Recommendations of (Dr.) Karnnika A Seth wrt The Draft Digital Personal Data Protection Rules,2025

The Digital Personal Data Protection Act, 2023 ("**DPDP Act**") was enacted on 11th August, 2023. On 3rd January 2025, MeitY notified the draft DPDP Rules,2025 and opened it for public consultation until 18th February 2025 ('the Draft Rules'). These rules aim to implement the Digital Personal Data Protection Act, 2023 (DPDP Act), in accordance with India's commitment to establishing a comprehensive framework for safeguarding digital personal information. The draft rules are designed to protect citizens' rights concerning their personal data. An Explanatory note to elucidate Draft Rules was also issued by MeitY. However, there are various concerns and implementation challenges in the provisions of the Draft Rules which are highlighted and solutions suggested herein. These have been duly submitted for kind consideration of Ministry of Electronics & Information Technology, Government of India.

I. **Requirement of Notice for Express Consent** (Rule 3) - Rule 3 envisages Data Fiduciaries are required to give a written notice to Data Principal before collecting any personal data from them. Such notice is required to include a link to the website or app where the Data Principal can withdraw their consent for data processing and/or exercise their rights under the Digital Personal Data Protection Act. The notice must include, interalia, the following –

(i) an itemized description of such personal data; and

(ii) the specified purpose of, and an itemized description of the goods or services to be provided or uses to be enabled by, such processing.

Comment- Such provision is subject to ambiguity in implementation unless a standard template for required Notice is appended as Schedule to the Rules.

1. **Prescribe a template for Notice**-For purposes of clarity, it is recommended that the Rules incorporate in a schedule, prescribed template for such Notice. This will bring uniformity, consistency and enable seamless compliance without any ambiguity or difference in formats.
2. **Language and Accessibility**: Notices should be available in major Indian languages and accessible to individuals with disabilities (e.g., screen-reader compatibility). The Provision needs to factor in this which is missing in current Draft Rules.

II. CONSENT MANAGERS (Rule 4 and First Schedule)- A person who fulfils the conditions for registration of Consent Managers set out in Part A of First Schedule may apply to the Board for registration as a Consent Manager. The Consent Manager has obligations as specified in Part B of First Schedule. The First Schedule provides Consent Managers must be a company incorporated in India, having sufficient financial and technical capacity to fulfil its obligations, with net worth not less than 2 crore rupees, amongst other requirements.

Part B of the First Schedule of Draft Rules provide obligations of a Consent Manager, interalia, to protect personal data with reasonable security safeguards. The Consent Manager is required to enable a Data Principal using its platform to give consent to the processing of her personal data by a Data Fiduciary onboarded onto such platform either directly to such Data Fiduciary or through another Data Fiduciary onboarded onto such platform, who maintains such personal data with the consent of that Data Principal.

1. **Clarity on reasonable security standards** – For clarity and ease of compliance, recommended Standard (such as ISO 27001) adopted for reasonable security practices (mentioned at item 7 of Part B of First Schedule of Draft Rules) to protect personal data ought to be specified. Compliance with such standard will constitute deemed compliance of this requirement akin to ISO 27001 standard mentioned in Rule 8(4) of SPDI Rules,2011.

2. **Methods for making format 'unreadable' be illustrated-** With respect to Obligations of consent managers (Part B of First Schedule), the sharing or availability of personal data must be in a format unreadable by the Consent Manager, ensuring data privacy and preventing unauthorized access. However, rules fail to specify any mechanisms such as encryption, redaction technology or blockchain technology. Such technologies can be set as illustrations or prescribed by Rules in a Schedule.

3. **Recommend a standard for audit**-The Consent Manager are required to have in place effective audit mechanisms to review, monitor, evaluate and report the outcome of such audit to the Board. It is suggested that standards that meet such audit mandate ought to be specified or atleast one standard of audit be mentioned for consistency

and clarity. For example, Bureau of Indian Standards issued a data privacy assurance standard of **IS 17428.1.** Moreover, for Data Impact assessments, standards may also be prescribed for consistency. Qualifications and eligibility for role of CISO/Data Protection officer may also be prescribed akin to role of Examiner of Electronic Records under Section 79A of IT Act,2000.

4. **No conflict of interest** - As a practice, Consent Managers within an entity were individuals. The Draft Rules propose Consent Manager to be a separate independent entity from a Data Fiduciary. To ensure no conflict of interest, a panel of consent managers may be registered with and maintained by the Data Protection Board (akin to a panel of arbitrators maintained by an arbitral institution). Moreover, government departments will need to make several changes in their internal rules if personal data of citizens is to be managed for notice and consent by an independent entity. This will require a close consideration.

5. **Attribution of liability** - Consent Manager entity ought to adhere to strict confidentiality and data encryption mechanisms to prevent unauthorized breaches of personal data within its own system. This brings forth enforcement challenges as to who would be punished for a personal data breach incase of a Consent Manager entity. The Draft Rules ought to clarify if deemed liability principle shall apply in respect of Consent Managers as provided in case of Section 85 of IT Act, 2000 ('deemed liability of directors').

