client alert

January 08, 2025

cyril amarchand mangaldas
ahead of the curve

The Draft Digital Personal Data Protection Rules, 2025: A step forward, but some way to go

The Ministry of Electronics and Information Technology (**MEITY**) released the Draft Digital Personal Data Protection Rules, 2025 (**Draft Rules**) under the Digital Personal Data Protection Act, 2023 (**Act**) on January 3, 2025, for public feedback.[1]

These long-awaited Draft Rules have been published in the Official Gazette following much discussion and inter-ministry consultation and are open for public comments until February 18, 2025. The Draft Rules aim to provide the operational framework for implementing India's new general personal data protection regime. It was anticipated (including in our prior analysis of the Act here and here) that the Draft Rules would provide bright line protection, or at least clarity on several matters under the Act. Much like the Act though, the Draft Rules are very brief, and remain a mixed bag. While they address some pain points and provide clarity on certain aspects, they leave several key areas ambiguous, and in some cases, introduce new complexities that could lead to material concerns for stakeholders.

The following is our high-level analysis.

Implementation

The Draft Rules provide welcome clarity on the manner in which they will be implemented. Once finalized, certain parts of the rules (largely, those dealing with the Data Protection Board (**DPB**)) and corresponding parts of the Act, will come into force upon their publication in the Official Gazette.[2]

The rest of the rules are scheduled to come into force on a later date, to be specified in the final rules.[3] This means

that the final rules will provide long awaited clarity on the implementation timeline for the Act. That said, some indication of what this timeline will look like, and whether extensions will be provided for specific types of entities (like SMEs and not-for-profits, which would benefit from staggered implementation), may make consultation around the Draft Rules more effective.

Interestingly, Rule 21, dealing with the Appellate Tribunal (being the Telecom Disputes Settlement and Appellate Tribunal), responsible for hearing appeals against decisions of the DPB, is proposed to come into force as part of this second tranche. If the intention is that the DPB, though constituted, will not take any substantive action until the Appellate Tribunal is operational, this approach requires explicit clarification.

1 The Draft Digital Personal Data Protection Rules, 2025 (**Draft Rules**), available here.
2 Draft Rules, Rule 1(3).
3 Paragraph 1, Explanatory Statement.

Notice and Consent

Under the Act, consent forms the basis for most types of data processing by private entities.[4] It was hoped therefore, that the Draft Rules would expand on how consent should be obtained, recorded, and managed in an efficient and user-friendly manner. While they provide some guidance, they fall well short of achieving that outcome.

Rule 3 deals with notices to data principals and lays down the minimum requirements that such notices must meet to ensure transparency and usability. The term "itemized", deleted from the Act, helpfully finds its way back into the Draft Rules.[5] While Rule 3 is clear that a notice for consent must include itemized descriptions of data being processed, along with products, services or uses enabled by such processing, the language requiring a "specified purpose" has the potential to be read restrictively, and could benefit from simplification.[6] This is more of a pressing concern as the Act defines specified purpose rather generally, and the Draft Rules may intend otherwise.

Rule 3 also reiterates the need for notices to use "clear and plain language",[7] consistent with the Act.[8] A notable addition in the Draft Rules is the requirement for notices to be "presented" independently,[9] which may be read as it being required to be distinct from any other document such as terms of use or privacy policies. As the Draft Rules provide "minimum" details, businesses could very well augment on what is included in the notice, and while doing so, it would be worthwhile to consider the stipulation in Rule 3 that notice must contain a "fair account of the details necessary to enable" specific and informed consent. Given the already high standard for consent under Section 6 of the Act, i.e., free, specific, informed, unconditional and unambiguous consent through with a clear affirmative action[10], the addition of these requirements will only increase complexity.

To mitigate this, it may be helpful if Rule 3(a) is modified in the consultation process to provide more prescriptive and bright line requirements for consent notices including potentially, template, formats.

Consent Managers

Consent Managers, a unique Indian innovation introduced under the Act, are intended to serve as a single point of contact to enable data principals to provide and manage their consents.[11] Rule 4, read with the First Schedule to the Draft Rules, prescribes a fairly detailed and granular regime surrounding their registration, obligations, and accountability. However, some criteria and the decision-making process are likely to have a higher degree of subjectivity.

