Key Changes in the Personal Data Protection Bill, 2019 from the Srikrishna Committee Draft

The Personal Data Protection Bill, 2019 ("the PDP Bill, 2019)" was tabled in Parliament on December 11th, 2019. The PDP Bill, 2019 has brought in some new clauses – compliance obligations for social media companies and enhanced State power to exempt any government agency from the purview of the Bill; relaxed some existing provisions – done away with mandatory mirroring requirements for all personal data and done away with certain offences for transferring/ selling personal data; and in some cases removed extant requirements such as the creation of the Data Protection Funds, as compared to the Draft Personal Data Protection Bill, 2018, which was released last year.

Some of the key changes brought in by the PDP Bill, 2019 are as follows:

1. **Social Media Intermediaries and voluntary verification of accounts (Sec. 26 and 28 of the Bill)**

The PDP Bill, 2019 extends the obligations of significant data fiduciaries to another class of entities called the social media intermediaries ("SMIs"). The Bill defines SMIs to mean intermediaries who primarily/ solely enable online interaction between two or more users and allow them to create, upload, share, disseminate, modify or access information using its services (it specially excludes entities like – e-commerce platforms, TSPs/ ISPs, search engines, cloud service providers, online encyclopedias, and email services from the definition of SMIs). Another qualification for an entity to be an SMI is – the likelihood or actual impact on electoral democracy, security of the State, public order or the sovereignty and integrity of India [see Sec. 26(4)].

In addition to obligations such as – data protection impact assessments (Sec. 27), maintenance of records (Sec. 28), audit of policies (Sec. 29), and appointment of a data protection officer (Sec. 30), which are applicable to all significant data fiduciaries, SMIs are required to provide an option to users (registering from India or using the services in India) for voluntary verification of their accounts [the methods of such voluntary verification will be notified by the Central Government as per Sec. 93(1)(d) of the Bill]. Verified user accounts will be marked with a demonstrable verification mark [See Sec. 28(4)]. As per Sec. 29, data auditors are required to evaluate SMIs for timely implementation of their obligations under account verification norms.

Social media verification requirements are misplaced in data protection legislation. As under existing provisions [see Sec. 26(1)] social media companies could easily fall under the ambit of significant data fiduciaries, the only basis for this distinct classification could be to introduce account verification mechanisms. This new concept of verification of social media accounts does not belong in a comprehensive data protection regulation and must be removed.

2. **Central Government can Exempt any Government Agency from the Bill (Sec. 35 of the Bill)**

Sec. 42 of the Draft Personal Data Protection Bill, 2018 ("the Srikrishna Bill") allowed access of personal data to the Government for security purposes based on principles of necessity and proportionality and on the basis of authorisation under law. The provision for Government access to personal data under the PDP Bill, 2019 (Sec. 35) is wider, gives the Central Government power to exempt any government agency from the purview of the Bill (all or select provisions) and does not codify the principles of necessity and proportionality as determinants to access.

Sec. 35 of the PDP Bill, 2019 effectively enhances existing surveillance powers of the government and gives the State over arching authority to access personal data. This provision enables government surveillance projects like the NATGRID, CMS, and the nationwide facial recognition program, effectively enabling the Government to collect and process any category of personal data per their requirements. Even the Srikrishna Committee Report recognised that unfettered access to the Government of personal data, without adherence to established safeguards (such as necessity and proportionality as expounded in the privacy judgment of the Supreme Court – *Puttaswamy*) is potentially unconstitutional. Granting access of personal data to the Government, without appropriate safeguards and judicial oversight is against established constitutional principles and should not form part of the PDP Bill, 2019.

