SQUIRE PATTON BOGGS

India Corporate Update – Data Localisation

Over the last year, the Indian government has proposed several measures for effective data protection, including through increased control on cross-border data flows by way of "data localisation". Data localisation is being used as a tool by a growing number of countries to control the transfer of data belonging to their residents across national borders. While countries like China, Australia, Russia and Canada already have data localisation provisions in place (e.g. Canada localises public interest data held by government agencies, schools and hospitals, and China localises internet-based mapping services, critical information infrastructure and banking data), India is still struggling to establish a regulatory framework for effective protection of data.

The recently enforced and proposed regulatory framework for data protection, particularly through data localisation, consists of:

- Draft Personal Data Protection Bill, 2018, released by the Ministry of Electronics and Information Technology in July 2018.
- Draft National Policy Framework on Electronic Commerce in India, released by the Ministry of Commerce and Industry in July 2018.
- Proposed amendments to the Drugs and Cosmetics Rules, 1945, released by the Ministry of Health and Family Welfare in August 2018.
- National Digital Communications Policy, 2018, released by the Department of Telecommunications, Ministry of Communications in May 2018 and approved by the Union Cabinet in September 2018
- Proposed cloud computing policy to be released based on a report prepared by a panel set up in July 2012 to recommend a framework for cloud computing services. The panel's report is expected to be released in the coming months.
- Directive on storage of payment system data, released by the Reserve Bank of India (RBI) in April 2018 with a timeline for compliance by October 2018.

These proposals are in addition to the Information Technology Act, 2000 and associated rules that have been the primary legislation for governing data privacy and protection in India.

Below is a brief description of the recently enforced and proposed regulations for data protection in India, along with an analysis on the possible outcomes of introducing such a regulatory framework.

The Draft Personal Data Protection Bill, 2018

One of the key pronouncements that aim to introduce data localisation measures in India is the Draft Personal Data Protection Bill, 2018 (DP Bill), which was prepared based on the report issued by the Committee of Experts under the chairmanship of B.N. Srikrishna on 27 July 27 2018.

The DP Bill states (i) all personal data to which the law applies must have at least one serving copy stored in India; (ii) the central government shall determine the categories of sensitive personal data that are critical to the nation's interests and such data must only be processed in a server/data centre located in India (no overseas transfer of data is permitted in such cases); and (iii) the central government will be vested with the power to exempt transfers on the basis of strategic or practical considerations.

Further information on the DP Bill is available.

Proposed National E-Commerce Policy

Though not publicly notified or discussed, the Ministry of Commerce and Industry is in the process of issuing a Draft National Policy Framework on Electronic Commerce in India (Draft Ecommerce Policy), which seeks to strengthen the regulatory regime for protecting consumers of e-commerce. One of the measures proposed for protecting consumers is localisation of several categories of data involved in e-commerce.

The Draft Ecommerce Policy proposes that the following categories of data will be required to be stored exclusively in India and a suitable framework will be developed for sharing such data within the country: (i) community data collected by Internet of Things (IoT) devices in public space; and (ii) data generated by users in India from various sources, including e-commerce platforms, social media, search engines, etc.

However, localisation is not expected to be absolute, and cross-border flow of data is permissible in certain cases, including for (i) data not collected in India; (ii) B2B data sent to India as part of a commercial contract between a business entity located outside India and an Indian business entity; (iii) software and cloud computing services involving technology-related data flows (which have no personal or community implications); (iv) multinational corporations moving data across borders (which is largely internal to the company and its ecosystem); and start-ups that meet specified criteria, such as turnover of up to ₹500 million.

While these measures are expected to be proposed under the Draft Ecommerce Policy, with numerous objections from various stakeholders over the last few months, it is expected that a draft for consultation will soon be released, and implementation of these measures will ultimately depend on the approval of the cabinet.

The Drugs and Cosmetics Act, 1940

In August 2018, the Ministry of Health and Family Welfare proposed certain amendments to be made to the Drugs and Cosmetics Rules, 1945 with respect to data localisation applicable to the growing number of e-pharmacies in India ("Draft E-Pharmacy Rules").

Under the Draft E-Pharmacy Rules, e-pharmacy web-portals have to be established in India for conducting the business of distribution or sale, stock, exhibit or offer for sale of drugs and the data generated by them has to be stored locally. The draft amendment clearly stipulates that under no means the data generated or mirrored through e-pharmacy portals shall be sent or stored outside India.

The Ministry of Health and Family Welfare sought comments and suggestions from the general public on the Draft E-Pharmacy Rules, and the aforesaid amendments (subject to their modifications in the rules finalised by the ministry) will come into force once published in the Official Gazette.

The National Digital Communications Policy, 2018

The National Digital Communications Policy, 2018 (NDCP), which was released for consultation by the Department of Telecommunications in May 2018, was approved by the cabinet in September 2018. The NDCP emphasises on establishing a comprehensive data protection regime for digital communications that safeguards the privacy, autonomy and choice of individuals. The NDCP provides that if India's economic, social and political interests in the emerging data economy are to be effectively secured, its "digital sovereignty" encompassing data privacy, choice and security of its citizens requires to be kept in prime consideration while participating in the global digital economy.

The NDCP is expected to be tabled in the Parliament of India for further action.

Proposed Cloud Computing Policy

The latest in the series of proposals relating to introduction of data localisation in India is the recommendation of localisation of cloud data by a panel formed by the government to work on India's cloud computing policy. The panel is expected to submit its report to the Ministry of Electronics and Information Technology in the coming months.

The ministry previously issued guidelines on setting up IT infrastructure by government departments using cloud computing technology with a clause mandating that all data must be stored within the country. These guidelines clearly provide that the condition of data location has to be specifically mentioned in the agreement with the service provider.