Both the concept of Consent Managers and the requirements under the First Schedule to the Draft Rules, clearly draw much inspiration from regulations governing account aggregators,[12] which emphasize user-centric control mechanisms. That said, some requirements for Consent Managers present potential challenges.

The Draft Rules are clear that Consent Managers will be, at their core, platforms, which will onboard both data principals and data fiduciaries,[13] facilitating consent management. Importantly, they are required to act in a fiduciary capacity in relation to the data principals,[14] which creates ambiguity. It is unclear whether "fiduciary capacity" would allow Consent Managers to act as independent data fiduciaries, enabling them to undertake processing activities standalone for purposes and using means as determined by them, outside of the consent management functions. The current formulation may require Consent Managers to devise mechanisms that prevent conflicts where they function both as Consent Managers and as data fiduciaries for a particular data principal.

For instance, the obligation under Entry 2 of Part B of the First Schedule to share personal data in a "blind" manner may be potentially onerous, particularly since consent itself may constitute and contain personal data. This is especially problematic given the detailed and itemized notice requirements around consent. Equally burdensome may be the requirement under Entry 4 to store records of consents permitted or denied, for seven years, which seems excessive, especially when compared with the

4 The Digital Personal Data Protection Act, 2023 (**Act**), Section 4(1)(a).
5 Draft Rules, Rule 3(b)(i).
6 Draft Rules, Rule 3(b)(ii).
7 Draft Rules, Rule 3(b).
8 Draft Rules, Rule 3 appears to incorporate large parts of Section 5(1)(i) to (iii) of the Act.
9 Draft Rules, Rule 3(a).
10 Act, Section 6(1).
11 Act, Section 2(g).
12 Master Direction - Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016, available here.
13 Draft Rules, Part B of the First Schedule.
14 Draft Rules, Entry 8, Part B of the First Schedule.

three-year retention period mandated under Rule 8 as detailed below. Similarly, some of the registration criteria, such as "volume of business" being "adequate" or the "general character" of management, including directors and KMPs needing to have "a general reputation and record of fairness and integrity", as well as operations being "in the interests" of data principals,[15] may need refinement. The subjective nature of these criteria could result in inconsistent application, creating potential barriers for smaller organizations or startups. Aligning these standards with established benchmarks, such as "fit and proper" management criteria, could ensure more fairness and predictability in the registration process for an important new class of stakeholders under the Act.

Reasonable Security Safeguards

Under the Act, data fiduciaries are required to maintain reasonable security safeguards to protect personal data.[16] While existing law often used compliance with the ISO 27001 standard to demonstrate reasonableness,[17] the Act leaves "reasonable" undefined, and clarity in terms of how reasonableness will be evaluated, such as in relation to the size of operations, volumes of data processed, and potential risk inherent in processed data sets, would be helpful.

Instead of providing more substance on contours of reasonable safeguards, Rule 6 provides some "minimum" security safeguards, including measures to prevent the breach such as encryption, obfuscation, masking, and access control, as well as measures to identify and address the breach such as logging, detection, and redundancy measures. Logs and data are required to be maintained for one year to enable this. Importantly, the Rule mandates "appropriate" technical and organizational measures to ensure "governance" and requires "appropriate provisions" in contracts with processors passing through such safeguards. However, it stops short of prescribing a template processing agreement, or indeed, recognizing the adequacy of compliance with international standards like ISO.

It may be relevant to note here that sectoral regulations like SEBI's Cybersecurity and Cyber Resilience Framework for SEBI Regulated Entities (**CSCRF**) clearly recognize this adequacy, and require certification with them.[18] Consequently, and given that ISO 27001 sufficed as deemed compliance under existing law,[19] audit and certification for compliance with international standards may end up becoming a *de-facto* standard.

