Nishith Desai Associates
LEGAL AND TAX COUNSELING WORLDWIDE

| MUMBAI | SILICON VALLEY | BENGALURU | SINGAPORE | NEW DELHI | NEW YORK | GIFT CITY |

Legal Update and Technology Law Analysis

January 07, 2025

INDIA'S NEW DATA PROTECTION REGIME, ONE STEP CLOSER: DRAFT COMPLIANCE RULES ISSUED

- Draft Digital Personal Data Protection Rules, 2025 issued by the Ministry of Electronics and Information Technology operationalise various provisions and throw light on the compliance under the Digital Personal Data Protection Act, 2023.

- The Digital Personal Data Protection Act, 2023, is India's first standalone data protection legislation which once brought into force, will govern the processing of personal data in digital form.

- Stakeholders are invited to submit objections and suggestions on the Draft Rules by February 18, 2025.

EXECUTIVE SUMMARY

The new data law i.e. Digital Personal Data Protection Act, 2023 is a standalone data privacy law, enacted by the Indian Government in August 2023. The provisions of the DPDPA are yet to be notified for enforcement. The Draft Digital Personal Data Protection Rules, 2025 provide guidance on implementation of several key provisions of the new data law. These draft rules will come into effect in the coming months after the conclusion of the public consultation period.

Applicability of New Data Law: The DPDPA is applicable to processing personal data within the territory of India and outside the territory of India, if such processing is in connection with any activity related to offering of goods or services to individuals (i.e. data principals) within India.

Consent and Notice: Data fiduciaries (akin to data controllers) are required to seek consent from data principals for collection and processing of their personal data. Along with obtaining consent, a notice (in English and other official Indian languages) should be provided detailing the specific types of personal data collected, the purposes for processing such personal data, the rights of the data principal among other aspects.

Consent Manager: A novel mechanism of consent managers have been introduced; entities meeting certain requirements may be registered with the Data Protection Board of India as "consent managers" that offer data principals a platform to give, manage, review, and withdraw their consent provided to data fiduciaries. The consent manager is responsible for managing the data principals' consents and implementing technical, and organisational controls, systems, procedures for safeguarding the consents and data in its possession.

Security of Personal Data: Data fiduciaries are free to adopt their chosen security standards and practices for safeguarding personal data collected and processed by them subject to certain bare minimum guardrails. These include ensuring appropriate data security measures, access control measures, maintenance of logs and periodic monitoring, detection of unauthorized access etc.

Children and Persons with Disabilities: In relation to processing of personal data of children and persons with disabilities, there are additional requirements for obtaining verifiable consent from the parent or legal guardian. The mode of seeking verifiable consent is left to the discretion of the data fiduciary.

Cross Border Transfer: Cross borders transfers of all personal data from India is permitted unless (i) the recipient jurisdiction has been notified as a restricted territory by the Indian government and/or (ii) the specific personal dataset intended to be transferred outside India is prohibited/restricted from being transferred. Seperately, the Indian Government may also prescribe additional compliances for undertaking cross-border transfers of personal data to certain jurisdictions.

Data Breach Intimation: Data fiduciaries are required to intimate affected data principals and the Data Protection Board of India of data breaches immediately upon becoming aware of the breach. Additionally, within 72 hours of awareness (or a longer timeframe approved by the Board), the data fiduciary should submit a detailed description of the breach to the Board.

DETAILED ANALYSIS

CONTENTS

INTRODUCTION

The *Digital Personal Data Protection Act, 2023* (**"DPDPA"**), India's first standalone personal data protection legislation, was released in August 2023. The law aims to strike a balance between protection of individuals' right to privacy and personal data, and lawful processing of such data, by data fiduciaries (akin to data controllers)[1]. The DPDPA prescribes several compliances for data fiduciaries processing personal data and imposes penalties for non-compliance. Our detailed analysis of the DPDPA is available here.

While the DPDPA was enacted in August 2023, it is not yet in force. Detailed rules were awaited for its implementation. The Ministry of Electronics and Information Technology (**"MeitY"**), the nodal ministry for implementation of the DPDPA, has on January 3, 2025, released the *Draft Digital Personal Data Protection Rules, 2025* (**"Draft Rules"**) for public

consultation. Stakeholders are invited to submit objections and suggestions on the Draft Rules by February 18, 2025. MeitY will not publicly disclose comments submitted to it but will release a consolidated summary without attributing comments to any specific stakeholder.[2]

The MeitY has also issued an explanatory note ("**Explanatory Note**") providing an overview of the contents of the Draft Rules in an easy to understand language.[3]

Ideally, the MeitY should also release FAQs clarifying certain aspects, as we have pointed out in this newsletter.

The Draft Rules aim to provide guidance on compliance, operational aspects, administration as well as enforcement under the DPDPA. The Draft Rules include provisions on notice requirements, registration and functions of consent managers, security compliances, data breach notification procedures, parental consent for children's data, redressal procedures, and the appointment and working of the Data Protection Board of India ("**Board**"). In this newsletter, we provide our comments on the provisions prescribed under the Draft Rules.

I. OPERATIONALIZING PROVISIONS

The Draft Rules specify that the provisions relating to the Board will be operationalised upon the publication of the rules in the official gazette.[4] These include provisions on the appointment of Chairperson and other Members of the Board, salary allowances and terms and conditions of service of the Board and other procedural aspects of the functioning of the Board. All other substantive rules will come into force on a date to be specified in the final version of the rules.[5]

Analysis: It is likely that the provisions related to the Board will come into force first. Other provisions are likely to come into effect at a later date. However, there is no clarity on the implementation time period and whether or not the substantive provisions on compliance may be introduced in a phased manner, giving data fiduciaries windows to comply. The Government should ideally notify separate dates for operationalizing the substantive provisions of the rules, for ease of compliance.

