A DEEPER INSIGHT INTO THE DIGITAL PERSONAL DATA PROTECTION BILL, 2022

-Dr. Karnika Seth, Advocate, Supreme Court of India

The Ministry of Electronics and Information Technology (MeitY) released a new data Protection Bill on November 18, 2022, i.e. three months after striking down a prior version which was named the Personal Data Protection Bill, 2019. The new Bill is titled as the ***Digital Personal Data Protection Bill, 2022*** ('The Bill'). The Centre has invited comments and suggestions from the public till 17 December 2022.Though the proposed Bill is much leaner, reduced from 99 sections to 30 sections but it proposes certain provisions which are favour the industry over civil society!

The proposed Bill aims to provide for the processing of digital personal data (collected online or offline and digitised) in a way that recognises both individuals' right to privacy and the necessity to process personal data for lawful purposes. Interestingly, the Bill does not distinguish between sensitive and critical personal data, but refers to only Personal Data. The Bill also excludes non-personal data. Hence, there are no stricter norms laid down for transfer of personal data of individuals that may primafacie be of sensitive nature such as payment data or health records.

Whereas users of internet and consumers of e-commerce companies are named as *Data Principals* in the bill , the body corporates are termed as *Data Fiduciaries* as these collect and process an individual's personal data under a relationship of trust.

The Bill mentions certain other specific officers/authorities including:

- **Data Protection Board :**The Board is empowered to oversee the compliance of companies to the proposed rules. An appeal against any order of the Board shall lie to the High Court.
- **Data Protection Officer (DPO):** An individual appointed as such by a Significant Data Fiduciary.
- **Consent Manager:** A Data Fiduciary enables a Data Principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform. A consent manager is accountable to the Data Principal and acts on behalf of the Data Principal.
- **Independent Data Auditor:** To be appointed by a Significant Data Fiduciary for evaluating the compliance with the Bill.

User's consent & other rights

This Bill adopts a consent-based approach which is also adopted in European Union's GDPR law. It includes provisions on 'purpose limitations' for data collection, reasons for collecting and processing personal data, rectifying errors in data or, withdrawal of consent by a user, easing of cross-border data flows, and imposes hefty penalties on organisations upto 500 crores that violate the Bill's data protection requirements. Th bill also provides for deemed consent by a user such as in cases of medical emergency or compliance with a judgement or order of a court.

The Bill also has an extraterritorial application, to the effect that if personal data is processed outside of India, or if the processing is in conjunction with the profiling/activity of supplying goods or services to Data Principals, compliance with the Bill shall be mandatory. According to Section 18(1)(d), Personal data of data principals outside India when processed in India will not require obtaining consent from such data principal if there is a contract with a person outside India by a person in India. This will facilitate Indian companies processing personal data of foreign nationals in India under a contract arrangement , however obligations in GDPR will still apply to such processing entities in India when they process personal data of Europeans in India.

Obligations on data fiduciaries

Section 6 of the Bill requires Data Fiduciaries to provide an itemised notice to Data Principals before consent is obtained for the processing of personal data. This itemised notice must include a description of the personal data intended to be collected as well as the purpose of such processing. Moreover, a Data principal is entitled to erasure of personal data where retention by a Data Fiduciary is no longer necessary.

According to the Bill, it is the obligation of Data Fiduciary to ensure that all reasonable safeguards are taken to prevent personal data breach. It puts an obligation on a Data Fiduciary to ensure that Data Principal is able to seek effective redressal of his grievances and requires appointment of a grievance redressal officer.

According to Section 9(9), a Data Fiduciary can engage, appoint, use or involve another Data Processor only under a valid contract, wherein such contract has been consented to by the Data

Principal. This will ensure that no unnecessary parties including a Data Fiduciary & Data Processor are added at a later stage without the consent or knowledge of the Data Principals.

Section 11(2)(c) of the Bill further lays additional obligations on Significant Data Fiduciaries to undertake extra measures like Data Protection Impact Assessment and Periodic Audits for compliance with data protection norms.

Section 10(3) of the Bill puts an obligation on the Data Fiduciaries to ensure that no kind of tracking or behavioural monitoring of children's personal data takes place and ensures that targeted advertising are not directed towards children.

Heavy penalties for breaches

The Bill proposes imposition of heavy penalties of upto 500 crores on Data Fiduciary for violating provisions of the bill. Earlier, the PDP bill ,2019 had proposed Rs.15 crore or 4% of global turnover of a company as penalty whichever is higher. In addition,the Bill imposes a fine of upto Rs. 10,000 for filing false information by a user or impersonation or filing frivolous complaints against internet based companies. This will ineffect weed out frivolous and reckless acts by any user or abuse of process of law.

