grants excessive discretionary power to the Central |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| | | Government to determine cross-border data transfers without clear legislative or procedural safeguards.<br>3. In this regard, reference may be made to APEC CBPR framework and Article 45 of the GDPR which provides for specific parameters to determine adequacy of such decisions and also establishes monitoring mechanisms.<br>**Score- 3.6* out of 7 (max)**<br>**Proposed Suggestions-**<br>1. We suggest establishing a clear framework for assessing the adequacy of data protection regimes in countries receiving personal data from India. This would ensure greater protection for data transferred outside India.<br>2. Rule 14 governs cross-border data transfers, a key |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| | | element of global data flows. To strengthen this provision, we suggest incorporating an adequacy assessment framework akin to GDPR Article 45 or the APEC CBPR system. This would ensure recipient countries uphold comparable data protection standards, offering clarity to Data Fiduciaries and robust safeguards for Data Principles.<br><br>If possible, introduce a mechanism for independent review or legislative scrutiny over executive orders restricting or permitting transfers. The government may specify conditions under which foreign states can access personal data, ensuring due process and protection against mass surveillance concerns.<br><br>***Note:** The aggregate score obtained from the expert rating is based on the legal alignment principles adopted from Law Commission Reports, Justice Puttaswamy Judgement, Justice Srikrishna Committee Report and JPC recommendations. |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| | | National Law University, Jodhpur reserves the right to revise the scores as per further research and evaluation. |
| 15. | **Draft Rule 15: Exemption from Act for research, archiving or statistical purposes.** | **Issues Identified-**<br>1. The rule provides for exemption for research, archiving or statistical purposes however, the relevant Schedule no. 2 bears the heading - 'standards for processing personal data by the State and its instrumentalities', this leads to the question of whether private entities and individual persons engaged in such activities would be allowed to avail these exemptions?<br>**Score- 5* out of 7 (max)** |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| | | **Proposed Suggestions-**<br><br>1. We recommend clarifying whether the exemption for research, archiving, or statistical purposes applies only to the state or also to private entities and individuals.<br><br>Rule 15 facilitates exemptions for research, archiving, and statistical purposes, supporting innovation and public interest. To enhance clarity, we suggest specifying in the Second Schedule whether these exemptions extend to private entities and individuals or are limited to State actors. Drawing from GDPR Article 89 and Brazil's LGPD, including private entities with appropriate safeguards could enhance research while ensuring consistent data protection standards.<br><br>***Note:** The aggregate score obtained from the expert rating is based on the legal alignment principles adopted from Law Commission Reports, Justice Puttaswamy Judgement, Justice |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| | | Srikrishna Committee Report and JPC recommendations. National Law University, Jodhpur reserves the right to revise the scores as per further research and evaluation. |
| 16. | **Draft Rule 16: Appointment of Chairperson and other Members** | **<u>Issues Identified-</u>**<br>1. Clause 4 suggests that the validity of the search-cum-selection committee's acts and proceedings cannot be contested solely on the grounds of a vacancy or a defect in its composition without elaborating on the scope of the said term. This raises concerns about fairness, transparency, and the legitimacy of decisions. If the committee is improperly constituted or lacks key members, its decisions may be seen as lacking credibility |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| | | and could therefore be subject to challenge.<br>2. Under Clause 1 of the rule, the phrase "two experts of repute" grants broad discretion, which may result in a lack of transparency and potential biases.<br>3. Additionally, there is no provision for a transparent or time-bound selection process and clarification regarding the duration of the terms of members as well as the chairperson is not clear in addition to the process of their removal and disqualification.<br>4. Moreover, the provisions give the impression that it is likely Search-cum-Selection Committee may prefer the retired civil servants likely to be appointed as Chairperson and Members.<br>**Score- 4* out of 7 (max)** |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| | | **Proposed Suggestions-**<br>1. We suggest clarifying the composition of the Search-cum Selection Committee and ensuring a transparent and time bound selection process. Incorporating judicial review provisions and clearly defining expert qualifications would enhance the legitimacy and fairness of the appointment process.<br>2. Rule 16(4) ensures the Search-cum-Selection Committee's continuity, a practical provision for effective governance. To further enhance transparency and trust, we suggest clarifying the scope of 'defect in composition.' While GDPR Article 72 offers a voting model, we recommend adopting Indian administrative law principles—such as mandating quorum or detailed appointment records—to ensure fairness and accountability in the selection |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| | | process.<br>3. The Search-cum-Selection Committee needs to have representation from the Judiciary to ensure neutrality and fairness in the selection of the Chairperson and Members. A nominee of the Chief Justice of India is recommended to be part of the Search-cum-Selection Committee.<br>It is proposed that the Search-cum-Selection Committee needs to have experts from a diversified pool of persons from Industry, Academia, Civil Society Judiciary, etc.