NUS National University of Singapore | ISAS Institute of South Asian Studies

ISAS Brief
No. 1198 – 27 January 2025

India's New Data Protection Regime

Karthik Nachiappan

Summary

The rules for India's 2023 data protection law have been formally released, creating a data protection regime in India.

India's new data protection law, the 2023 Digital Personal Data Protection (DPDP) Act, will come into force. While the law was passed in 2023, the government has fleshed out the rules for compliance and implementation. The draft rules, specifically 22 provisions, will effectively operationalise the 2023 DPDP Act. The rules will clarify key aspects of the bill, including consent and how it is obtained, security safeguards and protections, provisions to handle personal data breaches and how data can be transferred abroad. What provisions matter for domestic and foreign entities regarding data protection and management? And what does the new law tell us about how India has opted to govern data?

First, the DPDP Act does not impose unconditional data localisation requirements. Instead, localisation is a condition with the government relying on a 'blacklisting' approach to determine data flows between India and other jurisdictions. The government will specify, demarcate and restrict data flows between borders, depending on how Indian data is considered and treated in other jurisdictions. The 'blacklisting' approach differs from the European Union's (EU) General Data Protection Regulation which lays out guidelines for other countries to fulfil to allow for data sharing between EU member countries and others. Unlike the previous interactions of the bill, the DPDP Act also refrains from differentiating between data through subtypes like 'sensitive', 'critical' or 'non-personal'; the law now calls for protection for all personal data. New Delhi retains more power vis-à-vis data protection and flows, opening the door for potential sector-specific guidelines to ensure security. Given security concerns, the government has the right and authority to restrict data transfers to other specified countries. This provision, however, could inject uncertainty and potentially deter investment flowing into India from firms abroad.

Second, the draft rules lay out how the regulator or the Data Protection Board (DPB) will function. This body will be responsible for managing grievances and enforcing compliance. It will have to hold data fiduciaries accountable and ensure all bodies and organisations that deal with personal data manage it effectively. The rules also set out specific rules for data fiduciaries, how they should protect data, consent requirements when collecting and protecting data, and adopting robust security measures to ensure adequate protection. Organisations collecting data are also required to provide clear and transparent guidelines on the processing and storage of personal data. However, it is highly likely data fiduciaries will have to localise certain types of personal data or the retention of data, given security implications. That said, the DPDP rules do reflect a government that is willing to work with other partners and stakeholders instead of solely relying on state intervention to protect and manage data. In this law, both the state, its agencies, entities handling data and citizens

all contribute to ensure data is safe, protected, managed deftly, and deployed for innovation when required. Unlike other data protection regimes globally, the DPDP has sought to provide transparency and clarity to ensure innovation and digital trade are not hampered.

Third, the new rules will likely be onerous for most data fiduciaries, especially small and medium-sized businesses that will face stiff regulatory burdens. For instance, all firms and organisations handling personal data must institute robust measures to eschew data breaches. According to IBM, data breaches cost Indian firms US$2.35 million (S$3.16 million) in 2024; as a result, data protection and compliance become vital for business operations. By not giving such fiduciaries the option to finalise their measures and instead imposing certain rules, the law, however, does place considerable responsibilities on all entities.

Questions also exist on whether the new DPB can handle and manage the litany of data breaches that would ostensibly occur. This scenario could lead to over-reporting to the DPB, potentially saddling it with burdens beyond its capacity. In terms of consent, the new rules include provisions that state the consent requirements underpinning data collection and transfer. Organisations must appoint consent managers to manage the process. That said, questions remain over whether eliciting consent is adequate to safeguard data and privacy given that it will be obtained from different contexts and settings.

The implementation of the DPDP Act 2023 and the release of the draft DPDP rules are a significant juncture for India. Years of discussions, deliberations and negotiations have resulted in the drafting, passing and now executing of this critical task – data protection. India's digital future and transformation possibly hinges on the effectiveness of this execution.

. . . . .

Dr Karthik Nachiappan is a Research Fellow at the Institute of South Asian Studies (ISAS), an autonomous research institute at the National University of Singapore (NUS). He can be contacted at isaskn@nus.edu.sg.
The author bears full responsibility for the facts cited and opinions expressed in this paper.