III. Intimation of data breach- Rule 7 of Draft Rules provides Data Fiduciary is under an obligation to inform Data Principal about a data breach '*without delay'*. Rule 7(2) requires a Data Fiduciary to inform Data Protection Board about a personal data breach without delay. It further requires Data Fiduciary to, within seventy-two hours of becoming aware of the same, or within such longer period as the Board may allow on a request made in writing in this behalf, provide-

(i) updated and detailed information in respect of such description;

(ii) the broad facts related to the events, circumstances and reasons leading to the breach.

Comment- It is relevant to point out that under Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, an

intermediary is required to, as soon as possible, but not later than seventy two hours of the receipt of an order, provide information under its control or possession, or provide assistance to the Government agency which is lawfully authorised for investigative or protective or cybersecurity activities, for the purposes of verification of identity, or for the prevention, detection, investigation, or prosecution, of offences under any law for the time being inforce, or for cyber security incidents.

Interestingly, under GDPR law, the data controller is required to notify the relevant supervisory authority of a personal data breach within **72 hours** of becoming aware of it, provided the breach is likely to result in a risk to the rights and freedoms of individuals.

1. **Ambiguity in words used "without delay" in Rule 7-**There is ambiguity in words used 'without delay" in Rule 7 of Draft Rules which is subject to subjective interpretation. Would it mean 'reasonable time'? What would be its objective criteria to understand its meaning and scope for a clear and consistent application? It can be clarified by an Explanation in Rule that the term 'Without delay' means within reasonable time from becoming aware or knowledge of personal breach.
2. **Inconsistency with extant 6 hour timeline** -Rule 7 of Draft Rules is inconsistent with 6 hour timeline to report cyber incidents/data breach to CERT-In as per Directions under sub-section (6) of Section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet.

The cyber breaches covered by the said rules mentioned in Annexure I to the said Rules under Section 70(B) of IT Act, 2000 cover very wide categories of cyber incidents (including data breach and data leaks) and 6 hour reporting timeline prescribed therein is inconsistent with the 72 hour time stipulated under Rule 7 of Draft Rules. Explanation in Rules may clearly specify timeline to report breach will be 6 hours and not 72 hours (for sake of consistency & clarity in application) .

IV. Time period of retention of personal data- Under Rule 8 of the Draft Rules, Data Fiduciaries can only retain personal data for specified purposes and limited amount of

time. It emphasizes 'purpose limitation' which means that data fiduciaries must erase personal data when its specified purpose is no longer served and at the same time retain data if it is necessary for compliance with the law. It mandates a 48-hour notification before data erasure, ensuring that data principals are informed and have an opportunity to act if they wish to retain their data.

1.**Dormant Accounts should be an exception**– The Rules ought to introduce an exception for handling dormant accounts such as a separate process for notifying users about account inactivity and potential data erasure. Also, criteria to decide if an account is dormant could vary depending on sector concerned, for example in banking it is typically between 6 to 12 months but may be different incase of e-commerce/healthcare sector.

2.**Determining accounts as inactive** -Draft Rules donot envisage what is objective criteria for keeping three years of inactivity as benchmark for keeping personal data of users. If a service is requested and is delivered, personal data therein ought to be deleted unless user chooses to keep account active or such data is needed for legal compliance.

V. PROCESSING PERSONAL DATA OUTSIDE INDIA (Rule 14)

A Data Fiduciary must meet requirements that may be notified by the Central Government by general or special order for transferring personal data to any foreign State. India follows a blacklist approach for cross border transfer of personal data as a Govt appointed Committee has been empowered to ban data transfer to certain countries.

1. **Standard contractual clauses**- It is recommended for seamless compliance, a standard best practices SOP or contract clauses may be drafted and prescribed for meeting the requirements of reasonable safeguards for transfer of personal data to countries outside India. Akin to Standard Contractual Clauses (SCC) in EU's law, GDPR, such contract clauses or prescribed standard practices will lend it clarity and uniformity in adoption. These can be readily incorporated in contracts for cross border processing of data or transacting other business relationships and enable effective compliance.

2. **Localised Personal data** – There is need for restricting processing of certain sensitive data within India. In other words, processing of certain personal data must be localized.

However, the Draft Rules donot clarify the criteria for selecting data categories for localization, which could result in arbitrariness and ambiguity. Sensitive data such as health record and financial data must be stored and processed in India alone. Clear stipulation of such categories of personal data that must be localized is therefore recommended. Additionally, Applicable Sectoral laws (especially if more stringent in its regulations, such as in financial sector) will also apply alongside DPDP.

VI. **Verifiable consent in case of minors**- Rule 10 of the Draft Rules requires 'parental consent' incase a child below 18 years or a person with disability with a lawful guardian opens any social media account. A Data Fiduciary is required to observe due diligence, for verifying that the individual claiming herself as the parent is an adult (who is identifiable if required in connection with compliance with any law for the time being in force in India). The rules envisage age and identity verification of a parent through his/her details available with Data Fiduciary or through a voluntarily provided details provided by Data Principal or a virtual token mapped including Digi locker service provided by the government.