<br>***Note:** The aggregate score obtained from the expert rating is based on the legal alignment principles adopted from Law Commission Reports, Justice Puttaswamy Judgement, Justice Srikrishna Committee Report and JPC recommendations. National Law University, Jodhpur reserves the right to revise the scores as per further research and evaluation. |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| 17. | **Draft Rule 17: Salary, allowances and other terms and conditions of service of Chairperson and other Members.** | **Issues Identified-**<br>1. The temporary nature of the board of members is evident in the salary stipulations of Schedule V. Certain rules such as no pension indicate that the board will be ad-hoc.<br>**Score- 3.67* out of 7 (max)**<br>**Proposed Suggestions-**<br>1. Rule 17 and the Fifth Schedule provide clear terms for Board members' compensation, aligning with Indian regulatory norms. To attract and retain top talent for this critical role, we suggest exploring additional incentives, such as performance-based bonuses or professional development opportunities, rather than pensions. This could enhance long-term commitment |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| | | while maintaining fiscal prudence.<br>2. We suggest providing pensions and other benefits to board members to incentivize long-term commitment and expertise within the Data Protection Board.<br>Another measure to drive the permanency of the post could be to prohibit the board member from having any other position of profit under any Government, Indian or foreign.<br>***Note:** The aggregate score obtained from the expert rating is based on the legal alignment principles adopted from Law Commission Reports, Justice Puttaswamy Judgement, Justice Srikrishna Committee Report and JPC recommendations. National Law University, Jodhpur reserves the right to revise the scores as per further research and evaluation. |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| 18. | **Draft Rule 18: Procedure for meetings of Board and authentication of its orders, directions and instruments.** | **Issues Identified-**<br>1. Rule 18(4)<br>The questions give the chairperson the general power to make the casting vote. However, not all the questions decided will be similar. For instance, some questions may be hyper-technical while others will be general and more understandable. This distinction is necessary but absent.<br>2. Rule 18(5)<br>It is not implausible that a member may neglect deliberately or otherwise to disclose their compromising interest in a proceeding.<br>Rule 18(6)<br>Lack of procedure when emergent action is withdrawn before the end of seven days. |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| | | 4. Rule 18(7)<br><br>Lack of consultation and discussion in an issue decided by circulation.<br><br>5. Rule 18(8)<br><br>Overbroad persons that may be authorised for authentication. No way for stakeholders to verify whether a person is truly authorised by the board.<br><br>**Score- 3.5* out of 7 (max)**<br><br>**Proposed Suggestions-**<br><br>1. Rule 18(4) provides the Chairperson with a casting vote in tied decisions, a common governance mechanism. To optimize this process, we respectfully suggest limiting the casting vote to final adjudications of complaints, while allowing technical matters to be resolved by a majority |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| | | among relevant experts. This could ensure balanced decision-making reflective of both legal and technical perspectives.<br>2. We recommend clarifying the procedures for board meetings, including refining the Chairperson's casting vote, enabling impeachment of members with conflicts of interest, and establishing clear procedures for handling withdrawn actions. These clarifications would enhance transparency and accountability in decision-making.<br>3. If an action of the chairperson is withdrawn before completion of seven days from taking the action, in the subsequent meeting of the board, the action must be examined, and if found incorrect or unjustified, be followed by remedial measures.<br>4. Issues can be circulated in a set order, with each member |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| | | outlining her thoughts on the material before further circulation, making the decision *ad idem.*<br><br>The board can maintain a registry of persons authorised to authenticate a board order, or in this rule, be mandated to present the court order when authenticating the board order.<br><br>***Note:** The aggregate score obtained from the expert rating is based on the legal alignment principles adopted from Law Commission Reports, Justice Puttaswamy Judgement, Justice Srikrishna Committee Report and JPC recommendations. National Law University, Jodhpur reserves the right to revise the scores as per further research and evaluation. |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| 19. | **Draft Rule 19: Functioning of Board as digital office.** | **<u>Issues Identified-</u>**<br>Techno-legal means to conduct proceedings. Claims could include sensitive information, which would be disclosed in these virtual proceedings. Further, sensitive information could be regarding public figures or generally of a character that has the potential for grievous privacy breach for the individual and/or public security or law and order concerns. Hence, the rule, if not in the letter itself, in operative guidelines at least, needs a bare minimum system requirement so that these techno-legal means are safe from a data breach.<br>2. This concern also includes the records of the board. These are at a higher risk of a deliberate data breach than run-of-the-mill public institution databases due to their nature of adjudicating of data breach claims. |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| | | **Score- 4.2* out of 7 (max)**<br><br>**Proposed Suggestions-**<br><br>1. Rule 19's digital office framework is innovative and efficient. To further strengthen it, we suggest establishing guidelines for secure video conferencing and data handling during virtual proceedings. Referencing the Justice Puttaswamy Judgement and GDPR Article 32, measures like encryption and security audits could safeguard sensitive information, reinforcing public trust in the Board's operations.