To,

Shri S. Krishnan

Secretary, Ministry of Electronics and Information Technology

Government of India

5th March 2025

In Re: Submission of Comments from Public on the *Draft Digital Personal Data Protection Rules, 2025.*

Respected Sir,

This letter is in reference to the report dated 3rd January 2025, issued by the Ministry of Electronic and IT, Government of India, inviting comments from the public on the *Draft Digital Personal Data Protection Rules, (2025)*. In furtherance of our commitment to contributing towards the legal and technological discourse in the country and working for public welfare in the capacity of law students, the team at the Cell for Law and Technology ("CLT"), at National Law Institute University, Bhopal, hereby submits its suggestions in response to the Press Release.

At the very outset, we would like to express our appreciation for this progressive initiative taken by the Ministry to seek public participation in shaping the regulatory framework for Data Privacy. The inclusive approach towards policy formulation will ensure a balanced, transparent, and effective governance structure for protection of data privacy of citizens and corporations in India. As Digital Privacy continues to play an increasingly crucial role across industries, implementing robust and adaptable regulations will be vital to addressing ethical concerns, ensuring accountability, and fostering innovation.

The proposed framework has been thoroughly analyzed, and the team comprising members of CLT has identified various points that we would like to highlight as suggestions and comments. We hope that our submissions will contribute meaningfully to the ongoing discussions surrounding Data Privacy governance in India.

Thank you for your consideration.

Warm Regards,

Atul Kumar Pandey

(Professor of Cyber Law, Head, Department of Cyber Law Faculty in Charge, Cell for Law and Technology

The team which has been instrumental in putting forward this suggestion comprises of the following members of the Cell for Law and Technology, NLIU Bhopal:

1. Rishita Sethi (Convenor) (Final Year B.A.LLB. (Hons.) Student, NLIU Bhopal)
2. Hussain (Co-Convenor) (Final Year B.A.LLB. (Hons.) Student, NLIU Bhopal)
3. Samruddhi Memane (4th Year B.A.LLB. (Hons.) Student, NLIU Bhopal)
4. Hanshika Kumari (4th Year B.A.LLB. (Hons.) Student, NLIU Bhopal)
5. Amit Krishnan (4th Year B.A.LLB. (Hons.) Student, NLIU Bhopal)
6. Suvansh Shanker (3th Year B.SC.LLB. (Hons.) Student, NLIU Bhopal)
7. Lavya Bhasin (3th Year B.SC.LLB. (Hons.) Student, NLIU Bhopal)
8. Harshwardhan Yadav (3th Year B.SC.LLB. (Hons.) Student, NLIU Bhopal)
9. Khushi Dhingra (3th Year B.A.LLB. (Hons.) Student, NLIU Bhopal)
10. Ashmit Chauhan (3th Year B.SC.LLB. (Hons.) Student, NLIU Bhopal)
11. Gurman Narula (3th Year B.A.LLB. (Hons.) Student, NLIU Bhopal)
12. Sharad Khemka (3th Year B.A.LLB. Student, NLIU Bhopal)
13. Prabhash Shukla (2nd Year B.SC.LLB. (Hons.) Student, NLIU Bhopal)
14. Aman Garg (2nd Year B.SC.LLB. (Hons.) Student, NLIU Bhopal)
15. Shaurya Chauhan (2nd Year B.A.LLB. (Hons.) Student, NLIU Bhopal)
16. Rohini (2nd Year B.SC.LLB. (Hons.) Student, NLIU Bhopal)
17. Tamanna (2nd Year B.A.LLB. (Hons.) Student, NLIU Bhopal)
18. Arpit Dhadhich (2nd Year B.SC.LLB. (Hons.) Student, NLIU Bhopal)
19. Vismaya (2nd Year B.A.LLB. (Hons.) Student, NLIU Bhopal)
20. Vibhuti (2nd Year B.SC.LLB. (Hons.) Student, NLIU Bhopal)
21. Rajeshwari (2nd Year B.SC.LLB. (Hons.) Student, NLIU Bhopal)
22. Yash Bajpai (2nd Year B.SC.LLB. (Hons.) Student, NLIU Bhopal)
23. Rujuta Bapat (2nd Year B.A.LLB. (Hons.) Student, NLIU Bhopal)
24. Siddhant Samaiya (2nd Year B.SC.LLB. (Hons.) Student, NLIU Bhopal)

25. Yash Singh (2nd Year B.A.LLB. (Hons.) Student, NLIU Bhopal)
26. Sandali Akram (2nd Year B.SC.LLB. (Hons.) Student, NLIU Bhopal)
27. Avika (1st Year B.SC.LLB. (Hons.) Student, NLIU Bhopal)
28. Nandani (1st Year B.SC.LLB. (Hons.) Student, NLIU Bhopal)
29. Abhinav Saraswat (1st Year B.SC.LLB. (Hons.) Student, NLIU Bhopal)
30. Ananya Tiwari (1st Year B.SC.LLB. (Hons.) Student, NLIU Bhopal)

DRAFT DIGITAL PERSONAL DATA PROTECTION RULES, 2025

RECOMMENDATIONS

Rule	Existing Rule and Issues	Recommendations
1.	**Short Title and Commencement**	-
2.	**Definitions** This rule relies on definitions from the Digital Personal Data Protection Act, 2023, which may not cover all necessary terms relevant to modern data practices. Critical concepts like "data portability" and "algorithmic transparency" are absent, leading to potential ambiguities in interpretation. The term "legitimate uses" is vague, creating uncertainty for data fiduciaries regarding compliance.	Introduce formal definitions for at least 15 new terms relevant to current digital practices, such as "data anonymization," "automated decision-making," and "data minimization," to ensure clarity and comprehensive coverage. Ensure that definitions align with international standards such as GDPR and other Indian regulations (e.g., IT Act) to facilitate compliance for multinational organizations and enhance legal coherence. - **Clarify Ambiguous Terms**: Provide illustrative examples for ambiguous terms like "processing activities" to ensure uniform understanding. - **Define Emerging Concepts**: Formally introduce definitions for concepts such as "algorithmic transparency" and "data portability" to reflect current digital realities. - **Explanatory Notes**: Include explanatory notes for terms like "legitimate uses" to prevent misinterpretation and enhance clarity.
3.	**Notices given by Data Fiduciary to Data Principal**: This rule mandates that data fiduciaries provide clear notices in simple language about data processing. However, the requirement for "simple language" is subjective, leading to inconsistent implementations across different sectors.	- **Proposed Revised Language for R 3(b):** “(b) give, in clear and plain language, a fair account of the details necessary to enable the Data Principal to give consent that is specific, informed, freely and actively given through affirmative action for the processing of her personal data, which shall include, at the

