India Considers Stringent New Personal Data Privacy Law

AUGUST 3, 2018

The Indian government is currently considering a sweeping data privacy law which, if enacted, would mean significant changes for foreign companies doing business in the world's fastest-growing digital economy. The Personal Data Protection Bill of 2018 ("PDPB") was spurred in part by a landmark decision by the Supreme Court of India last year holding that privacy is a "fundamental right" under the Indian Constitution and calling on the Indian government to formulate a comprehensive regime for data protection. As a result, the government convened a ten-member expert panel, chaired by former Supreme Court Justice B.N. Srikrishna to draft a new data privacy law.

The bill is closely modeled after the European Union's General Data Protection Regulation ("GDPR"). It broadly applies to all "personal data,"[1] defined as any data of a "natural person," which allows direct or indirect identifiability; and envisions a regime where individual consent is the cornerstone of data-sharing.

Its key provisions include:

> **Citizen Rights:** The bill grants "data principals" (the equivalent of "data subjects" under the GDPR) four key rights against "data fiduciaries," including companies and government entities, including: (1) the right to confirm whether and how their data is being used; (2) the ability to correct misleading or false data; (3) data portability rights; and (4) a "right to be forgotten," or the authority to restrict companies from using data they previously shared. Unlike the GDPR, the PDPB *does not* require companies to delete such data altogether.
>
> **Establishment of Regulatory Agency:** The bill also calls for the establishment of a Data Protection Authority ("DPA"), which would have the power to investigate, enjoin, and fine non-compliant entities. All data fiduciaries would be required to disclose data breaches to the DPA. The DPA would also have the authority to label certain entities as "Significant Data Fiduciaries" ("SDFs") based on the volume and sensitivity of data they process, thus subjecting such entities to additional transparency, auditing, and reporting requirements. SDFs would be required to appoint a Data Protection Officer to oversee compliance with the law; comply with annual independent audits of their processing of personal data; and conduct impact assessments for new technologies or large-scale profiling or use of personal data. The DPA also would also have the authority to mandate that other data fiduciaries be subject to these requirements, even if they are not categorized as SDFs.

Finally, all data fiduciaries would be required to notify the DPA in the event of a data breach, which would also have the authority to mandate individual notification.

Data Fiduciary Obligations: All data fiduciaries would be required to implement "appropriate security safeguards," including de-identification, encryption, and tools to prevent misuse, unauthorized access, modification, disclosure, or destruction of personal data. The bill establishes temporal limitations on the processing and retention of personal data, prohibiting data fiduciaries from retaining personal data longer than "reasonably necessary" to satisfy its intended purpose or comply with legal obligation, and requires fiduciaries to undertake periodic review to ensure they are not unnecessarily retaining personal data.

Data Localization: The bill requires that one copy of all personal data to which the law applies be stored on a server located in India. The bill also gives the Indian government the authority to classify information as "critical personal data," which may only be stored within India. Importantly, this would broadly apply to any data, "collected, disclosed, shared, or otherwise processed within the territory of India," meaning, for example that it could capture *all* personal data provided by foreign entities to Indian IT companies for processing, even if such foreign entities do not process Indian citizens' data. The Indian IT sector's trade association, NASSCOM, has criticized this provision, raising concerns that the "mandat[ed] localization of all personal data… is likely to become a trade barrier" within India, disproportionately impacting smaller companies and start-ups."

Financial Penalties: Finally, the bill proposes strong punitive measures for companies that breach the law's provisions, proposing financial penalties of up to Rs. 15 crore (approximately $ 2,100,000) or 4% of its total worldwide turnover of its preceding financial year, whichever is higher.

The bill is currently under consideration by the Indian Ministry of Electronics and Information Technology. The bill is then slated to go before the Indian Parliament in its next legislative session. It will need to pass both chambers of Parliament by a majority vote before it becomes law. Interested stakeholders, including the IT industry, privacy advocates, academics, and others will likely offer input at that time. If enacted, the new law could well affect American companies' decisions on whether to use Indian data processors and whether to use and store the personal data, as defined, of millions of Indian consumers.

---

* *Meghan Koushik is a Summer Associate at WilmerHale, and is a rising third-year law student at Stanford Law School.*

[1] Specifically, the bill defines personal data as "data about or relating to a to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, or any combination of such features, or any combination of such features with any other information." The bill further defines "sensitive personal data" as data "revealing, related to, or constituting… (i) passwords; (ii) financial data; (iii) health data; (iv) official

identifier; (v) sex life; (vi) sexual orientation; (vii) biometric data; (viii) genetic data; (ix) transgender status; (x) intersex status; (xi) caste or tribe; and (xii) religious or political belief or affiliation." Personal Data Protection Bill, ch. 1, sec. 3 (29); (35).

Authors

Meghan Koushik *

SUMMER ASSOCIATE

Wilmer Cutler Pickering Hale and Dorr LLP is a Delaware limited liability partnership. WilmerHale principal law offices: 60 State Street, Boston, Massachusetts 02109, +1 617 526 6000; 2100 Pennsylvania Avenue, NW, Washington, DC 20037, +1 202 663 6000. Our United Kingdom office is operated under a separate Delaware limited liability partnership of solicitors and registered foreign lawyers authorized and regulated by the Solicitors Regulation Authority (SRA No. 287488). Our professional rules can be found at www.sra.org.uk/solicitors/code-of-conduct.page. A list of partners and their professional qualifications is available for inspection at our UK office. In Beijing, we are registered to operate as a Foreign Law Firm Representative Office. This material is for general informational purposes only and does not represent our advice as to any particular set of facts; nor does it represent any undertaking to keep recipients advised of all legal developments. Prior results do not guarantee a similar outcome.