PRIMUS PARTNERS®

Quote By Devroop Dhar- Co-Founder & Managing Director, Primus Partners

Published in Tech Circle
Jan 08, 2025

DPDPA draft rules bring new data localisation mandates, challenges for businesses

Authored by Shraddha Goled

Read on: https://www.techcircle.in/2025/01/08/dpdpa-draft-rules-bring-new-data-localisation-mandates-challenges-for-businesses

Article Content:

India's data localization requirements have again emerged as a pivotal discussion point for businesses. With the draft rules under the Digital Personal Data Protection Act (DPDPA) raising fresh complexities, companies are now expected to reevaluate their compliance strategies.

The DPDPA draft rules released on January 3 aim to provide clear information about how citizens' personal data is processed while offering them avenues to demand data erasures, appoint digital nominees, and access mechanisms to manage their data. The Ministry of Electronics and Information Technology (MeitY) has invited feedback from the public and stakeholders till February 18.

At the time DPDPA was first introduced in August 2023, it laid down restrictions for the cross-border transfer of data by a fiduciary through a whitelist-blacklist approach. It meant that cross-border personal data transfer would be allowed, except for countries restricted by the government.

The draft rules released last week, however, introduce a layered approach regulating cross-border data transfers. These rules empower the government-appointed committee to impose specific conditions on data being made available to foreign states or entities under their control, creating a dual-layered regulatory framework. Experts believe that this approach may add extra burden due to conflict with the regulatory obligations of other countries.

Additionally, the rules outline a new guideline for significant data fiduciaries (SDFs), subjecting them to restrictions on the personal data and traffic data of its flow to not be transferred outside India, based on the above-mentioned committee's recommendations, as applicable. This is new addition, which was not earlier outlined when DPDPA was introduced.

Shreya Suri, Partner with the TMT practice of IndusLaw, said that while the government has outlined its prerogative to impose additional obligations on SDFs, a key challenge lies in identifying who qualifies as such. "Many businesses, especially those working with clients

across various sectors, face uncertainty about whether they will be classified as SDFs. For some, this classification is expected, while others remain unsure." Additionally, Suri said that instead of broad prohibitions, the government should list specific use cases or classes of fiduciaries requiring localisation.

Echoing Suri's remarks, Rakesh Maheshwari, former senior director and group co-ordinator, Cyber Laws and Data Governance, MeitY, said that until the final guidelines are issued the distinction between data fiduciaries and SDFs will remain unclear. "Any mandate of this nature must be clarified as soon as possible, ensuring that entities identified as significant data fiduciaries have adequate time to prepare and implement the necessary measures."

Rakesh Maheshwari, former senior director and group coordinator for Cyber Laws and Data Governance at MeitY, explained that the rule regarding the retention period of consent hints at which entities might qualify as Significant Data Fiduciaries (SDFs).

He added that Rule 22 allows MeitY to request additional information to declare SDFs. This raises two key points: first, the government can notify SDFs before Rule 22 is fully operational; and second, Rule 22 may be necessary to identify and declare new SDFs in the future.

"These aspects highlight two critical issues. The first set of SDFs or classes of SDFs should be declared as soon as possible, allowing them sufficient time to prepare for the additional obligations applicable to SDFs. Secondly, for those Data Fiduciaries declared as SDFs after Rule 22 becomes operational, they must be given reasonable time to comply with the additional obligations. However, the current rules do not address this requirement, leaving a gap in the framework," he said.

Sector-based mandates

Notably, in media interactions following the release of draft rules, IT minister Ashwini Vaishanw has said that the suggested committee-based recommendations are not intended to disrupt cross-border data flow but to deal with specific sectoral requirements. This committee is expected to act as a central body to evaluate localisation needs raised by sectoral ministries.

Probir Roy Chowdhury, Partner at JSA Advocates & Solicitors, said that instead of relying on a new committee to set these requirements, it would be more practical to align with existing laws and regulations. He quotes existing sector-specific guidelines, such as the Reserve Bank of India (RBI) mandated localization for payment data. "Introducing specific data localisation obligations on SDFs through additional regulations seems redundant and unnecessary," he said.

How will it affect businesses

Experts said that the government's stance on localisation has been progressively clear in recent years. However, the new rules bring a somewhat unexpected shift in what appears to be a stricter approach even though it technically still remains within the scope of the Act, say experts.

The proposed data localisation for SDFs under the draft rules is a surprising development and may not have been foreseeable from the Act last year. It will likely spark discussions on its implications for global businesses, said Aaron Kamath, Leader, Commercial and Technology Practice, Nishith Desai Associates.

That said, Kamath feels that the rules at large may be accepted by the industry with limited feedback on a few concerns. "We've come a long way from detailed and stringent 2018 and 2019 Bills which took inspiration from GDPR and had around 100 provisions, to the detailed 2021 draft from the joint-parliamentary committee—all of which faced industry pushback. In

contrast, the current framework, including last year's Act and the draft rules, is much simpler and gives some flexibility to businesses in undertaking operational compliance."

"In terms of impact, DPDPA rules are likely to affect industries that handle large volumes of personal data or rely heavily on cross-border data transfers," added Devroop Dhar, Co-Founder & Managing Director, of Primus Partners.

Outlining specific sectors, Dhar said firms working with technology, IT services, and cloud computing may face challenges adapting to localisation mandates, while financial services and banks, already under RBI's rules, must align with additional requirements. Healthcare and pharma companies involved in clinical trials may struggle with international data sharing. Further, e-commerce and retail businesses relying on foreign payment gateways and CRM systems might need to revise strategies, and media platforms hosting user content may require local infrastructure. Telecom companies, managing vast personal data, will also need to adjust practices to meet the new draft norms, he said.