II. NOTICE TO DATA PRINCIPAL

The DPDPA requires data fiduciaries to provide data principals[6] with notice prior to, or at the time of obtaining consent for processing their personal data.[7]

The Draft Rules read with the Explanatory Note specify that the notice must be clear, standalone, and understandable, distinct from any other information shared by the data fiduciary. [8]The language of the notice must be clear and plain[9] and is required to include, at the minimum: (i) the specific purpose for processing,[10] (ii) an itemised description of

personal data being processed[11] and (iii) an itemised description of goods and services to be provided or used to be enabled by such processing.[12]

Analysis: The Draft Rules does not prescribe a rigid template or format for the notice, allowing flexibility for data fiduciaries to design their notices so long as other requirements are satisfied. However, the notice cannot be clubbed with other documentation such as an End-User License Agreement, General Terms of Service etc. The requirement for the notice to be standalone will prevent data fiduciaries from obscuring such essential information from unrelated contractual terms.

As per the DPDPA, a data principal can consent to the processing of her personal data for the specified purpose and such consent will be limited to such personal data as is necessary for the specified purpose.[13] If the notice exhaustively lists the items of personal data and specific purposes for each item, there may not be a requirement to separately categorize each purpose against each item of data for the purpose of consent.

Notice Requirements for Existing Datasets

In respect of consent for processing personal data provided before the commencement of the DPDPA, data principals are required to provide the notice as soon as it is reasonably practicable.[14] The DPDPA also specifically empowers the Indian Government to issue rules on the manner of providing notice in relation to such processing, independently from the manner of providing notice for consent provided after commencement of the DPDPA.[15]

Analysis: The Draft Rules do not specifically prescribe the notice requirements for such datasets. Also, the timeline for providing notice for processing of personal data for which consent was provided prior to the DPDPA is still unclear. Ideally, in some cases, public notice or notice on websites or apps could have been held sufficient.

Language Requirements

The DPDPA also requires that the notice be accessible in English, or any language specified in the Eighth Schedule to the Indian Constitution.[16] The Draft Rules do not address or alter this requirement.

Analysis: It would be helpful if the FAQs clarified that the notice is only required to be accessible in the languages supported by the platform of the data fiduciary, to prevent unnecessarily onerous translation requirements.

Withdrawal of Consent, Exercise of Rights and Complaint Process

The Draft Rules require the notice to provide a communication link of the platform of the data fiduciary and description of how the data principal may (i) withdraw her consent; (ii) exercise her rights under the DPDPA; and (iii) make a complaint to the Board.[17]

Analysis: The Draft Rules do not explicitly prescribe the manner of providing for the withdrawal of consent, or exercise of the data principal's rights (including grievance redressal right), allowing flexibility to data fiduciaries in implementing their own practices as per their operational and business needs.

III. VERIFIABLE CONSENT FOR PROCESSING DATA OF CHILDREN AND PERSONS WITH DISABILITIES

The Draft Rules require a data fiduciary to adopt appropriate technical and organizational measures to obtain verifiable consent of a parent for processing personal data of a child[18]. This can be undertaken through: (i) reliable details of identity and age of the parent, already available with the data fiduciary[19] or (ii) voluntary provision of such details or (iii) a virtual token mapped to such details, issued by an entity entrusted by law or the Government with the maintenance of such details, or a person appointed or permitted by such entity, including a Digital Locker[20] service provider.[21] Data fiduciaries are also required to observe due diligence to ensure that a person identifying themselves as the lawful guardian of a person with disability[22] has been duly appointed under applicable law.[23]

Analysis: In cases where details of age and identity of the parent are already available with the data fiduciary, in order to constitute "reliable" methods of identification, such identification may need to resemble a form of documentation similar to a government issued identification. A simple check-the-box criteria is unlikely to satisfy the requirement of reliable forms of identity or age.

Neither the DPDPA nor the Draft Rules require the data fiduciary to investigate the ages of their users to ascertain if they are in fact not children or the relationship between child and purported parent. The DPDPA/Draft Rules appear to rely upon self-identification by a user as a child, or by a parent, for compliances to trigger. However, it does not address a situation where there is no proactive identification by a child. Arguably, if a data fiduciary obtains actual knowledge about the age of a child either through alerts from a parent, other users or through other technical means, data fiduciaries may then take necessary steps for processing personal data of children as per the DPDPA. The Draft Rules do not prescribe a specific manner of obtaining verifiable parental consent and simply refer to reliable details of age or identity, providing flexibility to data fiduciaries in adopting their own standards.

There is also no clarity on the scope of the due diligence obligation under the said rule.

For example, the *Rights of Persons with Disabilities Act, 2016* ("**RPWD Act**")[24] empowers district courts or designated authorities notified by the State Government to appoint limited guardians for persons with disabilities. It is unclear 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.

IV. EXEMPTIONS FROM CERTAIN OBLIGATIONS FOR PROCESSING OF CHILDREN'S PERSONAL DATA

Processing of personal data by certain classes of data fiduciaries or for certain purposes are exempt from the verifiable parental consent obligation under Section 9(1) of the DPDPA, and the prohibition on tracking or behavioural monitoring of children or targeted advertising directed at children and Section 9(3) of the DPDPA.[25] Part A of the Fourth Schedule sets out the classes of data fiduciaries and their conditions of processing which are exempt from the said obligations. Part B of the Fourth Schedule sets out the purposes of processing and conditions in relation to such processing which are exempt from the said obligations.