Section 24 of the Bill defines *'Voluntary Undertaking'* a concept introduced for the first time, with the objective to encourage timely admission and rectification of lapses. This new provision is,however, controversial as it involves submission of a voluntary undertaking by an entity such that no further action would lie in law against such person who has defaulted. However, it is pertinent to note that it sets to naught the right of a user to seek redressal by way of compensation for breach of data protection norms. The same is inconsistent with current IT Act provisions, particularly Section 43A where a user who suffers loss on account of unauthorised access to data or disclosure by a body corporate can seek compensation by filing a complaint with the Adjudicating Authority. The bill seeks to omit Section 43A of IT Act,2000 and consequently the IT (Sensitive Personal Data or Information) Rules, 2011 passed under the said Section of the ITAct,2000 would also become inoperable.

Data localisation deleted

The bill eases cross border transfer of data unlike previous versions where sensitive and critical data were defined separately under PDP bill,2019 and the Bill does not impose any data

mirroring or localisation obligations. The Bill provides “the Central Government may, after an assessment of such factors as it may consider necessary, notify such countries or territories outside India to which a Data Fiduciary may transfer personal data ,in accordance with such terms and conditions as may be specified” . In my view, Section 17 of the bill requires at least principle of adequacy of reasonable security practices or appropriate safeguards to be incorporated, as no factors have been mentioned nor underlying basis of factors for transfer of personal data outside India. In EU, GDPR mentions adequate data protection laws must exist in a country. Personal data is transferred to, and privacy shield explains this principle.\

State’s exemptions

Further, the bill also gives the Centre the Authority to exempt State agencies from the bill's provisions in the interest of India's sovereignty and integrity, friendly relations with other States and reasons stated also in Art.19(2) of the Constitution of India. As per the bill, State can retain personal data even beyond lawful or business purposes as provided in the Bill. However, the same needs to be for a justifiable and lawful purpose and within the confines and in accordance with the rule of law. Therefore, Section 18(4) of the bill also needs a serious review.

More delegated legislation powers to the State

The Bill dilutes the powers of the Data Protection Board and more powers are vested with the Central Government to prescribe regulations as part of delegated legislation. For example, the Central government is empowered to appoint members of the Data Protection Board and decide other role that the DPB will play in the data protection regime besides other regulations it is authorised to provide under the Bill.

In a nutshell, there are various pros and cons of the Personal Data Protection bill, 2022 but it has a clear tilt in favour of industry and needs to incorporate more robust provisions to ensure individuals data is adequately safeguarded, particularly at a time when personal data is being largely processed using Artificial Intelligence. The concept of Data localisation is omitted altogether. In my view, atleast a mirror image copy is necessary in respect of critical data such as health records or payment data of individuals to facilitate efficiencies in law enforcement processes and investigation of cybercrime cases. Also, the Bill’s provisions aim to omit Section 43A of IT Act,2000 (Liability of Body Corporates) and consequently SPDI Rules will also cease to apply and the right to claim compensation available to a user under extant IT Act,2000 would cease. The PDP Bill 2022 provides such Data Fiduciaries can give a voluntary

undertaking to the Data Protection Board and acceptance thereof by the Board bars any proceedings/redressal mechanisms under the Act except cases where such companies fail to abide by the voluntary undertaking. Therefore, in my view the Bill is not exhaustive enough to protect users personal data with enough safeguards which a special law of this nature and extent of application ought to address! The bill ,perhaps by way of a new regulation, would address retention norms to retain personal data , interalia, for how long data must be stored if an account is deleted by a user. As on date of writing,the IT (Intermediaries Guidelines and Digital Media Ethics Code) Rules, 2021 lays down such timeline as 180 days in respect of intermediaries and for data centres, payment gateway providers as 5 years (Notification No. 20(3)/2022-CERT-In of 28 April 2022 issued by MEITY).The new bill needs to also factor in any overlap or inconsistency with the Telecom Bill 2022 released by the Department of Telecommunications as regards users data to avoid any inconsistencies or overlap as both these bills are expected to be tabled in Parliament during the budget session. The Telecom bill obligates companies collecting user data to adopt KYC norms and makes users also responsible to provide their accurate personal data. The Digital Personal data protection bill,2022 goes a step further and imposes fines upto Rs.10,000 on users for intentionally providing false or misleading personal data! Thus, the Digital Personal Data Protection bill needs to be deliberated in conjunction with Telecom Bill, 2022 during the public consultation process and before both the Houses of the Parliament!