<br><br>2. We recommend providing clear criteria for fee reduction or waiver in appeals to the Appellate Tribunal. Defining 'techno- legal measures' and ensuring due process in digital hearings would enhance fairness and transparency.<br><br>Adequate public infrastructure shall be extended to the rural |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| | | areas where internet accessibility issues persist<br><br>***Note:** The aggregate score obtained from the expert rating is based on the legal alignment principles adopted from Law Commission Reports, Justice Puttaswamy Judgement, Justice Srikrishna Committee Report and JPC recommendations. National Law University, Jodhpur reserves the right to revise the scores as per further research and evaluation. |
| 20. | **Rule 20: Terms and conditions of appointment and service of officers and employees of Board.** | No Comments. |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| 21. | **Rule 21: Appeal to Appellate Tribunal** | **Issues Identified-**<br>1. The extensive discretionary authority vested in the Chairperson to remit or cut fees, in the absence of any specified criteria or guiding principles, leaves vast room for arbitrariness and uneven exercise of discretion.<br>2. The term "techno-legal measures" remains undefined within the rule, leaving its scope and application overly broad and ambiguous. This absence of clarity and procedural safeguards creates the risk of arbitrary or inconsistent adoption of technological tools and processes.<br>**Score- 4.27* out of 7 (max)**<br>**Proposed Suggestions-**<br>Rule 21(2) empowers the Chairperson to waive fees, promoting access to justice. To ensure transparency |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| | | and consistency, we suggest introducing illustrative guidelines— such as for indigent appellants or public interest cases—to guide this discretion. This would align with principles of fairness and enhance confidence in the Tribunal's processes.<br>2. We recommend providing clear criteria for fee reduction or waiver in appeals to the Appellate Tribunal. Defining 'techno- legal measures' and ensuring due process in digital hearings would enhance fairness and transparency.<br>The rule either defines techno-legal measures or requires them. We recommend the Tribunal publish a set of standard operating procedures (SOPs) outlining approved digital tools, cybersecurity standards, and procedural safeguards to ensure due process is maintained in digital hearings.<br>***Note:** The aggregate score obtained from the expert rating is |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| | | based on the legal alignment principles adopted from Law Commission Reports, Justice Puttaswamy Judgement, Justice Srikrishna Committee Report and JPC recommendations. National Law University, Jodhpur reserves the right to revise the scores as per further research and evaluation. |
| 22. | **Rule 22: Calling for information from a Data Fiduciary or intermediary** | **Issues Identified-**<br>1. Unrestricted Government Demand– No threshold of the nature, scope, or limitations while empowering the government to call for information, creating room for unchecked data collection.<br>2. Vague & Overbroad Grounds – The terms "sovereignty and integrity of India" and "security of the State" are broad and undefined, allowing subjective interpretation for precisely the kinds of cases where the government can impose non- |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| | | disclosure of information.<br>3. Overarching effect of Section 36– When combined with Section 36 of the Act, this rule enables sweeping government access to data without adequate judicial or procedural safeguards.<br>**Score- 3.5* out of 7 (max)**<br>**Proposed Suggestions-**<br>1. Rule 22 enables the government to request information for essential purposes like security, with some disclosure safeguards in place. To align with Justice Puttaswamy's Judgement and take insights from the German Federal Data Protection Act, we suggest refining this provision with oversight mechanisms, such as prior approval from an independent body. This would ensure requests are proportionate and necessary, enhancing both |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| | | accountability and public trust.<br>2. We suggest incorporating safeguards to ensure that government demands for information are proportionate and subject to appropriate oversight. This would help prevent potential misuse of data access powers and protect the privacy of individuals. Precise and objective thresholds as to what should entail 'prejudicially affecting the sovereignty, integrity and security of India.'<br>We suggest incorporating safeguards to ensure devised tests of *proportionality, necessity and reasonableness* to minimise the infringement of Article 21.<br>***Note:** The aggregate score obtained from the expert rating is based on the legal alignment principles adopted from Law Commission Reports, Justice Puttaswamy Judgement, Justice Srikrishna Committee Report and JPC recommendations. |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| | | National Law University, Jodhpur reserves the right to revise the scores as per further research and evaluation. |
| 23. | **Schedule I: Part A - Conditions of registration of Consent Manager** | We recommend considering financial stability evidence like credit scores and compliance histories as indicators of the financial ability of firms seeking registration as Consent Managers. This would provide a more comprehensive assessment of their suitability. |
| 24. | **Schedule II** | No Comments |
| 25. | **Schedule III** | To ensure that the DPDP Rules encompass the evolving landscape of data processing, we suggest explicitly including AI |

