Digital Personal Data Protection Rules, 2025

MeitY released the Draft Digital Personal Data Protection Rules, 2025 on January 3, 2025, for public consultation. Initially, stakeholders were invited to submit their feedback by February 18, 2025. However, following requests for additional time, the deadline was extended to March 5, 2025. In response, a secure analysis process was initiated, which involved processing 6,951 comments and submissions received via the MyGov portal.

In addition to online submissions, inputs were gathered through physical consultations held in various cities. These sessions began in Delhi on January 14, 2025, and concluded in Guwahati on March 4, 2025, and featured a diverse group of stakeholders, including representatives from GCC, consulting and law firms, start-ups, healthcare, academia, and other sectors.

Furthermore, ministries and other government organizations submitted their feedback by letters and emails. Additional responses were also received from individuals, industry stakeholders, and industry associations, both electronically and in written form.

The most substantial feedback has clustered around several key provisions: Rule 3 (notice), Rule 4 (consent manager), Rule 6 (reasonable security safeguards), Rule 8 (purposes no longer being served), Rule 10 (processing children's data), Rule 11 (exemptions from obligations applicable to processing children's data), Rule 12 (additional obligations of SDFs), Rule 15 (exemption from the Act for research, archiving, and statistical purposes), and Rule 22 (calling for information).

All the rule-specific feedback gathered from these varied consultative channels after analysis shall result into an output encapsulating the rules on which significant feedback has been received alongside the detailed observations.

Rule 1: Short title and Commencement

1. **Transition Period & Phased Implementation**
   - Need for a clearly defined implementation period and calls for phased rollouts and exemptions based on entity size.
   - Allow additional time for notified significant data fiduciaries (SDFs) to comply once designated.

Rule 2: Definitions

1. **Definitions**
   - Provide definitions for terms like "reasonable security safeguards," "personal data breach," "Data Principal", "Data Processor," "Public Interest," and "Consent Manager".
2. **Consent Specificity and Clarity**
   - Informing users about automated decision-making processes and ensuring they have the right to request human intervention or explanations.
3. **Use of Real-World Examples and Illustrations**
   - Feedback indicates that including real-world examples and practical illustrations would enhance understanding.

Rule 3: Notice given by Data Fiduciary to Data Principal

1. **Defined Timelines and Process Clarity**
   - Specify timeframes for all data principal right requests in the notice itself.
   - Clarity on how far back in time should a Data Fiduciary go to obtain consent for legacy data. How quickly Data Fiduciaries must act when a Data Principal revokes consent, to avoid ambiguity that might lead to disputes or noncompliance.
2. **Standardised Notice Template and Format**
   - A standardised template that outlines all required content for notice.
3. **Comprehensive Content in the Notice**
   - The notice must include the data retention period and details on any automated decision-making processes (including profiling), with a requirement that an explanation be offered where significant outcomes are involved.
   - A new sub-rule stating that "the Data Fiduciary must disclose to the Data Principal whether any data processor has been engaged or if there are other persons with whom the personal data will be shared."
   - Some comments propose removing optional language (such as the phrase "if any") to ensure that the notice requirements are mandatory rather than discretionary.
4. **Clarity on Legacy Data and Consent**
   - Guidance on the handling of legacy data. There is a need for clear instructions on how to provide notices for data collected before the Act's commencement, with some proposals suggesting a defined period (e.g., for data processing activities from the past 3 years) and explicit rules for validating legacy consents.
5. **Additional Specific Clarifications and Use-Case Considerations**
   - Clarifying the difference between "notice" and "intimation".
   - How consent should be obtained for non-traditional data channels (e.g., via IoT devices or verbal interactions).
   - Specifying that notice provisions for Data Principals should also include details about the use of data in automated decision-making processes, as well as special considerations for sectors like journalism or payment aggregation where operational practices may differ.