	There is also no standardization for how these notices should be delivered across various platforms (web, app, SMS), nor are there provisions for accessibility for disabled users.	minimum,— (i) an itemised description of such personal data; and (ii) the specified purpose of, and an itemised description of the goods or services to be provided or uses to be enabled by, such processing;" Rationale for the changes: The proposed revisions emphasize the importance of consent being "freely and actively given through affirmative action." This aligns with best practices established under international frameworks such as the General Data Protection Regulation (GDPR), which underscores that consent must not only be informed but also unambiguous and provided through a clear affirmative act. 1. **Clarity on Consent**:[1] By explicitly stating that consent must be "freely[2] and actively given," we ensure that Data Principals understand their rights regarding personal data processing. This change helps mitigate risks associated with coercive or misleading consent practices. 2. **Alignment with Global Standards**: Incorporating terminology from GDPR enhances consistency with global data protection norms. This alignment is crucial for organizations operating

[1] https://gdpr-info.eu/recitals/no-32/
[2] https://gdpr-info.eu/recitals/no-43/

		internationally, facilitating smoother compliance across jurisdictions. 3. **Empowerment of Data Principals**: The revised language empowers Data Principals by ensuring they are fully informed about their rights and the implications of their consent. Clear communication fosters trust between individuals and data fiduciaries. 4. **Affirmative Action Requirement**: Specifying that consent must be given through affirmative action reinforces the need for explicit agreement rather than passive acceptance. This can help prevent issues related to implied consent or pre-checked boxes that may not reflect genuine user intent. - **Standardized Notice Templates**: Develop government-approved templates that sector-specific organizations can use to ensure consistency and clarity in communication. These templates should include mandatory readability scores (e.g., ≤8th-grade level) to promote understanding among users. - **Accessibility Compliance**: Mandate compliance with WCAG 2.1 AA standards for digital notices, ensuring that they are accessible to individuals with disabilities. Additionally, consider introducing audio or video formats of notices for low-literacy populations or those with visual impairments. - **User Engagement Strategies**: Implement visual or gamified consent interfaces on digital

		platforms to enhance user engagement and understanding of their rights regarding personal data processing.
4.	**Registration and obligations of Consent Manager** This rule establishes a framework for consent managers but lacks detailed technical specifications regarding their operations and responsibilities. There is no liability framework in place for consent managers in case of failures or breaches, nor are there adequate grievance redressal mechanisms for users affected by such failures.	- **Technical Specifications**: Publish detailed technical guidelines outlining the required infrastructure and security measures for consent managers, ensuring they adhere to best practices in data protection. - **Liability Framework**: Introduce a liability framework requiring consent managers to maintain a minimum insurance coverage (e.g., ₹50 lakh) to compensate users in case of consent-related failures or breaches. - **Grievance Redressal Mechanism**: Establish a clear grievance redressal process with a mandated resolution timeframe (e.g., 72 hours) for user complaints related to consent management failures, ensuring accountability and user trust.
5.	**Processing for provision or issue of subsidy, benefit, service, certificate, licence or permit by State and its instrumentalities-** This rule allows state entities to process personal data under the guise of providing benefits or services without clearly defined boundaries around what constitutes "public order." The broad interpretation of this term raises concerns about potential misuse and overreach into citizens' privacy rights. Furthermore, there are no sunset clauses for data retention in welfare schemes, which	-**Definition of instrumentality:** The term "instrumentality" is not defined within the Rules or the Act, leading to potential ambiguity and disputes regarding its interpretation. This broad terminology may result in excessive data processing authority being granted to various entities without clear boundaries. Additionally, while the standards outlined in the Second Schedule appear substantive, there is a lack of specific techno-legal procedures for their implementation. This absence creates uncertainty regarding how these safeguards will be enforced effectively. Furthermore, the rule does not adequately address concerns related to

	could lead to unnecessary data accumulation over time. Rule 5 states that the State and any of its instrumentalities may process the personal data of a Data Principal under clause (b) of section 7 of the Act to provide or issue any subsidy, benefit, service, certificate, licence, or permit that is provided or issued under law or policy or using public funds. This processing must conform to the standards specified in the Second Schedule, which includes safeguards such as purpose limitation, storage limitation, data security measures, and access channels for Data Principals to exercise their rights.	national security exemptions and their potential for misuse. Defining "instrumentality" explicitly or using a more precise term like "State as per Article 12" will eliminate ambiguity and ensure that only authorized entities are permitted to process personal data. This change will help prevent misuse of data processing powers by entities that may not have been intended to have such authority. **- Create a detailed list of permissible uses under "public order,":** specifying at least 53 scenarios where state processing is justified (e.g., disaster response, public health emergencies). This will provide clarity on when state entities can process personal data without infringing on individual rights. The revised language should also incorporate provisions that explicitly outline how national security-related exemptions can be invoked while ensuring that such exemptions are not misused. This will help maintain a balance between legitimate state interests and individual privacy rights. **- Data Retention Policies**: Implement mandatory sunset clauses that require automatic data deletion after five years unless explicitly authorized by law. This measure will minimize unnecessary data retention and enhance citizens' privacy rights by ensuring that personal data is not held indefinitely without justification. **- Public Accountability Measures**: Establish a public dashboard that tracks government data processing activities related to welfare schemes. This initiative will enhance transparency and

