KOCHHAR&CO.
ADVOCATES & LEGAL CONSULTANTS

Technology Law Advisory – Digital Personal Data Protection Bill, 2022

INTRODUCTION

On November 18, 2022, the Government of India released the long awaited fourth draft of India's proposed privacy law, now renamed as the Digital Personal Data Protection Bill ("Bill"). The Government has sought for feedback on the draft Bill by December 17, 2022.

At first glance, the Bill is quite a surprise – it is a completely new draft and not a redraft of the previous versions of the Bill and is much shorter and simpler. It departs substantially from the GDPR model of privacy laws that is quite commonplace today.

APPLICABILITY

The law applies only to personal data that is collected online or which is collected offline, but which is digitized. The law will apply to processing of personal data outside India if such processing is in connection with any profiling of principals in India or activity of offering goods or services within the territory of India. The law also exempts processing of data in India of persons located outside India under a cross border contractual arrangement - this essentially covers the offshore/outsourcing industry.

DEFINITIONS

The Bill uses similar nomenclature as the previous versions. A data subject is referred to as a data principal and a data controller is referred to as a data fiduciary. There is no concept or definition of sensitive personal data. The DPA is referred to as the Data Protection Board of India ("DPBI").

GROUNDS FOR COLLECTION AND PROCESSING

Consent continues to be the main ground for processing of personal data. It must be "freely given", "'specific", "informed" and an "unambiguous indication of consent" through a "clear affirmative action". It seems clear that explicit consent would be required. Consent can also be withdrawn, the consequences of which would be borne by the data subject.

The draft Bill also includes obvious grounds for processing of personal data such as compliance with laws and court orders, actions dealing with epidemics or law & order situations.

The concept of legitimate interest appears to be captured in different ways. Several situations are mentioned whereby consent is deemed to have been given. These include processing of personal data "in public interest" including to prevent or detect fraud, for network and information security, credit scoring, processing of publicly available personal data and for recovery of debt. It seems unclear though whether private enterprises can use these grounds given that the processing needs to be "in public interest". There is also the ground of "fair and reasonable purpose" but in this case, the government has to notify what is a fair and reasonable purpose. In this regard, the law prescribes that the government can consider legitimate interests of the data fiduciary.

One key ground is where processing of personal data is "necessary" and where personal data is provided voluntarily and "it is reasonably expected that the data subject would provide such personal data". One would have to show that the processing is "necessary" and the personal data was provided "voluntarily" and the data principal would reasonably be expected to provide such data. On wonders whether this provision could have been drafted better, assuming this is intended to be a legitimate

interest type of ground. It will likely become the most important provision of the new statute for businesses that do not wish to go down the consent route.

NOTICE

The previous versions of the Bill provided for extensive information to be provided as part of notice to data principals. That was hugely an overkill. This version covers only two things – the types of personal data to be processed and the purposes of processing. This information has to be provided in an itemized manner.

APPLICABILITY TO CHILDREN

The draft Bill keeps the threshold for children at 18 years. This will be seen as a disappointment for the online world as global standards tend to be closer to 16 years. Verifiable parental consent is required for collection of personal data of children. Further, the Bill prohibits profiling of children or behavioral monitoring or targeted advertising to children. However, the Government has the power to exempt these requirements through notification.

RIGHTS AND DUTIES OF DATA PRINCIPALS

There are several rights of data principals. This includes the right to know what personal data is being processed and the right to have inaccurate personal data corrected. A data principal can also ask for personal data to be deleted on the ground that its storage no longer serves the purpose for which it was collected. Interestingly, the Bill includes duties of data principals. This pertains essentially to a duty not to provide false information and not to lodge frivolous or false grievances.

STORAGE OF PERSONAL DATA

The draft law requires the data fiduciary to ensure that personal data maintained is accurate and to use appropriate organizational and technical measures to comply with the law. Data fiduciaries must also use reasonable security measures to prevent data breaches. A data fiduciary may maintain personal data only as long as it serves the purpose for which it was collected or for a legal or business purpose. Thereafter, the personal data needs to be deleted.

PERSONAL DATA BREACH

The draft Bill defines a 'personal data breach' to mean any unauthorized processing or accidental disclosure, use, alteration, or destruction of personal data, that compromises its confidentiality, integrity, or availability. In case of personal data breach, the data fiduciary or data principal must inform both the DPBI as well as the affected data principal, in a manner prescribed by the government. The broad definition of a personal data breach would cover small instances of data breaches for which notification to the government and data principals seems quite onerous.

SIGNIFICANT DATA FIDUCIARY

The draft law retains the concept of a Significant Data Fiduciary ("SDF"). This is a data fiduciary that fulfills the criteria set forth by the government. In determining who would be an SDF, the government would consider factors such as volume of data and risk of harm. Interestingly, such factors also include "potential impact on the integrity and sovereignty of India" and "risk to electoral democracy". SDF's are required to appoint Data Protection Officers, who must report to the Board of the company. Further, they have to appoint an independent data auditor to audit compliance with the privacy law. The Government can also notify when SDF's have to conduct privacy impact assessments.

DATA PROTECTION OFFICER

Only a SDF is required to appoint a Data Protection Officer. However, every data fiduciary must appoint a person to act as the point of contact for anyone who wants to file a grievance. The contact details of the grievance officer needs to be published.