Rule 4: Registration and Obligations of Consent Manager

1. **Technical and Operational Standards & Audit**
   - Lack of guidance on technical and operational benchmarks for Consent Managers.
   - Calls for mandatory annual independent security audits, defined audit standards (for example, referencing IS 17428).
2. **Financial Threshold and Tiered Registration**
   - The current threshold net worth requirement of INR 2 crores as being too high, potentially discouraging startups and smaller organizations.
   - Suggestions include a tiered registration system based on the scale of operations.
3. **Mandatory Requirement and Scope of Consent Manager Role**
   - Clarity on whether having a dedicated Consent Manager is mandatory for organizations that already have an internal platform to capture consent.
   - Additional comments recommend restricting the role of Consent Managers strictly to managing consent without overlapping into other business activities or data processing functions.
4. **Registration Process, Timelines, and Governance**
   - Specific timelines throughout the registration process.
   - Mandatory reporting by Consent Managers to the DPB within 10 working days on adherence measures.
   - If a Consent Manager fails to meet requirements, they should be given a defined time to rectify deficiencies, failing which the registration should be cancelled.
   - There is a need for a formal appeal mechanism in case of suspension or cancellation of Consent Manager registrations.
5. **Conflict of Interest and Transparency**
   - Need for clear provisions to prevent conflicts of interest.
   - One suggestion calls for new clauses such as:
   - "The Consent Manager shall avoid conflict of interest with Data Fiduciaries, including in respect of their promoters and key managerial personnel… [and] shall clearly and upfront disclose all its fees and charges… Whenever engaging with a new Data Fiduciary, or when the terms of engagement change, it shall disclose how such new engagement cannot be considered as a conflict of interest."
6. **Cost Burden, Foreign Entities, and Additional Clarifications**
   - Whether fees charged by Consent Managers should come from Data Principals rather than Data Fiduciaries.
   - Entities like LLPs should be allowed to register as Consent Managers, with calls for expanding the eligibility criteria to include more types of organizations.
   - Clarifying roles in cases of inoperative accounts (such as in the banking sector).
   - Establishing clear contractual requirements between Consent Managers and Data Fiduciaries.

Rule 5: Processing For Provision or Issue of Subsidy, Benefit, Service, Certificate, Licence or Permit by State and Its Instrumentalities

1. **Oversight, Accountability, and Review Mechanisms**
   - A centralized review board to monitor state data processing under Section 7 and Rule 5.
2. **Scope, Exemptions, and Definitions (Including 'Instrumentalities')**
   - Concerns that the term "instrumentalities" is ambiguous and there is a request to provide a definition.
3. **Minimalism, Necessity, and Proportionality in Data Collection**
   - Any data processing by the State should adhere to the principles of minimal data collection, necessity, and proportionality. Only the minimum personal data necessary for the specific

purpose should be collected and processed, with additional use requiring explicit consent or a separate legal basis.

4. **Additional Clarifications and Suggested Amendments**
   - Add accountability language, for instance, one recommendation suggests modifying Rule 5 by incorporating "an opportunity to withdraw or deny consent" in Section 7(b)(i).
   - Inserting new accountability points in the Second Schedule regarding factors for sharing sensitive data and replacing ambiguous language with clear, enforceable standards.

Rule 6: Reasonable Security Safeguards

1. **Clarity, Specificity, and Standardization**
   - The current language is vague and subject to differing interpretations and there is a call for clear definitions and specific guidelines on what constitutes "reasonable security safeguards".
   - Adopt a defined set of baseline security standards, for example, compliance with internationally recognized standards (such as ISO 2700 or NIST frameworks).
   - Terms like "encryption," "obfuscation," and "masking" should be clearly defined whether they are alternatives or must be implemented together.
2. **Risk-Based and Tiered Approach**
   - A risk-based framework to tailor security safeguards according to the sensitivity, volume, and risk profile of the data processed.
   - To allow flexibility for smaller organizations and MSMEs through tiered security requirements.
3. **Log Retention and Traceability**
   - Clarity on when the log retention periods begin.
   - Retention of logs requirement should be aligned with other regulatory standards (e.g., maintaining logs for 180 days as per CERT-In, or even longer for forensic purposes).
   - One suggestion advocates for clear guidance stating that "logs and personal data related to a data security breach" be retained based on a flexible, risk-based timeline.
4. **Guidance on Implementation and Compliance Verification**
   - rule should provide explicit implementation guidelines and a mechanism for periodic third-party audits or certification to verify that organizations have properly deployed the necessary safeguards.
   - One recommendation calls for the Board to issue technical directions and standards for encryption, masking, and the use of virtual tokens, along with mandates for regular reviews and updates of security controls.
5. **Flexibility, Adaptation, and Minimizing Operational Burden**
   - Suggestions include modifying phrases such as "at the minimum" to "as appropriate" and allowing organizations to determine retention periods and specific security measures based on their own risk assessments.
   - There is a shared sentiment that the rule should avoid a one-size-fits-all approach and instead encourage flexibility and adaptability to evolving digital threats.
6. **Additional Considerations and Future Enhancements**
   - Include anonymization as a security measure and define "erasure" and "deletion".
   - Make data fiduciaries and processors jointly or severally liable for breaches if they fail to maintain the mandated security safeguards