Measures Introduced by the RBI

Of greater imminence is the RBI's circular directed at payment settlement systems. In order to ensure effective monitoring of data stored by payment systems in line with its Statement on Development and Regulatory Policies of the First Bi-monthly Monetary Policy Statement for 2018-2019, the RBI issued a notification on 6 April 2018 (RBI Notification) that mandated:

- All payment system providers to ensure that the entire data relating to payment systems operated by them are stored in a system "only" in India. This is applicable to all payment system operators in India, including multinational companies operating in India.
- Compliance with the above directive within six months, i.e. latest on or before 15 October 2018. Such compliance is required to be reported to the RBI.
- System providers to submit a System Audit Report (SAR) on completion of the above requirement. Such audit is to be conducted by Indian Computer Emergency Response Team (CERT-In) (Ministry of Electronics and Information Technology) empanelled auditors certifying completion of the above activity.
- SAR duly approved by the board of the system providers to be submitted to RBI, not later than 31 December 2018.

The RBI clarified that the data to be stored by the payment system providers must include the full end-to-end transaction details, information collected, carried or processed as part of the message or payment instruction.

An exemption from data localisation requirement has, however, been provided by the RBI as follows, "for the foreign leg of the transaction, if any, the data can also be stored in the foreign country, if required."

Implementing the RBI Notification

- "Data", and what it comprises, has not been expressly defined in the RBI Notification. Further, the RBI Notification states, "data should include the full end-to-end transaction details ... as part of the message/ payment instruction." There is limited understanding on what kind of data the requirements relate to, i.e. whether it is limited to payment data of an individual or extends to other types of data such as personal data of an individual that may be required in payment transactions.
- The RBI Notification requires that data must be stored in a system "only" in India, raising concerns on whether copies of such data can be stored elsewhere, particularly in situations that do not involve "foreign leg of the transaction".
- The term "foreign leg" has not been defined in the RBI Notification, leading to an ambiguity as to what data can be stored overseas.

While the deadline of complying with the RBI Notification has already expired, with lack of clarity on applicability of these requirements, the RBI may not immediately penalise non-compliant entities and may seek regular updates on the steps taken to implement these measures, with queries being addressed separately with each concerned entity.

Analysis

The government is determined to introduce data localisation in almost all sectors with the objective of having greater control to facilitate efficient monitoring of such data. From the government's perspective, data localisation is a step towards greater security of data, with reduced vulnerability to threats and attacks compared to situations involving cross-border data transfers. Further, with complete localisation of critical data, there is an attempt to prevent any form of foreign surveillance of India's internal affairs. These norms are also being implemented to boost India's digital infrastructure. Pooling and storing data locally is expected to create opportunities for domestic players for harnessing data.

While the intent of the government is to protect user privacy, the measures for storing data "only" in India give rise to multiple issues. Storing data outside India typically enables foreign companies to analyse and understand global user behaviour to develop new products and antifraud mechanisms. The government's concern on effective data supervision may be adequately addressed with requiring that such data be stored in India, without going further to suggest that it cannot be stored elsewhere. With the implementation of data localisation norms as proposed through various ministries, global businesses are likely to be at a disadvantage as in spite of providing services through cloud or third-party service providers, companies will not be able to move data outside India.

Increased data localisation measures will also increase the cost of doing business for various global entities in terms of setting up new data centres, restructuring network architecture, and/or using a local cloud vendor. On the other hand, Indian companies, especially homegrown payment settlement systems, are already subject to periodic audit requirements and RBI scrutiny and incur significant compliance costs that non-Indian companies have not been subject to. However, with increased requirements, small businesses are also likely to be impacted. An overhaul of this nature will also result in significant time and costs spent by Indian companies that currently house their data outside India in countries with a more evolved data centre infrastructure.

Conclusion

Centralisation of all data can make a greater volume of data susceptible to a single breach, compared to decentralising such data. Storing data locally in India may allow better supervision and protection, but it also implies increased costs associated with such protection. Moreover, decentralised storage of data or having mirror sites/copies in other geographies reduces the risks of hacks, thefts or other destruction of hardware storing such data.

While various ministries may further refine their policies based on suggestions from key stakeholders, the greater challenge lies in implementing these practices. To begin with, there is still no clear and harmonious definition of "data".

Although all the laws stated above (current as well as proposed) mention localisation of data, the term "data" itself has either not been defined or does not have an exhaustive definition. This ambiguity is bound to raise many questions on the type of data that is subject to localisation requirements.

Further, the fragmented and overlapping nature of such reforms is likely to reduce the efficiency of such a regime. While the central government has been given power under the DP Bill to bifurcate data into critical and non-critical, in order to determine whether such data can be processed or transferred overseas, different agencies/regulators are imposing data localisation obligations on the entities governed by them. This is likely to result in multiple laws governing a particular type of data that is serving different objectives, which may ultimately result in different agencies having authority over the same data.

In an era where India is moving towards simplifying its statutes (e.g. the proposed consolidation of the 44 existing labour laws into four codes and consolidation of various insolvency laws into the Insolvency and Bankruptcy Code, 2016), the introduction of data protection and localisation requirements in different legislations will only add to administrative and interpretation issues, and may ultimately fail to achieve its objective of improving the ease of doing business in India.

Contacts

Biswajit Chatterjee
Partner, Singapore
T +65 6922 8664
E biswajit.chatterjee@squirepb.com

Kaustubh George
Senior Associate, Singapore
T +65 6922 8658
E kaustubh.george@squirepb.com

Anandee Banerji
Associate, Singapore
T +65 6922 8677
E anandee.banerji@squirepb.com

Nabil Shadab
Associate, Singapore
T +65 6922 8668
E nabil.shadab@squirepb.com