CLEARY GOTTLIEB | KHAITAN &CO Advocates since 1911

12 March 2019

The Indian Personal Data Protection Bill 2018: *a view through the lens of the EU GDPR*

In summer 2018, a new Indian Personal Data Protection Bill was released by a Committee of Experts formed under the Chairmanship of Justice B.N. Srikrishna (the "Bill"), accompanied by a report titled "A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians." After several months' hiatus, reports are emerging of renewed impetus from India's Ministry of Electronics and Information Technology ("MEITY") for the Bill to be put before Parliament.

The proposed introduction of the Bill continues a global trend in the revision of data protection laws: from California to Canada, from Bahrain to Brazil, many jurisdictions have recently proposed, or are in the process of adopting, new, stricter data protection legislation that, to varying degrees, bears the hallmarks of the recently-effective EU General Data Protection Regulation ("GDPR").

As the global data protection map evolves, what should multinational organisations do to remain compliant? National legislatures are contributing to a global patchwork of data protection policy and each new law has been shaped by different political and cultural motivations. Consequently, areas of incompatibility between regimes are becoming visible.

The GDPR was intended to increase consumer welfare and enhance the protections available under the former regime. By contrast, the Bill promises to deliver the first comprehensive data protection framework for India, which is seen as vital for the continued success of the country's outsourced IT services industry.

This article recaps on the key provisions of the proposed Bill, examines potential incompatibilities with the GDPR, and concludes with what this means for multinational organisations who may be required to navigate both frameworks.

Status of the Bill

On 16 August 2018, MEITY invited comments from the general public on the Bill by 10 October 2018. The Bill is yet to be listed for introduction in Parliament (though reports suggest there is momentum for this to happen soon) and therefore remains subject to changes pursuant to the public consultation. Thereafter the Bill will be finalised and tabled before the legislature before it becomes a law.

Similar law, different motivations?

It is worth recapping the legislative background. Currently, India lacks a structured and dedicated data protection law and data protection regulator. The current laws governing data protection in India[1] have not proved up to the task of protecting personal data in the modern age, and enforcement of these laws has been largely non-existent. With growing internet penetration and digitisation in India, combined with a strong outsourced IT services industry which needs to be supported by standards reflective of global data security demands, this lacuna in the legal framework has turned out to be a matter of concern for the Indian Government in recent years. There have also been significant judicial developments relating to privacy in India[2] that have built the momentum for a new, comprehensive privacy framework.

National legislatures are contributing to a global patchwork of data protection policy and each new law has been shaped by different political and cultural motivations. Consequently, areas of incompatibility between regimes are becoming visible.

How does this compare to the GDPR's legislative history? The GDPR places the fundamental rights of EU persons and their right to protection of personal data[3] at its heart. To protect these rights in a digital world, the GDPR has an extraterritorial effect: organisations that process the personal data of data subjects located in the EU (in relation to the offering of goods or services to them in the EU or the monitoring of their behaviour in the EU), or which process personal data in the context of an establishment located within the EU, can be caught by the GDPR despite not being established within the EU themselves.

The GDPR's extraterritorial reach protects EU consumers from foreign processors whose domestic legislation does not regulate data processing to the same standard. It also has the added consequence of ensuring that EU businesses are not placed at a competitive disadvantage by being subject to more regulation than their non-EU competitors.

1 Namely, the Information Technology Act 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

2 See, for example, the Supreme Court of India's landmark [2017] judgment in the case of *Justice K.S. Puttaswamy v Union of India* which held that the right to privacy is a fundamental right under the Constitution of India.

3 As enshrined in the Charter of Fundamental Rights of the European Union and the Treaty for the Functioning of the European Union.

Practical considerations for compliance with both regimes

How might organisations develop a data protection compliance program that meets the needs of both the Indian and EU regimes? Although the Bill may change in the months ahead, some areas of alignment are already apparent:

i. Key concepts

The Bill seeks to regulate the processing of personal data and sensitive personal data of data principals (i.e. natural persons) by data fiduciaries (i.e. entities including the State, or individuals who determine the purposes and processing of personal data) and data processors (i.e. entities including the State or persons who process personal data on behalf of data fiduciaries). The Bill's concepts of "data principals" and "data fiduciaries" are broadly analogous to the concepts of "data subjects" and "data controllers" under the GDPR. The Bill envisages that a Data Protection Authority of India (the "Authority") will be established to implement the new legal regime as well as to adjudicate on breaches of the law and determine the appropriate penalties under the Bill through a separate adjudicating wing. The Bill envisages the introduction of new data protection principles such as privacy by design and transparency in processing of personal data that are reminiscent of the equivalent principles in the GDPR.

ii. Extraterritorial applicability

The Bill proposes that the law apply to processing of personal data (i) within the territory of India by Indian data fiduciaries and data processors; and (ii) crucially, to foreign data fiduciaries and data processors where personal data is processed by them in connection with:

— any business carried on in India; or

— the systematic activity of offering goods or services to data principals within the territory of India; or

— any activity which involves profiling of data principals within India.