Analysis: We have analysed some of the exemptions. In relation to Part A, which sets out the classes of exempt data fiduciaries, we have taken the example of educational institutions. The exemption for educational institutions is only in relation to the prohibition on tracking and behavioural monitoring: (i) for the educational activities of such institutions; or (ii) in the interests of safety of children enrolled with such institutions.[26] It may not extend to permitting targeted advertisements directed towards such children. Thus, while the exemption is stated to generally apply to Sections 9(1) and 9(3) of the DPDPA, technically the exemption applies only to purposes specified in the Conditions column in Part A of the Fourth Schedule.

In relation to the purposes exempted in Part B of Schedule 4, we have taken the example of the purpose of processing childrens' personal data for the creation of a user account by a data principal for communication by email. Processing personal data for this purpose will only be exempt from the verifiable consent obligation and is unlikely to be exempt from the tracking, behavioural monitoring and targeted advertisement prohibition.[27]

Part B of the Fourth Schedule also provides an exemption for processing of personal data, for confirmation by the data fiduciary that the data principal is not a child and observance of due diligence under Rule 10.[28] If such processing is restricted to the extent necessary for such confirmation or observance, the data fiduciary is not prohibited from tracking or behavioural monitoring.

Analysis: While the Draft Rules do not specifically obligate data fiduciaries to specifically identify if a user is a child, this provision appears to exempt data fiduciaries from the prohibition on using methods of tracking or behavioural monitoring, to ascertain that a user is in fact a child. This may include, for example, quizzes or logic-based questions, user patterns, language, preferences or interactions with specific features etc.

V. REASONABLE SECURITY SAFEGUARDS

The DPDPA requires data fiduciaries to protect personal data in its possession or under its control, including in respect of any processing undertaken by it or on its behalf by a data processor,[29] by taking reasonable security safeguards to prevent personal data breach.[30] The Draft Rules reiterates this requirement.[31]

A breach of the obligation to maintain reasonable security safeguards is subject to a penalty that may extend to INR 250 Crores (approximately USD 29 Million).[32]

The Draft Rules prescribe minimum security standards. These safeguards, amongst others, include: (i) implementing data security measures including encryption, obfuscation, masking or use of virtual tokens,[33] (ii) retention of logs and personal data for one year to detect unauthorized access,[34] and (iii) inclusion of "*appropriate*" contractual provisions in the contract between the data fiduciary and the data processor to adopt reasonable security safeguards.[35]

Analysis: The language used in the Draft Rules suggest that all of the listed reasonable security safeguards are required to be adopted at a minimum, to demonstrate compliance. Data fiduciaries appear to have flexibility in implementing security standards, as long as they meet the minimum requirements prescribed. Overall, these standards are reasonably balanced and are likely to gain acceptance within the industry.

VI. PROCESSING PERSONAL DATA OUTSIDE INDIA

The Draft Rules specify that any entity processing personal data within India, or outside India in connection with offering goods or services to data principals in India, may transfer personal data to a foreign state or persons/entities under its control, only if it complies with restrictions imposed by the Indian Government on transferring such data.[36]

Analysis: The cross-border transfer restrictions under the DPDPA empowers the Indian Government to restrict the transfers of personal data to specified countries or territories.[37] Under the Draft Rules, it appears that the powers of the Indian Government has been expanded to issue orders imposing additional compliance measures for data fiduciaries undertaking cross-border transfers of personal data to foreign states and persons/entities under its control. The intent behind this provision could be that cross-border transfer of personal data may be permitted, subject to compliance with the prescribed conditions (instead of blacklisting certain foreign states). However, this could also empower the Central Government to impose conditionalities for countries which otherwise would not have been subject to any restrictions.[38]

It remains unclear whether such restrictions will apply solely when personal data is physically transferred outside India's territory, or if they will also extend to data shared with individuals and entities within India that are affiliated with or controlled by a foreign state

(For example, diplomats, sovereign wealth funds, private companies funded by foreign government etc.). Further, it may also lead to potential conflict with foreign laws that require access to such personal data pursuant to their domestic laws (for instance, anti-corruption laws). It may potentially restrict entities in India/doing business in India from transferring the requested personal data to such foreign government body.

VII. OBLIGATIONS OF SIGNIFICANT DATA FIDUCIARIES

The Draft Rules reiterate the obligations on Significant Data Fiduciaries ("**SDF**") (i.e. data fiduciaries which will be notified under the DPDPA basis factors such as volume and sensitivity of personal data processed) to undertake annual data protection impact assessment ("**DPIA**") and audit.[39] There is no further clarity provided regarding the manner of conducting such assessments. The Draft Rules also introduce a new provision requiring SDFs to undertake due diligence to verify that algorithmic software deployed by it (if any) are not likely to pose a risk to the rights of data principals.[40]

Additionally, the Draft Rules propose new data localization obligations restricting SDFs from transferring certain categories of personal data identified by a "committee" which will be constituted by the Indian Government.[41]

Analysis: The DPIAs and periodic audits are independent obligations under the DPDPA[42]; however, the Draft Rules do not distinguish between DPIAs and audits, and they appear to be overlapping. Further, in terms of the due diligence obligations, there is vagueness regarding what is "*likely to pose a risk to the rights of data principals*"[43] and may lead to subjective enforcement. Notably, the DPDPA does not propose the establishment of any committee to impose restrictions on the cross-border data transfers for categories of personal data, particularly for SDFs. It may be noted that the DPDPA itself does not include provisions for regulating non-personal data, such as traffic data.

Furthermore, SDFs who are foreign entities or global group companies may not only be required to localise the notified personal dataset, but also the logs and traffic data which are ancillary to such primary personal data set.