		public trust in state actions regarding personal data usage, allowing citizens to understand how their data is being handled and processed. By requiring a defined procedural framework for implementing safeguards, stakeholders can better understand their obligations and responsibilities. This transparency fosters accountability among state entities and builds public trust in how personal data is handled.
6.	**Reasonable security safeguards-** Rule 6 outlines the requirement for data fiduciaries to implement reasonable security safeguards for protecting personal data. However, its lack of specificity regarding several critical aspects limits the rule's effectiveness. These include the prioritization of breach types, clear technical and organizational standards, and the implementation of regular security audits. This rule requires data fiduciaries to implement security measures such as encryption and access controls but cites outdated encryption standards (e.g., AES-128). The phrase "appropriate measures" lacks specificity, leading to varying interpretations of what constitutes adequate security protocols across different organizations. Additionally, the one-year log retention period may be insufficient for forensic investigations in certain sectors like finance or healthcare.	- **Lack of breach prioritization:** Establish a classification system for data breaches (minor, moderate, serious) based on volume and sensitivity of affected data. This will help organizations prioritize response efforts effectively. - **Absence of specific security standards:** Mandate adoption of advanced encryption standards (e.g., AES-256) by 2027 and align with recognized frameworks like NIST CSF 2.0 or ISO/IEC 27001. This provides clear guidelines for organizations to follow. - **Insufficient log retention:** Extend log retention periods to three years for critical infrastructure sectors (e.g., banking, healthcare) to facilitate thorough forensic investigations when breaches occur. - **No mandatory security audits:** Require annual security audits by certified firms to assess compliance with established security standards and identify potential vulnerabilities.
7.	**Intimation of personal data breach-**	- **Inconsistent Reporting Timelines:** The current 72-hour reporting timeline in Rule 7

	This rule mandates that data fiduciaries notify affected individuals and the Data Protection Board (DPB) within 72 hours of becoming aware of a breach. However, this timeframe may be impractical for complex breaches requiring extensive investigation before accurate reporting can occur. Additionally, there is no classification system for breach severity, which could lead to inconsistent responses based on the impact of the breach on affected individuals.	conflicts with the 6-hour reporting requirement for cyber incidents under Section 70B(6) of the IT Act. Reconcile this discrepancy by amending Rule 7 to mandate reporting data breaches to the Board within 6 hours, aligning with the CERT-In reporting timeline. This will eliminate confusion and ensure quicker notification during incidents. **- Unspecified Data Principal Notification Timeline:** Rule 7 does not specify when affected Data Principals must be informed about a breach, potentially causing delays in individuals taking protective measures. Require notification to affected Data Principals "without undue delay, but in any event, no later than 24 hours" after determining the breach. This ensures individuals are promptly informed to mitigate potential harm. **- No Breach Severity Classification:** The absence of a system to categorize data breaches hinders appropriate response efforts, as all breaches are treated the same regardless of their severity. Introduce a tiered breach classification system (critical, major, minor) based on factors like data volume and sensitivity. This enables tailored responses, with shorter notification timelines and more intensive measures for severe breaches. **- Lack of Independent Audits:** The rules lack a mechanism to verify that organizations are adhering to breach notification procedures and maintaining adequate data security practices. Mandate annual independent audits

		by certified firms to assess compliance with breach notification procedures and overall data security practices. This provides an objective evaluation of security measures. **- Absence of Penalties for Delayed Reporting:** Rule 7 does not include penalties for delayed reporting beyond the established timelines, reducing the incentive for timely compliance. Implement penalties for delayed reporting beyond the established timelines, with fines escalating based on the severity of the delay and the organization's size. This reinforces the importance of prompt notification. **- No Public Disclosure Provision:** The absence of a requirement for public disclosure of large-scale breaches limits transparency and accountability, preventing the public from being informed about significant security incidents. Add a provision for public disclosure of large-scale breaches affecting 100,000+ users, providing details about the breach, mitigation efforts, and steps to prevent recurrence. **- Inadequate Victim Support**: There is no provision for direct assistance to individuals affected by data breaches, leaving them to manage potential fallout (e.g., identity theft) without organizational support. Establish a Breach Response Fund, allocating 0.5% of corporate turnover to support victims by providing credit monitoring, identity theft protection, and other necessary services.

		- Lack of Preparedness: Many organizations lack adequate preparation for data breaches, resulting in delayed and ineffective responses. Require large organizations (₹500 crore+ turnover) to conduct regular breach simulation drills, enabling them to test incident response plans, train personnel, and identify vulnerabilities proactively.
8.	**Time period for specified purpose to be deemed as no longer being served-** Rule 8 addresses data retention and erasure, stating that Data Fiduciaries processing personal data for purposes specified in the Third Schedule must erase such data if the Data Principal neither approaches the Fiduciary for the specified purpose nor exercises their rights in relation to such processing for the time period specified in the schedule. The rule also requires Data Fiduciaries to inform Data Principals at least forty-eight hours before data erasure, allowing them to prevent deletion by logging into their user account or contacting the Fiduciary.	**- Lack of Sector-Specific Inactivity Parameters**: The rule's one-size-fits-all approach may lead to inappropriate data handling as sectors differ in user engagement patterns. Define inactivity metrics tailored to specific sectors (e.g., fintech—3 years, healthcare—10 years, social media—1 year) to align data retention with industry-specific needs and user expectations. **- No Data Hibernation Protocol**: Users may be caught off guard by data deletion, leading to unintended loss of valuable information. Implement a mandatory "data hibernation" period (e.g., 90 days) during which users are notified before permanent account deletion, providing an opportunity to retain their data. **- Absence of Public Interest Exemptions**: Strict data erasure could hinder valuable research or historical preservation. Create exceptions allowing specific historical or research-related data (e.g., medical archives) to be retained under ethical guidelines, balancing privacy with societal benefits.

