Published on *The National Law Review* https://natlawreview.com

India Welcomes Landmark Data Protection Law

Article By:

Malcolm Dowden

Charmian Aw

Bindu Janardhanan

On 11 August 2023, after close to a decade since its initial conception, India's Digital Personal Data Protection Act (Act) received presidential assent, formalising the nation's first ever comprehensive data protection law.

Definitions

There are several key definitions and references adopted in the Act, as follows:

- "Data principal" means a data subject.
- "Data fiduciary" means a data controller.
- "Data processor" means a data processor, but it is remains unclear if it includes a sub-processor.
- "Consent manager" means a person registered with the Data Protection Board of India (Board), who acts as a point of contact to enable a data principal to give, manage, review and withdraw their consent.
- Prior references to sensitive personal data and critical personal data found in the earlier 2022 version of the Digital Personal Data Protection Bill (Bill) have since been removed.

Scope and Applicability

The Act applies to digital personal data, including non-digital data that is subsequently digitised.

Similar to the EU GDPR and UK GDPR, the Act asserts extraterritorial reach, applying to the "processing of digital personal data outside the territory of India, if such processing is in connection with any activity related to the offering of goods or services to Data Principals within the territory of India". As such, overseas entities that offer goods or services in India may find themselves subject to the obligations under the Act. However, unlike the EU GDPR, UK GDPR and even the earlier 2022 version of the Bill, those extraterritorial reach provisions do not apply to processing in connection with profiling of individuals within India. That omission is potentially helpful to organisations outside India looking to use data to, for instance, train artificial intelligence (AI) models using big datasets likely to

include personal data relating to individuals within India. It potentially allows AI service providers to scrape publicly available personal data from the internet without consent and without being swept up by other provisions of the Act.

A noteworthy aspect is that business process outsourcing (BPO) providers are exempted from the Act for offshore personal data processing. More specifically, the exclusion applies where “personal data of Data Principals not within the territory of India is processed pursuant to any contract entered into with any person outside the territory of India by any person based in India”. This, in effect, insulates BPO service providers in India from many of the Act’s provisions, though not from the obligation to implement “reasonable safeguards to prevent [a] personal data breach”. This seems particularly pertinent, given that India houses the world’s largest BPO industry.

Further, the Act does not apply where processing is necessary for “research, archiving or statistical purposes” if the personal data is not used in any decision specific to a data principal and is carried on in accordance with standards that are to be prescribed.

There are also narrower exemptions (specifically, exclusions from most of the obligations imposed on data fiduciaries, save for implementing reasonable security measures to protect the data) in respect of processing of personal data:

- That is necessary for enforcing any legal right or claim
- In the interest of prevention, detection, investigation or prosecution of any offence or contravention of any law
- That is for a scheme of arrangement, merger or amalgamation, or transfer of an undertaking, or involving the division of one or more companies, approved by a court or tribunal or other competent authority
- For debt recovery purposes as circumscribed under the Act

Legal Bases for Processing

The Act only recognises two main lawful grounds for processing personal data, namely:

- Consent from data principals
- Certain “legitimate uses”, such as:
    - A data principal voluntarily providing, to the data fiduciary, their personal data for a specified purpose, without indicating that they do not consent to the use of such data[1]
    - Where the state provides or issues to the data principal any subsidy, benefit, service, certificate, licence or permit, or performs any functions at law or in the interest of India’s sovereignty, integrity or security
    - To fulfil any legal obligation or comply with any judgement, decree or order at law
    - To respond to a medical emergency, provide medical treatment or health services during an epidemic, or for the safety of or to provide assistance during a disaster

Notice and Consent

Notices have the following content requirements:

- They must be in clear and plain language, either in English or, at the data principal’s option, any of the 21 languages specified in the Eighth Schedule to the Constitution of India.

- Notices must include:
- The nature of personal data being collected and processed
- The purpose of processing
- The mechanism or process through which a data principal can exercise their rights in relation to their personal data
- The mechanism or process through which a data principal can make a complaint to the Board
- If a data fiduciary is a significant data fiduciary (see below), the contact details of the data protection officer or any other person authorised by the data fiduciary to respond to complaints and grievances

Unlike its earlier 2022 version of the Bill, however, an itemised notice is not required. Further requirements in relation to notices may be prescribed by the central government from time to time.

Notably, a recent committee report[2] on the new bill contains statements from the Ministry of Electronics and Information Technology, which suggest that these forthcoming rules may require data fiduciaries to provide videos and animations to help data fiduciaries actually understand the notice and any consent form used.

The Act introduces the concept of a consent manager. Data principals can give, manage, review or withdraw their consent to the data fiduciary through a consent manager, who remains accountable to the data principal and must act on their behalf in such manner and subject to such obligations as may be prescribed. Consent managers must also be registered with the Board in such manner and subject to such technical, operational, financial and other conditions as may be prescribed.

Where personal data was collected prior to the enactment of the Act, the data fiduciary must notify the data principal of such collection and use of their data within a reasonably practicable time. If the processing is based on consent from the data principal, then the data fiduciary can only continue to process their personal data until such time as the data principal withdraws their consent.