The Bill therefore envisages the extraterritorial application of Indian data protection laws to companies without any establishment or physical presence in India. This is a significant legislative development that will, if implemented, have far-reaching implications for companies doing business in India, in the same way that the equivalent (though differently-worded) extraterritorial clauses of the GDPR have had for companies doing business in the EU.

iii. Data principal rights

The Bill has introduced key data principal rights, such as the right to be forgotten, the right to confirmation and access, the right to data portability, and the right to correction. Equivalent rights are also enshrined in the GDPR; businesses operating across EU/Indian borders may therefore already have systems set up to be responsive to requests from data principals looking to exercise such rights.

iv. Key compliance requirements

The Bill introduces a number of compliance requirements for data fiduciaries and in some cases, data processors as well. The collection and processing of personal data should only be for purposes that are clear, specific and lawful. Clear notice is required to be provided at the time of collection of personal data specifying details such as the purpose of processing and the categories of personal data being collected. The notice must also mention the individuals or entities with whom personal data will be shared. The notice is required to be provided in a manner that is easily comprehensible and in multiple languages, where necessary and practicable. Reasonable steps are required to be taken to ensure that the personal data processed is complete, accurate, not misleading and kept up to date. Personal data should be retained only as long as may be reasonably necessary to satisfy the purpose of processing.

Another important obligation is data localisation whereby at least one serving copy of personal data is required to be stored on a server or data centre located in India. Furthermore, the Central Government has the power to issue a notice setting out certain critical personal data which is mandatorily required to be processed in a server or data centre located in India.

As the global data protection map evolves, what should multinational organisations do to remain compliant?

Security safeguards are required to be implemented and periodically reviewed considering the nature, scope and purpose of processing of personal data. Some of the measures prescribed include de-identification and encryption. Separately, notification to the Authority is required where a personal data breach is likely to cause harm to the data principal. The Authority may direct that a notification be made to the affected individuals and also that details of the breach must be published on the concerned entity's website.

Data fiduciaries may also be designated as 'significant data fiduciaries' by the Authority based on certain parameters such as the volume of personal data processed or the sensitivity of personal data processed. These entities will have additional obligations such as registration with the Authority, appointment of a data protection officer, conducting data audits, data impact assessments, and record keeping (all of which may also be applicable under the GDPR).

v. Cross-border data transfers

The Bill introduces a restrictive regime for transfers of personal data out of India to third countries, which is reflective of the EU model under the GDPR. Under the Bill, Cross-border data transfers are only possible where: (a) made subject to standard contractual clauses or intragroup schemes in each case as approved by the Authority, (b) the Central Government after consultation with the Authority determines that certain countries/ sectors are permissible locations / recipients of data transfers, (c) consent of the data principal (explicit consent in the case of sensitive personal data) has been obtained, or (d) the Authority approves a transfer due to a situation of necessity.

Impact of the Bill on IT outsourcing and technology multinationals

IT companies and technology multinationals deal with large personal data pools, undertake complex processing and in some cases are using machine learning applications for the development of technological solutions. Due to the extraterritorial applicability of the Bill, IT outsourcing companies based outside of India but which are providing services to Indian persons, will fall within the ambit of the regime. IT companies based inside India with a global customer base could see an increased demand for their services to the extent they can attest to being compliant with the Bill. Companies are facing increased scrutiny with respect to the vendors they select, so high local standards for data protection may be seen as an important part of their service offering.

Notably, however, the Bill permits the Central Government of India to exempt from its application (by notification) any processing of personal data relating to data principals located outside the territory of India, if such processing is undertaken pursuant to a contract entered into between (i) an Indian data processor (incorporated under Indian law), and (ii) a foreign data fiduciary. This could provide relief for Indian outsourcing companies as well as foreign data fiduciaries from dual obligations under the Bill and GDPR, provided that the personal data in question relates to data principals outside India.

The potential exemption described above may be of particular value to Indian data processors (with non-Indian customer bases) due to the fact that it could allow them to escape expensive and burdensome data localisation requirements. Additionally, it would take them out of the scope of any designation as a "significant data fiduciary", which gives rise to various additional compliance measures.

Shortcomings of the Bill

Most strikingly, the Bill does not define 'business carried out in India'; this will inevitably cause difficulties for foreign data fiduciaries and data processors who are seeking to determine whether the new law applies to them. Furthermore, the Bill fails to consider the interaction of the new rules with (and potential scope for harmonisation with) the data norms already established with sectoral regulators such as the Reserve Bank of India and the Telecom Regulatory Authority of India. Certain areas of the Bill also need to be clarified; for example, the Bill introduces the concept of a "purpose limitation" (i.e., that personal data may only be processed for the purpose for which it was collected) but permits processing to the extent carried out for purposes *incidental* to the purposes specified while collecting personal data,

where such incidental purpose may be reasonably expected by the data principal in the context and circumstances. Guidance will need to be published, with the aim of unpacking and clarifying concepts such as the "incidental" purpose "reasonably expected by the data subject", before data fiduciaries can confidently rely on them.