1. **No penalty for false declaration of age –** It is pertinent to note that no punishment is prescribed for false declaration of age and identity of a child below 18 years is provided by the Draft Rules. Whereas in Telecom Act,2023 and Rules framed thereunder penalty of Rs. 10,000 in respect of subscribers is provided if a subscriber gives false particulars of identity or impersonates another or suppresses information. A practical challenge is that a minor is legally incompetent to contract as per Indian law and incapable of giving a valid consent. Enforcing the rule becomes challenging incase a child gives false declaration of his age or other particulars and difficulty is penal or penalty provision for such false declaration by minors will, in my view, not be advisable. Can a penalty be imposed on a child for false declaration? Rather in my view, approach to implementation should be -how to make due diligence by intermediary as regards age verification more effective?
2. **Age verification mechanisms recommended as part of due diligence**-An intermediary may request for ID proof of a child such as student ID (not a Voter ID /

Driving License / Aadhaar) or his birth certificate which rules currently don't envisage. However, if a false age is given this rule will be circumvented. Intermediaries need to abide by due diligence to do age verification. In other jurisdictions, this is being achieved by companies like Meta by age gating mechanisms such as asking user to record a video selfie or ask mutual friends to verify their age. Other companies use age verification by collecting real-time photo using, for example, Yoti's facial age estimation technology, which analyzes facial pixels to estimate age without linking the image to a name.

3. **Verification of lawful guardian**- It is ambiguous if Data Fiduciaries will be required to collect and/or verify such court orders granting guardianship or other such directions under the relevant statutes such as the Guardians and Wards Act, 1890, National Trust for the Welfare of Persons with Autism, Cerebral Palsy, Mental Retardation and Multiple Disabilities Act, 1999, or the Mental Health Act, 2017, in order to fulfil the due diligence obligation of a Data Fiduciary.
4. **Ambiguities in mandatory reporting to the Board**- In respect of Significant Data Fiduciaries (SDF), Rule 12 of Draft Rules visavis Mandatory Reporting to the Board, requires DPIA report to be submitted to the Board.

   i.Need for clarification -There is a lack of clarity on what constitutes "significant observations" in DPIA. Confidentiality concerns may arise if sensitive details are disclosed in the reports unless it is redacted / encrypted. These or other reasonable security parameter should be prescribed by the Rules.

   ii.Adoption of ethical AI framework must be prescribed by the Rules for AI based technologies used for data protection - Algorithmic Software deployed by a SDF for the purpose of hosting or sharing personal data should not pose a risk to the rights of Data Principals. However, the rule does not specify the criteria or standards for verifying the algorithms. If Algorithms use Artificial Intelligence these algorithms must be audited for compliance (such as with ISO 42001) with AI ethical framework and globally accepted best practices for Responsible AI.

VII. **Grievance redressal timeline is missing**- DPDP Act requires every Data Fiduciary to resolve grievances of Data Principal within such timeperiod as is

prescribed. However, Draft Rules lack a provision of such timeline for any or different class of Fiduciaries, which means there would be inconsistency in grievance redressal timeline as it is left to discretion of a Data Fiduciary by Rule 13(3) of Draft Rules.

It is suggested that Draft Rules provide for 72 hour timeline for responding to grievances of Data Principal.

VIII. EXEMPTION FOR RESEARCH, ARCHIVING, OR STATISTICAL PURPOSE (Rule 15)

As per Rule 15 of Draft Rules, the provisions of the DPDP Act shall not apply to processing of personal data necessary for research, archiving or statistical purpose if it is carried on as per the standards in the Second Schedule. It is suggested that the data kept for such purposes (ought to as far as possible) be prescribed to be in pseudonymized or anonymized manner for protection of privacy and data. Section 17(2)(b) in DPDP Act states such standards shall be prescribed under the DPDP Act. The Second Schedule in DPDP rules mentions criteria to be fulfilled (such as Processing is done while making reasonable efforts to ensure the accuracy of personal data) but not mention technologies needed to meet the criteria such as pseudonymization, redaction, encryption etc. The Rule states that such other standards as may be applicable to the processing of such personal data will be provided under policy issued by the Central Government or any law for the time being in force. Therefore, such standards ought to be prescribed for effective implementation of this Rule.

IX. Implementation Concerns: The rules have phased implementations without specific timelines, causing uncertainty and will make it difficult for businesses to plan and align operations.Thus, it is recommended that specific timelines be set for implementation of various provisions in the Draft Rules.

Set Specific Implementation Timelines: Introduce phased timelines for the implementation of different provisions, ensuring businesses have clarity and sufficient time to comply. An additional provision to seek extension for extending time of compliance in justifiable cases may be introduced keeping in mind principles of natural justice.

In view of the above, these key concerns may be addressed during the public consultation process of DPDP Rules by MeitY alongwith practical suggestions to deal with these concerns contained herein.

Yours sincerely,

(Dr.) Karnnika A Seth
Advocate & Cyberlaw Expert