VIII. CONSENT MANAGER

Eligibility

The DPDPA contemplates establishment of "consent managers"[44] that offer data principals a platform to give, manage, review, and withdraw their consent provided to data fiduciaries. These consent managers are held accountable to the data principals for ensuring proper management of their consent.[45]

Consent managers are also required to register with the Board[46] and the eligibility conditions for such registration have been prescribed in Part A of the First Schedule to the Draft Rules. These conditions include the following:

- It is a company incorporated under Indian law[47] with minimum net worth of INR 2 Crores (approximately USD 240,000).[48]

- It has financial, technical and operational capability,[49] including adequate volume of business, capital and earning prospects.[50]

- Its financial condition and general character of management are sound.[51]

- Fairness and integrity of its directors, senior management and other key personnel.[52]

- Its governing documents (such as memorandum of association and articles of association) contain sufficient conflict of interest provisions.[53]

- Independent certification that (i) the consent manager's platform is in accordance with standards prescribed by the Board,[54] and (ii) appropriate technical and organisational measures to comply with such standards,[55] and (iii) adherence to obligations on disclosure of information regarding key personnel, including shareholding information.[56]

Conflict of Interest and Transparency

Consent managers are required to act in a fiduciary capacity[57] and avoid conflict of interest with the data fiduciary. Such conflict may be on account of promoters, key managerial personnel,[58] directors,[59] and senior management[60] (i) holding directorship, financial interest, employment or beneficial interest with data fiduciaries and/or (ii) a material pecuniary relationship between such persons and data fiduciaries[61] To this extent, consent managers are also required to transparently disclose (i) details of their promoters, directors, senior management, key managerial personnel or senior management holding more than 2% of shares in every body corporate and (ii) details of every person that holds more than 2% shares in the consent management company.[62] Further, transfer of control in the consent manager is not permitted unless authorised by the Board.[63]

In addition to this, the consent manager must obtain independent certification confirming that its interoperable platform enables data principals to give, manage, review, and withdraw their consent in compliance with data protection standards and assurance frameworks issued by the Board.[64] Independent certification is also required to confirm that appropriate technical and organizational measures have been implemented to ensure adherence to the Board's standards and frameworks, and that the publication of information about the company's employees and shareholding on its website, application, or both has been done.[65]

Obligations

Consent managers are obligated to maintain records of: (i) consents, (ii) notices and (iii) data-sharing transactions related to their platform.[66] These records must be stored for a period of seven years or longer as may be agreed or as required by law.[67] Consent managers shall conduct periodic audits and share records with the Board pertaining to its compliances and technical, and organisational controls, systems, procedures and safeguards.[68] Further, the consent manager must not sub-contract or assign its obligations under the DPDPA and the Draft Rules to another person.[69] The consent manager is also required to respond and address data principal's requests and grievances[70] (*discussed further below in Data Principal Rights*).

Failure to adhere to the obligations may result in the suspension or cancellation of registration granted by the Board[71] and/or could lead to monetary penalties under the DPDPA.[72]

Analysis: The broad restrictions placed with respect to conflict of interest may prohibit data fiduciaries and its group entities from acting as consent managers for datasets processed within the same group. It should be clarified that the conflict of interest may be only in relation to data fiduciaries being onboarded by the consent manager.

Further, one of the key takeaways regarding the operational aspects of the consent manager is that both the data principal and the data fiduciary should be onboarded on the consent manager platform in order to enable the data principal to provide and manage their consents.[73] It may also be noted that it is not mandatory for data fiduciaries to integrate with consent managers; the data fiduciary may continue to independently manage its data principal's consents and grievances. Additionally, while the consent manager represents the data principal, the revenue model of the consent manager is still unclear.

Considering that the position of a consent manager is a novel concept under the DPDPA, and its operational functionality is not tested under other data protection laws, one would have to wait and see how the practical nuances and implementation challenges play out.

IX. DATA PRINCIPAL RIGHTS

The DPDPA prescribes data principals rights including right to access information about their personal data[74]; correction, completion, updation and erasure[75]; right to appoint a nominee[76] and grievance redressal[77]. The Draft Rules further elaborate that data fiduciaries and/or consent managers (where applicable) should publish on their application and/or websites: (i) the procedure for the data principals to make a request for exercise of their rights[78] and (ii) the details of the data principal required to identify them (such as user name or other identifier) as per the terms of service of the data fiduciary/consent manager[79]. Accordingly, the data fiduciaries and consent managers are required to implement technical and organizational measures to respond to data subject requests and

grievances.[80] Data fiduciaries and consent managers are allowed to establish their own timelines for addressing grievances.[81] The data principal may make a request to exercise their rights in accordance procedure published by the data fiduciary/consent manager.[82]

Analysis: From a compliance perspective, the absence of prescriptive and coded grievance redressal/data principal request procedures is beneficial for data fiduciaries. It provides flexibility to entities to adopt procedures suitable to their business model.

Right to Nominate

Under the DPDPA, the data principal may nominate one or more individuals to exercise their rights.[83] The Draft Rules clarify that the nomination must be carried out using the methods and providing the details of the nominee in accordance with the terms of service of the data fiduciary and applicable laws.[84]

Analysis: It is advantageous that there are no defined procedures for appointing a nominee and data fiduciaries have the flexibility to establish their own terms and conditions for such nominations. However, there are currently no specific laws governing the appointment of nominees under the DPDPA. This provision seems intentionally open-ended, allowing the Indian Government to introduce specific requirements in the future.