Areas of incompatibility between the Bill and the GDPR

As already noted in this article, the Bill and the GDPR can be considered both complementary to each other and also conflicting. Areas of tension include:

The incompatibility of the principles of data minimisation and storage limitation (under the GDPR) and data localisation (under the Bill)

While the GDPR encourages a minimalist approach to the collection and prolonged retention of personal data, the Bill requires that a copy of all personal data collected be maintained in India. The limits of the Indian requirement are not yet clear, but it is possible that it would require records to be maintained in India even where they have been purged from systems where the GDPR applies.

Consent withdrawal and grounds for processing

Under the GDPR, the data subject (data principal) has the right to revoke consent at any time, where relied upon as the legal grounds for processing. Consequently, data controllers are moving away from reliance on consent and are relying on other grounds such as the processing being necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. However, under the Bill, consent of the data principal is the primary ground for processing. Businesses caught by both regimes will therefore need to carefully consider the grounds upon which processing is based, as reliance on consent could give rise to disruption where the right to withdrawal is used.

Areas of divergence between the Bill and the GDPR

In addition to the seemingly contradictory provisions described above, there are other areas where the Bill does not mirror the GDPR, including:

Information requirements

The Bill does not require the data fiduciary (data controller) to provide the data principal (data subject) with information about the fact that profiling and automated decision making may be undertaken as part of the data processing.

Subject access requests

Under the GDPR a data subject (data principal) has a right to request a copy of their personal data from the data controller (data fiduciary). The Bill only requires that the data principal be provided with a "brief summary" of the personal data.

Right of erasure

Under the GDPR, the data subject has the right to request the erasure of personal data and the controller is required to erase personal data without undue delay, subject to certain exceptions contained therein. While the Bill gives the data principal a right to be forgotten, this right only restricts any continuing disclosure of such personal data and does not extend to erasure of the same.

Conclusion

Many multinational organisations have used the GDPR as a "gold standard" for global data protection compliance, while reviewing local law for compatibility on a case-by-case basis. A GDPR compliant multinational organisation with operations in India will therefore be comfortably ahead of the curve when the time comes to implement the new Indian data protection law. Equally, Indian companies which have achieved compliance with the new Indian law will have already undertaken a lot of the work required to become compliant with the GDPR and will therefore find it easier to do business with the EU and/or set up an establishment in the EU.

While the GDPR remains a "gold standard", careful analysis of the requirements in each jurisdiction will be necessary as the global data protection landscape grows in complexity.

However, as the Bill shows, it may be increasingly common for data protection laws to contradict each other in certain fundamental ways. While the GDPR remains a "gold-standard", careful analysis of the requirements in each jurisdiction will be necessary as the global data protection landscape grows in complexity.

Authors:

Supratim Chakraborty
Partner
Khaitan & Co LLP

Sumantra Bose
Associate
Khaitan & Co LLP

Nallini Puri
Partner
Cleary Gottlieb Steen and Hamilton LLP

Gareth Kristensen
Associate
Cleary Gottlieb Steen and Hamilton LLP

Natalie Farmer
Associate
Cleary Gottlieb Steen and Hamilton LLP

KHAITAN &CO
Advocates since 1911

Founded in 1911, **Khaitan & Co** combines a rich heritage of over a hundred years with modern, cutting edge and solution oriented legal practices and offers full service legal solutions to its domestic and international clients. The firm has a strength of over 570 fee earners, including 130 partners and directors across India. The firm's corporate/M&A practice and several other practice areas including banking and finance, capital markets, competition/ antitrust, dispute resolution, energy, infrastructure and resources, private clients, funds, hospitality, intellectual property, labour and employment laws, real estate, taxation, technology, media and telecom, and white-collar crime are considered independent top-tier practices and feature prominently in various leading international and Indian publications. The firm has also developed expertise in regulated or highly-specialised industries with cross-practice teams of lawyers.

khaitanco.com

CLEARY GOTTLIEB

Cleary Gottlieb Steen and Hamilton LLP is a truly international law firm, with a network of specialists in 16 integrated offices on four continents. Cleary Gottlieb regularly advises global clients in diverse industries on the privacy, data protection and cybersecurity challenges impacting their businesses. The Cleary Gottlieb privacy and cybersecurity task force, comprising lawyers from practice areas across the globe (including banking and financial institutions, commercial litigation, corporate governance, intellectual property, sanctions and anti-money laundering, and white-collar defence and investigations), works collaboratively across disciplines and jurisdictions to advise domestic and multinational clients not only on legal obligations and liabilities, but also on anticipated changes in laws and enforcement practices, strategies for managing compliance and risks, and minimising the costs and efforts of compliance.

clearygottlieb.com