KOCHHAR & CO.
ADVOCATES & LEGAL CONSULTANTS

Technology Law Advisory – Analysis of the Personal Data Protection Bill

INTRODUCTION

The committee appointed by the Government of India to draft a new data privacy law for India released a draft law called the Personal Data Protection Bill. Since then, there have been numerous public consultations on the bill. It is believed that the bill will be finalized by the government and introduced in Parliament shortly.

The bill appears to be somewhat styled on GDPR, having extensive obligations relating to the basis for processing of personal data ("PD"), provisions on data portability, right to be forgotten, privacy by design, etc. The bill also provides for a Data Protection Authority of India with extensive powers of delegated legislation. The bill uses the terms data fiduciary instead of data controller and data principal instead of data subject.

This update is not meant to provide a summary of the law but to examine some key aspects of the bill that are of concern to companies doing business in India.

KEY ASPECTS OF THE BILL

Applicability to foreign data

The bill has fairly wide applicability as it relates to PD that has been "collected, disclosed, shared or otherwise processed" within the territory of India. In addition, it relates to the processing of PD by the government, an Indian citizen or entity incorporated in India.

A key issue relates to its applicability to foreign data that may be processed in India. This is particularly relevant in the context of the huge offshore processing industry in India, which processes so much of the world's PD. Even if the data is stored offshore and accessed remotely, Indian law will still apply as the law also covers data processed in India. This is somewhat alarming for the offshore industry as the grounds for processing data are stricter under this law than in many countries. For example, consent is more or less an absolute required under the bill whereas even under GDPR, PD can be processed without consent under the principle of legitimate consent.

It is noted however that with regard to foreign data processed in India, the bill gives the government the power to exempt any aspect of the new law from such data processing. This may assuage the fears of the offshore industry somewhat but there is still some concern whether a new regulator will understand the issues involved well enough so as to craft an exemption that works well.

Notice requirements

The bill contains some fairly onerous notice requirements that may be difficult to implement in practice. For example, the notice must include the details of individuals or entities with whom the PD would be shared. This is simply not feasible as service providers who access the PD will keep changing. The notice should also include other information such as the purpose for which the PD is processed, categories of PD to be collected, the identity and contact details of the data fiduciary, the right to withdraw consent, the basis of processing, etc. It also needs to mention information regarding any cross border transfer of PD that is intended. Overall, while standard information relating to purpose, categories, etc, can be included in a privacy policy, disclosing information on entities with whom the data would be shared is difficult.

Basis of collection and storage

The bill applies standard principles to the collection of storage of data. The data processor owes a duty to process PD in a fair and reasonable manner. It can be processed only for purposes specified and for incidental purposes which the data principal would reasonably expect it to be used for. Such collection should be limited to data that is necessary for the purpose of processing. It should be ensured that the data is complete, accurate, not misleading and updated and should be retained for only as long as is reasonably necessary to satisfy the purpose of use.

Consent as a ground for processing

One key aspect of the bill is the near absolute requirement of consent in order to process PD. There are several grounds for processing of PD but those are fairly specific – for functions of the state, fulfilling orders of a court or tribunal, medical or public order emergencies, etc. One key ground is employment related - where PD is necessary for recruitment, termination, providing benefits and conducting assessments of employees. Other than the above, the only ground for processing of PD is consent. This makes the new law stricter than GDPR which allows a business to process PD under the ground of "legitimate interest". As can be seen below, the manner of obtaining consent is quite onerous and not easy to satisfy. This will make finding a ground for processing PD to be difficult. It is noted that PD can be processed if it is for a "reasonable purpose" but only if such reasonable purpose has been notified by the authority. Until then, except for specific instances, consent is the only ground for processing PD.

Requirements for obtaining Consent

The bill includes requirements for obtaining consent. Consent needs to be free, informed (notice requirements), specific, clear (through an affirmative action) and capable of being withdrawn. Significantly, the law states explicitly that for data which is "not necessary" for the purpose of processing any PD, provision of service cannot be made conditional on consent being provided for the processing of such data. This runs somewhat contrary to an earlier provision which makes it clear that collection of data itself should be limited to data that is necessary for the purpose of processing.