Significant Data Fiduciaries

The central government is empowered to classify any persons or category of persons as “significant data fiduciaries” based on the following factors:

- The volume and sensitivity of personal data processed
- Risk to the rights of harm to the data principal
- Potential impact on the sovereignty and integrity of India
- Risk to electoral democracy
- Security of the state
- Public order

Once designated, significant data fiduciaries will be required to carry out periodic data protection impact assessments and independent audits, and appoint a data protection officer, who must be an individual based in India, and responsible to the company’s board of directors.

Accuracy

Compared to the earlier 2022 version of the Bill, the obligation to keep personal data accurate has been enhanced. A data fiduciary must ensure the completeness, accuracy and consistency of any personal data it processes, so long as that data is likely to be disclosed to another data fiduciary, or

used to make a decision affecting the data principal.

Protection and Security

A data fiduciary must protect personal data in its possession or under its control, by taking reasonable security safeguards to prevent a personal data breach. This extends to where a data fiduciary engages a data processor to carry out processing of personal data on its behalf.

Cross-border Transfers

Unlike the earlier 2022 version of the Bill, the Act adopts a “negative list” approach for cross-border transfers of personal data from India overseas. It remains to be seen whether neighbouring countries will be included in this negative list, similar to the approach taken in the regulation of foreign direct investment. Additionally, this provision potentially allows sectoral regulatory bodies to introduce specialised legislation aimed at overseeing the storage and transfer of personal data within their respective sectors.

If there are other such requirements or rules that accord a higher standard of protection or impose stricter restrictions for the transfer of data than those under the Act, then these latter requirements will prevail over the Act.

Data Principal Rights

Data principals have the following rights under the Act:

- Right of access
- Right to correction
- Right to erasure[3]
- Right to withdraw consent
- Right to grievance redressal
- Right to nominate any other individual who, in the event of death or incapacity of the data principal, can exercise their rights under the Act.

Retention

Data fiduciaries must erase personal data upon a data principal withdrawing their consent or as soon as the purpose for its processing no longer exists, whichever is sooner. This extends to its having to procure its data processor to erase such data, where the data was made available to such data processor. Under the Act, the central government is entitled to set maximum retention periods for personal data; however, no further details have been provided yet.

Data Breaches

The Act does not prescribe any thresholds or timelines for data breach notifications. It stipulates that in the event of a personal data breach, the data fiduciary must give the Board and each affected data principal “intimation of such breach in such form and manner as may be prescribed”. These aspects are expected to be addressed in forthcoming rules to be issued by the government of India. It is unclear whether exceptions will be granted for minor breaches.

Notwithstanding, this is a notable new obligation, especially when compared to the existing

requirements of having to report to the Indian Computer Emergency Response Team (CERT-In) within six hours of an incident, or to a sectoral regulator, where these rules do not appear as actively enforced.

Additionally, the Act makes it clear that data security and breach reporting now lie solely on data fiduciaries and not processors.

Children

Data fiduciaries must, prior to processing any personal data of children under 18 years of age, obtain verifiable consent of their parents or legal guardians. There are also prohibitions imposed on the tracking or behavioural monitoring of children or advertising targeted at children.

Implementation Period

While the industry has generally embraced this legislation, certain concerns regarding its implementation have arisen. There has not been any definitive stipulation of an implementation timeframe for the Act. It is generally expected that businesses will be given a transitional period of between six and 10 months, though this has yet to be formally published or announced. The Indian government has expressed a willingness to engage in discussions with stakeholders to address the transition period, ensuring a seamless implementation process. Therefore, it is also presently uncertain whether all provisions will come into effect simultaneously or in phases.

Authority

The Board has been vested with the authority to handle complaints in connection with the Act. Aggrieved parties that wish to appeal against a decision by the Board can do so to the Telecom Disputes Settlement and Appellate Tribunal of India.

The central government has very broad discretion and powers under the Act[4], including to exempt certain startups and other data fiduciaries from any specific obligations. The decision to grant such exemptions would typically be based on factors like the volume and nature of personal data being processed.

Penalties

The Board is entitled to impose up to US$30 million in regulatory fines for contraventions of the Act, as well as to compel the blocking of applications and services for repeat offenders.

Takeaways

Now that India has enacted a comprehensive law on data privacy, the importance of undertaking thorough data mapping and information governance cannot be overstated. It forms a crucial starting point for businesses operating in India to ascertain what obligations apply to the data collected, processed and transferred and what compliance measures need to be adopted under the Act, including determining the notices, consents, and protocols needed to respond to data principal rights, conducting periodic trainings on data policies, implementing data management, retention, security, incident response measures, and ensuring robust and compliant contracts with third-party processors. Businesses with significant data processing activities (and thus likely to be classified as a significant data fiduciary down the road) should also consider appointing a data protection officer.

While enactment of the Act is certainly a monumental step for a nation that has a population of a whopping 1.43 billion people, it is also expected that further regulations and guidance will be issued to provide clarity and certainty over specific aspects of the law. With this in mind, businesses should regard compliance with the Act as an ongoing exercise, failing which they risk incurring large regulatory fines and potential lawsuits for infringements.

---

[1] This has replaced the reference to “deemed consent” in the earlier 2022 version of the Bill.

[2] 48th report of the Standing Committee on Communications and Information Technology of the Lok Sabha on the new bill.

[3] Data fiduciaries are obliged to erase personal data that they hold, upon withdrawal of consent by the relevant data principal(s), unless retention is necessary for a specified purpose or to comply with applicable law.

[4] Section 40

National Law Review, Volumess XIII, Number 227