ALBRIGHT STONEBRIDGE GROUP

Data Protection in India's Draft E-Commerce Policy: Key Takeaways for Businesses

February 26, 2019

Context and Overview

On Saturday, February 23, 2019, India's Department for Promotion of Industry and Internal Trade (DPIIT) released India's draft e-commerce policy, inviting stakeholder comments through March 9. The draft addresses various issues in India's e-commerce space, including matters related to data protection.

In parallel, India's Ministry of Electronics and Information Technology (MeitY) is developing a cross-sector data protection bill, likely to be submitted in Parliament after the country's May general election *(see ASG's analysis of the draft bill)*.

The draft e-commerce policy presents new potential challenges for companies that have been tracking India's moves toward a data protection regime. First, language in the draft policy suggests it may apply much more broadly than just to India's e-commerce space. Additionally, consistent with the spirit of MeitY's cross-sector draft bill, the draft e-commerce policy imposes several obligations related to cross-border data flow. Further, in relation to these obligations, certain details appear to differ between the two documents; whether and how those differences will be resolved is unclear. The draft policy also suggests businesses should share data with the government and Indian competitors.

Businesses seeking to address challenges that the draft policy poses should consider robust and timely engagement with key stakeholders.

Key Takeaways for Businesses

- *A potentially overbroad scope.* The draft policy repeatedly notes its intent to apply to the e-commerce sector but defines e-commerce so broadly that it potentially applies to all web services: "*e-Commerce includes buying, selling, marketing or distribution of…goods, including digital products and…services; through electronic network*." In other words, even web services that are free to consumers (e.g., search; social media; email; most websites; many applications), or other services that many may not consider e-commerce per se (e.g., file storage services) may qualify as e-commerce under this definition. Notably, when discussing restrictions on cross-border data flow in section 1.1(b), the draft policy expressly distinguishes between e-commerce platforms and other web services (such as social media and search engines) but applies the restrictions to those services too.

- *Unclear interplay with MeitY's cross-sector data protection law.* Regardless of the draft e-commerce policy's scope, synchronizing the policy with MeitY's data protection law is critical, because that law is cross-sector and will apply to all businesses, including those impacted by the draft e-commerce

policy. Without synchrony, those businesses may face conflicting and unclear data protection obligations. As indicated below, the draft e-commerce policy's data protection requirements appear consistent with the spirit of MeitY's cross-sector draft bill, but certain details differ or may differ given ambiguity in the draft e-commerce policy. Potentially signaling the intent to synchronize, the draft e-commerce policy repeatedly acknowledges MeitY's cross-sector draft bill, and separately notes that policymakers will attempt harmony between various government initiatives impacting e-commerce. Businesses should view such assurances with, at most, cautious optimism.

- *Ambiguous and potentially onerous restrictions on cross-border data flow.* Echoing a key theme of MeitY's cross-sector draft data protection bill, Section 1.1 of the draft e-commerce policy calls for "*restrictions on cross-border data flow*." However, it does not specify the restrictions. It is unclear if that silence is deliberate (potentially signaling deference to MeitY) or meant, somewhat peculiarly, to be filled by language in an entirely different section of the draft e-commerce policy (Section 2.2) which states: "*Steps will be taken to develop capacity for data storage in India…A time-frame would be put in place for the transition to data storage within the country. A period of three years would be given to allow industry to adjust to the data storage requirement*." This language, even if meant to fill the silence of Section 1.1, calls for clarity. It refers to "*the data storage requirement*" but does not explain what the requirement is. Some observers interpret this language as prohibiting any data (barring expressly exempt categories) from leaving the country (starting three years after the policy is implemented); that would exceed the demands of MeitY's cross-sector draft bill.

- *Unclear and overly restrictive treatment of sensitive data transferred outside India.* Section 1.2 of the draft e-commerce policy lists conditions applying to sensitive data transferred outside India. Several aspects of Section 1.2 are notable.

  – First, by acknowledging that sensitive data can leave India, it suggests that the policy does not call for the prohibition discussed above, unless of course Section 1.2 is meant to apply only until the aforementioned three-year clock runs out (which is unclear).

  – Second, Section 1.2 does not define "*sensitive data*." MeitY's cross-sector draft bill defines "*sensitive personal data*" but also identifies a separate category called "*critical data*," both with significant and different implications for cross-border data flow. It is unclear if Section 1.2 intends to refer to one of these categories, and if so, which one. It arguably refers to the former, given the use of the term "*sensitive*," but the draft e-commerce policy nowhere mentions "*critical data*," potentially signaling conflation.

  – Third, Section 1.2 demands that no sensitive data stored outside India be shared with a third party even if the user consents to such sharing. This strikingly restrictive demand exceeds the obligations of MeitY's cross-sector draft bill. Additionally, it appears unnecessary given MeitY's requirement that consent be meaningful. Notably, by imposing this restriction only on sensitive data stored *outside* India, rather than also on sensitive data stored *in* India, Section 1.2 embodies a key theme of this draft policy: grave mistrust of foreign nations and entities.

  – Fourth, Section 1.2 requires that companies comply "*immediately*" with requests from the Indian government for access to sensitive data stored outside India. The precise meaning of *"immediately"* is unclear. Clarity here is critical because compliance can take time no matter how willing the company is. However, potentially providing some relief to businesses, this requirement

(by demanding access to data stored abroad) appears to implicitly acknowledge that data – or even its copy – need not be stored in India to meet the government's law enforcement goals.

- *Welcome but ambiguous exemptions to cross-border data flow restrictions.* Section 1.3 of the draft e-commerce policy articulates categories of data to which the policy's cross-border flow restrictions do not apply. These exemptions will likely help reduce the disruption businesses experience when the policy (and potentially MeitY's cross-sector law) take effect. However, there is room for clarity. For example, one exempt category of data is "*B2B data sent to India as part of a commercial contract between a business entity located outside India and an Indian business entity*." MeitY's draft cross-sector bill onerously suggests that a regulatory body (the Data Protection Authority envisioned in the draft bill) would need to approve such a contract; it is unclear if Section 1.3 intends that. Another exempt category is "*Software and cloud computing services involving technology-related data flows, which have no personal or community implications*." It is unclear whether any data can literally have "*no personal or community implications*." Section 1.3 should, in consultation with industry, more clearly describe this category. Further, MeitY's draft cross-sector bill articulates additional categories of data that companies are allowed to transfer outside India; it is unclear if the draft e-commerce policy intends to include those categories.

- *Requirements to share data, potentially undermining innovation and competition.* The draft e-commerce policy frequently suggests that businesses should share data, not just with the Indian government to help policymaking, but also with Indian companies to help them grow. There are several concerns with this requirement. For example, it is unclear whom businesses must share what type of data with. The draft policy sometimes refers to sharing "*community data*" (but does not define it precisely) and sometimes appears to suggest that the sharing requirement may extend to all types of data. It notes that data must be shared with Indian start-ups and small-and-medium enterprises, but elsewhere suggests that data should be shared with the government. Additionally, the requirement to share data – particularly with competitors – is not just onerous but risks discouraging investment and innovation, and significantly undermining competition on the merits. In an attempt to promote competition, the draft policy appears to do the opposite, by promoting free-riding and therefore penalizing success rather than penalizing only the abuse of dominance.

About ASG

Albright Stonebridge Group (ASG) 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 Nikhil Sud.