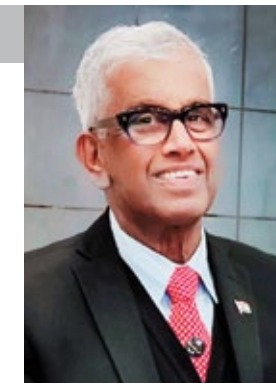
TV RAMACHANDRAN



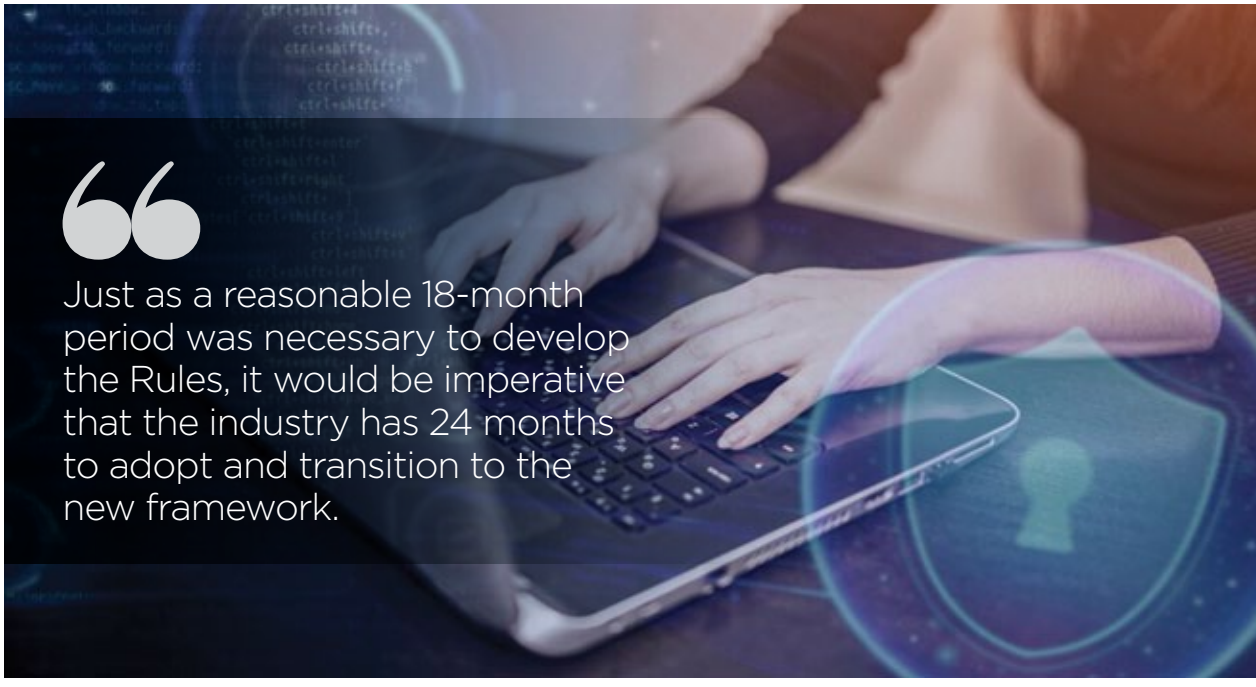
INDIA'S ODYSSEY TO A ROBUST PERSONAL DATA PROTECTION REGIME

India's Digital Personal Data Protection Act marks a pivotal moment in digital governance, setting the stage for comprehensive data privacy and security frameworks.

The creation of the first-ever Digital Personal Data Protection Act (DPDP Act) was a historic milestone in the annals of India's digital progress. Following this notification on 11 August 2023, India's Ministry of Electronics and IT (MeitY) launched a marathon Odyssey to discover and develop the optimum rules to implement the Act effectively.

The Odyssey sailed through nine stakeholder consultations across major cities, including Delhi, Bengaluru, Mumbai, Hyderabad and Chennai. The eventful voyage, lasting close to 18 months of intensive discussions and consultations, resulted in the release of comprehensive DPDP Rules on 3 January 2025. The MeitY sought responses and feedback from stakeholders till 18 February. When refined and finalised based on stakeholder comments, these rules can be a big march forward in the alignment of India's data protection framework with global best practices.

The Rules appear to strike a commendable balance between regulation and innovation while prioritising the privacy of Indian citizens. The primary objective of India's data protection law is to safeguard personal data, establishing clear obligations for data fiduciaries, rights for data principals, provisions for verifiable children's consent, exemptions, and guidelines for cross-border data flows.



> Concerns around data localisation under Rule 12(4) could disrupt cross-border data flows, impacting businesses and the broader digital economy in India.

India's data protection framework presents a unique opportunity to establish a robust, citizen-centric digital ecosystem. With that in mind, further refinement of the rules, focusing on clarity and minimising ambiguities, would be beneficial in a few areas.

NEED FOR A PHASED IMPLEMENTATION

Just as a reasonable 18-month engagement period was necessary to develop the Rules, it would be extremely important that the industry gets 24 months to adopt and transition to the new framework. This timeframe would allow all small, medium, or large organisations to develop and deploy crucial technical infrastructure, including robust, verifiable parental consent mechanisms and consent manager systems.

This view is consistent with global best practices, which provide compliance windows ranging from 12 to 24 months, demonstrating the necessity of adequate preparation time. For instance, in 2016, the European Union adopted the General Data Protection Regulation (GDPR); however, member states had two years to ensure that it was fully implementable in their countries (until May 2018).