Rule 7: Intimation of Personal Data Breach

1. **Notification Timelines and Clarity**

- Breach notifications to affected Data Principals be mandated within a specific period for example, one proposal states that notifications should be made "within 72 hours of becoming aware of the breach."
- Recommendation to replace phrases "without delay" with more precise language for instance "…notify the affected individuals in a clear and plain manner, within 72 hours of becoming aware of the breach…".
- Inclusion of periodic updates on the breach investigation and mitigation measures rather than a one-off notification.

2. **Risk-Based and Tiered Breach Reporting**
   - Mandating notification for every minor breach would impose an undue compliance burden on Data Fiduciaries, instead, many suggest that only breaches which pose a significant risk or cause notable harm to Data Principals should trigger the notification requirement.
   - Notification to Data Principals should be mandatory if the DPB directs it.
   - Breach reporting as part of a broader risk-based reporting framework, with periodic summary reports (e.g., monthly or quarterly) submitted to the Board.
3. **Standardization, Templates, and Communication Process**
   - Establishing a unified portal for reporting breaches to respective authorities.
   - Clarity on concerns about conflicting reporting requirements, especially when comparing the 72-hour notification rule with other regulatory obligations (for instance, CERT-In's 6-hour reporting requirement).
   - Need for clarity on what constitutes "sufficient communication" to ensure that Data Principals fully understand the implications of a breach.
4. **Compensation**
   - Need for financial accountability towards Data Principal.

Rule 8: Time Period For Specified Purpose To Be Deemed As No Longer Being Served

1. **Definitions & Scope Clarifications**
   - Definitions of "specified purpose" and "user account."
   - Several feedbacks clarifying that Rule 8 applies only to Data Fiduciaries listed in the Third Schedule.
   - Suggestions to empower the Data Protection Board to add new classes of Data Fiduciaries.
   - Recommendation to replace "registered users" threshold with "active users" in order to correctly gauge the status.
2. **Retention & Deletion Timelines**
   - The 48-hour notice and the 3-year deletion mandate are too rigid, feedbacks requesting to extend both notice and overall retention. Suggestions include a 30-day advance notification before erasure.
   - Rule 8 should explicitly state that data erasure shall occur: 1.1. Upon the expiration of the specified purpose for data collection, 1.2. Upon the expiration of the regulatory/statutory retention period (if applicable), 1.3. Or upon the expiration of [X] years of inactivity, whichever comes first.
3. **Sector-Specific & Exceptions**
   - Sector-based retention guidelines (fintech, non-banking finance, healthcare, education, telecom, research institutions).
   - Requests allowance for anonymized data retention for research and policy analysis.
4. **Enforcement & Auditability**
   - Mandate detailed record-keeping of deletion activities, including timestamps and processor confirmations.
   - Require issuance of a data deletion certificate to the Data Principal.
5. **Definition of Archiving**

- Differentiate “deletion” versus “archival” within the definitions.

