Quote by Devroop Dhar, Co-founder & Managing Director, Primus Partners

Published in ForbesIndia
Jan 14, 2025

Digital Data Protection Rules 2025: Here's what needs to change

Despite the sixteen-and-a-half-month wait for these rules, experts have criticised the rules for being vague and lacking clarity

Authored by Naini Thaker

These draft rules "seek to protect citizens' rights in accordance with the DPDP Act, while achieving the right balance between regulation and innovation, so that the benefits of India's growing innovation ecosystem are available to all citizens and India's digital economy Image: Shutterstock

Read on: https://www.forbesindia.com/article/take-one-big-story-of-the-day/digital-data-protection-rules-2025-heres-what-needs-to-change/95059/1

Article Content:

January 3, the Ministry of Electronics and Information Technology (MeitY) published the long-awaited Draft Digital Personal Data Protection Rules, 2025. These rules were eagerly anticipated since the Digital Personal Data Protection Act, 2023, was passed in the Parliament on August 11, 2023. According to news reports, the Minister for Electronics and Information Technology Ashwini Vaishnaw is scheduled to meet industry stakeholders to seek feedback today.

These draft rules “seek to protect citizens’ rights in accordance with the DPDP Act, while achieving the right balance between regulation and innovation, so that the benefits of India’s growing innovation ecosystem are available to all citizens and India’s digital economy”, stated the Press Information Bureau press release.

They provide some clarity on, among others, how data fiduciaries should comply with certain requirements, registration and obligations of consent managers, processing of personal data by the state for subsidies, personal data breaches, details of the data retention period by data fiduciaries amongst others.

One of the more important inclusions is the creation of the Data Protection Board (DPB), an adjudicatory independent body that facilitates complaints resolution and thereby enhances transparency and accountability. “This measure can be used to ensure data privacy has a magnified approach where each case is treated independently,” explains Shravishtha Ajaykumar, associate fellow, Centre for Security, Strategy and Technology, Observer Research Foundation (ORF). The government is now inviting feedback on the draft rules, with a deadline set for February 18, 2025.

Ironically, there is no mention of the word ‘privacy’ in the Draft Digital Personal Data Protection Rules or The Digital Personal Data Protection Act, 2023, published in The Gazette of India. “In fact, the word ‘privacy’ appeared only once in the Digital Personal Data Protection Bill, 2023... which is also where it’s repealing a section of the Right to Information Act,” says Prateek Waghre, technology policy researcher.

Despite the sixteen-and-a-half-month wait for these rules, experts have criticised the rules for being “vague” and “lacking clarity”.

“The Digital Personal Data Protection Act, 2023, had a lot of shortcomings,” explains Waghre. The Draft Digital Personal Data Protection Rules are the mechanism to enforce the provisions of the DPDP Act, 2023. “We have seen the trend continue, and there are a lot of things that were in the Act, that have remained a question mark in the rules. So, it hasn’t succeeded in clarifying a lot of things,” he adds.

However, in a recent interview with CNBC TV18, Ashwini Vaishnaw, the minister for MeitY, clarified that this approach was intentional. “We have made sure that the rules are not very prescriptive, because digital technology doesn’t stand.... it evolves every week. Every week a new thing happens, so the law should be able to catch up with those developments,” he said. Vaishnaw is confident that, with these draft rules, we have a good framework that continues to encourage innovation. He said, “We understand, from whatever we have heard from our international counterparts, along with the compliance burden, which happened in Europe and damaged the innovation ecosystem in a very big way... that will not happen—our innovation ecosystem will continue to grow with the proper legal framework.”

However, industry stakeholders believe there are some areas that need further clarification and deliberation.

Data Localisation

The Draft DPDP rules indicate that there will be categories of data for which it is mandatory to process and store in India and where transfer outside India is only permissible under certain conditions.

“Larger companies have made efforts on both ends to ensure data can be localised without sharing data with the government and to allow cross-border data and easy flow of data. The rules currently mandate a government prerogative on which data can cross borders,” states Ajaykumar. The rules do not contain an absolute prohibition of data transfer, and there is still room for some discretion by the government.