		- Limited User Control: The rule does not provide users with immediate control over their data's deletion; they must wait for the pre-set inactivity period to expire. Introduce a "Right to Be Forgotten," enabling users to request data deletion at any time, enhancing their autonomy and control over personal information. **- Potential for Unnecessary Data Hoarding**: Fixed retention periods may incentivize businesses to retain data longer than necessary, increasing privacy risks. Instead of fixed retention periods, businesses should justify why they need to retain data, and This prevents unnecessary data hoarding. **- Risk of Misuse of Research & Public Interest Exceptions**: Allowing data retention for research and public interest purposes could be misused to retain personally identifiable information longer than needed. Allow Data Retention for Research & Public Interest, but with Safeguards, which should not be misused to retain personally identifiable information longer than needed. **- Inadequate User Notifications**: Notifications before data erasure may not be clear or understandable, potentially leading to unintentional data loss. Strengthen Notifications Before Data Erasure, Users should get clear, easy-to-understand notifications explaining why their data is being deleted and what they can do if they want to keep it. **- Risk of Unauthorized Data Recovery**: Lack of standardized data deletion processes may

		leave data vulnerable to unauthorized recovery. Define a Standardized & Secure Deletion Process, and Companies should also keep a log of deletion activities. **- Narrow Definition of User Account**: The current definition may not encompass evolving digital identities, such as cloud storage accounts or AI-based profiles. Expand the Definition of "User Account," digital identities are evolving, and the law should recognize things like cloud storage accounts, digital wallets, and AI-based profiles. **- Lack of Transparency**: Users may not be aware of how long their data will be kept or when it will be deleted. Require Businesses to Publish Clear Data Retention Policies, Users should be able to easily access and understand how long their data will be kept and when it will be deleted.
9.	**Contact information of person to answer questions about processing-** Rule 9 requires Data Fiduciaries to prominently publish contact information for a Data Protection Officer (DPO), if applicable, or a designated person to answer questions about personal data processing. This rule requires organizations to display contact details for their Data Protection Officer (DPO); however, it does not set qualification standards or response timelines for user inquiries about personal data rights.	**- Subjective Interpretation of "Prominently Publish":** The term lacks specific guidelines, leading to varying interpretations regarding visibility and accessibility. Define "prominently publish" with clear requirements for font size, placement on websites/apps, and accessibility standards to ensure Data Principals can easily find contact information. **- Vague Definition of "Business Contact Information":** The rule does not clarify which specific contact details must be provided, potentially leading to insufficient communication channels. Specify mandatory

		contact information, including at least one direct email address and phone number, to facilitate effective communication. **- Ambiguity Regarding DPO Appointment:** The phrase "if applicable" creates uncertainty about when a DPO is required, leading to inconsistencies in compliance. Clarify the conditions under which a DPO must be appointed based on organizational size or data processing volume, ensuring accountability. **- Lack of Qualification Standards for DPOs:** Without specified qualifications or certifications, underqualified individuals may handle crucial data protection responsibilities. Mandate DPO Certification Standards requiring recognized certifications (e.g., IAPP/CIPP) to ensure adequate knowledge of data protection laws and practices. **- Absence of Response Timelines:** There are no mandated timelines for acknowledging or resolving user inquiries related to their rights or data processing, potentially causing delays and frustration. Implement Service Level Agreements (SLAs) mandating acknowledgment of inquiries within 48 hours and resolution within 30 days to enhance user confidence in organizational accountability. **- Limited Transparency on DPO Performance:** There is no mechanism for Data Principals to assess the effectiveness or responsiveness of DPOs. Create a Centralized DPO Registry with Performance Metrics that

		includes performance metrics regarding query handling effectiveness, promoting transparency and allowing users to gauge DPO responsiveness. **- Unclear Scope of Contact Person's Role:** The responsibilities of the designated contact person are not clearly defined, leading to inconsistent practices across organizations. Clarify that the designated contact person is responsible for providing substantive responses and has the authority to resolve data protection inquiries effectively. **- Lack of Clarity on Exercising Data Principal Rights:** The rules do not specify how users can exercise their rights (e.g., access, correction) or what identification is required. Provide clear mechanisms for exercising these rights, including any necessary identification details such as usernames or user IDs. **- No Grievance Redressal Mechanism Timeline:** The absence of specified timelines for addressing grievances related to data processing can lead to delays. Establish timelines for resolving grievances similar to those in other regulatory frameworks (e.g., Consumer Protection Act), ensuring timely responses.
10.	**Verifiable consent for processing of personal data of child or of person with disability who has lawful guardian-** Rule 10 outlines the requirements for obtaining verifiable consent from a parent before processing a child's personal data and	**- Limited Accessibility of Age Verification**: Over-reliance on DigiLocker excludes individuals without access to digital resources, especially in rural areas. Enhance Age Verification Mechanisms, Integrate Aadhaar-based offline verification options through

	emphasizes due diligence in confirming the adult identity of the parent. It references the use of reliable identity details or a virtual token verified by a Digital Locker service provider.	Common Service Centers (CSCs) in rural areas where DigiLocker access is limited, ensuring inclusivity while verifying age accurately. **- Lack of Protection Against Behavioral Profiling**: The rule does not explicitly prohibit behavioral profiling and targeted advertising toward minors. Ban Behavioral Profiling of Minors, prohibit all forms of targeted advertising directed at individuals under the age of 18 to protect children from exploitation through manipulative marketing practices. **- Weak Age-Gating Mechanisms**: The rule does not mandate robust mechanisms to prevent minors from circumventing age restrictions. Mandate Robust Age-Gating Mechanisms, require platforms targeting minors to implement age-gating mechanisms with liveness detection features ensuring proper verification before granting access to enhance safeguards against unauthorized access. **- Absence of an Internet-Wide Age-Gating Mechanism**: There is no universal system to prevent minors from bypassing age limits by misrepresenting their age. Implement a graded consent model, distinguishing between younger children (below 13) who need parental approval and teenagers (13–18) who can provide consent with parental notification instead of strict verification. **- Lack of Clarity on VPC Method**: There is unclarity as to what the method for "verifiable parent consent" would be. For example, would it be Aadhar-based verification, digital

		signatures, or other government based credentials. This lack of clarity can lead to inconsistent implementation and potential security vulnerabilities. **- Ambiguity in Parentage Verification Obligation**: Data Fiduciaries may not be explicitly required to verify actual parentage, creating a legal gray area for potential misrepresentation. The rule should explicitly state whether data fiduciaries must verify actual parentage or merely confirm that the individual claiming to be a parent is an adult. **- Discrepancy in Standards for Parents and Guardians**: There is an unequal burden of compliance, requiring lawful guardians of persons with disabilities to provide official proof of appointment, while parents of children need only verify adulthood. Ensure Parity in Verification Standards for Parents and Guardians should not be disproportionately stringent compared to parental verification for children. - Instead of requiring verifiable parental consent (VPC) through government credentials, the rule should allow alternative verification methods which do not mandate government ID linking to address privacy concerns. - To prevent data over-collection and prolonged storage, the rule must specify a clear retention limit for verification data, ensuring that platforms do not store parental credentials indefinitely.