15 Draft Rules, Part A, First Schedule.
16 Act, Section 8(1)(5).
17 The Information Technology (Reasonable Security Practices and Procures and Sensitive Personal Data or Information) Rules, 2011 (**SPDI Rules**), Rules 8(2) and 8(4).
18 Cybersecurity and Cyber Resilience Framework for SEBI Regulated Entities, August 20, 2024, Section 4, Circular No. SEBI/HO/ITD-1/ITD_CSC_EXT/P/CIR/2024/113, available here.
19 SPDI Rules, Rules 8(2) and 8(4).

Recommending suitable standards (which may of course, be overridden by sector-specific regulations) and explicitly recognizing well-known privacy-preserving measures like de-identification and anonymization, could lead to broader adoption and consistency as the Act is rolled out.

Breach Notification

Again, India is a global outlier in requiring all data breaches to be notified to affected data principals, regardless of the harm and materiality of the breach. While it was anticipated that this requirement would be mitigated under the Draft Rules, perhaps through the modality of seeking an exemption from the DPB, Rule 7 only expands upon the existing requirements, making them more complex.

At the outset, it requires that data fiduciaries notify, to the best of their knowledge and without delay, all data breaches to each affected data principal, including providing them various details of the breach through their user account or other means registered with them.[20] Issues of inevitable notice fatigue aside, some of the details required, such as the impact of the breach and mitigating measures, are typically almost never available in the immediate aftermath of the breach. Additionally, data fiduciaries have the absolute obligation to notify the DPB of the nature, extent, timing and location of occurrence and the likely impact of each breach without delay.[21]

Further, within 72 hours of becoming aware of the breach (which period must now be considered while interpreting the term "without delay") a further report containing details such as findings in relation to the person causing the breach, needs to be provided to the DPB. It may still be possible to notify users based on available information, while seeking extensions from the DPB for phased reporting. Allowing breach notifications to proceed in stages, with updates provided to both users and the DPB as more details are uncovered, may make these breach notification requirements more palatable and practical.

Additionally, it was expected that the Draft Rules would provide necessary clarity regarding the dual reporting mechanism created by the Act, requiring data fiduciaries to now report data breaches under the Act (which includes reporting to data principals and the DPB) as well as to the Indian Computer Emergency Response Team (**CERT-In**) under the Directions issued by CERT-In on April 28, 2022.[22] However, no such clarity has been provided, and data fiduciaries must now factor in reporting to multiple stakeholders into their information security policies and procedures, to avoid significant penalties.

Data Retention

Under the Act, data fiduciaries are required to erase personal data, upon the earlier of the relevant data principal withdrawing consent, or when it can be reasonably assumed that the specified purpose is no longer being served, i.e. where the data principal does not seek performance of the specified purpose or exercise any rights in relation to the relevant processing.

Rule 8, read with the Third Schedule to the Draft Rules, specifies a timeframe for certain entities to erase data, unless retention is mandated by law. While both the Act and Rule 8 contemplate that retention periods will be carefully specified for specific purposes, the Third Schedule to the Draft Rules take a contrary approach. Specified entities, namely, e-commerce entities[23] and social media intermediaries[24] (each with over 20 million registered users in India) and online gaming intermediaries[25] (with over 5 million registered users in India) are required to delete personal data that they process for all purposes within three years from the date the data principal last

20 Draft Rules, Rule 7(1).
21 Draft Rules, Rule 7(1)(a).

22 Directions issued by CERT-In 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, Circular No. 20(3)/2022-CERT-In, available here.
23 Draft Rules, Third Schedule defines an 'e-commerce entity' as "any person who owns, operates or manages a digital facility or platform for e-commerce as defined in the Consumer Protection Act, 2019 (35 of 2019), but does not include a seller offering her goods or services for sale on a marketplace e-commerce entity as defined in the said Act".
24 Draft Rules, Third Schedule defines a "social media intermediary" as "an intermediary as defined in the Information Technology Act, 2000 (21 of 2000) who primarily or solely enables online interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using her services".
25 Draft Rules, Third Schedule defines an "online gaming intermediary" as "any intermediary who enables the users of its computer resource to access one or more online games".

seeks performance of the specified purpose, or to exercise rights. The only purpose excluded from this requirement, is enabling access to old user accounts or stored value which can be used against products and services.