| S. No. | Rule/Schedule | Proposed Amendments |
|---|---|---|
| | | Service Providers like ChatGPT and Gemini in the relevant categories of Data Fiduciaries. |
| 26. | **Schedule IV** | No Comments. |
| 27. | **Schedule V** | No Comments. |
| 28. | **Schedule VI** | No Comments. |
| 29. | **Schedule VII** | No Comments. |

**Legal Analytical Matrix for Evaluating Draft DPDP Rule:**

The purpose of this matrix is to provide a structured method to assess how well the draft rules align with established legal and policy principles. Each criterion will be scored on a scale of 1 to 7, where:

- 1 = Very Poor Alignment/Compliance
- 2 = Poor Alignment/Compliance
- 3 = Somewhat Poor Alignment/Compliance
- 4 = Moderate Alignment/Compliance
- 5 = Good Alignment/Compliance
- 6 = Very Good Alignment/Compliance
- 7 = Excellent Alignment/Compliance

## I. Principles from *Puttaswamy* Judgment:

| Criterion | Description | Scoring* | Justification/Evidence |
|---|---|---|---|

| | | | |
|---|---|---|---|
| | | **(1-7)** | |
| **Recognition of Privacy** | The extent to which the rules acknowledge privacy as a fundamental right under Article 21. | **1** | Does the language used in the draft rules reflect the principles laid out in the Puttaswamy Judgement Does it treat privacy as a fundamental right? |
| **Informational Privacy** | How well the rules protect informational privacy, extending to personal data and its processing. | **3** | Do the rules adequately define personal data and outline provisions for data processing and consent? |
| **Legitimate Aim** | To what extent the rules are formulated to pursue a legitimate aim, ensuring that the law is not arbitrary? | **2** | Do the rules define 'legitimate aim' and give examples of the types of objectives that are permitted? Are the conditions for exemptions defined precisely? |
| **Necessity and Proportionality** | How well the rules ensure that restrictions on privacy are necessary, narrowly tailored, and proportionate to | **2** | Are limitations on privacy rights balanced against the need for such limitations? Do any exemptions adhere to the |

| | | | |
|---|---|---|---|
| | the stated purpose. | | proportionality test? |
| **Fair, Just, and Reasonable Procedure** | The degree to which the rules guarantee procedures that are fair, just, and reasonable when processing personal data, with sufficient safeguards to prevent arbitrariness in data processing. | **3** | Do the rules describe clear and fair procedures for data handling and dispute resolution? |
| **Data Security Safeguards** | The extent to which rules require data fiduciaries to maintain robust data security safeguards. | **6** | Are there specific provisions for data security, including data breach reporting? |
| **Link to Dignity and Liberty** | To what degree do the rules ensure the protection of human dignity and liberty, aligning with the spirit of the Puttaswamy judgment, when processing personal data? | **3** | Do the rules recognize the link between privacy and human dignity? |