DATA LOCALIZATION AND DATA TRANSFERS

The draft Bill does not directly include provisions on data localization. Gone is the requirement that critical personal data needs to be stored only in India or that sensitive personal data can be transferred outside India but a copy must be retained in India. The Bill states that the Government would notify countries to which personal data can be transferred. It would appear that until the Government notifies these countries, personal data can be freely transferred outside India though perhaps the notification will be issued at the time the law comes into force. The law is absent on other means of allowing data transfers such as through standard contractual clauses – this is after all the method by which personal data is transferred from the EU to India.

EXEMPTION TO GOVERNMENT

The Bill grants the power to the Government to exempt itself and its agencies from any requirement of the Bill. The grounds mentioned, such as sovereignty and integrity of India, security of state, etc., are taken from the Constitution of India and also cited by the Supreme Court of India as grounds on which privacy rights can be restricted. These grounds are however quite broad and proportionality and reasonableness are not essential ingredients.

PENALTIES

The draft new law prescribes penalties for non-compliance. There is a schedule which mentions penalty caps for specific violations. For example, failure to take reasonable security safeguards to prevent personal data breach would involve a penalty of up to Rs 25 million (approx. USD 30 million). Penalties in general can go up to Rs 50 million (approx. USD 60 million). Interestingly, there is no provision for awarding compensation to affected data subjects.

ANALYSIS

In concept, the Government has taken a decidedly Indian approach to drafting this legislation. It is far simpler than past versions and goes against the current trend of the GDPR model of privacy legislation. This type of legislation is quite appropriate for India given its huge unorganized and SME sector and given that standards of privacy compliance are quite low in India. It probably does mean though that the legislation will fail to obtain an adequacy ruling from the EU. In any case, due to not having independent oversight over government surveillance, Indian law does not fully comply with Schrems II.

There are however a host of issues that need to be dealt with in the law. Most important is to clarify the language surrounding the legitimate interest type of ground which we believe is at the heart of privacy legislation. Is the concept of necessity sufficient to deal with legitimate situations of collection and processing of personal data? It would also appear that notice requirements apply only when consent is being obtained. This means that when personal data is being processed under other grounds, that fall under deemed consent provisions, no notice is required. The need to prescribe consent is itself debatable. Consent has been found to not really be a means of protection to data subjects especially since in most cases, data subjects have no choice but to give consent.

One recommended approach has all along been to have a light touch legislation and to allow the DPA to build further regulation slowly through delegated legislation. This draft legislation partially follows that approach. While the DPBI does have powers to pass regulations, this relates only to carrying out the provisions of the law. It is debatable whether it has powers to pass regulation on matters not mentioned in the law. For example, issues such as data portability, privacy by design, etc., find no place in the Bill. It would have been better for the powers given to the DPBI to have been spelled out in greater detail.

The blanket ban on tracking of children's activity on the internet and behavioral advertising seems somewhat unreasonable. How would an online video or music channel for example recommend movies or music to children based on their tastes without tracking their activity?

The Bill also gives the government the power to exempt any of its instrumentalities from any of the provisions of the law. There is no reasonableness or proportionality threshold mentioned. Perhaps it can be read into the law given pronouncements already made by the Supreme Court of India. The blanket exemption to the Government on the need to delete data that no longer serves the purpose for which it was collected is also unfortunate. It is also unfortunate that the composition of the DPBI has not been prescribed in the law thereby leaving it to the Government to appoint whoever they want. A tech savvy and nimble DPA is very much required in order to manage data privacy regulation in India especially given that some of the requirements of the law will be "as may be prescribed" later.

Overall, the approach adopted makes sense given the Indian environment and can be a launching pad for more extensive privacy related regulation in the future. There are obviously gaps and drafting errors but that must be expected in a simpler legislation that also strikes a new path and is drafted by people who are not privacy experts. It is hoped that the Government will work with the privacy community to iron out these issues and take this document to enactment.

XXX

ABOUT KOCHHAR & CO

Kochhar & Co is a leading full service commercial law firm with a national presence in India. The firm mostly represents international companies doing business in India and offers a high quality, business oriented service to its clients. The firm takes great pride in its client servicing approach which is focused on clarity, accessibility and providing business solutions. The firm has a large national presence in India with offices at Delhi, Gurgaon, Mumbai, Bangalore, Chennai, Hyderabad and Chandigarh as well as overseas offices in Dubai, Singapore and Chicago.

TECHNOLOGY LAW PRACTICE

Kochhar & Co set up India's first Technology Law Practice, which has been a leading tech practice in the country ever since. The practice covers areas such as licensing, outsourcing, e-commerce, telecom, intellectual property, privacy, regulation of STP/s and SEZ's, etc. The firm has a large clientele of international technology companies doing business in India. Legal 500 rates Kochhar & Co as a Tier 1 firm for TMT work.

DATA PRIVACY PRACTICE

Kochhar & Co has a large data privacy practice, assisting multinationals in understanding the applicability of Indian law to the processing of personal information and in advising on data security issues. The firm also advises on sectoral regulations especially in telecom, banking and the payments sectors. The firm has also handled numerous matters concerning data security breaches, including criminal action in cases of data theft.

CONTACT DETAILS

Stephen Mathias stephen.mathias@bgl.kochhar.com
Suhas Srinivasiah suhas.srinivasiah@bgl.kochhar.com
Arun Babu arun.babu@bgl.kochhar.com