		- The rule should shift towards platform accountability rather than individual user verification, mandating that companies provide age-appropriate content filtering and default safety settings instead of blanket age-gating, to prevent government identification.
11.	**Exemptions from certain obligations applicable to processing of personal data-** Rule 11 exempts specific classes of Data Fiduciaries (Part A of Fourth Schedule) and processing purposes (Part B of Fourth Schedule) from certain obligations related to child data processing, subject to conditions specified in the Schedule.	**- Undefined Data Fiduciary Qualifications**: Lack of clear definitions of which data fiduciaries qualify for exemptions, leading to potential misuse by commercial platforms. Explicitly specify which categories of entities qualify for exemptions, such as non-commercial educational institutions, healthcare services, and child welfare organizations, excluding commercial platforms like social media and gaming companies that collect data for profit. **- Potential for Commercial Exploitation**: Exempted platforms may engage in aggressive data collection and profiling under the guise of child-friendly services. Even for exempted platforms, the rule should prohibit behavioral profiling, targeted advertising, and unnecessary data collection. It should also require platforms to process only essential data strictly for child-centric purposes, preventing misuse under the pretext of providing "child-friendly" services. **- Lack of Oversight and Reporting**: There are no reporting or audit requirements for data fiduciaries using these exemptions, preventing independent oversight of their data processing practices. Data fiduciaries using exemptions must be required to submit periodic reports to an independent regulatory body, detailing the

		purpose, scope, and duration of child data processing. Random audits should also be conducted to ensure compliance. **- Absence of Additional Safeguards**: The Rule relaxes data processing restrictions without imposing additional safeguards, creating risks for children's data. Even under exemptions, platforms should be bound by purpose limitation (data should only be used for a clearly defined and lawful purpose), automatic deletion after a reasonable period, and mandatory parental/guardian oversight. **- Broad Definition of "Educational Activities"**: This term's lack of clarity allows platforms to justify behavioral tracking, targeted advertising, or unnecessary data collection under the pretext of education. Define “Educational Activities” to Prevent Misuse, The rule should clearly specify that educational activities do not include behavioral tracking, marketing, or any data collection beyond what is strictly necessary for learning purposes. **- Potential Misuse of Safety Monitoring Provisions**: The rule allows individuals responsible for child care to process data for safety monitoring but does not establish strict limitations. Restrict Safety Monitoring to Essential Use Cases, the rule should impose strict necessity and proportionality requirements on safety monitoring, ensuring that data collection is justified and limited to legitimate child protection purposes. Additional oversight mechanisms should be introduced to prevent the

		misuse of exemptions for unnecessary surveillance.
12.	**Additional obligations of Significant Data Fiduciary-** Rule 12 outlines additional obligations for Significant Data Fiduciaries (SDFs), including conducting annual Data Protection Impact Assessments (DPIAs) and audits, verifying algorithmic software, and ensuring restricted data remains within India.	**- Lack of Specific DPIA Standards:** The rule doesn't provide detailed guidance on how DPIAs should be conducted, potentially leading to inconsistent assessments. *Establish Specific DPIA Standards:* Mandate the use of a standardized DPIA framework aligned with international best practices, outlining assessment criteria, documentation requirements, and reporting templates. **- Unclear Algorithmic Verification Process:** The "due diligence" requirement for algorithmic software lacks specifics, making it difficult to ensure effective risk mitigation. *Define Algorithmic Verification Process:* Provide a clear process for verifying algorithmic software, including regular bias audits, transparency reports, and mechanisms for addressing discriminatory outcomes. **- Limited Guidance on Data Localization:** The rule allows the government to specify data that must remain in India but lacks transparency on the decision-making process. *Establish Transparent Data Localization Criteria:* Clearly define the criteria used to determine which data categories require localization, ensuring decisions are based on legitimate national security or public interest concerns. **- Lack of Independent Oversight of DPIA Reports:** While SDFs must submit DPIA reports to the Board, there's no mechanism for

		independent verification of their findings. *Implement Independent Review of DPIA Reports:* Establish a process for independent experts to review DPIA reports submitted by SDFs, ensuring thoroughness and objectivity in their assessments. **- No Requirement for Public Summary of DPIA Findings:** The lack of transparency around DPIA findings hinders public accountability and understanding of data protection risks. *Require Publication of DPIA Summary Reports:* Mandate SDFs to publish anonymized summary reports of their DPIA findings, promoting transparency and building public trust. **- Absence of Specific Penalties for Non-Compliance:** The rule lacks specific penalties for failure to meet the additional obligations, potentially reducing incentives for SDFs to comply fully. *Introduce Specific Penalties for Non-Compliance:* Establish tiered penalties for non-compliance with Rule 12, commensurate with the severity of the violation, to ensure accountability and deter negligent practices.
13.	**Rights of Data Principals-** Rule 13 outlines how Data Fiduciaries and Consent Managers should enable Data Principals to exercise their rights under the Act, including providing details on request mechanisms, required identifiers, grievance redressal periods, and nomination processes.	**- Lack of Specificity on "Enabling" Data Principal Rights:** The term "enabling" is vague, leading to inconsistent implementation. Clearly define "enabling" to mean providing active assistance and clear instructions, not just information, to Data Principals exercising their rights. **- Absence of Maximum Timeframe for Grievance Redressal:** Allowing Data