X. RETENTION PERIOD FOR PERSONAL DATA

The DPDPA requires erasure of personal data as soon as it is reasonable to assume that the specified purpose is no longer being served.[85] The Draft Rules prescribe specific time periods to ascertain the same, in the Third Schedule, for e-commerce entities, online gaming intermediaries and social media intermediaries (that satisfy certain thresholds of users) processing personal data for specific purposes.[86] It sets out a three-year time period from the data principal last approaching the data fiduciary for the performance of the specified purpose or exercise of her rights, or the commencement of the Digital Personal Data Protection Rules, 2025, whichever is later.[87] The time period is generally applicable to all purposes by such classes of data fiduciaries, except for the purposes of accessing the user account or enabling access to a virtual token issued by the data fiduciary used to get money, goods or services.

Data fiduciaries are also required to notify data principals at least 48 hours prior to erasure that her personal data will be erased if she does not log in to her user account, approach the data fiduciary for performance of the specified purpose or exercise her rights.[88]

Analysis: While the Draft Rules set out explicit time periods to determine when the specified purpose is no longer being served for certain identified data fiduciaries in the Third Schedule, there is no clarity or guidance on the manner of ascertaining when the specified purpose is no longer being served for other data fiduciaries. In the absence of a

specific timeline, data fiduciaries will have varying standards to determine erasure of personal data.

Further, there is no clarity on why a timeline has only been prescribed for the said three classes, as opposed to other data fiduciaries, such as those in possession of large volumes of personal data.

Data fiduciaries will also be required to create automated processes to track the activity of the data fiduciary to determine the intimation period of 48 hours prior to erasure of personal data and then to erase data.

XI. INTIMATION OF PERSONAL DATA BREACH

Under the DPDPA, in the event of a personal data breach,[89] the data fiduciary shall notify the Board and each affected data principal in the below manner.[90]

Analysis: The DPDPA lacks a "materiality threshold" for breach notifications, requiring all breaches, regardless of severity, to be reported. This could overwhelm data principals and organizations, leading to desensitization and reducing responsiveness to critical breaches. While the industry was hoping for some relaxation in this regard, the Draft Rules do not provide any leeway.

Intimation to Data Principals

Upon "*becoming aware*" of a personal data breach, the data fiduciary must "*without delay*" notify the affected data principals. The intimation must be done using the data principal's user account or any registered mode of communication with the data fiduciary.[91] The notification given to the data principal must include details such as a description of the breach, potential consequences for the data principal and safety measures that the data principal shall adopt, among other particulars.[92]

Intimation to the Board

The data fiduciary, upon "*becoming aware*" of a personal data breach, must notify the Board in two phases:

- Without delay, a description of the breach, including its nature, extent, timing, and impact must be provided to the Board.[93]

- Within 72 hours of awareness, or a longer period if permitted by the Board, the data fiduciary must submit an updated and detailed description of the breach.[94]

Analysis: The timelines appear very difficult to comply with. Collating and sharing such information within a short timeline, particularly for intimations to affected data principals which require the inclusion of multiple details, may pose significant compliance challenges.

The Draft Rules do not specify requirements for measures to be taken following a personal data breach that must be detailed in the intimations. It may be clarified what risk mitigation or safety measures may be adopted by data fiduciaries or affected data principals following a personal data breach.

Existing reporting requirements under the Information Technology Act, 2000, directed to the Indian Computer Emergency Response Team,[95] as well as cyber security and reporting obligations under other sectoral laws (such as banking, insurance, financial sector) , may need to be harmonized with the reporting obligations prescribed under the Draft Rules, so that there is no undue burden on the data fiduciaries. To ensure compliance, organizations may implement internal monitoring mechanisms and have dedicated IT personnels in place to detect, escalate and report incidents in alignment with the diverse requirements of applicable laws.

XII. CONTACT INFORMATION OF DATA PROTECTION OFFICER

The DPDPA requires data fiduciaries to publish the business contact information of the Data Protection Officer or person capable of answering the data principal's questions about processing of her personal data.[96] The Draft Rules require that such information is "prominently published" on the data fiduciaries' website or app and mention the same in every response to a data principal's communication regarding exercise of her rights.[97]

Analysis:

Meaning of 'Prominently Publish'

The *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021* ("**IT Rules**") define the term "*prominently publish*" to mean publishing in a clearly visible manner on the homepage of the website or the home screen of the mobile based application, or both, as the case may be, or on a web page or an app screen directly accessible from the home page or home screen.[98] Guidance may be taken from such definitions to understand the requirement under the Draft Rules.

Publishing Officer Information

As per the DPDPA, SDFs are required to appoint individuals as Data Protection Officers.[99] However, as per the DPDPA, other data fiduciaries may appoint persons, which include artificial persons, to answer questions on the exercise of rights of data principals. However, there appears to be a trend in which Indian courts are increasingly requiring individual officers' information to be published by platforms to enable greater accessibility by users, and responsiveness by platforms.

XIII. EXEMPTIONS FOR RESEARCH, ARCHIVING AND STATISTICAL PURPOSES

The processing of personal data necessary for research, archiving or statistical purposes is exempt from most provisions of the DPDPA if the personal data is not to be used for making any decision specific to a data principal, and such processing is carried on in accordance with prescribed standards.[100] The Draft Rules propose standards for processing personal data under the said exemption: processing in a lawful manner; processing is limited to only necessary personal data; accuracy of data; adoption of reasonable security safeguards to prevent personal data breaches etc.[101]

Analysis: There is no further clarity regarding what purposes fall within the ambit of "research, archiving or statistical purposes". Further, it is unclear whether the reasonable security safeguards that data fiduciaries are required to implement under this provision align with the general requirements for reasonable security safeguards prescribed for all personal data under Rule 15 of the Draft Rules.