Rule 9: Contact Information of Person To Answer Questions About Processing

1. **Contact Information Completeness & Accessibility**
   - Feedbacks call for specifying minimum contact details and clarify what qualifies as “business contact information.”
   - Ensure this information is prominently published (website/app) and easy to find, avoiding dark patterns.
2. **Response Timelines & Service Levels**
   - Submissions are suggesting a defined SLA for query responses. One such language:
     “The Data Protection Officer, or the person … shall respond to such questions within two weeks of the receipt of question and provide periodic updates to the Data Principal until the question is answered to the satisfaction of the Data Principal.”
3. **Roles, Qualifications & Accountability**
   - Define eligibility criteria and minimum qualifications for the DPO (e.g., IT/cybersecurity experience, Indian resident).
   - Allow multiple personnel, regional SPOCs or a dedicated compliance team and permit one DPO to cover multiple entities of a group.
4. **Communication Channels & Grievance Escalation**
   - Mandate multiple modes of contact: email, phone, SMS, chat support, ticketing system, and web forms catering to different types of users.
   - Require inclusion of the full grievance-redressal process alongside contact details, with clear escalation paths from level-1 automated support to the DPO.
5. **Maintenance & Updates of Contact Information**
   - Obligate Data Fiduciaries to promptly notify Data Principals of any changes to contact details or responsible persons via appropriate communication channels.

Rule 10: Verifiable Consent For Processing Of Personal Data Of Child Or Of Person With Disability Who Has Lawful Guardian.

1. **Verification Mechanisms and Methodology**
   - Need for clearer, standardized methods for verifying parental consent. Feedbacks recommend that Data Fiduciaries should “specify acceptable verification methods (e.g., government-issued IDs or secure digital tokens)” and consider options such as digital signatures, multifactor authentication, email-based OTP, or even biometric solutions.
   - Adopting a “reasonable efforts” standard rather than a rigid, two-method approach.
2. **Clear Guidelines**
   - Request that the rule provide guidance on what constitutes “reliable details” of age and identity as well as proof of the parent–child or guardian–child relationship.
3. **Risk-Based and Graded Approach**
   - A risk-based, tiered approach to verification. The consent process should be stricter for high-risk data processing (e.g., in gaming or social media) and more flexible for low-risk services.
   - For persons with disabilities (PwD), several responses call for an approach that respects their autonomy by promoting supported decision-making rather than mandating full guardianship in every case. This would align with the RPwD Act and international standards such as the UNCRPD.
4. **Challenges for Small Entities and Scalability**
   - Flexibility is essential so that smaller data fiduciaries are not forced into overly complex or costly verification mechanisms. Suggestions include allowing alternative verification measures (e.g.,

parental self-declaration cum undertaking) in cases such as when a minor is merely a beneficiary (for example, in insurance policies).

5. **Privacy, Autonomy, and Guardianship Nuances**
   - The current language may assume that all children or all persons with disabilities lack decision-making capacity. There is a call to clarify that verifiable consent should only be required when a Data Fiduciary has actual knowledge that it is processing a child's data or when a disability is voluntarily disclosed, rather than imposing a blanket requirement.
   - Need to define whether parental consent should be based solely on one parent's details (noting that many government documents only record the father's information) and to address scenarios involving children of PwD parents.
   - There is also concern over ensuring that the rules do not inadvertently force data maximization.
6. **Periodic Review and Grievance Redressal**
   - Verifiable consent should be reviewed periodically to ensure that the parental or guardian status remains valid.
   - Establish a grievance redressal mechanisms specifically for issues arising under this rule, ensuring that concerns raised by children or their guardians are addressed promptly and on priority.

Rule 11: Exemptions From Certain Obligations Applicable To Processing Of Personal Data of Child