**II. Principles from the Justice Srikrishna Committee Report**

| Criterion | Description | Scoring* (1-7) | Justification/Evidence |
|---|---|---|---|
| **Technology Agnosticism** | How well the rules are designed to be adaptable to changing technologies and compliance standards. | **5.6** | Do the rules avoid prescriptive technological requirements? |
| **Holistic Application** | To what extent the law applies to both private and public entities, with specific carve-outs for legitimate state aims. | **5.2** | Do the rules apply uniformly to both private sector and government entities? Are there differential obligations, and if so, are they justified? |
| **Informed Consent** | How well the rules uphold the principle of informed consent, requiring that consent be freely | **3** | Are the rules clear about what constitutes valid consent? Do they allow for easy withdrawal of consent? |

| | | | |
|---|---|---|---|
| | given, specific, and informed. | | |
| **Data Minimization** | To what extent the rules ensure that data collected and processed is limited to what is necessary for the specific purpose. | **4** | Do the rules have provisions to minimize data collection and processing? |
| **Data Portability** | To what degree the rules enable data subjects to access and transfer their personal data to other service providers. | **6** | Is there a provision that gives data subjects the ability to port their data? |
| **Accountability** | Does the framework ensure accountability of data fiduciaries through the establishment of a DPA and other mechanisms? | **3** | Are there clear lines of accountability for data breaches? |
| **Co-Regulatory Approach** | To what extent do the rules implement a system of co-regulation that balances self-regulation with | **4** | Do the rules specify the role of self-regulatory organizations and their responsibilities? |

| | | | |
|---|---|---|---|
| | government oversight? | | |

**III. Principles from Law Commission Reports**

| Criterion | Description | Scoring* (1-7) | Justification/Evidence |
|---|---|---|---|
| **Clarity and Precision** | How clearly and precisely the rules define key terms and concepts, reducing ambiguity and uncertainty. | **4** | Do the rules use clearly defined terminology, and are these aligned with established legal definitions? |
| **Effective Enforcement** | To what extent do the rules establish effective mechanisms for enforcement, including penalties, adjudicatory processes, and appellate mechanisms? | **3.5** | Are there clear penalty provisions that are proportionate and dissuasive? Is there a defined process for dispute resolution with an independent adjudicatory body? |

| | | | |
|---|---|---|---|
| **Remedies and Redressal** | How effectively the rules provide remedies for data subjects whose rights have been infringed, including compensation and other forms of redressal. | **4** | Do the rules allow for class action suits? Are there effective remedies available to data principles? Is there a clear process for filing complaints? |
| **Cross-Border Data Flow** | To what degree do the rules address cross-border data flow and ensure that data transferred outside of India remains protected with an adequacy standard? | **5** | Are there clear provisions governing international data transfer, with adequate safeguards? Are there restrictions on transfers of sensitive data? |
| **Independent Oversight** | To what extent do the rules ensure independent oversight of the DPA with transparent and accountable processes? | **4** | Are there provisions for independent oversight of the DPA? Does the DPA have an adjudicatory wing that is separate from its other functions? |
| **Data Retention and Erasure** | To what degree do the rules ensure that data is not retained longer than | **6** | Do the rules provide a right to erasure? Are there guidelines on the retention of data and |

| | | | |
|---|---|---|---|
| | necessary, with a right to erasure or correction of data? | | timelines? |