XIV. PROCESSING OF PERSONAL DATA BY STATE (AND ITS INSTRUMENTALITIES)

One of the grounds for the State and its instrumentalities to process personal data is for "*legitimate use*"[102] (i.e., without issuing notice to the data principal and obtaining consent) for providing or issuing subsidies, benefits, services, certificates, licenses, or permits ("**State Services**")[103] in two scenarios: (i) when the data principal has previously provided their consent for the processing of personal data for any State Service or (ii) such personal data is already available with the State and has been notified by the Indian Government. Further, such processing is required to comply with standards provided under the Second Schedule to the Draft Rules.[104] Such standards include providing the data principal with (i) an intimation, (ii) contact information of a representative of the data fiduciary to respond to queries, and (iii) access to a communication links to exercise their rights under the DPDPA.[105]

Analysis: As per the Draft Rules, if a data principal has previously consented to any State Service, the State or its instrumentalities may subsequently process such personal data for any other unrelated State Service. This raises significant concerns about the expansive scope of the Government's power and potential for overreach. The provision should have been drafted to explicitly require that subsequent processing by the State should be associated or closely linked to the original State Service to which the data principal had provided consent.

Nevertheless, there is a requirement under the standards set out in the Second Schedule to intimate the data fiduciary regarding such processing. There are also requirements of lawful processing, purpose limitation, data minimization, ensuring accuracy of personal data, reasonable security safeguards, accountability etc. to ensure there are sufficient safeguards in respect of such data processing.

XV. CALLING FOR INFORMATION FROM DATA FIDUCIARY AND INTERMEDIARY

The DPDPA empowers the Central Government to require data fiduciaries or intermediaries to furnish specific information.[106] The Draft Rules notify the government authorities authorised to make such requests and elaborate the purposes for making such requests in the interest of sovereignty, integrity and security of the state:

- The use of a data principal's personal data by the State or its instrumentalities[107] in the interest of India's sovereignty, integrity, or state security.[108]

- The use of personal data by the State or its instrumentalities for: performing any function mandated by laws currently in force in India; or disclosing information to fulfil obligations under such laws.[109]

- Conducting assessments for designating any data fiduciary or category of data fiduciaries as SDFs.[110]

At the time of making the information request, the requesting State/its instrumentality should specify the time period within which the requested information should be provided. The Draft Rules prohibit disclosures by the data fiduciary that could endanger the sovereignty, integrity, or security of the state, unless written permission is provided by the authorised person.

Analysis: This prohibition could extend to preventing disclosures of the information request itself and information shared pursuant to the same, by the data fiduciaries to other entities, including its group companies.

XVI. DATA PROTECTION BOARD

Lastly, the Draft Rules prescribe the constitution and functions of the Board. The Central Government will form the Board with a chairperson and other members.[111] The Draft Rules do not specify any qualification and candidature requirements for the appointments.

The functions of the Board include overseeing complaints and notifications regarding data breaches, complaints from data principals, and enforcement compliance with DPDPA obligations.[112] In cases of non-compliance, the Board is authorised to issue directives, suspend operations, or revoke registrations (of consent managers).[113] Individuals dissatisfied with the Board's decisions will be able to file appeals before the appellate tribunal (i.e. Telecom Disputes Settlement and Appellate Tribunal).[114] The Draft Rules prescribe guidance regarding payment of fees for filing an appeal.[115] In emergencies which warrant immediate action by the Board and where it is not feasible to call a meeting of the Board, the chairperson may take necessary action (while recording reasons in writing for

necessity for such immediate action), which shall be communicated within seven days to all members and subsequently be ratified by the Board at its next meeting.[116]

The Draft Rules reiterate that the Board shall function as a digital office and hence, may adopt techno-legal measures to conduct its proceedings.[117]

Analysis: The Draft Rules do not get into specific details regarding the conduct of business of the Board leaving room for further standard operating procedures to be adopted by the Board for its functions. However, to avoid arbitrariness, certain guardrails must be included for the exercise of emergency powers by the Chairperson of the Board.

CONCLUSION

The industry should actively provide feedback to the Draft Rules and seek publication of FAQs on issues in the DPDPA that remain unclear. Given that general direction is now available, businesses should evaluate their existing data protection practices, based on the industry, sector and nature of personal data in their possession. Accordingly, businesses will need to update their technological infrastructure and internal processes and documentation to include these requirements. Given the Draft Rules introduce the novel concept of a consent manager, data fiduciaries will need to consider onboarding on to the consent manager platform and integrating their data protection processes with such platform. They will also need to revisit their notices to include the required information set out in the Draft Rules. SDFs that are in the practice of sharing personal data to entities situated abroad may be impacted by potential data localization requirements enabled by the Draft Rules, which may require changes to the data sharing arrangement amongst corporate groups. The Draft Rules have largely avoided prescriptive standards, providing data fiduciaries with considerable flexibility in achieving compliance. There are some aspects which are yet to be prescribed through specific notifications, such as notification of SDFs, countries or territories to which personal data may not be transferred, databases of personal data maintained by the Indian government for processing personal data for State Services, categories of personal data that may be subject to additional cross-border transfer restrictions etc. These matters are expected to be clarified upon notification of the final rules.

Authors

- Technology Law Team

You can direct your queries or comments to dataprotection.nda@nishithdesai.com.

---

[1]As per Section 2(i) of the DPDPA, "data fiduciary" means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data.

[2]Notice on Feedback/Comments on the Draft Rules, available here.

[3]Explanatory Note to the Draft Rules, available here.

[4]Rule 1(2), Draft Rules.

[5]Rule 1(3), Draft Rules.