		Fiduciaries to determine their grievance redressal period can lead to delays. Establish a maximum timeframe (e.g., 30 days, aligning with GDPR) for resolving grievances, ensuring timely responses to Data Principals' complaints. **- Discretionary Terms for Nomination Process:** Allowing Data Fiduciaries to set the terms for nomination can result in overly restrictive conditions. Standardize the nomination process, setting clear and reasonable criteria, and preventing Data Fiduciaries from imposing burdensome requirements. **- Unclear Scope of Required Identifiers:** The rule does not specify what types of identifiers can be requested, potentially leading to excessive data collection. Limit the types of identifiers that can be requested to only what is strictly necessary for verification, minimizing privacy risks. **- Possibility of Denying Data Principal Requests:** The wording "request to exercise such rights" implies that Data Fiduciaries can deny requests. Clarify that Data Fiduciaries must generally comply with Data Principal requests, with clearly defined and limited exceptions (e.g., legal obligations, fraudulent requests). **- Ambiguity Regarding Consent Manager Applicability**: The phrase “where applicable” makes the role and accountability of Consent Managers unclear. It should clearly define where the consent managers will be applicable

		- Rule Does Not Clearly Define Data Principal Rights: With the heading of Rights of data subjects – the rule simply states the obligations that a data controller is to adhere, in order to facilitate exercise of such rights – but does not materialise such rights in text. **- Lack of clarity on alternative proof of identity** Whether in Rule 13 (1)(b) an alternative proof of identity (like email or Aadhaar) can be used **- Lacks grounds on rejecting the request** Rule 13(2) states that a DP can make a request for data access or erasure, but it does not specify: Whether the DF can reject a request and what are the grounds ? **- Lacks clarity on nomination** Rule 13(4) allows Data Principals to nominate someone else to act on their behalf but does not explain: o Whether proof of consent is required for nomination? o Whether nominations can be challenged or revoked? o How the nominee's rights compare to those of the Data Principal? **- Lacks third party involvement** Rule 13(3) states that the DF must publish the grievance redressal period, but does not specify: o What happens if the grievance is not resolved within that period? o Whether a third-party authority (like the Data Protection Board) must be notified?

14.	**Processing of personal data outside India-** Rule 14 addresses the transfer of personal data outside India by Data Fiduciaries, subjecting such transfers to requirements specified by the Central Government regarding availability of data to foreign states or entities under their control.	**- Lack of Transparency in Government Requirements**: The absence of clear, publicly available criteria for Central Government's requirements creates uncertainty and potential for arbitrary restrictions. *Establish Transparent Criteria for Data Transfer Requirements:* Mandate the Central Government to publish clear, specific, and publicly accessible criteria for specifying requirements related to cross-border data transfers, based on considerations like national security, data protection standards, and international agreements. **- Potential for Overly Broad Restrictions**: The rule's wording could allow for overly broad restrictions on data transfers, hindering legitimate business operations and international collaborations. *Implement a Risk-Based Approach to Data Transfer Restrictions:* Adopt a risk-based approach that differentiates restrictions based on the sensitivity of the data, the destination country's data protection laws, and the purpose of the transfer, ensuring that restrictions are proportionate to the identified risks. **- Absence of Due Process and Appeal Mechanisms**: The rule lacks provisions for Data Fiduciaries to seek clarification, challenge requirements, or appeal decisions related to data transfer restrictions. *Establish Due Process and Appeal Mechanisms:* Create a formal process for Data Fiduciaries to seek clarification on requirements, challenge decisions, and appeal

		restrictions, ensuring fairness and transparency in enforcement. **- Limited Consideration of International Data Protection Standards**: The rule does not explicitly reference or consider international data protection standards or agreements, potentially leading to inconsistencies and compliance challenges. *Align with International Data Protection Standards:* Ensure that requirements for cross-border data transfers align with internationally recognized data protection standards (e.g., GDPR adequacy decisions, APEC CBPR) to promote interoperability and reduce compliance burdens. **- No Guidance on Data Localization Requirements**: The rule focuses on restrictions but provides no guidance on situations where data localization (requiring data to be stored within India) might be mandated. *Develop a Clear Data Localization Framework:* Establish a transparent framework outlining specific circumstances under which data localization may be required, based on well-defined criteria such as national security or critical infrastructure protection. **- Lack of Periodic Review Mechanism**: There is no mechanism for regular review and updating of the specified requirements, potentially leading to outdated or ineffective restrictions. *Implement a Periodic Review Mechanism:* Mandate regular review (e.g., annually) of the requirements by an independent body, taking into account evolving technological

		landscapes, international agreements, and stakeholder feedback.
15.	**Exemption from Act for research, archiving or statistical purposes-** Rule 15 exempts the processing of personal data necessary for research, archiving, or statistical purposes from the provisions of the Act, provided that it is carried out in accordance with the standards specified in the Second Schedule.	**- Lack of Definition for Key Terms**: The terms "research," "archiving," and "statistical purposes" are undefined, leading to potential misuse and overbroad application of the exemption. Define "research," "archiving," and "statistical purposes" with specific criteria and examples, distinguishing between commercial and non-commercial activities and ensuring that the exemption is limited to legitimate and ethical uses. **- Vague "Reasonable Efforts" Standard**: The term "reasonable efforts" in clause (d) of Schedule II is too vague, making it difficult to enforce data protection standards effectively. Replace "reasonable efforts" with specific, measurable requirements for anonymization, de-identification, and data security, ensuring consistent and enforceable standards. **- Potential for Commercial Exploitation**: The exemption could be exploited by commercial entities to collect and process personal data under the guise of research or statistical purposes. Exclude commercial platforms from utilizing such data **- Lack of Transparency and Oversight**: There are no specific requirements for transparency or independent oversight of research, archiving, or statistical activities, hindering accountability and public trust. Require Data Fiduciaries claiming the exemption to publish details of their research, archiving, or statistical activities,

		including purpose, scope, data sources, and safeguards implemented to protect personal data. **- Limited Consideration of Ethical Concerns**: The rule does not explicitly address ethical considerations related to research, archiving, or statistical purposes, potentially leading to unethical data processing practices. Incorporate ethical principles (e.g., respect for autonomy, beneficence, non-maleficence, justice) into the Second Schedule, requiring Data Fiduciaries to demonstrate adherence to ethical standards in their research, archiving, or statistical activities. **- Inadequate Safeguards for Sensitive Data**: The rule does not provide specific safeguards for processing sensitive personal data (e.g., health data, financial data) for research, archiving, or statistical purposes. Impose stricter safeguards for processing sensitive personal data, including explicit consent requirements, enhanced security measures, and restrictions on data sharing. **- Risk of Re-Identification**: The rule does not adequately address the risk of re-identification of individuals from anonymized or pseudonymized data used for research, archiving, or statistical purposes. Require Data Fiduciaries to implement state-of-the-art techniques to minimize the risk of re-identification, regularly assess the effectiveness of these techniques, and establish protocols for responding to re-identification incidents.

