PaymentsCompliance

Industry Given Glimmer Of Hope By India Privacy Reforms

6TH AUG 2018 | WRITTEN BY: FRAN WARBURTON

India's long-awaited personal data protection bill has given hope to payments firms that stringent data localisation requirements recently imposed by the central bank could be relaxed.

After months of anticipation, the Srikrishna Committee, which was tasked with overhauling the country's privacy legislation, recently unveiled legislative proposals that will redefine how companies store, collect and process personal information of Indian citizens.

Reflecting concepts reminiscent of the EU's General Data Protection Regulation (GDPR), the draft bill contains a raft of measures around customer consent, envisages a new regulatory authority and threatens big fines and even criminal prosecution for violations.

Although the recommendations were met with disappointment by some stakeholders, legal experts have said that, crucially, they indicate a more favourable approach to data localisation for international payments firms.

"The recommendations split data into two kinds of data: they talk about personal data and critical personal data," said Shilpa Mankar Ahluwalia, a partner at Shardul Amarchand Mangaldas & Co.

"They've extended the data localisation requirement to only what they categorise as critical personal data — but they've left it to the regulator to clarify what they mean by that."

Earlier this year, the Reserve Bank of India (RBI) issued a demand to payment firms that all data is stored only in India, in a move that caused shockwaves through the industry and has since led to fallouts between international and local payments companies.

Mankar Ahluwalia said she expected that the RBI may provide more information on how the two respective sets of rules will work together, which could make life easier for financial firms.

"Currently the RBI circular says all payments data," she said. "One possibility is that the RBI issues a clarification or FAQ saying that, following the recommendations, what is meant by all payment data is critical personal data and then they dovetail that into the recommendations.

"This is more likely than the government rolling back the recommendations of the committee and extending the data localisation requirement to all personal data."

Lobbying efforts from international players have been in full swing. According to meeting minutes seen by PaymentsCompliance, the major card schemes and other payments heavyweights had complained that the RBI's rule would make is difficult to comply with foreign laws.

For Akash Karmakar, an associate and fintech expert at Veritas Legal, it is more than likely that international giants have "enough bargaining power to at least bring some sort of equilibrium to the issue if not tilt the balance in their favour".

"While the local companies are looking at this as a welcome measure given that by design or default, this offers a protectionist advantage, the foreign companies are looking at this as something that is perverse because it is protectionist," he said, speaking in a personal capacity.

> "Foreign firms continue to wield a significant amount of influence in India because of the penetration of Facebook and WhatsApp and how accustomed the Indian population has become to these two things there are associated economic ecosystems," said Akash Karmakar of Veritas Legal.

"There is however a risk, even though it is remote, that Indian regulators may continue to not consult industry participants before issuing directives," the lawyer added.

Aaron Kamath, a technology and data privacy lawyer at Nishith Desai Associates, said that a relaxation in the data localization requirement for foreign payment system providers "maybe likely to some extent", with a possible solution being mirroring the data stored both in India and in the country where the data is currently stored.

However, such a relaxation should be specifically issued by the central bank in order to take effect, and the enactment of the new data protection bill alone may not nullify the RBI's requirements unless it explicitly overrides them.

For Kamath, the payments data storage issue is an industry-specific requirement and so "may continue to stand".

"Access to data is unfortunately being confused with localisation," he said.

Plans to overhaul India's privacy framework initially came in light of a Supreme Court decision last year that held that the right to privacy is a fundamental right for every person.

Although fundamental rights are claimed against state actors, it was widely expected that the implications of the decision would spread to the private sector in the form of legislative changes.

The Srikrishna Committee was set up as a result of that judgment to make policy recommendations.

Deepa Christopher, managing associate at TT&A in Mumbai, said that having roots in the Supreme Court judgment makes the completion of legislation a priority.

Although noting the bill is still in its draft form and may look different in its final form, the lawyer said that even presuming half of the current proposals are implemented would "still be a big jump" from the existing framework.

She pointed to potential gaps within the recommendations, such as the level of information that needs to be shared and the obligation on firms to establish they have obtained valid consent.

Christopher also questioned the motive behind the data localisation requirements, pointing out there are other ways authorities can supervise information held by financial firms.

"Unfettered access is important, but that could also be achieved through having another copy stored in India," she said. "All the reasons are not clear but may also be linked to limiting the level of access that other authorities have to the data."

Veritas Legal's Karmakar added: "The RBI circular is still effective, but the hope is that the expectation for data localisation is retention of a copy in India, as prescribed in the Personal Data Protection Bill, 2018 rather than a restriction on sending payments data out of India."

The committee has proposed to introduce four additional data principle rights: the right to confirmation and access; the right to correction; the right to data portability; and the right to be forgotten.

Matters related to Aadhaar, India's national identity scheme, are still under consideration of the Supreme Court. That outcome will be monumental in deciding whether non-regulated financial entities such as prepaid payment instruments can use the ID system for know your customer (KYC) checks.