KOCHHAR & CO.
ADVOCATES & LEGAL CONSULTANTS

Technology Law Advisory – Digital Personal Data Protection Act, 2023

INTRODUCTION

During the week of August 7, 2023, the Indian Parliament passed the Digital Personal Data Protection Act ("Act") thereby bringing to a close a 5 year process to introduce a data privacy law for India. The Act was assented to by the President of India and will come into force once notified by the Government. It is now a foregone conclusion that this Act will be the data privacy law of India in the days to come.

The Act follows on the lines of the previous version – a much simpler version that departs substantially from the GDPR model of privacy laws that is commonplace today. However, it contains significant changes apart from dealing with several of the concerns relating to the previous draft.

DEFINITIONS

The Act uses similar nomenclature as in 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 of sensitive personal data. The Data Protection Authority is referred to as the Data Protection Board of India ("DPBI").

APPLICABILITY

The law applies only to personal data that is maintained in digital form. The law will apply to processing of personal data outside India if such processing is "in connection with any activity related to offering goods or services to data principals within the territory of India".

GROUNDS FOR COLLECTION AND PROCESSING

Consent continues to be the main ground for processing of personal data. It must be "freely given", "'specific", "informed", "unconditional", 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 Consent can also be withdrawn, the consequences of which would be borne by the data principal. One can also use a consent manager to manage the consent process.

The Act also includes obvious grounds for processing personal data without consent, for 'legitimate uses' such as compliance with laws and court orders, actions dealing with medical emergencies and epidemics and law & order situations. Further, processing of personal data for certain employment purposes or for protecting an employer from liability, constitutes legitimate use under the Act, and consent is not required for such processing.

Another key ground which qualifies as a legitimate use, is where the data principal voluntarily provides her personal data to the data fiduciary for a specified purpose and where the data principal has not indicated that she does not give her consent for use of her personal data. This appears to deal with automatic collection of personal data – the illustration covers a situation where a person visits a shop and hands over her personal information.

LEGITIMATE INTEREST

As in the previous versions, there is no clear "legitimate interest" ground. The situations of legitimate uses are borne of necessity and don't cover as much ground as the concept of legitimate interest under the GDPR. Except for the limited grounds that qualify as 'legitimate use', consent seems to be the only route to processing personal data.

NOTICE

The notice to be given to the data principal covers two key aspects – the personal data to be processed and the purposes of processing. In addition, the data principal should be informed of her right to withdraw consent and the grievance redressal procedure available to her. It appears that the notice must be made accessible in English and in all 22 languages specified in the Eighth Schedule of the Constitution.

APPLICABILITY TO CHILDREN

The law 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 Act prohibits processing that may have a detrimental effect on the well-being of the child as well as behavioral monitoring or targeted advertising to children. However, the Government has the power to exempt some of these restrictions through a notification.

RIGHTS AND DUTIES OF DATA PRINCIPALS

There are several rights of data principals. These include the right to know what personal data is being processed and the right to have inaccurate personal data corrected or personal data to be updated. A data principal can also ask for personal data to be deleted unless it is still required for the specified purpose for which it was collected. However, these rights exist only when personal data is provided voluntarily or with consent. Interestingly, the Act 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 law requires the data fiduciary to ensure completeness, accuracy, and consistency of personal data where it is used to make a decision that affects a data principal or where it is disclosed to another data fiduciary. This may have implications for the use of AI on personal data. Data fiduciaries must also use reasonable security measures to prevent data breaches. A data

fiduciary must delete personal data when the specified purpose for which it was collected has been served unless such personal data is required to be retained for compliance with any law.

PERSONAL DATA BREACH

The law 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 a 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 even small instances of data breaches and situations of vulnerability for which notification to the DPBI and data principals seems quite onerous.

SIGNIFICANT DATA FIDUCIARY

The 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 a SDF, the government will consider factors such as volume of data processed by the data fiduciary and risk to rights of the data principal. Interestingly, such factors also include "potential impact on the integrity and sovereignty of India" and "risk to electoral democracy". An SDF's is required to appoint a Data Protection Officer, who must report to the Board of the company. Further, it must appoint an independent data auditor to audit compliance with the privacy law. They also have to conduct privacy impact assessments.

DATA PROTECTION OFFICER

Only an 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 data principals who wish to raise any issues. The contact details of the Data Protection Officer and the grievance officer need to be published.

DATA PROCESSORS

The law requires data fiduciaries to execute a data processing agreement with a data processor. Data fiduciaries are responsible for compliance of the law by data processors.

DATA LOCALIZATION AND DATA TRANSFERS

The law includes a right on the government to notify a "negative list" of countries to whom personal data cannot be transferred. Other than this list and in the absence of a notification being issued, one can transfer personal data to any country. There is no requirement for adequacy in the statute or for retaining copies of the personal data in India. Other means of transferring personal data to blacklisted countries such as standard contractual clauses, explicit consent or inter-group transfers are not covered in the Act. The Act does however permit sectoral data localization regulations such as the one that exists in the payments sector.

EXEMPTION TO GOVERNMENT

The Act grants the power to the government to exempt itself and its agencies from most requirements of the Act. The grounds mentioned, such as sovereignty and integrity of India, security of state, etc., are taken from the Constitution of India and are 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. These are also grounds of legitimate use for which processing of personal data by the government does not require consent. Unfortunately, the law has extended a direct exemption to the judiciary to bodies that have regulatory or supervisory functions. No government notification is required for this exemption to apply; these organizations are directly exempted under the law.