		- Lack of Clarity on Retention Periods: The rule does not specify how long personal data can be retained for research, archiving, or statistical purposes, leading to potential data hoarding. Establish clear data retention limits for research, archiving, and statistical purposes, balancing the needs of these activities with the data minimization principle.
16.	**Appointment of Chairperson and other Members-** Rule 16 outlines the process for appointing the Chairperson and Members of the Data Protection Board of India (DPBI) through Search-cum-Selection Committees primarily composed of government officials.	**- Lack of Board Independence**: Heavy reliance on government officials in the appointment process threatens the Board's independence. Reconstitute the Search-cum-Selection Committees to include a retired Supreme Court/High Court judge as Chairperson, representatives from academia and the private sector, and independent experts with relevant experience. **- Vague Definition of "Experts of Repute"**: The phrase is too broad, lacking clarity regarding required qualifications, which creates room for arbitrary selections. Define "experts of repute" with specific criteria, such as a minimum of 15 years of experience in technology law, competition law, or arbitration. **- Potential for Political Influence**: The structure allows for political influence, undermining the DPBI's credibility and impartiality. Introduce a transparent and competitive evaluation process for selecting independent experts, ensuring that appointments are based on merit and expertise. **- Lack of Transparency and Public Consultation**: There is no public consultation or

		involvement of external stakeholders. Incorporate a public consultation process, seeking input from stakeholders on the qualifications and selection of board members. **- Potential Conflicts of Interest**: There is no consideration of potential conflicts of interest among committee or board members. Establish clear guidelines to identify and address potential conflicts of interest, ensuring objectivity and impartiality in decision-making. **- Absence of Appointment Timelines**: The rule does not specify timelines for the appointment process, potentially causing delays. Set specific timelines for each stage of the appointment process, from constituting the Search-cum-Selection Committee to finalizing the appointments. **- Lack of Checks and Balances**: There is no provision for reviewing or challenging appointments made by the Central Government. Introduce a review mechanism, allowing for challenges to appointments based on defined criteria (e.g., lack of qualifications, conflicts of interest). **- Independent Expert Selection Criterion** The independent experts shall be selected based on voting and competitive evaluation in order to have qualified people be a part of the Committee
17.	**Salary, allowances and other terms and conditions of service of Chairperson and other Members-** Rule 17 stipulates that the Chairperson and Members of the Data Protection Board of	**- Lack of Transparency in Determining Remuneration**: The process for determining the salary, allowances, and other terms and conditions in the Fifth Schedule may lack transparency, potentially leading to public

	India shall receive salary, allowances, and other terms and conditions of service as specified in the Fifth Schedule.	concerns about fairness and equity. *Establish a Transparent Remuneration Framework:* Mandate that the determination of salary, allowances, and other terms and conditions of service for the Chairperson and Members be based on a transparent framework, taking into consideration factors such as the scope of responsibilities, qualifications, experience, and prevailing compensation standards for similar positions in other regulatory bodies or the private sector. **- Risk of Inadequate Compensation**: Insufficient remuneration may discourage qualified individuals from seeking positions on the Data Protection Board, hindering the Board's effectiveness. *Ensure Competitive Compensation:* Regularly review and adjust the compensation package to ensure that it is competitive and sufficient to attract highly qualified candidates with diverse expertise in data protection, technology law, and related fields. **- Potential Conflicts of Interest**: The absence of clear guidelines regarding potential conflicts of interest related to the financial interests of Board members may compromise their impartiality. *Implement Conflict of Interest Guidelines:* Develop and implement comprehensive conflict of interest guidelines that require Board members to disclose any financial interests or affiliations that may create a conflict of interest and establish procedures for

		recusal from decisions where such conflicts exist. **- Lack of Independence in Setting Terms of Service**: Government control over setting the terms of service may compromise the Board's independence and autonomy. *Establish an Independent Committee for Reviewing Terms of Service:* Create an independent committee, comprising representatives from relevant stakeholder groups (e.g., legal experts, academics, civil society organizations), to periodically review and make recommendations regarding the salary, allowances, and other terms and conditions of service for Board members. **- Absence of Performance-Based Incentives**: The lack of performance-based incentives may reduce accountability and motivation among Board members to effectively fulfill their responsibilities. *Introduce Performance-Based Incentives:* Consider incorporating performance-based incentives into the compensation structure, rewarding Board members for achieving specific objectives related to data protection enforcement, public awareness, and stakeholder engagement. **- Limited Public Disclosure of Remuneration Details**: Lack of transparency regarding the remuneration details of Board members may hinder public trust and accountability. *Mandate Public Disclosure of Remuneration Details:* Require the public disclosure of the salary, allowances, and other terms and conditions of service for the Chairperson and

		Members of the Data Protection Board, ensuring transparency and promoting public trust. By implementing these changes, Rule 17 will
18.	**Procedure for meetings of Board and authentication of its orders, directions and instruments-** Rule 18 outlines the procedures for Board meetings, decision-making processes, and authentication of orders. It covers aspects such as meeting arrangements, quorum, voting, conflict of interest, emergency decision-making, and inquiry timelines.	**- Insufficient Conflict of Interest Provisions**: The rule lacks clarity on what constitutes a conflict and fails to prescribe enforcement mechanisms. Define conflict of interest broadly, covering financial, professional, and familial interests. Mandate prior written disclosure of conflicts and prescribe penalties for non-disclosure, including potential removal from office. **- Vague Emergency Decision-Making Criteria**: The provision for emergency decisions lacks specific criteria for "emergent situations". Define emergencies narrowly, limiting them to situations posing immediate legal or operational risks. Require detailed documentation of reasons and make emergency decisions subject to mandatory ratification within a stipulated timeframe. **- Uncapped Inquiry Timelines**: The lack of a final cap on inquiry duration risks delays and administrative inefficiencies. Cap total inquiry duration at twelve months, including all extensions. Require written justification for extensions and implement oversight for cases exceeding the timeline. **- Lack of Transparency in Decision-Making**: The rule doesn't mandate public disclosure of Board decisions. Require publication of anonymized summaries of Board decisions to enhance transparency and accountability.

