DENTONS LINK LEGAL

The Digital Personal Data Protection Act, 2023

India's new data privacy law sees the light of the day

Grow | Protect | Operate | Finance

INTRODUCTION

Following a unanimous acceptance by both houses of the Parliament, the President of India, Ms. Droupadi Murmu on August11, 2023, has granted assent to the Digital Personal Data Protection Act, 2023 ("**Act**"). The underlining objective of the Act is to reinforce the 'Right to Privacy', which has cast a prominent impact on data privacy with the advancement of technology over the past several years, particularly in the wake of the Supreme Court's decision in the celebrated case of '*Justice K.S. Puttaswamy (Retd.) vs. Union of India*'.

The Act attempts to bring about a significant change in the data protection regime by seeking to protect the rights of data principals (*that is*, the individuals to whom the personal data relates) and regulating data fiduciaries, including companies and businesses that determine the purpose and means of processing the personal data. Importantly, the Act limits the processing of personal data to the extent that there ought to be a lawful purpose in respect thereof, and that the same should be necessary to be obtained by data fiduciaries. The Act holds data fiduciaries, including internet companies, mobile applications and other related businesses, accountable for their data practices provided to data principals.

The Act now awaits notification by the Central Government in the Official Gazette, in respect of appointment of dates for its provisions to come into force thereon, which would replace the existing legal framework governing data privacy in India.

SCOPE AND APPLICABILITY

The Act focuses on processing of digital personal data in India, that is to say, personal data that is either collected: (i) in a digital form; or (ii) in a non-digitized format but subsequently digitized. *As a result, the non-digital personal data and non-personal data would fall outside the purview of the Act.* Similarly, the Act does not apply to: (i) the data processed for personal or domestic purposes; and (ii) personal data that is made or caused to be made publicly available by (a) the data principal to whom such personal data relates, or, (b) any other person acting a legal obligation to make the personal data publicly available.

Consistent with the European Union's General Data Protection Regulation, the Act also has an extra-territorial applicability, such that it applies to processing of digital personal data outside the territory of India, *provided that such processing is in connection with an activity related to offering of goods or services to data principals within the territory of India*. A key departure under the Act from the Digital Personal Data Protection Bill, 2022 ("**DPDP Bill**") in this regard, is the exclusion for 'profiling' of data principals within India from its extra-territorial scope.

NOTICE AND CONSENTS

Under the Act, the data fiduciaries are required to obtain an affirmative consent from the data principal, which needs to be free, specific, informed, unconditional, and unambiguous. Every request for obtaining such consent must be accompanied by a notice informing the data principal in respect of details of personal data sought to be collected and the purpose underlying the proposed collection. The Act imposes an additional obligation on data fiduciaries, which was absent in the previous DPDP Bill, whereby the data fiduciaries need to inform the manner in which the data principal may exercise her rights, and the method in which a complaint can be submitted to the Data Protection Board of India ("**Board**"). *The Act further proposes a retrospective applicability, insofar as the personal data already in process under consent and obtained prior to the commencement of the Act, a notice in the manner described above must be given as soon as reasonably practicable by the data fiduciary to the data principal.*

While an informed 'consent' continues to remain the fundamental premise for processing personal data under the Act, it has also introduced the concept of 'legitimate uses' replacing that of 'deemed consent' as was envisaged under the DPDP Bill. The data fiduciary can process the personal data of a data principal now, without obtaining her consent, for legitimate uses including for purposes of employment, responding to medical emergencies, performing any function under law or the State providing any service or benefit to the data principal, compliance with a judgment or order, among others.

The Act allows the data principal to withdraw consent at any time with the same level of ease with which it was provided. Unlike the DPDP Bill, the Act specifies that such withdrawal of consent would not affect the legality of processing of the personal data based on consent obtained prior to the withdrawal.

CONSENT MANAGER

The Act identifies the role of consent manager and defines it as a person registered with the Board, who acts as a single point of contact to enable a data principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform. Through the consent manager, a data principal can provide, manage, review, and withdraw the consent given to a data fiduciary. Under the Act, the consent manager is accountable and obligated to work in favor of the data principal and in certain cases, may also be made subject to penalties.

DATA PRINCIPAL'S RIGHTS AND DUTIES

In line with provisions under the DPDP Bill, the Act stipulates that data principals can seek information on the personal data being processed, the processing activities and the identities of all data fiduciaries and processors that their data has been shared with. Data principals may also require the data fiduciaries to correct or erase their personal data. Data principals also have a right to nominate an individual to exercise the rights on their behalf in the event of death or incapacitation.

At the same time, the Act requires a data principal to exhaust all available options for grievance redressal before approaching the Board – a requirement that was absent from DPDP Bill. The Act further imposes certain duties on the data principals which, *inter alia*, include compliance with 'all applicable laws' while exercising their rights under

the Act, prohibition on impersonating another person or suppressing information when applying for any document or proof from the State.

OBLIGATIONS OF DATA FIDUCIARIES

Data fiduciaries are primarily responsible for compliance with provisions under the Act, in respect of any processing undertaken on their behalf by a data processor. They are required to establish grievance redressal mechanisms and ensure accuracy and completeness of the personal data, if it is used to make a decision that affects a user or is to be shared with another data fiduciary.

CROSS BORDER DATA TRANSFER

As a stark deviation from the DPDP Bill, the Act provides that the Central Government may restrict the transfer of personal data to such countries outside India as may be notified. In essence, the Act contemplates a 'negative list' (instead of a 'whitelist' under the DPDP Bill) of countries to which data transfers would be barred. The criteria and principles for barring a jurisdiction are yet to be specified and notified.