The objective of data localisation is to provide the Indian government with more control over Indian citizens’ private data, enhance national security protections, “and provide accountability for the use of Indian citizens’ data by foreign entities. However, this does not address the question of government access and how certain companies may not want to share data with the Indian government. There is a risk of losing international business, similar to what happened with MasterCard here, if not adequately addressed,” she explains. Mastercard was barred from onboarding new customers in July 2021 for failing to comply with RBI’s data localisation norms issued in April 2018. This led to Mastercard losing a lot of business, and many banks including RBL Bank and Yes Bank—that earlier relied only on Mastercard—shifted to rival Visa.
However, this might lead to both opportunities and challenges for the data centre business in India. First, an increase in demand for local data storage, might lead to a substantial expansion of the data centre industry in India. However, reckons Ajaykumar, “scaling the infrastructure to cope with this demand has its cost in the form of investment in data centre infrastructure, security, ongoing maintenance, even climate impact and water access”.

Data Breaches
Rule 7 of the draft rules addresses the notification of personal data breaches—’without delay, a description of the breach, including its nature, extent, timing and location of occurrence and the likely impact’ are to be notified, within ‘seventy-two hours of becoming aware of the same.’
“It is yet to be seen how companies will implement mechanisms to comply with some of the more impractical aspects such as the 72-hour timeline to provide detailed breach-related information to the DPB; and data localisation obligations,” says Probir Roy Chowdhury, partner, JSA Advocates & Solicitors.

“The proposed timelines for a data breach notification are similar to what other prominent data privacy laws such as GDPR have. The only way to adhere to such a timeline is to have a robust data breach notification procedure in place which can be integrated with your security operation control management system and data loss prevention techniques,” says Vikas Bansal, partner, IT risk advisory and assurance, BDO India.

Hence, a better way to go about it would be establishing a one-stop reporting portal. “Instead of requiring companies to notify multiple entities—such as CERT-In, the Data Protection Board, financial regulators, stock exchanges, and data subjects—a unified reporting mechanism could streamline and centralise the process. This approach would minimise administrative burdens and enable companies to concentrate on effectively mitigating the breach,” explains Devroop Dhar, co-founder & managing director, Primus Partners.

Additionally, implementing Harm-Based Reporting Thresholds—where only breaches with the potential to cause significant harm to individuals or systems are reported—would help avoid overwhelming regulators with minor incidents. “This approach ensures that regulatory resources are directed toward serious breaches while upholding the principles of data protection,” adds Dhar.

Parental Consent

The draft rules state specify that parent's verifiable consent will have to be obtained by social media or online platforms before children can create any account. It states: “A Data Fiduciary shall adopt appropriate technical and organisational measures to ensure that verifiable consent of the parent is obtained before the processing of any personal data of a child...” This, as per experts needs a lot more clarity.

“The challenge with this clause, is you could create a situation where you could age-gate the entire internet. What is the only effective way of verifying that someone is a minor or not? To do that you have to verify someone who isn't a child, which means you have to do this to everyone. There is still a lack of clarity on such clauses,” explains Waghre.

Additionally, parents' identity and age will also have to be validated and verified through voluntarily provided identity proof "issued by an entity entrusted by law or the Government", as per the draft rules. Entities will be able to use and process personal data only if individuals have given their consent to consent managers, which will be entities entrusted to manage records of consents of people.

Here, experts foresee that businesses are likely to face complex challenges in managing consents. “Maintaining consent artefacts and offering the option to withdraw consent for specific purposes could necessitate changes at the design and architecture level of applications and platforms. Further, organisations will need to invest in both technical infrastructure and processes to meet these requirements effectively,” says Mayuran Palanisamy, partner, Deloitte India. This includes relooking into data collection practices, implementing consent management systems, establishing clear data lifecycle protocols and actually percolating down these practices at an implementation level.

Lastly, says Shruti Aggarwal, co-founder, Stashfin, “the algorithmic accountability for organisations (deemed to be significant data fiduciaries) and using AI-based systems must be more precise since, in its current form, it’s too broad.” As per the current rules, there is no mention of what happens to the data that is used for training AI models. Says Ajaykumar, “Limitation on data access may restrict the classes of data that might be needed for AI model training or machine learning, hence hampering the pace of data-driven innovation.”