Overall, these GDPR type requirements will make obtaining consent difficult and the right to withdraw consent would trouble data fiduciaries. It should be noted however that anonymized data is not covered by the law, but only if the data is anonymized irreversibly.

Sensitive PD

Sensitive PD (SPD) covers passwords, financial data, health data, sexual orientation, biometric and genetic data, caste, religious data and political beliefs. The provisions on obtaining consent for collecting PD apply but there are some additional conditions. Some other grounds for collection of PD such as employment do not apply. Overall, the inclusion of passwords and financial data as SPD is questionable.

Breach notifications

The law provides for notification to the authority by a data fiduciary in case of a PD breach but only where such breach is "likely to cause harm" to a data principal. The authority thereafter has the right to notify the concerned data principals and its decision would be based on the extent of severity of the harm that may be caused to the data principals. It is not clear whether existing obligations to report data breaches to the CERT would continue.

Data portability and right to be forgotten

The bill includes several rights of the data principal including the right to information on what PD has been processed and the right to correction of data. It also includes a right to portability of data in a structured, commonly used and machine readable format. It is not clear to what extent derivative data needs to be included since even data generated in the course of provision of services or use of goods is covered. It is also not clear whether a copy can be retained when PD is ported.

There is also a right to be forgotten but the data subject has to apply to the authority for approval of the same. One wonders how this will work – we expect that thousands of applications will pile up with the authority in a short time and this process will become unmanageable. A better approach would be for the authority to have the power to apply the right in specific situations and build a set of rules surrounding this over time.

These concepts are fairly new globally and jurisprudence is yet to be adequately developed. Applying these provisions directly by statute especially applicability to derivative data is of concern particularly in the world of big data and artificial intelligence.

Significant data fiduciaries, data audits and PDA's.

The law prescribes a category of data fiduciaries as "significant data fiduciaries". The authority would notify who would be covered under this category based on various factors such as volume of data, sensitivity of the data, turnover, likelihood of harm being caused, etc. The requirements of data audit, privacy impact assessments (PDA's"), record keeping and appointment of a data privacy officer are applicable only to significant data fiduciaries. Significant data fiduciaries also need to register with the authority.

The law requires a PDA to be conducted in certain circumstances – where the processing involves new technologies, large scale profiling, use of sensitive PD such as genetic data or biometric data or any data that carries significant risk to the data principals. The PDA must describe the processing, assess the harm that might be caused and describe measures to minimize such harm. The PDA has to be conducted and submitted to the authority and thereafter, the authority may decide that harm may arise and the processing should cease or can impose conditions. The law also prescribes an annual data audit to be conducted by an independent data auditor, who would need to be registered with the authority.

The requirement that only significant data fiduciaries need appoint a data privacy officer is somewhat surprising as many other large businesses that collect PD should have a DPO. The requirement of registration may appear unnecessary at first glance but if it is a non discretionary online registration, it may be useful in terms of communicating with significant data fiduciaries. Some of the grounds for PDA are inappropriate covering for example, processing involving "new technologies". Businesses are regularly employing new techniques to deal with data and it is difficult to determine what is a new technology. A broad principle covering high risk may be more appropriate. A focus on building a case for legitimate interest as an earlier step may also be a way forward.

Data Localization and cross border transfers

The bill includes extensive provisions on data localization and cross border transfers. "Critical data" can only be processed on a server located in India. The law does not define what is critical data and leaves it to the Government (significantly, and not the authority) to notify its meaning. It is believed however that critical data will have a very narrow meaning. There is also some ambiguity surrounding this rule as it refers only to the processing needing to be done on a server in India and does not appear to prevent data mirroring outside India.

As regards all other data, a "serving copy" is required to be maintained in India, in other words, the data needs to be mirrored on a server in India. This may be less of a concern for retail data such as from social media which is already mirrored in India to reduce latency by employing CDN's.

The bill allows for cross border transfer of PD in certain circumstances. The key aspect of this is that consent of the data principal is an absolute requirement. In addition, grounds for transfer include through use of standard contractual clauses or inter group transfers approved by the authority, transfer to countries approved by the authority and particular types of transfers approved by the authority. In fact, any transfer of PD even within India must be done only through a valid contract.