The Act clarifies that if any Indian law provides for a higher degree of protection as compared to transfer of personal data outside India, then such other law would prevail. Such clarification aims to accommodate a stricter sector-specific restriction on data transfers, such as the Reserve Bank of India and Securities and Exchange Board of India's prescriptions on data localization.

SIGNIFICANT DATA FIDUCIARIES

The Act envisages the concept of Significant Data Fiduciaries ("**SDFs**"), a class of data fiduciaries to be identified by the Central government if they handle high volume and sensitivity of personal data or impact the sovereignty and integrity of India, security of State or public order.

As before, the SDFs have been made subject to additional obligations such as appointing a data protection officer, an independent data auditor, conducting periodic audits and periodic data protection impact assessments. The Act sets forth the process pertaining to data protection impact assessment, whereby it shall comprise a description of the rights of data principals together with the purpose of processing of personal data, assessment and management of risks to and rights of the data principals.

EXCEPTIONS

The Act does not apply in cases where the data processing is: (i) necessary to enforce any legal right or claim; (ii) undertaken by a court or tribunal or other body entrusted by law; (iii) in the interest of prevention, detection, investigation or prosecution of any offence or contravention of any law; (iv) of data principals not within the territory of India pursuant to any contract entered into with any person outside the territory of India by any person based in India; (v) necessary for a scheme of compromise or arrangement or merger or amalgamation; (vi) for ascertaining financial information of any person who has defaulted in payment.

Notably, the above points (v) and (vi) did not find mention in the DPDP Bill. In furtherance to the above, the Act empowers the Central Government to exempt certain classes of data fiduciaries including start-ups from their obligation, by way of notification.

PROCESSING DATA OF CHILDREN AND PEOPLE WITH DISABILITY

The Act mandates the data fiduciaries to obtain 'verifiable consent' from parents and legal guardians before processing personal data of children (individuals below 18 years of age) and persons with disability respectively. In

its present form, the Act does not set out the manner for obtaining such verifiable consent, however, the same is expected to be prescribed under the rules issued pursuant to the Act.

The Act further prohibits: (i) tracking or behavioral monitoring of, and targeted advertising directed at, children; and (ii) processing of children's data that is likely to cause any detrimental effect on the well-being of a child. Having stated that, the Act contemplates an exemption for certain classes of data fiduciaries from stricter obligations in relation to children's personal data, subject to conditions as may be prescribed. The Act also empowers the Central Government to notify the age above which certain data fiduciaries would be exempt from these additional obligations, if it is satisfied that the processing of children's personal data has been carried out by a data fiduciary in a 'verifiably safe' manner.

ENFORCEMENT MECHANISM

The Act proposes the setting up of the Board, an enforcement body, having powers to direct any urgent remedial or mitigation measures on receipt of intimation regarding a personal data breach, inquire into such breach, impose penalties for non-compliance, inspect any document, summons and enforce attendance of any person, etc. Deviating from the DPDP Bill, the Act sets forth the composition of the Board along with salary, allowance, term, disqualification, resignation of the chairperson and members.

The Board encourages alternative dispute resolution mechanisms, and the Act empowers the Board to direct the concerned parties to resolve any dispute through the mediation process, if deemed fit. The Board may also accept voluntary undertaking from the any person pertaining to compliance with provisions of the Act at any stage of the complaint proceedings. The sum and substance of the voluntary undertaking is to: (i) undertake certain actions within a certain time-frame determined by the Board, (ii) refrain from undertaking specific actions, (iii) publicize the voluntary undertaking. Once accepted, such voluntary undertaking imposes a bar on proceedings under the law with respect to the subject matter of the undertaking, until a person fails to adhere to its terms.

Including other powers, the Act empowers the Central Government to call for any information from the Board, data fiduciary, or any intermediary. Based on the advice received from the Board, the Central Government can also direct blocking of access by public of any information in the public interest.

Substituting the appellate jurisdiction of High Courts, the Act now allows either party to file an appeal before the Telecom Disputes Settlement and Appellate Tribunal ("**TDSAT**") established under the Telecom Regulatory Authority of India Act, 1997, against an order of the Board. A further appeal may be filed before the Supreme Court of India.

PENALTIES

To tighten the ropes and simultaneously to ensure reasonableness to data fiduciaries, the Act encapsulates penalty of up to INR 250 crores, on an entity for a personal data breach and INR 200 crores for non-fulfilment of obligation for children. While imposing such penalties, several factors are to be considered including, nature, gravity, and duration of breach, type of personal data affected, repetitive nature of breach, etc. However, it is relevant to note that no portion of the compensation would go to data principal, who is the victim of the data breach.

CONCLUSION

After long anticipation since 2018, the Act has finally seen the light of the day, which is expected to impart meaningful effect to the 'right to privacy'. This law promises to be more robust and suited for current business requirements. It outlines the rights and obligations of data principals and data fiduciaries and lays out the methods and standards for data collection when it comes to entities. It has covered some of the industry's key requirements such as cross-border data transfers but has left out certain aspects like notice requirements, procedure for data breach

notifications, parental consent for children's data, exemptions for processing of personal data, etc. for delegated legislation.

The Act sets a remarkable precedent that India is upping its efforts by safeguarding not only personal information but also the very infrastructure that holds it, ensuring a landscape where trust, innovation, and progress can thrive unhindered for building a new regulatory architecture in the Indian technology sector and the digital ecosystem. Having said that, the most immediate concern pertains to the increased cost of compliance that may hurt small businesses and Indian startups.

Contributed By – Dentons Link Legal Privacy & Cybersecurity Group