[6]As per Section 2(j) of the DPDPA, "data principal" means the individual to whom the personal data relates and where such individual is: (i) a child, includes the parents or lawful guardian of such a child; (ii) a person with disability, includes her lawful guardian, acting on her behalf.

[7]Section 5, DPDPA.

[8]Rule 3(a), Draft Rules.

[9]Rule 3(b), Draft Rules.

[10]Rule 3(b)(ii), Draft Rules.

[11]Rule 3(b)(i), Draft Rules.

[12]Rule 3(b)(ii), Draft Rules.

[13]Section 6(1), DPDPA.

[14]Section 5(2)(a), DPDPA.

[15]Section 40(2)(b), DPDPA.

[16]Section 5(3), DPDPA.

[17]Rule 3(c), Draft Rules.

[18]As per Section 2(f), DPDPA, "child" means an individual who has not completed the age of eighteen years.

[19]Rule 10(1)(a), Draft Rules.

[20]Digital Locker is a state-owned cloud service which enables individuals to upload and verify state-issued certificates and ID documents.

[21]Rule 10(1)(b), Draft Rules.

[22]Rule 10(3)(f), Draft Rules.
(f) As per Rule 10(3)(f) of the Draft Rules, "person with disability" shall mean and include—(i) an individual who has long term physical, mental, intellectual or sensory impairment which, in interaction with barriers, hinders her full and effective participation in society equally with others and who, despite being provided adequate and appropriate support, is unable to take legally binding decisions; and (ii) an individual who is suffering from any of the conditions relating to autism, cerebral palsy, mental retardation or a combination of any two or more of such conditions and includes an individual suffering from severe multiple disability.

[23]Rule 10(2). DPDPA.

[24]Section 16, RPWD Act.

[25]Section 9(4) DPDPA read with Rule 11, Draft Rules.

[26]Part A, Row 3, Fourth Schedule, Draft Rules.

[27]Part B, Row 3, Fourth Schedule, Draft Rules.

[28]Part B, Row 5, Fourth Schedule, Draft Rules.

[29]As per Section 2(k) of the DPDPA, "data processor" means any person who processes personal data on behalf of a data fiduciary. Please note that there are no specific compliance requirements for data processors prescribed under the DPDPA and Draft Rules.

[30]Section 8(5), DPDPA.

[31]Rule 6(1), Draft Rules .

[32]Serial No. 1, The Schedule, DPDPA.

[33]Rule 6(1)(a), Draft Rules .

[34]Rule 6(1)(e), Draft Rules .

[35]Rule 6(1)(f), Draft Rules .

[36]Rule 14, Draft Rules.

[37]Section 16(1), DPDPA.

[38]Under Section 16 of DPDPA, the Central Government is authorised to notify specific countries or territories to which transfers of personal data may be restricted.

[39]Rule 12(2), Draft Rules.

[40]Rule 12(3), Draft Rules.

[41]Rule 12(4), Draft Rules.

[42]Rule Section 10(2)(c), DPDPA.

[43]Rule 12(3) of the Draft Rules prescribes an obligation on SDF to observe due diligence to verify that algorithmic software deployed by it for hosting, display, uploading, modification, publishing, transmission, storage, updating or sharing of personal data processed by it are not likely to pose a risk to the rights of data principals.

[44]As per Section 2(g) of the DPDPA, "consent manager" means a person registered with the Board, who acts as a single point of contact to enable a Data Principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform

[45]Sections 6(7), 6(8) and 6(9), DPDPA.

[46]Part A, First Schedule read with Rule 4, Draft Rules .

[47]Paragraph 1, Part A, First Schedule, Draft Rules.

[48]Paragraph 4, Part A, First Schedule, Draft Rules.

[49]Paragraph 2, Part A, First Schedule, Draft Rules.

[50]Paragraph 5, Part A, First Schedule, Draft Rules.

[51]Paragraph 3, Part A, First Schedule, Draft Rules.

[52]Paragraph 6, Part A, First Schedule, Draft Rules.

[53]Paragraph 7, Part A, First Schedule, Draft Rules.

[54]Paragraph 9(a), Part A, First Schedule, Draft Rules.

[55]Paragraph 9(b), Part A, First Schedule, Draft Rules

[56]Paragraph 9(b), Part A, First Schedule, Draft Rules

[57]Paragraph 8, Part B, First Schedule, Draft Rules.

[58]Paragraph 8, Part B, First Schedule, Draft Rules.

[59]Paragraph 9, Part B, First Schedule, Draft Rules.

[60]Paragraph 9, Part B, First Schedule, Draft Rules.

[61]Paragraph 9, Part B, First Schedule, Draft Rules.

[62]Paragraph 11, Part B, First Schedule, Draft Rules.

[63]Paragraph 13, Part B, First Schedule, Draft Rules

[64]Paragraph9(a), Part A, First Schedule, DPDP Rules.

[65]Paragraph9(b), Part A, First Schedule, DPDP Rules.

[66]Paragraph 3, Part B, First Schedule, Draft Rules.

[67]Paragraph 4(c), Part B, First Schedule, Draft Rules

[68]Paragraph12, Part A, First Schedule, Draft Rules

[69]Paragraph 6, Part B, First Schedule, Draft Rules .

[70]Rule 13(3), Draft Rules.

[71]Rule 4(5), Draft Rules .

[72]Section 27(c), DPDPA. Under the DPDPA, different penalties for different types of breaches, in the range of INR 50 Crore (approximately USD 6 million)- INR 250 Crore (approximately USD 30 million).

[73]Illustrations, First Schedule.

[74]Section 11, DPDPA.

[75]Section 12 (1), DPDPA.

[76]Section 14 (1), DPDPA.