While the prescribed thresholds are admittedly high, and the exceptions prescribed are essential, the approach in the Third Schedule risks challenges on grounds of arbitrary classification by selective application and absence of uniform retention standards, i.e.,:

a. specifying mandatory periods for one set of entities (admittedly, already classified distinctly under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021), while ignoring others (non-social media intermediaries, sellers, retailers, etc.) who may be similarly situated; and

b. specifying mandatory periods for all purposes of processing by such entities, rather than following a nuanced approach. For instance, it could be argued that processing of employee data by the listed entities should not be treated differently from its processing by other entities.

Children and Exclusions

Section 9 of the Act, as analyzed previously here, requires data fiduciaries to obtain verifiable parental consent before processing the data of persons under the age of eighteen. This provision also imposes limitations on tracking or behavioral monitoring in relation to them. The creation of means to allow exceptions to these limitations is a welcome move, addressing practical challenges faced by entities dealing with children's data.

With one in three internet users globally being under the age of eighteen,[26] structuring these exceptions judiciously, while enabling a practical mechanism for recordal of verifiable parental consent, was a key outcome hoped for from the Draft Rules. Rule 11, read with the Fourth Schedule to the Draft Rules, provides for these long awaited (albeit debatable) exceptions.

Part A of the Schedule provides exclusions for specific categories of data fiduciaries, including healthcare providers, educational institutions, creches and providers of transport to children. These exemptions are tightly defined, allowing processing (and in the case of educational institutions and creches, tracking and monitoring), for specific narrowly defined purposes.

On the other hand, Part B of the Fourth Schedule prescribes much more wide-ranging exceptions ranging from the discharge of duties or performance of functions in the interests of a child under any law, provision of benefits, creation of user accounts, restricting access to harmful information, confirming that a data principal is not a child, and ensuring that individuals providing consent, are indeed identifiable adults.

These exclusions, which may be expanded in the consultation process, seem to address the several key needs of platforms which engage with children.

Verifiable Parental Consent

In contrast with the nuanced approach above, Rule 10, which deals with the manner of recording verifiable parental consent, seems somewhat more prescriptive and rigid. Broadly, it requires that before engaging with a person under the age of eighteen, data fiduciaries must:

a. ensure that it has recorded verifiable parental consent, on the basis of "reliable" details available with it; or

b. ensure that the person recording such consent is an identifiable adult, basis proofs of age and identity submitted by the purported parent, as issued by entity authorized under law to do so, including as verified by a Digital Locker service provider.[27]

It also requires entities to maintain suitable technical and organizational measures to enable the above but stops short of mandating a specific age gating mechanism. While these requirements seem conceptually sound, the accompanying illustrations indicate that the above consent recordal may occur most smoothly when both parents and children are digitally literate, and users can either engage directly with the relevant platform or utilize tools like DigiLocker to provide a valid identity document.

Given that platforms may, in effect, be restricted from engaging with persons under the age of eighteen until they

26 UNICEF, Child Rights and Responsible Technology, available here.

27 Please see: DigiLocker:Signin Signup (digitallocker.gov.in) and The Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016.

record valid consent, introducing transitional provisions could be crucial. Allowing for the continued provision of essential services and the retention of legacy data during this interim period would greatly assist in ensuring seamless compliance and minimizing service disruptions.

Significant Data Fiduciaries

The Act imposes material additional obligations in relation for Significant Data Fiduciaries (**SDFs**), which are to be identified individually, or as a class under the Act.[28] While the criteria and timeline for such notifications remains vague, Item 3 of the Seventh Schedule portends that MEITY will designate officers responsible for identifying SDFs. These officers will have the ability to seek necessary information to make their determination.

Further, the Draft Rules clearly specify periodic impact assessments and audits for SDFs, and potentially dispense with the need to use CERT-In empaneled auditors. Results from audits are required to be submitted to the DPB by auditors. Ensuring that these are handled confidentially, and sensitively by the DPB, would help drive compliance here.