**IV. Principles from the Joint Parliamentary Committee on the Data Protection Bill, 2018**

| Criteria | Description | Scoring* (1-7) | Justification/Evidence |
|---|---|---|---|
| **Data quality principle** | Whether the Rules allow data principles to correct or rectify, erase and access their data? | **5.4** | Do the rules provide clear rights for individuals to modify or erase their data? Is there a mechanism for challenging inaccurate data retention? Are data fiduciaries obligated to inform third parties about rectifications made? |
| **Data localisation** | Whether the Rules ensure national security, employment generation, privacy and bargaining power as envisaged | **3** | Do the rules mandate that certain types of data be stored within India? Are there specific justifications provided for localisation requirements? How do they balance security concerns with ease of doing |

| | | | |
|---|---|---|---|
| | by the Joint Parliamentary Committee Report? | | business? |
| **Processing of personal and non-personal data** | Whether the Rules protect personal and non-personal data as discussed in the Report? | **5.2** | Do the rules differentiate between personal and non-personal data? Are there specific safeguards for anonymised or non-personal data? How do they regulate data aggregation practices? |
| **Transition time period** | Whether the Rules provide sufficient time period to different stakeholders to prepare and comply with the new framework? | **4** | Is there a phased implementation plan to allow different sectors to comply? Are MSMEs and start-ups given differentiated timelines? How does the transition period compare with global data protection regimes? |
| **Children's consent post attaining majority** | Whether the Rules provide guidance on the steps to be taken with regard to the processing of data post the time a 'child' attains majority? | **5** | Do the rules require re-consent once a child reaches adulthood? Are there provisions for data erasure or modification of prior consent given by guardians? How are social media and ed-tech platforms expected to handle such transitions? |

| | | | |
|---|---|---|---|
| **Social media and privacy** | Do the Rules cater to the need for regulation of data processing by social media platforms? | **5** | Are social media intermediaries required to comply with stricter privacy norms? Do the rules impose specific obligations on platforms handling large volumes of sensitive data? Are there provisions for algorithmic transparency and content moderation accountability? |
| **Right to be forgotten** | Do the Rules incorporate the right to be forgotten in a substantive manner? | **4** | Are individuals given the right to request erasure of their personal data? Do the rules provide clear guidelines on balancing this right with freedom of speech and public interest? How is the enforcement mechanism structured? |
| **Financial data privacy** | Do the Rules provide a specific framework for the regulation of data pertaining to a person's finance? | **4** | Are financial institutions subject to additional compliance requirements? Do the rules provide adequate security measures for sensitive financial data? Are fintech companies and digital lenders covered under the framework? |

| | | | |
|---|---|---|---|
| **Protecting in a holistic manner** | Whether the Rules create a distinction between processing of personal and non-personal data or apply uniformly to both? | **4** | Do the rules explicitly define different standards for personal and non-personal data processing? Are safeguards placed against re-identification of anonymised data? How do the rules integrate with broader data governance policies? |
| **Non-consensual Processing** | Whether the grounds for non-consensual processing are free from ambiguity? | **4** | Are the justifications for processing data without consent narrowly defined? Do they align with global privacy principles such as necessity and proportionality? Are there safeguards to prevent excessive data processing under exemptions? |
| **Wide exemptions for the government and no surveillance reform** | Whether the Rules adequately allay the concerns regarding surveillance by different entities and the Government? | **3.5** | Do the rules impose any checks on government access to personal data? Are there independent oversight mechanisms for government surveillance? How do the exemptions compare with international data protection standards? |
| | Does the framework for the | **5** | Is the Data Protection Board structurally |

| | | | |
|---|---|---|---|
| **Independence of regulatory authority** | independence of the Data Protection Board, as established under the Act, ensure a balanced regulatory approach? | | independent from executive control? Are its members appointed through a transparent and independent process? Does it have adjudicatory powers separate from regulatory functions? |

**IV. Additional Considerations**

| Criterion | Description | Scoring* (1-7) | Justification/Evidence |
|---|---|---|---|
| **Consistency with other laws** | How well the rules ensure consistency with existing laws and regulations and also provide for situations of conflict. | **5** | Do the rules clarify their relationship with other laws? Does the data protection law have an overriding effect over inconsistent legislation? |
| **Public** | The extent to which public | **5.5** | To what degree are comments from public |

| | | | |
|---|---|---|---|
| **Consultation** | comments have been considered in the formulation of the rules. | | consultation reflected in the rules? |
| **Adaptability** | How well can the rules adapt to future technological changes and social developments? | **5.5** | Do the rules have mechanisms to update in response to changing technological and social environments? |

***Savings:** The aggregate score obtained from the expert rating; National Law University, Jodhpur, reserves its right to revise the score as per the continuous assessment and research.