KOCHHAR&CO.
ADVOCATES & LEGAL CONSULTANTS

Technology Law Advisory – Analysis of the Data Protection Bill, 2021 – INDIA

INTRODUCTION

The Joint Committee of Parliament ("Committee") appointed to review the draft Personal Data Protection Bill submitted its report to Parliament on December 16, 2021. The report also includes a revised draft Bill which has now been renamed as the Data Protection Bill, 2021 ("Bill").

As there is less than a week left of the winter session of Parliament, it is very unlikely the Bill will be passed by Parliament in 2021. However, there is a strong likelihood that the Bill will be passed by Parliament during the budget session of Parliament in February 2022. Given the extensive review conducted, it is also unlikely that there will be substantial changes to the Bill going forward and this now paves the way for businesses to begin preparing for compliance with the new law.

This note examines the key changes recommended by the Committee. This note is focused on businesses who would be covered by the law and does not cover administrative changes such as composition of the Data Protection Authority ("DPA"), etc. It also does not cover guidance provisions such as grounds the DPA must consider in taking certain decisions since these do not directly impact businesses. We have also covered to some extent, provisions of concern that have not been changed in the revised Bill.

KEY ASPECTS OF THE BILL

Applicability

There is no implementation period specified during which businesses can prepare for compliance with the new law. However, the Bill does allow the government to notify when the Bill should come into force, including notifying parts of the law to come into force at different times. This has been done before with other legislations. Further, the Committee recommended that implementation of the new law should be done in a phased manner starting with appointment of the DPA, adjudicators, etc., and that the new law be fully in force within 24 months.

The Bill continues to apply to foreign personal data that is processed in India. It therefore covers foreign personal data being processed in India, such as data processed by India's huge outsourcing industry. This would apply even if the data is stored outside India and remotely accessed from within India. The previous version of the Bill had included an enabling provision for exemptions to be granted as to applicability of the law to such data. This provision remains unchanged in the Bill. However, unless a specific notification is passed, the exemption would not apply to foreign personal data processed in India.

The law continues to apply to inferred data, which is included in the definition of personal information. However, one has to look at specific provisions relating to data portability, right to be forgotten, etc., to determine actual applicability to inferred data.

Non-Personal Data

The Bill covers not just personal data but non personal data as well. This follows the report of a committee appointed by the government on non-personal data. This is why the nomenclature of the Bill has been changed

from the Personal Data Protection Bill to the Data Protection Bill. The exemption given to anonymized data has also been removed.

However, the inclusion of non-personal data is not of too much concern at this stage. Most of the provisions of the Bill still pertain only to personal data.

Section 92 which deals with sharing of data mandated by the government remains and refers only to data being shared "to enable better targeting of delivery of services or formulation of evidence-based policies by the government". This is far less than what was recommended by the Committee on non-personal data which recommended that data fiduciaries would be forced to share data with other businesses so that other businesses could also benefit from such data.

However, it should be noted that the same section clarifies that nothing in the law would prevent the government from framing any policy for the digital economy including measures for growth, security, integrity, and prevention of misuse. This clause now covers handling of non-personal data, including anonymized personal data. At least this allows the government to slowly develop a jurisprudence around non-personal data rather than rush in with an unprecedented, detailed statute on non-personal data that is hard to implement and extremely controversial.

Purpose requirements

Surprisingly, the language that requires that the purpose be specific, clear, and lawful has been deleted. However, there is language in the Bill that the notice given to the data principal must be clear, concise, and easily comprehensible. One would need to observe to what extent these requirements follow GDPR jurisprudence and practices in terms of the ease in preparing privacy policies and obtaining consent.

Consent still required

The Bill still requires consent from the data principal as the key ground for collecting and processing personal data. While there are extraordinary grounds such as compliance with law, directions of a court, etc., the key ground remains consent.

Reasonable purpose and legitimate interest

The previous version did not have a "legitimate interest" type ground. It did however allow the government to notify reasonable purposes for which personal data could be processed without obtaining consent. Though the language of the provision has been changed, the effect is the same. There is no direct reasonable purpose or legitimate interest ground that a business can use to justify collecting and processing of personal data and consent is more or less the only ground. It can use this route only if and when the DPA notifies reasonable purposes. Incidentally, one of the aspects to be considered by the DPA in notifying reasonable purpose is the "interests" of the data fiduciary and this has been modified to read as "legitimate interests". But as stated above, this is not a direct ground, just an aspect for the DPA to consider while notifying the reasonable purposes.

Applicability to Children

There are some minor changes to the Bill with regard to processing of personal data of children. The definition of "child" continues to be persons who have not attained the age of 18. Further, the prohibition on profiling, tracking, behavioural monitoring and targeted advertising or any other processing that causes significant harm continues.

Fairness of algorithms

There is a provision whereby certain information has to be provided by the data fiduciary in order to ensure transparency. The revised Bill provides for an additional requirement to provide information on the fairness of the algorithm or method used for processing of personal data. This means the data fiduciary must explain how the algorithms are being used in a fair manner. This may infringe on intellectual property and/or trade secrets of the data fiduciary.

Breach notifications

One key change in the revised Bill is on breach notifications. The previous version obligated notification only if the data fiduciary concluded that significant harm would be caused. This has been removed and breach notification is now mandatory. The breach notification by the data fiduciary must be issued within 72 hours of becoming aware of such breach. The DPA also has authority to direct that the data fiduciary report the breach to the data principal and take remedial measures.

