DENTONS GLOBAL ADVISORS | ASG ALBRIGHT STONEBRIDGE GROUP

ASG Analysis: India's Data Protection Framework Comes Into Focus

December 20, 2021

Key takeaways

- The Joint Parliamentary Committee (JPC) on the 2019 Personal Data Protection Bill (PDP Bill) released its long-anticipated, 543-page report on December 16. As expected, the recommendations set the stage for a far broader and more intrusive regulatory system around data collection, storage, and usage across industries.

- The report recommends more than 90 amendments to the 2019 bill that, in effect, recast the law into an omnibus regulatory structure that applies well beyond issues traditionally viewed as relating to personal data protection. These include content regulation, age verification of social media users, artificial intelligence and algorithmic fairness, non-personal data governance, and media regulation.

- We anticipate the Modi government will aim to be less disruptive in rolling out the PDP Bill than it has been in previous instances, particularly given the government's challenging experience in managing the rollout of the 2021 Information Technology Rules. The JPC recommended, for example, that the implementation period of the PDP regulations be extended to 24 months to allow private corporations and other stakeholders sufficient time to comply with the new requirements.

- There are significant opportunities for key partner and industry stakeholders to engage with the Modi government in the next few months as the PDP Bill is shaped into its final form prior to parliamentary passage.

Key elements

Scope and aim of the PDP Bill: The new report recommends fundamental changes in scope, including: restricting the scope of the 2021 Information Technology (IT) Rules to privacy in the digital space and excluding "digitised data"; subjecting data privacy to the "interests and security of the State"; and extending coverage of the bill to both personal and non-personal data (NPD). The 2019 bill applied to personal data "collected, disclosed, shared, or processed," and the report proposes expanding the scope of the 2021 IT Rules to include "stored" data as well.

Data Protection Authority: The report also proposes expanded central government authority in the decision-making process of the Data Protection Authority (DPA).

It recommends that the central government has significant authority over the DPA's decisions, saying that the DPA should be bound by directions of the central government not only in matters of policy, but in all cases, and that on matters relating to cross-border data transfers, the DPA must consult with the central government.

The report recommends that the DPA be responsible for regulating both personal and non-personal data, reflecting the proposal to expand the scope of the bill.

Data localization: The report reiterates India's commitment to data localization due to both national security concerns and because of the government's duty to safeguard the privacy of its citizens. The report also asserts that no reciprocal treatment should be allowed; that data generated in India must not be regulated by other countries, particularly given national security concerns.

Importantly, the report recommends that the government ensure that all sensitive and critical personal data that is *already* in possession of foreign entities be mirrored in India in a time-bound manner. No clause-by-clause changes are recommended corresponding to this.

The report contains the following broad recommendations to the government, though the roadmap for implementation is unclear:

- The government, in consultation with all sectoral regulators, should prepare an extensive policy on data localization, which includes: developing storage infrastructure for such data; promoting investment, innovation, and fair economic practices; properly taxing data flow; and ensuring compliance efficiency for local business entities and start-ups.
- The government should use revenue generated by localizing data for citizen welfare.
- The government should ensure ease of doing business for companies.
- Any surveillance the government implements on stored data should be based on necessity.

Data breaches: The report defines certain guiding principles to handle data breaches, including that the DPA should ensure citizens' privacy while posting the details of a personal data breach; data fiduciaries should be held responsible for harm suffered by the data principal on account of the delay of reporting of a personal data breach; the DPA should require data fiduciaries to maintain a log of all data breaches.

Social media platforms: The report represents a hard-line position on social media platforms, and recommends that there be specific sectoral regulations to regulate social media platforms, in addition to a unified statutory regulator to regulate all types of media.

The report states that the 2019 bill's classification of social media platforms as "intermediaries" is a misnomer, since these platforms actually act as publishers. The report makes the case that these platforms select the receiver of the content, as well as control access to content posted on their platforms. The report proposes that platforms should:

- Mandate account verification;
- Be held responsible for unverified content on their platforms; and
- Set up local offices in India.

Further, the report suggests that content on platforms be regulated by a statutory media regulatory authority, along the lines of the Press Council of India. While the report argues that social media platforms should be designated as publishers, the clause-by-clause proposed amendments do not set out specific amendments to this effect.

Data protection officers and liability: The 2019 bill required that all sensitive data fiduciaries appoint a Data Protection Officer based in India; the report recommends this be expanded to require that the Data Protection Officer be either a senior-level officer in the government or a member of the entity's key management. The report also proposes to extend the liability provisions beyond corporate officers, to independent directors and non-executive directors, if they can be shown to have knowledge of or consented to decisions contrary to the PDP Bill.

Children's data: The report proposes significantly expanding the scope of regulation by creating a general obligation for all data fiduciaries to protect children, including around identity verification and restrictions on data use.

The report suggests that data fiduciaries should be required to seek consent from data principals when they attain the age of majority i.e., 18 years, and that the process should require data fiduciaries to inform the child of their right to provide consent three months before the age of majority. The report also recommends that data fiduciaries dealing exclusively with children's data must register themselves with the DPA. These changes are not reflected in clause-by-clause amendments.

Right to be forgotten: In addition to the data principal having the right to restrict the continuing disclosure of data, the report argues that this restriction be extended to the "processing" of personal data as well. The report argues that these changes are being proposed to make the right to be forgotten more comprehensive.

Timeline for implementation: The report suggests a phased implementation of the new data protection legislation over an approximate period of 24 months. This would include:

- 3 months to appoint chairperson and members of the DPA;
- 6 months to commence activity of the DPA;
- Registration of data fiduciaries to start within 9 months and be completed within a specified timeline;
- Adjudicators and appellate tribunal to commence work within 12 months; and
- The new legislation to become effective within 24 months from the date of its notification.

The JPC report marks the beginning of the next stage of the Modi government's effort to create a robust and progressive data protection framework. As described in this brief analysis, the report recommends a significant broadening of the scope of this framework. The resulting bill, when enacted, is likely to have significant ramifications for all companies that collect, process, store, or utilize data as part of their normal operations, across sectors. While there will be significant opportunities for key partner and industry stakeholders to engage with the Modi government in the next few months as the PDP Bill is shaped into its final form prior to parliamentary passage, the scope of potential adjustments is likely to narrow to technical matters that could reduce the quality of services available to the Indian people or put at risk India's competitiveness in a given sector.

The next steps on the PDP Bill rest with Prime Minister Narendra Modi's government, and in particular the Ministry of Electronics and Information Technology. Though the government could move to enact the PDP Bill as soon as the current session, the more likely timeline for parliamentary action appears to be either the budget parliamentary session in February or the monsoon parliamentary session in summer 2022.

About ASG

Albright Stonebridge Group (ASG), part of Dentons Global Advisors, is the premier global strategy and commercial diplomacy firm. We help clients understand and successfully navigate the intersection of public, private, and social sectors in international markets. ASG’s worldwide team has served clients in more than 120 countries.

ASG's South Asia practice has extensive experience helping clients navigate markets across South Asia. For questions or to arrange a follow-up conversation please contact James Schwemlein.