[77]Section 13 (1), DPDPA.

[78]Rule 13(1)(a), Draft Rules.

[79]Rule 13(1)(b), Draft Rules.

[80]Rule 13(3), Draft Rules.

[81]Rule 13(3), Draft Rules.

[82]Rule 13(2), Draft Rules.

[83]Section 14 (1), DPDPA.

[84]Rule 13(4), Draft Rules.

[85]Section 8(7)(a), DPDPA.

[86]Rule 8(1), Draft Rules.

[87]Third Schedule, Draft Rules.

[88]Rule 8(2), Draft Rules.

[89]As per Section 2(u) of the DPDPA, "personal data breach" means any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data.

[90]Section 8(6), DPDPA.

[91]Rule 7(1), Draft Rules . As per Rule 7(3), Draft Rules , the term "user account" means an online account that may be registered by the data principal with the data fiduciary such as a profile, page, handle, email address, mobile number and other similar presences through the data principal can access the services offered by the data fiduciary.

[92]Rule 7(1), Draft Rules .

[93]Rule 7(2)(a), Draft Rules .

[94]Rule 7(2)(b), Draft Rules .

[95]Section 70-B, *Information Technology Act, 2000*; *Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013*.

[96]Section 8(9), DPDPA.

[97]Rule 9, Draft Rules.

[98]Rule 3(2), IT Rules..

[99]Section 2(l), DPDPA.

[100]Section 17 (2)(b), DPDPA

[101]Rule 15, Draft Rules.

[102]Section 7(b), DPDPA.

[103]Rule 5(1), Draft Rules.

[104]Second Schedule, Draft Rules.

[105]Paragraph(g). Second Schedule, Draft Rules.

[106]Section 36, DPDPA.

[107]Specifically, such requests may be made by officers and instrumentalities which are notified under Section 17(2) of the DPDPA.

[108]S. No. 1, Seventh Schedule, Draft Rules.

[109]S. No. 2, Seventh Schedule, Draft Rules.

[110]S. No. 3, Seventh Schedule, Draft Rules.

[111]Rule 16, Draft Rules.

[112]Section 27(1), DPDPA.

[113]Section 27(3), DPDPA read with Rule 4(5), Draft Rules.

[114]Rule 21(1), Draft Rules.

[115]Rule 21(2), Draft Rules.

[116]Rule 18 (6), Draft Rules.

[117]Rule 19, Draft Rules.

DISCLAIMER

The contents of this hotline should not be construed as legal opinion. View detailed disclaimer.

This hotline does not constitute a legal opinion and may contain information generated using various artificial intelligence (AI) tools or assistants, including but not limited to our in-house tool, NaiDA. We strive to ensure the highest quality and accuracy of our content and services. Nishith Desai Associates is committed to the responsible use of AI tools, maintaining client confidentiality, and adhering to strict data protection policies to safeguard your information.

This hotline provides general information existing at the time of preparation. The Hotline is intended as a news update and Nishith Desai Associates neither assumes nor accepts any responsibility for any loss arising to any person acting or refraining from acting as a result of any material contained in this Hotline. It is recommended that professional advice be taken based on the specific facts and circumstances. This hotline does not substitute the need to refer to the original pronouncements.

This is not a spam email. You have received this email because you have either requested for it or someone must have suggested your name. Since India has no anti-spamming law, we refer to the US directive, which states that a email cannot be considered spam if it contains the sender's contact information, which this email does. In case this email doesn't concern you, please unsubscribe from mailing list.

NDA Introduction

Research Papers

Opportunities in GIFT City

October 2024

Telemedicine in India

August 2024

Clinical Trials and Biomedical Research in India
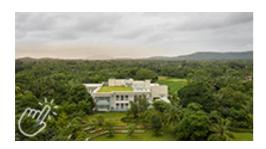
August 2024

Compendium of Research Papers

August 2024

Proud Moments

Chambers and Partners Asia Pacific 2024: Top Tier for Tax, TMT, Employment, Life Sciences, Dispute Resolution, FinTech Legal

Want to work with us?

We aspire to build the next generation of socially-conscious lawyers who strive to make the world a better place.

At NDA, there is always room for the right people! A platform for self-driven intrapreneurs solving complex problems through research, academics, thought leadership and innovation, we are a community of non-hierarchical, non-siloed professionals doing extraordinary work for the world's best clients.

We welcome the industry's best talent - inspired, competent, proactive and research minded- with credentials in Corporate Law (in particular M&A/PE Fund Formation), International Tax , TMT and cross-border dispute resolution.

Write to happiness@nishithdesai.com

To learn more about us Click here.

Legal 500 Asia Pacific 2024: Top Tier for Tax, TMT, Labour & Employment, Life Sciences & Healthcare, Dispute Resolution

Benchmark Litigation Asia Pacific 2024: Top Tier for Tax, Labour & Employment, International Arbitration

AsiaLaw Asia-Pacific 2024: Top Tier for Tax, TMT, Investment Funds, Private Equity, Labour and Employment, Dispute Resolution, Regulatory, Pharma

IFLR1000 2024: Top Tier for M&A and Private Equity

FT Innovative Lawyers Asia Pacific 2019 Awards: NDA ranked 2nd in the Most Innovative Law Firm category (Asia-Pacific Headquartered)

RSG-Financial Times: India's Most Innovative Law Firm 2019, 2017, 2016, 2015, 2014

NDA Hotline

Click here to view Hotline archives.

Nishith TV

March 09, 2024

Sprinting to the Future of Law

Nishith Desai Associates

93-B, Mittal Court, Nariman Point

Mumbai 400021, India

concierge@nishithdesai.com

www.nishithdesai.com