India's Draft Personal Data Protection Bill, 2018: Charting the "Fourth Way"

August 2018

Hogan Lovells

India's Draft Personal Data Protection Bill, 2018: Charting the "Fourth Way"

India's Committee of Experts under the Chairmanship of Justice B.N Srikrishna (the "**Srikrishna Committee**") has submitted a draft Data Protection Bill (the "**Bill**") for review by the Ministry of Electronics and Information Technology ("**MEITY**"). The Srikrishna Committee tabled the Bill alongside a report entitled "A Free and Fair Digital Economy – Protecting Privacy, Empowering Indians"(the "**Committee Report**").

India Charts its "Fourth Way"

The Bill represents an important milestone for India, which has yet to enact comprehensive, principles-based data protection regulation, lagging a trend set in recent years by Singapore, the Philippines and others in the region playing catch up to Hong Kong and Japan, which have both had such regulation in place for years now.

India's growing importance as a regional economic power, and its position as the world's leading offshore service provider, underlines the significance of India's approach to data protection regulation. India's take on data protection law is sure to be influential to developments elsewhere in the region. Coming as it does in the wake of China's introduction of its Cyber Security Law and the European Union's implementation of its General Data Protection Regulation (the "**GDPR**"), the introduction of the Bill also represents an important reference point in the validation of differing approaches to this new generation of data regulation taking hold in the digital age.

The Srikrishna Committee makes these points directly in the Committee Report, promising the approach set out in the Bill to be a "template for the developing world", a "Fourth Way" that attempts a triangulation amongst: (i) the "*laissez-faire* approach" of sector-based laws and private rights of action taken in the United States, based on constitutional understandings of liberty from state control; (ii) the focus on individual dignity and fundamental rights to privacy enshrined under the GDPR and its predecessor laws in the EU; and (iii) China's approach to data protection, having its pronounced focus on state and national security.

The Srikrishna Committee writes that the "Fourth Way" should reflect India's unique understanding of the appropriate balance to be struck between individual freedoms recognized by its Supreme Court in the *Puttaswamy* decision and the common good. The Committee Report emphasizes that the common good in this context includes free data flows in aid of a growing data ecosystem and in support of a free and fair digital economy. The Bill's understanding of the common good, then, appears to at least in part echo the sentiment found in the APEC Privacy Framework, which took the advancement of digital economies and consumer confidence in the digital economy as its key rationale.

In India as elsewhere, achieving a balance between individual rights and the common good is easier said than done. The Bill has already generated significant commentary in India and observers expect significant parliamentary debate across a wide range of issues.

Points of Reference from an International Perspective

The Bill raises a number of striking points of comparison to international developments. At a high level, many of the Bill's provisions suggest that the Fourth Way is most closely aligned to positions taken in the GDPR, but there are important departures here and much will need to be resolved in the details of administration of the law. The following are key points of reference:

Creation of a dedicated regulator

In a point that is likely to be critical to the implementation of the law, the Bill makes provision for a dedicated data protection regulator in the form of the Data Protection Authority of India. In practical terms, we see the presence of a dedicated data protection authority as being key to the practical

administration and enforcement of data protection laws in the Asia-Pacific region.

Scope of application – extra-territorial effect

The Bill proposes three key criteria for application, applying to:

i. all personal data collected, used, shared disclosed or otherwise processed within the territory of India;
ii. the processing of personal data by the state, any Indian company, any Indian citizen or any person or body of persons incorporated or created under Indian law; and
iii. echoing provisions in the GDPR extending data protection principles beyond physical establishment to distance selling and online profiling activities (irrespective of establishment in jurisdiction), the law would also apply to the processing of personal data by organizations not present within the territory of India, if such processing is: (a) in connection with any business carried on in India, or any systematic activity of offering goods or services to data subjects within the territory of India; or (b) in connection with any activity which involves profiling of data principals within the territory of India.

Mandatory appointment of a Data Protection Officer

Like the GDPR, the Bill would require that organizations appoint a data protection officer responsible for advising the organization on its compliance with the law and for being a principal point of contact in relation to compliance matters. There does not appear to be any *de minimus* threshold of the scale of business or the scale or nature of data processing that would trigger this requirement. Organizations subject to the law who are not present within the territory of India would be required to appoint an officer based in India.

Basis for processing – consent, exemptions and reasonable purposes

The Bill also sets out a "reasonable purposes"/"legitimate interests" basis for processing that is more aligned with European law then many of the national laws in the Asia-Pacific region, which typically provide for consent and certain specific exemptions as the only lawful bases for processing personal data, without a "legitimate interests" basis.

Data subject rights

Strikingly, the Bill incorporates a number of the "second generation" data subject rights found in the GDPR, including a "right to data portability" founded in the right to receive personal data in the form of a "structured, commonly used and machine-readable format" and a "right to be forgotten".

Mandatory data breach notification obligation

Organizations would be required to notify the Data Protection Authority of India as soon as possible and not later than the time period specified by the Authority, following any personal data breach that is likely to cause harm to any data subject.

Data localization

In a move many would see as surprising in the context of an economy with heavy reliance on offshore data processing from other jurisdictions, the Bill would require organizations to 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. Going further than this "mirroring" requirement, which would generally permit international transfers subject to certain restrictions, the Indian government could designate categories of personal data as "critical" that would be fully localized to India without any scope for international transfer.

Significant enforcement powers

The Bill has also attracted much attention for the potential scale of financial penalties, which in respect of a number of offences could be up to one hundred and fifty million rupees (more than USD 2,000,000) or four per cent of its total world-wide turnover of the preceding financial year. The calculation of a fine based on world-wide turnover is another innovation the Bill takes from the GDPR.

Key take-aways

The Bill, accompanied by the 213 page Committee Report, represents an important statement of intent for the advancement of India's data protection laws.

There has been much critical commentary on the Bill in India across a range of issues. Some focus on how government use of personal data would be constrained under the law, a key issue in light of privacy concerns already raised in connection with India's Aadhaar biometric-based identity system.

The data localization measure has also attracted significant attention, representing a clear outlier from the Bill's overall alignment with the GDPR. The technology sector in India has raised concerns about this measure, which could hinder the international expansion of Indian technology businesses, and would of course impose constraints on market access to India by foreign-based players. More broadly, there are concerns that ambitions for a growing and robust technology sector, stated to be a key ambition for India, are not best served by alignment with the EU model.

We expect to see a vigorous and robust debate in the coming months as India refines its vision for the Fourth Way.

Contacts

Mark Parsons
Partner, Hong Kong
Tel +852 2840 503
mark.parsons@hoganlovells.com

George Willis
Registered Foreign Lawyer, Hong Kong
Tel +852 2840 5915
george.willis@hoganlovells.com

Alicante
Amsterdam
Baltimore
Beijing
Birmingham
Boston
Brussels
Budapest
Colorado Springs
Denver
Dubai
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta
Johannesburg
London
Los Angeles
Louisville
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Moscow
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
Rio de Janeiro
Riyadh
Rome
San Francisco
São Paulo
Shanghai
Shanghai FTZ
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar
Warsaw
Washington, D.C.
Zagreb

Our offices
Associated offices

www.hoganlovells.com