Localization, AI, and Access

By providing for a notified "black list" of territories under Section 16(1) of the Act, and removing any additional obligations in relation to "automated processing", the Act had taken a widely praised (including by us here) pro-innovation approach to regulating cross-border data transfers and AI use.

Some of this good work risks being undone if Rule 12(3), which requires additional "due diligence" for "algorithmic software" deployed by it to ensure it does not pose a "risk" to rights of data principals, is notified. In a world where algorithms (including old fashioned non-learning algorithms) are widely used to determine a broad spectrum of matters, including underwriting premiums and loan eligibility, this may prove very difficult indeed. It will also be interesting to see (given that the Rule sits within the Act) how violations will be penalized where an algorithm poses a risk to a right which is not related to personal data.

Rule 12(4) and Rule 14 revive concerns around data localization, with the former empowering the central government to impose restrictions on cross-border transfers of specified types of personal data by SDFs, and the latter providing for measures to ensure data is not made available to a foreign state or entity controlled by such foreign state. Further, it is unclear whether surveillance legislation (or practices) in a foreign state will result in data being considered as being "available" to such foreign state (or its agency).

While data localization itself is increasingly prevalent in India, with the most recent iteration being specified by SEBI under the CSCRF,[29] the Draft Rules appear open-ended, allowing sudden restrictions for certain types of data, or types of transfers. A more sustainable approach here may be the one originally contemplated under Section 16(2) of the Act and to use sector specific regulations (which will typically define special category data) to override the general permission for cross border transfers.

The Draft Rules also envisage an expansion of the general power under Section 36 of the Act through the proposed Rule 22 read with the Seventh Schedule to the Draft Rules. While instrumentalities having the ability to seek access to data in the interest of sovereignty and integrity is not uncommon, the breadth of Item 1 of the Seventh Schedule (combined with the ability to direct that access be kept confidential and the absence of a clear appeal procedure) portends both potential constitutional challenges and

28 Act, Section 10.

29 The CSCRF provides that Regulatory Data (as defined therein) will be stored "within the legal boundaries of India".

complexities in enabling cross-border transfers under the Schrems II standard.[30] These concerns are magnified in the context of Items 2 and 3 of the Seventh Schedule, where the potential for broader access requests amplifies concerns around scope and implementation.

While the need for some of the above powers is understandable in the current geopolitical and strategic context, and some consultation appears to have taken place on these Draft Rules, one hopes that these powers are refined during the consultation process to ensure more predictability in their invocation, and that in practice, this "stick" will be used lightly and with great caution.

Conclusion

Overall, while the Draft Rules represent a significant step forward towards implementing the Act, refining, and clarifying these aspects would help preserve the spirit of the Act, and create a robust, sustainable framework for its enforcement. The consultation window and timeline leading up to implementation of the seminal law is a critical phase for businesses to participate in the consultation process, alongside meticulously analyzing the different prescriptions, tallying them with existing processes in place, identifying gaps, and making progress towards compliance.

30 Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems (C-311/18) (the Schrems II case), Court of Justice of the European Union (CJEU), July 16, 2020.

Key contacts

Cyril Shroff
Managing Partner
cyril.shroff@cyrilshroff.com

Arun Prabhu
Partner (Head - Technology)
arun.prabhu@cyrilshroff.com

Arjun Goswami
Director - Public Policy
arjun.goswami@cyrilshroff.com

Arya Tripathy
Partner
arya.tripathy@cyrilshroff.com

Lakshmi Rajagopalan
Partner
lakshmi.rajagopalan@cyrilshroff.com

Disclaimer

All information given in this alert has been compiled from credible, reliable sources. Although reasonable care has been taken to ensure that the information contained in this alert is true and accurate, such information is provided 'as is', without any warranty, express or implied as to the accuracy or completeness of any such information.

Cyril Amarchand Mangaldas shall not be liable for any losses incurred by any person from any use of this publication or its contents. This alert does not constitute legal or any other form of advice from Cyril Amarchand Mangaldas.

Should you have any queries in relation to the alert or on other areas of law, please feel free to contact us on cam.publications@cyrilshroff.com

2025 © Cyril Amarchand Mangaldas