Overall, the provisions seem quite restrictive both in terms of strict data localization and data mirroring. Further, the grounds for cross border transfers seem impractical, including in particular the requirement of inter group schemes and clauses needing to be pre-approved by the authority. The data localization provisions are perhaps the most controversial especially for multinationals operating in India who house their data in a few data centres around the world and not necessarily in India. But in reality it will affect start ups, medium sized and larger Indian businesses more as many of them use cloud based applications which are hosted overseas that serve businesses in multiple countries.

Penalties and remedies

There are several criminal penalties prescribed including violation of the law relating to the collection, disclosure or transfer of PD which results in "significant harm" if the collection, disclosure, etc, is done "knowingly, intentionally or recklessly". This attracts imprisonment of up to 3 years or a fine of up to Rs 200,000 or both. A standard provision in Indian laws concerning offenses by companies is also mentioned – that the concerned individual who was "responsible to the company for the conduct of the business" would be liable though he can take the defense that the offense was committed without his knowledge or that he exercised due diligence to prevent the commission of the offense. Significantly, section 72A of the IT Act, which provides for a criminal penalty when a person discloses PD without consent or in breach of contract "with the intention of or knowing it is likely to" cause wrongful gain or wrongful loss is proposed to remain on the statute.

There are elaborate provisions on penalties as well. The two key provisions divide obligations into two categories. One category provides for a penalty up to Rs 50 million or 2 percent of worldwide revenue, whichever is higher and the other category provides for a penalty of up to Rs 150 million or 4% of worldwide revenue, whichever is higher. One wonders whether the connection to worldwide revenue is at all necessary considering this is a law that in essence deals with PD of Indian citizens.

Exemptions for manual processing by small entities

There are some exemptions applicable to small entities where PD is processed through means other than

automated means. A small entity however has a narrow definition and applies to a data fiduciary that has less than Rs 2 million turnover in a year, does not disclose PD and processes PD of less than 100 people in a year. The definition is particularly troubling for small vendors who may accept credit cards, digital wallets or Aadhaar based payments and who will surely have more than 100 customers in a year.

GENERAL COMMENTS

In general, the bill appears to adopt a great deal from GDPR. For a country like India which does not have a strong record of protection of privacy rights, this seems like a incredible leap ahead. It has to also be kept in mind that a large part of the Indian economy comprises of small and medium enterprises, many of whom would be covered by the new law. These businesses are only partly digitized. There is a strong likelihood that a large part of the industry will simply ignore the law and not be compliant.

Overall, the bill seems to be an overkill. It is stronger than GDPR in many ways and referred to by many as GDPR+. It is a typical case of Indian overregulation – a schoolmasterly direction of what to do and not do. This is not appropriate for a privacy law when modern privacy law is itself changing, moving away from the consent based model and towards more principles based approaches. A strict, inflexible law will make it difficult for India to keep up with global privacy jurisprudence.

The requirement of consent does not seem workable. Instead, the law could prescribe legitimate interest as a ground and require businesses to build a case for their legitimate interest to process PD based on the benefits derived and the risks involved and by balancing and weighing both aspects. Data localization provisions are likely to hurt the economy, partly the big multinationals who have to spend the money to move data to India but more so smaller Indian businesses who rely on cloud based applications hosted overseas. We believe several of the provisions, especially data portability and the right to be forgotten should merely be documented as rights to be developed and implemented in a phased manner by the authority.

In this technology and data focused law, it is imperative that delegated legislation should be as collaborative as possible. Except when security and emergency issues are involved, the law should require all delegated legislation to be built in a collaborative manner – through consultation papers, discussions with stake holders, draft regulations and finally notification. Industry and government need to collaborate together closely for a law of this nature to work.

Finally, the institution of criminal remedies for non compliance in any area where compliance is often a judgment call is inappropriate. It should have been restricted to situations of data theft.

ABOUT KOCHHAR & CO

Kochhar & Co is a leading full service commercial law firm with the best national presence among all law firms 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 the largest national presence in India with offices at Delhi, Gurgaon, Mumbai, Bangalore, Chennai and Hyderabad..

TECHNOLOGY LAW PRACTICE

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

CONTACT DETAILS

Stephen Mathias stephen.mathias@bgl.kochhar.com
Suhas Srinivasiah suhas.srinivasiah@bgl.kochhar.com
Naqeeb Ahmed Kazia naqeeb.ahmed@bgl.kochhar.com