Summary of DSCI's submission to MEITY on Draft Digital Personal Data Protection Rules, 2025

The Data Security Council of India (DSCI) has provided feedback on India's draft Digital Personal Data Protection Rules, 2025, appreciating the principle-based approach while offering targeted recommendations to improve clarity and implementation feasibility.

Key Concerns and Suggestions

Rule 3: Notice Requirements

- **Concern**: The draft rules don't distinguish between provision of notices for new data processing activities which will be undertaken after the commencement of the DPDP Act and the retrospective provision of notices for legacy data already being processed by Data Fiduciaries.
- **Recommendation**: Creation of distinct requirements for retrospective notices where consent has already been sought in the past. For example, mechanisms allowing for mass communication methods may be more feasible than itemized descriptions of historical data processing.

Rule 6: Reasonable Security Safeguards

- **Concern**: The current one-size-fits-all approach for implementing reasonable security safeguards may not accommodate different sectors and contexts.
- **Recommendation**: Modify phrasing in Rule 6(1) from "shall include, at the minimum" to convey that the security measures are indicative rather than mandatory in all contexts. This would prevent impractical interpretations such as requiring encryption of all personal data being processed by a Data Fiduciary. Additionally, the language of the provision should clarify that only such logs which are necessary for breach detection and investigation need to be retained for a period of one year.

Rule 7: Intimation of Personal Data Breach

- **Concern**: Absence of a threshold for notifying Data Principals of personal data breaches and a strict interpretation of reporting requirements for personal data breaches could create practical compliance challenges for Data Fiduciaries.
- **Recommendation**: Modify requirements to include an assessment of severity, scope, etc. of a personal data breach before notifying data principals and specify that information provided to the Data Protection Board should be on a best-efforts basis.

Rule 10: Verifiable Consent for Children and Persons with Disabilities

- **Concerns**: The threshold for "verifiable" consent from parents/guardians needs clarification. Additionally, the definition of a 'person with disability' has a wide scope which may not be relevant in the context of processing of digital personal data.
- **Recommendations**:
    - Align the main provision with the intent reflected in supporting illustrations which indicates that Data Fiduciaries are expected to seek parental/guardian consent after they have actual knowledge of existence of the Data Principal being a child.
    - Narrow the scope of the definition of 'person with disability' to focus only on disabilities that hamper a person's ability to make legally binding decisions, recognizing that many physical disabilities may not necessarily affect decision-making capacity to give informed consent for processing of digital personal data.

Rule 12: Additional Obligations of Significant Data Fiduciary

- **Concerns**:
    - Mandatory annual Data Protection Impact Assessments (DPIAs) may not align with actual changes in data processing context.
    - Rule 12(4) on data localization seemingly exceeds the scope of the Act.
- **Recommendations**:
    - Remove the annual DPIA requirement, allowing flexible timing based on significant changes to processing activities.
    - Clarify that DPIAs can be conducted by internal functions with necessary expertise.

- Remove Rule 12(4) as it potentially restricts global data flows, contradicting the Act's intent, while also potentially negatively impacting India's digital economy.

Rule 22: Information Requests from Government

- **Concern**: Clarity needed on exemptions for Data Processors and processing by Data Processors in India of personal data of foreign Data Principals.
- **Recommendation**: Explicitly state that processing of personal data of non-Indian Data Principals is exempt from the application of Rule 22 and the Seventh Schedule.

Fourth Schedule, Part B

- **Concern**: Lack of clarity on which purposes of processing are exempt from which requirements.
- **Recommendations**:
  - Clearly delineate which purposes are exempt from verifiable parental consent (Section 9(1)), the prohibition on tracking/behavioral monitoring (Section 9(3)), or both.
  - Add an exemption for personalization of digital services that doesn't cause detrimental effects on children's well-being.

Overall Perspective

For each issue and recommendation highlighted above, DSCI has also suggested alternative drafting of the rules that could address these gaps. Overall, an attempt has been made by DSCI to advocate for the following:

1. **Contextual Implementation**: Recognizing that data protection needs vary across sectors and processing contexts.
2. **Operational Feasibility**: Ensuring rules don't create disproportionate compliance burdens.
3. **Global Data Flows**: Maintaining India's position in the global digital economy by avoiding potentially restrictive data localization requirements.
4. **Proportional Obligations**: Tailoring requirements to actual risk levels rather than imposing blanket requirements.

***