1. **Establish an Independent Review Mechanism**
   - Need for an independent review process to monitor and safeguard how exemptions are applied. They recommend that a review mechanism be set up to ensure the protection of minors' privacy when data fiduciaries invoke these exemptions.
2. **Clear Criteria and Specific Scenarios for Using Exemptions**
   - Processing without verifiable parental consent for user account creation may defeat the purpose of protecting minors. They suggest listing concrete scenarios and limitations to prevent retention of data used only for account creation or communications.
3. **Precise Definitions and Scope Clarification**
   - Clarification on terms and categories in the Fourth Schedule—for example, providing a more detailed definition of "educational institution" to determine whether ed-tech companies or learning platforms fall within the exempted group.
   - Guidance is sought to clarify the meaning of "detrimental effects" and to ensure exemptions do not inadvertently expose children to inappropriate profiling or tracking.
4. **Safeguards and Regular Reviews**
   - While certain processing exemptions are necessary, they should be accompanied by mandatory audits, periodic reviews, and compliance checks to ensure that the exemption is not misused and that the protection of children's data remains robust.
7. **Considerations for Digital Platforms and Targeted Advertising**
   - Blanket bans on tracking or targeted advertising might limit a child's access to beneficial online services and the child will be exposed to generic content.
   - Any exemptions should clearly state that commercial exploitation via targeted or behavioural advertising for children is not permitted while allowing context-specific and age-appropriate personalization for educational or safety purposes.

Rule 12: Additional Obligations of Significant Data Fiduciary

1. **Clear Audit and Transparency Mechanisms**

- Instituting annual independent third-party audits (accredited by the Data Protection Board) for Significant Data Fiduciaries (SDFs), with audit reports covering data breaches, resolution times, and overall compliance scores.
- Creating public compliance dashboards on websites/apps that display user data requests, audit outcomes, and Data Protection Impact Assessment (DPIA) results.
- Implementing periodic self-certification using a standardized checklist, with disclosures (e.g., quarterly) available to users or submitted to the Board.

2. **Defined Guidelines for DPIA and Audit Procedures**
   - Limiting DPIAs to high-risk or sensitive data processing activities rather than making them an annual blanket requirement for all SDFs.
   - Outlining the elements required in a DPIA (e.g., a description of processing, risk assessment, and remedial measures) and specifying who can conduct these assessments (internal vs. external auditors).
   - Clarifying the qualifications required for personnel (such as CISOs or DPOs/ Third Party auditors) carrying out DPIAs and audits.
3. **Algorithmic Accountability and Due Diligence**
   - Rules to specify due diligence requirements for algorithmic decision-making processes including the definition of "algorithmic software" and limiting the obligations to AI-driven decision-making functions that pose a risk to data principals.
     Suggested language, "A Significant Data Fiduciary shall observe due diligence to verify that algorithmic software deployed for decision-making does not pose a risk to the rights of Data Principals."
   - Avoiding regulatory redundancy if existing measures (like DPIAs or audits) already address algorithmic risks.
4. **Additional Obligations**
   - SDFs document and report significant observations from DPIAs and audits, either on a routine basis or when triggered by customer complaints or Board investigations.
5. **Simplification for MSMEs and Smaller Entities**
   - Compliance burden especially regarding DPIAs, audits, and transparency requirements could be excessive for smaller organizations.
   - Relaxing or modifying certain requirements for MSMEs and allowing alternative, cost-effective internal assessments in cases of low-risk processing.

Rule 13: Rights of Data Principals

1. **Response Timelines & Grievance Redressal**
   - Absence of clear timelines for responding to Data Principals' requests and grievances. Feedbacks have suggested a timeline of 15/30 days for responding to/ resolving of grievance.
2. **Nomination Process – Clarity & Verification**
   - Define procedures for **nominating a representative** under Rule 13(4). Feedbacks suggest that the process should be secure and verifiable, and should limit the number of nominees or allow Fiduciaries to impose such limits.
     Suggested verbatim: "DP should be able to nominate an individual through a secure, and verifiable process and a digital record of the same which can be stored and reviewed periodically."
   - Where no nominee is appointed, suggest allowing heirs to exercise rights, per succession laws.
3. **Publication of Identifiers – Misinterpretation**
   - Multiple concerns that Rule 13(1)(b) could be misread as requiring public disclosure of usernames.
4. **Sectoral Compatibility & Operational Issues**

- Concerns from telecom, insurance, financial sectors on how existing KYC or nominee rules interact with DPDP.
- Request to **harmonise Rule 13** with existing frameworks (e.g., NPCI consent flows, RBI Ombudsman).