		- Insufficient Quorum Requirements: One-third membership quorum may be inadequate for critical decisions. Increase the quorum requirement to half of the Board membership for decisions on significant matters.
19.	**Functioning of Board as digital office-** Rule 19 mandates that the Board function as a digital office, adopting techno-legal measures to conduct proceedings without requiring physical presence, while retaining the power to summon and examine individuals under oath.	**- Exclusive Reliance on Digital Means**: The rule may alienate individuals lacking digital literacy or access. Implement a hybrid approach allowing both digital and physical participation in proceedings to ensure inclusivity and accommodate varying levels of technological access. **- Lack of Provisions for Essential In-Person Interactions**: The rule doesn't address situations where physical presence is necessary for certain proceedings or testimonies. Create guidelines for determining when in-person interactions are essential, such as complex hearings or witness examinations, and provide mechanisms for these instances. **- Potential Procedural Difficulties in Digital Transition**: The rule doesn't address potential procedural challenges arising from a complete digital transition. Develop clear guidelines outlining how procedural flexibility will be maintained in a digital environment, ensuring rights protection amid technological transitions. **- Absence of Digital Literacy Support**: The rule assumes digital competence without providing support for those who may struggle with digital processes. Establish digital literacy programs for stakeholders to ensure effective

		engagement with digital processes, and provide technical assistance during proceedings. **- Lack of Fallback Mechanisms**: The rule doesn't account for potential digital system failures or inaccessibility. Create fallback procedures for instances where digital systems fail, maintaining traditional methods alongside digital ones during the transition phase.
20.	**Terms and conditions of appointment and service of officers and employees of Board-** Rule 20 allows the Board to appoint officers and employees with prior approval from the Central Government. The terms and conditions of service are specified in the Sixth Schedule.	**- Potential Delays Due to Central Government Approval**: The requirement for prior approval may lead to operational inefficiencies. Implement a streamlined approval process with defined timelines for government responses to avoid unnecessary delays in appointments. **- Risk of Government Interference**: Central Government's influence on appointments may compromise the Board's impartiality. Establish an independent oversight committee to review government requests for data and appointments within the Board, ensuring transparency and accountability. **- Lack of Transparency in Appointment Process**: The current rule doesn't mandate disclosure of appointment reasons or selection processes. Require public disclosure of appointment reasons and selection processes on the Board's official website to enhance transparency. **- Absence of Internal Grievance Mechanism**: The rule lacks provisions for addressing grievances of Board officers and employees. Establish an internal mechanism for addressing

		grievances of officers and employees in a time-bound manner. **- Vague Language in Appointment Criteria**: The phrase "as may be deemed necessary" provides broad discretion without clear guidelines. Define specific criteria and qualifications for appointments to ensure consistency and prevent arbitrary decisions.
21.	**Appeal to Appellate Tribunal-** Rule 21 outlines the procedure for filing appeals to the Appellate Tribunal, including digital filing, fee payment, and procedural guidelines.	**- Excessive Appeal Fees**: The rule links appeal fees to the Telecom Regulatory Authority of India Act, potentially imposing excessive fees (Rs. 10,000) that impede access to justice. Govern appeal fees under a separate rule (or amend the Rules, 2003) to reduce fees for appeals preferred under Section 29 of the DPDP Act, making the appeal process more accessible. **- Lack of Clarity on Fee Waiver**: The rule allows fee reduction or waiver at the Chairperson's discretion, but lacks clear criteria. Establish transparent criteria for fee reduction or waiver based on factors like financial hardship, public interest, or the complexity of the case, ensuring fairness and consistency in decisions. **- Potential Digital Divide**: Requiring digital filing and payment may disadvantage individuals lacking digital literacy or access. Provide alternative filing and payment options (e.g., physical filing, postal payment) to ensure inclusivity and accommodate individuals with limited digital access. **- Absence of Standardized Appeal Format**: The rule doesn't specify a standardized format for appeals, potentially leading to

		inconsistencies and delays. Develop a standardized appeal format with clear instructions on required information, making it easier for appellants to file complete and well-organized appeals. **- Limited Guidance on Tribunal Procedures**: While the rule allows the Tribunal to regulate its procedure, it lacks guidance on key aspects like evidence admissibility and hearing protocols. Develop detailed procedural guidelines for the Appellate Tribunal, addressing evidence admissibility, hearing protocols, and other relevant aspects to ensure fairness and consistency in proceedings. **- No Provision for Legal Aid**: The rule doesn't address the availability of legal aid for indigent appellants. Explore options for providing legal aid to appellants who cannot afford legal representation, ensuring equal access to justice.
22.	**Calling for information from Data Fiduciary or intermediary-** Rule 22 allows the Central Government, through authorized persons specified in the Seventh Schedule, to require Data Fiduciaries or intermediaries to furnish information for purposes specified in that Schedule. It also allows the government to restrict disclosure of such requests if it affects national security.	**- Potential for Arbitrary Government Powers**: The rule grants broad authority for data collection, potentially infringing on individual privacy rights. Establish specific and justifiable criteria for government data requests, ensuring they are proportionate to the stated purpose and subject to independent review, with justifications published on a website. **- Risk of Government Interference**: The provision enables significant government interference, which may compromise impartiality in data handling and oversight. Create an independent oversight body to review

		government requests for data access, ensuring transparency and accountability. **- Vague Language in Provisions**: The use of "as may be deemed necessary" lacks clear guidelines. Replace vague language with specific, measurable, achievable, relevant, and time-bound (SMART) criteria to prevent potential misuse of power. **Compromised Encryption Protections**: Government access to personal data may undermine promises of end-to-end encryption. Mandate that government access to encrypted data comply with strict conditions prioritizing individual privacy rights, ensuring encryption remains effective against unauthorized access and detailed records are kept of how data is handled.