EXEMPTION TO OTHERS, START UPS

The Government has the power to exempt certain data fiduciaries including start ups from some provisions of the law (right to access, requirement to give notice, limitation on retention). It appears the government will implement some kind of regulatory standbox for start ups to make it easier for them to comply with the new law.

CONTENT BLOCKING

The law grants powers to the government to block public access to any information generated, received, stored, or hosted in any computer resource used for providing services within India, in the 'interests of the general public', upon receiving a reference from the DPBI. While the government has similar powers under the Information Technology Act, 2000, such powers do not relate directly to the protection of personal information.

PENALTIES

The law prescribes penalties for non-compliance. There is a schedule which mentions a maximum penalty for specific violations. For example, failure to take reasonable security safeguards to prevent personal data breach would involve a penalty of up to Rs. 2.5 billion (approx. USD 30 million). This is the maximum penalty prescribed. Interestingly, there is no provision for awarding compensation to affected data subjects.

ANALYSIS

Approach. When the previous draft was released in 2022, we said that the government's approach was appropriate for a country like India. India does not have a long history of compliance with privacy standards and also has a huge unorganized and SME sector. At the same time, most businesses will have stored some personal data, especially payment information, in digital form. This means that almost all of Indian industry will be covered by the law. In this context, a simpler legislation with fewer obligations will be a good start.

Notice. The requirement to make the notice accessible in English and in 22 other languages, would be too onerous for most data fiduciaries and may not serve its purpose, since most digital

services and related documentation are anyway made available exclusively in English. Perhaps there will be a clarification that the data fiduciary can provide the notice in English and the most appropriate language among the list of 22 languages.

Legitimate Interest. The government has stuck to its stand from the beginning that legitimate interest, as it is understood in the EU, will not be a part of the law. There are legitimate uses such as statutory necessity, but these are standard and fairly narrow grounds.

Consent. The main ground for processing personal data is consent. The language defining consent is identical to the GDPR leading us to wonder whether India will require consent based on the same standards as in the EU. The addition of the word “unconditional” for collection of all personal information sets a potentially higher standard for obtaining consent than under GDPR.

Voluntary provision of personal data. The provision which allows processing of personal data shared “voluntarily”, is poorly drafted as a data fiduciary can list various specified purposes and the data principal will then “voluntarily” provide her personal data. Perhaps the government meant to refer to a situation where the personal data is provided on the initiative of the data principal. It remains to be seen whether this provision would be abused. The reference to “specified purpose” is also confusing in a situation where personal data is given automatically as part of a transaction and no notice of specified purpose is given.

Purpose Limitation. The language on purpose limitation is not well defined. It is not entirely clear that there is a prohibition on a data fiduciary providing a laundry list of “specified purposes”. It can be interpreted that as long as the personal data is processed for the specified purpose mentioned in the notice, it is permitted. Legitimacy of purpose does not appear to be a part of the law.

Exclusion to Government. The Act contains provisions that exclude the government directly and indirectly. While granting power to the government to exclude some of its instrumentalities is justified, the lack of standards to do so, such as reasonableness and proportionality, is unfortunate. This may however be supplied by the judiciary as the jurisprudence is already developed through past judgments. However, the most unfortunate provision is where the exception granted to the judiciary has been expanded to include bodies that have regulatory or supervisory powers. This would directly exclude vast sections of the government.

Foreign Personal Data. The law excludes most provisions from applicability to foreign personal data that is processed in India. This is somewhat counterproductive as one of the reasons for having a privacy law is to assure the world that it is safe to send personal information to India. It also means 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. The extraordinary powers and exemptions to the government would also make that seemingly impossible.

Data Breach Notification. The insistence on notification of data breach or vulnerability in every case, not just to the DPBI but to concerned data principals goes against global standards. This is one of those instances where the law is stricter than the GDPR. Added to that is the existing and

unfeasible 6 hour breach notification requirement to the CERT-In, the deadline of which appears to be observed mostly in the breach.

Powers of DPBI. The most disappointing aspect of the Act is the lack of powers given to the DPBI. All powers of delegated legislation rest with the government. The DPBI is purely an adjudication body. Personal data is so ubiquitous that it is very hard to pass regulation while understanding all its implications. One needs a tech savvy and nimble DPBI who can issue clarifications, discuss with stakeholders, issue consultation and recommendation papers and guidance notes. None of these powers have been provided to the DPBI. The nature of personal information and the technology world dictates that privacy law be as dynamic as possible. This is not likely to happen in the current scheme of things.

Privacy v. Right to Information. Finally, the law amends the Right to Information Act. Whereas previously, a senior government officer would determine whether public interest outweighed the need to protect personal information, the new legal position would be that personal information can never be disclosed as part of a right to information request.

The Way Forward

The law does not provide for a gestation period for compliance. The Government has announced that it would implement the law within 10 months. We assume that the government will bring the law into force in stages as it has done for some other legislations. It would however be appropriate for the government to notify immediately when exactly the substantive provisions will come into force so that the industry can prepare for it with a clear deadline in mind.

In the days to come, we will be rolling out our own program to train clients and prepare them for compliance with the new law. More on that soon!

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 businesses 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

-§-