Similarly, Malaysia's Personal Data Protection (Amendment) Act, which officially came into operation in 2025, will not be implemented immediately. Instead, it will be rolled out in three stages. In India, too, the great benefits that could potentially flow from the Act and the Rules could remain a mere potential and not be realised if adequate time is not given to effect a smooth and complete transition to the new regime.

Secondly, it is noted that, under Rule 7 concerning intimation of personal data breach, the Data Fiduciary—the company or business handling the personal data of the data subject—must promptly notify each affected Data Principal of the violation and notify the Board with specific requirements. While support for data principals' right to know about data breaches as prescribed under Rule 7 is well accepted, it is, however, felt by experts that mandatory notification for every violation, regardless of impact, may lead to unnecessary confusion and overwhelm the Data Protection Board.

Instead, a more practical approach would be to limit notification to breaches that pose a real risk of significant harm, aligning with global practices in other jurisdictions. For instance, Japan mandates notification only for breaches likely to harm rights or interests, with waivers for impractical individual notifications.

Similarly, Singapore requires notification after regulatory reporting but allows exemptions when actions to prevent significant harm have been taken or prior technological measures have mitigated risk. India could benefit significantly from reconsidering Draft Rule 7 to align it with such good practices.

Thirdly, while Rule 10, which focuses on 'verifiable consent for processing personal data of a child or person with disability who has a lawful guardian', is commendable, it might be better to provide clear options for verifiable parental consent without being overly prescriptive. To enhance clarity, Rule 10(1) could be segmented into three distinct categories: (a) reliable details of identity and age available with the Data Fiduciary; (b) a virtual token mapped to the same, issued by an entity entrusted by law; and (c) details or token verified and made available by a Digital Locker service provider.

REFINING THE RULES FOR BETTER CLARITY AND IMPLEMENTATION

The government is already working on safeguards to protect customers. Such a categorisation would provide a more structured and easily navigable framework for data fiduciaries. Additionally, the draft rules could benefit from guidance on what constitutes "reliable" identity and age verification, while adhering to the principle of data minimisation. This definition could clarify acceptable elements such as the parent's name, age, email, or phone number previously provided.

Understandably, Rule 10 is proposed to apply only when a lawful guardian proactively approaches a Data Fiduciary. However, the current provision's process could

> The DPDP Act establishes a clear framework to protect personal data, ensure privacy, and foster innovation across India's digital ecosystem.

pose practical and operational challenges and ultimately impact vulnerable citizens. Clear guidelines on verification elements and the application of the rule would facilitate smoother implementation and help maintain a balanced approach to data protection for children and PWDs.

Another significant point of concern among stakeholders has been on the perceived "return" of data localisation through Rule 12(4), which outlines specific obligations for "significant" Data Fiduciaries. While the DPDPA 2023 generally allows for cross-border data flows, the provisions within Rule 12(4), particularly the establishment of a government-appointed committee, have raised apprehensions particularly since the government had earlier provided clarifications that its "...intent is not to disrupt cross-border data flows but to address specific sectoral requirements where localisation is necessary for citizen safety".

Hence, the provision raises concerns, particularly related to the uncertainty regarding international data transfers, which could impact the operations of Data Fiduciaries, limit exports, increase cybersecurity risks, and create other operational difficulties for India-based businesses. If not suitably clarified, the unintended effects of this draft rule could result in significant economic harm to the digital economy.

Data localisation in India should be promoted, incentivised, or encouraged. However, it should not be mandated at this stage, given the logistical constraints associated with increased creation of data centres, viz., availability of power, land, water, and computing capabilities and costs. Also, since the parent DPDPA legislation and the government's intention are pretty clear on cross-border data flows and other sectoral regulations by RBI, SEBI, and IRDAI have mandated localisation only for certain kinds of data, Rule 12(4) may need to be reviewed.

BALANCING DATA LOCALISATION WITH CROSS-BORDER DATA FLOWS

Let us now discuss Rule 22, which requires 'Calling for Information from Data Fiduciary or Intermediary' by statutory or government agencies. Given that similar provisions also exist in some other relevant applicable laws, such as the Information Technology Act and the Rules thereunder, the Bhartiya Nagarik Suraksha Sanhita, and the Indian Telecommunications Act and Rules thereunder, it may be beneficial for the sake of uniformity, in terms of clarity and applicability, to appropriately use additional language (from the quoted laws) here.

Another suggestion is that even if the language of the draft rule is retained, a few other safeguards could be considered to be added, including (a) mentioning the specific purpose for which information is collected from the Data Fiduciary; (b) applicability of necessity and Proportionality principle; and (c) considerations around proprietary data and safeguards to prevent unauthorised disclosure.

India is already the largest data-consuming democracy in the world, with strong ambitions of expeditiously growing to be a largely self-reliant and fully developed advanced digital economy. Moreover, the country is likely to register a multiple-fold growth in per capita data consumption since India is currently making a massive thrust for the proliferation of fibre-based fixed broadband.

The global finding is that the latter averages at least 257 GB per capita data (ITU,2022), while the USA has already touched 698 GB per capita and Europe over 500 GB. India is bound to match or exceed these leers. The government's current actions for safeguarding personal data through the DPDP Act and the Rules, which are currently being finalised, are both timely and praiseworthy. In this last mile of the Odyssey, there are some critical opportunities for finetuning the course so that we finish with complete success.

It is also hoped that the government will put in the final touches to complete the rules with a flourish and make them great for India and possibly a fine benchmark for many other countries.

The author is Hon. FIET (London) and President of BIF.
The views are personal.
Research inputs by Mira Swaminathan.
feedbackvnd@cybermedia.co.in