Rule 14: Processing of Personal Data Outside India

1. **Contractual Safeguards and Transfer Mechanisms**
   - The rule should address the use of globally accepted mechanisms such as Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs) to enable secure transfers.
2. **Timeline, Enforcement, and Transition Provisions**
   - Provide clarity on transitional periods for organizations to adjust to new requirements.
   - Suggested language, "Any orders (under this rule) shall be limited to a specified finite period not exceeding in any case fifty years, and subject to the Data Fiduciary and receiving party(ies) ensuring the data is rendered inaccessible in any manner whatsoever in the territory outside of India at the end of the said specified period."
3. **Clarification on Scope and Definitions**
   - Feedbacks call for a clear definition of "agencies of the State," the scope of control under the rule, and specific criteria (for example, for CBDT or for determining when data transfers are restricted).

Rule 15

1. **Lack of Clear Definitions and Scope**
   - Terms such as "research," "archiving," and "statistical purposes" are overly broad. There is a call to clearly define these terms to distinguish legitimate academic or scientific inquiry from market research, advertising, or other commercial uses.
   - Suggestion to include journalistic purposes in the exemption list, while also clarifying if private or commercial research can qualify.
2. **Safeguards, Anonymization, and Ethical Standards**
   - Need for safeguards like mandating anonymization or pseudonymization of personal data to ensure privacy protection and to prevent re-identification.
   - Call for a schedule to specify minimum safeguards for processing research data, including encryption, ethical oversight, and defined retention periods.
   - A practical guidance, such as conducting Data Protection Impact Assessments (DPIA) and regular audits to ensure that data processed under the exemption adheres to established standards.
3. **Risk of Misuse and Need for Accountability**
   - Suggestion to conduct periodic reviews of exempted activities to prevent misuse and recommending clear accountability measures and transparent disclosure to data principals regarding how their data is used under the exemption.

Rule 16: Appointment of Chairperson and other Members

1. **Independence and Transparency**
   - The search-cum-selection committee should include independent experts. For example, representatives from the judiciary, industry, academia, or civil society to mitigate risks of bias and conflict of interest.
   - Suggestions include publishing the selection criteria, the reasons for candidate choices, and the list of considered candidates to enhance transparency.

- Suggested language, “The Central Government shall, on the public recommendation of the Search-cum-Selection Committee, appoint the Chairperson and other Members within a month of such recommendation having been made. The Central Government may, for reasons to be recorded in writing, request the Committee to reconsider any recommendation but the Committee's decision in this regard shall be binding on the Central Government.”

2. **Enhancing Board Composition and Oversight**
   - Include experts from various fields such as governance, operations, audit, and law.
   - The DPB appointment process include periodic audits or reviews by third-party experts to reinforce transparency and accountability.
   - Mandate representation from the private sector and judiciary to avoid a quasi-judicial body being entirely controlled by the government.
3. **Structural and Procedural Modifications**
   - Others suggested that the process be decentralized by involving state-level boards or additional oversight bodies to handle grievances and enhance operational capacity.

Rule 17: Salary, Allowances And Other Terms And Conditions Of Service Of Chairperson And Other Members

1. **Clarity and Detailed Specification**
   - It was noted that these details need to precisely outline remuneration, responsibilities, and expense reimbursements, ensuring the compensation is both adequate and commensurate with the scope of responsibilities.
2. **Compliance with Labour Laws and Ethical Standards**
   - Multiple comments called for alignment of the service terms with relevant labour laws and ethical standards.
   - The feedback emphasizes that the Rules must fully account for all statutory and ethical employment practices to safeguard the interests of the DPB office bearers.

Rule 18: Procedure For Meetings Of Board And Authentication Of Its Orders, Directions And Instruments