This relates only to personal data. However, the law allows the DPA to pass regulations on the effect of data breaches in respect of non-personal data as well.

Significant Data Fiduciary

What is meant by a significant data fiduciary has to be notified by the DPA. This remains unchanged. However, there is a change in the nomenclature of social media intermediary to social media platform. Two new categories may be considered – data fiduciaries who process data of children and data fiduciaries above a particular threshold whose actions have or are likely to have a significant impact on the sovereignty and integrity of India, electoral democracy, security of the state or public order". It is reiterated that the Bill does not specify who is a significant data fiduciary and it is left to the DPA to notify this and only the grounds to be considered by the DPA have been expanded.

Data Protection Officer

The Bill requires that a DPO be appointed only by a significant data fiduciary and not by other data fiduciaries. This requirement is unchanged. The Bill now specifies that the DPO must be "key managerial personnel" which covers the CEO, company secretary, whole time director or CFO. This is an unusual requirement because the persons mentioned are not normally appointed as the DPO and are mostly not even qualified to act as such. The DPO is normally a data privacy/cyber security professional who has been certified by IAPP or other organizations. The revised draft does allow the DPA to prescribe other personnel and it is hoped that the DPO would do so fairly quickly to enable businesses to appoint suitable persons as soon as possible. It should be noted though that organizations who voluntarily appoint a DPO because they need to in order to manage compliance with the law would not need to meet these requirements of appointment.

Data Localization

There is no change in the data localization provisions and the provisions are not even discussed in the report. The provisions remain the same that (a) critical data must be stored only in India; (b) SPD can be transferred outside India but must continue to be stored in India. It is relevant to note that financial information, official identifiers, and biometric information (including photographs) are covered in the definition of SPD. These three types of SPD could trigger data localization requirements for many multinationals operating in India.

Cross Border Data Transfers

There are some minor changes to the provision on cross border data transfers including that the DPA should not approve such transfers if they are against public policy or state policy. A more important addition is that SPD cannot be shared with any foreign government unless such sharing is approved by the government. This may be a problem for some organizations if they store India data overseas and are subject to requests from home governments for information that may include India data.

Exemption to small entities

Small entities may be exempted by the DPA based on certain considerations as long as they engage only in manual processing of personal data. The term "manual" in the previous version of the Bill was somewhat confusing and could be seen as non-electronic. The revised Bill retains the exemption but uses the term "non automated". This clarifies the meaning of the clause.

Focus on Government power

There is extensive focus on government power with the applicability of some provisions being varied if they would be prejudicial to the exercise of government power. There are some additional provisions that require the DPA to consult with the government and for the government to issue directions to the DPA. In practice, this is unlikely to make a difference as the DPA would very likely be someone who has a good rapport with the government.

There is concern expressed in most of the dissenting notes of members of the Committee that the Bill enables sweeping exemptions to the government. Some members suggested that at least basic requirements be included such as that personal information be processed in a fair and reasonable manner by the government and that security requirements should be applicable to the Government.

There is however a provision that appears to have been added after the final draft was approved which was suggested in some of the dissenting notes of the members that the procedure to be followed by the exempt agency must be just, fair, reasonable, and proportionate apart from following safeguards and oversight mechanism as may be prescribed. It is not certain though that these standards make a difference unless they relate to the substance of the exemption and not just the procedure.

Policy related recommendations.

There are several recommendations in the report which do not find place through a proposed amendment to the Bill. Some of these recommendations are somewhat ominous. However, it would require further effort from the government separate from the enactment of the Bill. They include:

- A requirement to treat a social media intermediary as a publisher and not as an intermediary where the social media intermediary has the ability to select the receiver of the content and also exercises control over access to such content. This is somewhat controversial especially in the case of automated distribution of content.

- A power given to the DPA to frame regulations to regulate hardware manufacturers and to put in place a certification process for hardware and IoT devices and also set up testing laboratories across the country. It should be noted that all telecom equipment is already subject to this certification.

- An alternate payment system to SWIFT to be set up by the Government to reduce dependence on SWIFT.

- A recommendation to create a new regulatory body to regulate all kinds of media including online media, to replace the Press Council of India.

GENERAL COMMENTS

Overall, there is little change in terms of substance. Most of the changes are adding grounds for the DPA to consider or granting powers to the government or language changes that do not change the substance of the draft law. While this is a large report and changes have been suggested in many provisions, in the context in which regulation operates in India, the changes are not substantial.

There are several disappointments, particularly the requirement of consent and the absence of a direct "legitimate interest" ground. The definition of sensitive personal data and the requirement to have a copy of the data in India would result in substantial data localization in India.

Overall, the Bill continues to be quite burdensome on businesses and particularly so in a country like India that has seen very low levels of privacy protection. This may be the most impactful law to hit Indian businesses in many years.

We believe the time has come for businesses to start preparing to comply with the draft law as it is very likely to be enacted in the first few months of 2022.

XXX

ABOUT KOCHHAR & CO

Kochhar & Co. is one of India's pre-eminent corporate law firms. 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 full-service presence in six (6) prominent cities namely New Delhi, Mumbai, Bangalore, Chennai, Gurgaon, and Hyderabad and three (3) overseas offices – Dubai, Singapore, and Chicago.

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, privacy, etc. The firm is the preferred legal counsel to many of the world's largest information 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 payments sectors. The firm has also handled numerous matters concerning data security breaches, including criminal action in cases of data theft.

CONTACT DETAILS

rohit.kochhar@kochhar.com
stephen.mathias@bgl.kochhar.com
tomio.isogai@kochhar.com