18 JANUARY 2019

All You Need to Know About RBI's Data Localisation Directive

Abhishek Senthilnathan and Aaron Kamath of leading law firm Nishith Desai Associates share their insights on the RBI's Data Localisation directive and what it means for foreign payment enablers operating in India.

Rapid growth of the payments ecosystem in India coupled with recent data breaches and security concerns may have led the RBI to mandate that all authorized payment companies need to store payment systems related data only in India.

The RBI may have undertaken this step to protect consumer interest and to secure its unfettered access to such data.

In fact, RBI's quarterly report "Statement on Developmental and Regulatory Policies", issued on April 5, 2018, mentions that RBI decided that all payment system operators should ensure that payment systems data are stored only inside the country, in order to have unfettered access to such data for supervisory purposes.

What is the mandate and what does non obedience entail?

The directive directs all payment system providers to ensure that

the entire data relating to their payment systems including complete transaction data should be stored in systems located only in India.

The data to be stored only in India includes *"full end-to-end transaction details / information collected / carried / processed as part of the message / payment instruction."*

For a foreign leg of a transaction (if any), the data can also be stored in a foreign country, if required.

Payment system providers had time till October 15, 2018 for compliance with the directive, and were to submit a compliance report to the RBI by the end of 2018. In case of breach of the directive, as in the case of breach of other directives and regulations issued by the RBI, the RBI has discretionary power the impose fines or even imprisonment in certain cases.

In addition, the RBI was contemplating issuing certain clarifications or FAQs in relation to implementation of the directive, which however has not been issued till date.

What challenges will the industry face to meet these guidelines?

The directive is said to have the biggest impact on multinational payment system providers operating in India. These corporations may require to conduct inter-company cross-border transfers of data for data analytics and to comply with their group security policies on a global level. This will not be possible in light of the directions, under the directive. Further, such multinational corporations may need to comply with numerous international laws across various jurisdictions, such as anti-money laundering, countering financing of terrorism, detecting tax evasion, etc. which may require them to deal with or furnish the payments

systems data from India in other countries. In the absence of the ability to export or copy payment system data from India, compliance with these requirements may be seriously affected.

We understand from media reports that two US Senators - John Cornyn and Mark Warner have also written to the Prime Minister of India, urging the Indian Government to soften its stance on data localization. According to news reports, the senators warned the Prime Minister that the directive would present "key trade barriers" between India and the US.

Is Mirroring an option available to the industry?
Yes. In June 2018, the Government conducted a closed-door meeting along with representatives from various departments such as the Department of External Affairs, Department of Financial Services, Enforcement Directorate (ED) and National Security Council along with the RBI and US-India Business Council (USIBC) (consisting of representatives from industry players such as Visa, American Express, PayPal, MasterCard, MoneyGram and Paytm) to discuss issues and concerns emanating from the directive. Based on the discussions in the meeting, it was noted that mirroring the data in India along with the country where the data is currently stored could be a possible solution. However, an exemption to the localization requirement in the form of data mirroring has not been prescribed till date.

Are there any similar precedent cases in other countries?
Russia has a detailed data localization law in place, which was implemented in 2015, in relation to all personal data of Russian nationals which requires that any organization that stores any personal data or information of Russian nationals, whether of customers or social media users, must move and store that data on Russian servers. Compliance with the new legislation is strictly monitored and enforced by Russia's Federal Service for

Supervision of Communications, Information Technology and

Mass Media, known as “Roskomnadzor”.

China is also in the process of implementing a detailed / comprehensive data localization law, which will be fully implemented by 2019. It covers not only the personal data collection, but also “important data” concerning “critical information infrastructure” This appears wide enough to include all major aspects of everyday life such as all “personal data” and also all “important data” of Chinese nationals. However, ‘important data’ has not been specifically defined, till date.

What is the way forward for multinational firms operating in India?

At present, MNC payment system providers would need to comply with the directive as long as they are operating in India, as there have been no exemptions in the requirement or extension in the deadline issued by the apex bank.

As per news reports, we understand that some MNCs may not have complied with the notification till date, even though the deadline has passed. Earlier, certain operators had even requested the RBI for an extension of deadline which was not granted. It is left to be seen as to the action that RBI may initiate against defaulters.

Earlier and even well before the deadline, the RBI had asked the payment system operators to submit a report on a fortnightly basis to the RBI on their status of compliance and efforts being made. We understand that the RBI is closely monitoring compliance and contemplating action to take against defaulters for non-compliance.

A beta version of Whatsapp pay which was launched in May last year, is yet to be rolled out on full scale. It is being delayed over

issues of RBI's data localisation norms. Supreme Court recently (January 14), in response to a petition filed by an NGO, ordered to make RBI a party in the plea to check WhatsApp's adherence to data localisation norms for setting up it's payment business in the country.

This blog post is based on personal views of the authors and are not to be construed as legal advice.