

Study Finds Personal Data Protection Draft Ambiguous

Our Bureau

New Delhi: The draft Personal Data Protection Bill 2018 resembles the European Union's General Data Protection Regulation (GDPR) and comes with ambiguities and has its own pain points, said a joint study by PricewaterhouseCoopers and Associated Chambers of Commerce & Industry of India.

The draft Bill submitted to the Centre by the Justice BN Srikrishna committee in July seeks to create a comprehensive framework for data protection. It suggests companies to adopt certain practices to collect, process and store consumers' data, and recommends a range of penalties including jail term for privacy violations.

"The proposed Personal Data Protection Bill runs into 112 sections and is very similar to the EU's GDPR. However, it comes with its own challenges and ambiguities," the study report said, adding that even as organisations were coming to terms with GDPR, they found themselves confronted with another regulation.

The draft recommends every data fiduciary — an entity processing personal data — shall ensure the storage, on a server or data centre located in India, of at least one serving copy of personal data to which the Act applies. This means that companies will be required to build servers locally.

To protect national interests and containing the risk of surveillance from foreign states on critical data, the draft Bill also suggests preventing data fiduciaries from sending such data outside the territory of India. However, what constitutes personal data and "critical" personal data is a decision that has been left to the authority, the 21-page study added.

Tech Talk PwC-Assocham report says maintaining data locally would hit cloud-led businesses

'Under Scrutiny'

MAINTAINING DATA locally would impact cloud-led businesses, would increase general cost of doing business



SYSTEM INTEGRITY COULD COME UNDER THREAT WHEN PURGING DATA AS REQUIRED UNDER PROPOSED REGULATION

PROPOSAL TO bring criminal liability may force private sector executives to face conviction

LIMITATION OF processing and publishing analysis of anonymised data should be evolved

The intentions behind the move are good, but maintaining data locally would have an impact on businesses across multiple industries that are today cloud-led, and it would increase the general cost of doing business across industries, the PwC-Assocham study said.

The Srikrishna committee's proposal to bring criminal liability, making offences cognisable and nonbailable, may force private sector executives to face conviction, a clause contested by various stakeholders.

Following the Supreme Court's recognition of the right to privacy as a fundamental right under the Constitution of India in August 2017, the draft Bill guidelines, have attracted much attention. The study said system integrity could come under threat when purging data as required under the proposed regulation. Companies may have to retune systems to address challenges, it said.

The proposal to exclude anonymised data from restrictions will

considerably bring down the obligations on entities — both in the private and public sector.

The study suggested that in order to prevent harm to specific groups of individuals, limitation of processing and publishing analysis of anonymised data should be evolved. Companies will have to limit collection and reuse of data in line with the consent obtained from data subjects, which according to the finding would be challenging because organisations would have to change the mindset of collecting and keeping more data than necessary.

Data breaches, according to the PwC-Assocham study, are a serious business issue, and the Bill proposes a layered approach for levying penalties for non-compliance.

In order to avoid significant business ramifications due to data breaches, organisations need to outline a well-defined testing mechanism to assess readiness to address any eventualities, the report added.