1. **Enhanced Procedural Safeguards and Digital Security**
   - Recommendation to mandate the use of secure digital tools for Board meetings.
   - Suggestions include requiring secure digital signatures and detailed audit trails to authenticate orders and directives, preventing unauthorized changes and ensuring document integrity.
2. **Quorum Requirements and Key Member Attendance**
   - Increase the quorum for decision-making from the current level to at least two-thirds or ideally 75% of the Board.
   - For decisions involving penalties or other significant actions, mandatory attendance of the Chairperson, legal member, or other key representatives should be ensured to strengthen accountability.
3. **Clarity in Language and Role-Specific Amendments**
   - One suggestion is to amend rule 18(1) by replacing the term “any Individual” with “such member of the board” to confine decision-making powers strictly to Board members.
4. **Decision-Making Transparency**
   - The proposal includes defining what constitutes an “emergent situation” and ensuring that such decisions are not unilaterally taken by a single individual (for example, preventing the Chairperson from having a casting vote in judicial or quasi-judicial matters) and to define the consequences if actions taken in an “emergent situation” are not ratified by a majority of Board members and to utilize penalty monies for compensating affected victims.
5. **Jurisdictional and Oversight Clarifications**

- Need to clarify jurisdictional overlaps for instance, between the Data Protection Board and CERT-In regarding data breaches.

Rule 19: Functioning Of Board As Digital Office

1. **Digital Security and Techno-Legal Measures**
   - The term "techno-legal measures" is too vague and should be defined in detail. Suggested language, "Techno legal measures can be defined to include e-filing systems, video conferencing, electronic hearings, secure online submissions."
2. **Accessibility, Digital Literacy, and Hybrid Model**
   - Concerns that a completely digital DPB may exclude individuals due to varying digital literacy levels and limited internet access.
   - Suggestion to develop a delayed hybrid model that initially supports a physical presence while progressively building the digital infrastructure.
   - Alternative channels such as allowing physical complaint submissions are recommended for those lacking internet access.
   - There is also a suggestion to publish periodic reports or dashboards on the Board's activities, decisions, and resolutions to foster accountability.

Rule 20: Terms And Conditions Of Appointment And Service Of Officers And Employees Of Board

1. **Feedback on Recruitment Guidelines and Eligibility Criteria**
   - Several feedbacks noted the need to specify minimum education qualifications in the technical field for both employees and officers.
   - Language suggestion, "Appointment: one-year probation, extendable at the authority's discretion.
     Confirmation: Post-probation, appointee can continue if confirmed for a regular post.
     Resignation and Termination: Appointees need to give three months' notice; others, one month. Notice must be accepted by the appointing authority.
     Pay and Allowances: Defined by the Board via regulations.
     Leave: Conditions set by the Central Government.
     Work Outside Duties: Requirement of Central Government's permission for unrelated tasks.
     Regulations: Article 309 of the Constitution of India allows Parliament to regulate recruitment and service conditions for public service and Union-related posts."
   - Expand the scope of Rule 17 so that the roles and responsibilities of each Board member are explicitly detailed.

Section 21: Appeal to Appellate Tribunal

1. **Feedback on Fee Structure and Financial Barriers**
   - Concerns that linking appeal fees to the Telecom Regulatory Authority of India Act, 1997, may impose undue financial burdens on small businesses and individuals.
   - Current language does not specify critical procedural details, including timelines for resolving appeals and the period of limitation for filing an appeal.
2. **Additional Clarifications and Considerations**
   - One feedback query raised the issue of whether the DPDP Rules would supersede the RTI Act with respect to sharing PII, suggesting that this matter be clarified possibly through FAQs.

Section 22: Calling For Information From Data Fiduciary Or Intermediary

1. **Ambiguity and Overbroad Scope of Information Requests**
   - Concern about the unclear definitions of what categories of information can be sought. Advocacy for language that restricts requests to "specific grounds" and ensures that any information requested is both necessary and proportionate to the purpose.
   - There are calls to narrow vague terms such as "authorized person" and "applicable law" and to introduce an independent ethics or judicial committee to oversee requests.
2. **Procedural Clarity and Transparency**
   - Additional procedural proposals include establishing secure transmission protocols, mandating that data be destroyed once the intended purpose is fulfilled, and requiring that the data requester provide clear justification for each request.
3. **Alignment with Global Standards and International Considerations**
   - Recommendation to harmonize the rule with internationally recognized frameworks such as the OECD Trusted Government Access Principles.
   - There is a call to ensure that the rule does not inadvertently cause conflicts for foreign Data Fiduciaries or lead to legal standoffs between Indian and international authorities.