3. **Dilution of Data Localisation Requirements (Sec. 33 and 34 of the Bill)**

The mandatory requirement for storing a mirror copy of all personal data in India as per Sec. 40 of the Srikrishna Bill has been done away with in the PDP Bill, 2019. Localisation requirements are only on sensitive and critical personal data (stored in India with conditions for transfer overseas). Critical personal data may only be processed in India [See Sec. 33(2)]. Sensitive personal data ("SPD") may be transferred outside India based on explicit consent and a) if the transfer is made per a contract or intra-group scheme (approved by the data protection authority); or b) Central Government allows transfer to a country, entity or international organization; (requisite safeguards for protection of such personal data are prescribed under these provisions) or c) data protection authority may allow a transfer of SPD for specific purposes.

Similarly, for critical personal data, transfers may be allowed for health or other emergency services or where the Central Government approves transfers to a country, entity or international organization.

Though, removing the mandatory mirroring requirement is an appropriate change, users/ data principals should be given rights over where they wish to store their personal data and the State should not impose restrictions on transfer of such data, specially once explicit consent has been given.

4. **The Right to Erasure (Sec. 18 of the Bill)**

The Srikrishna Bill did not contain a right to erasure, even under the right to be forgotten ("RTBF") (See Sec. 27 of the Srikrishna Bill). The PDP Bill, 2019 has brought the right to erasure alongside the right to correction of personal data [See Sec. 18(1)(d)]. The data principal may request data fiduciaries for a right to erasure of personal data when such data is no longer necessary for the purpose of processing. Data fiduciaries may refuse such requests for erasure, but data principals may require fiduciaries to take reasonable steps to indicate, alongside the relevant personal data, that the same is disputed by them.

This is a good inclusion as it enhances data principal rights to request the erasure of data which is no longer needed for the purpose of processing. Such a right was missing from Srikrishna Bill. A right to erasure should also be incorporated under the RTBF (under Sec. 20 of the PDP Bill, 2019), as presently, RTBF only includes a right to non-disclosure and not erasure.

5. **Removal of Judicial Member from Selection Committee Recommending Members to the Data Protection Authority (Sec. 42 of the Bill)**

The PDP Bill, 2019 has removed the inclusion of a judicial member (the Chief Justice of India or another Supreme Court Judge) from the selection committee which is empowered to give recommendations to the Central Government for the appointment of members of the Data Protection Authority ("the DPA") [the Srikrishna Bill included a judicial member in the selection committee - see Sec. 50(2) of the Srikrishna Bill]. Now, as per Sec. 42(2) of the PDP Bill, 2019, the selection committee will comprise of – a) the Cabinet Secretary (who's also the Chairperson); b) Secretary, Department of Legal Affairs; and c) Secretary, Ministry of Electronics and Information Technology.

The DPA is completely dependent on the Central Government for its formation and membership. Considering that the PDP Bill, 2019 applies to the Government agencies as well, the regulatory body, which is tasked with enforcement of the Bill, is not independent from the State.

To ensure the independence of the DPA, there should be sufficient involvement of judicial members in the selection committee as well as in the DPA. This will guarantee judicial review and will quell concerns of conflict of interest.

6. **Central Government can direct Data Fiduciaries to share Anonymized Personal Data/ Non- Personal Data (Sec. 91 of the Bill)**

Sec. 105 of the Srikrishna Bill, gave powers to the Central Government to formulate appropriate policies for the digital economy, including measures for its growth, security, integrity, prevention of misuse, in context to 'non-personal data'. That Bill did not define what was meant by non-personal data or how was it to be utilized by the government. The PDP Bill, 2019, under Sec. 91, goes a step further – a) it defines non-personal data as data that does not fall

under the definition of personal data [for the definition of personal data see Sec. 3(28)]; and b) empowers the Central Government to direct any data fiduciary/ processor to provide any anonymised personal data or non-personal data *"...to enable better targeting of delivery of services or formulation of evidence-based policies by the Central Government, in such manner as may be prescribed."* [See Sec. 91(2)]. Sec. 2(B) of the PDP Bill, 2019 specifies that the Bill would not apply to anonymised data, other than as provided by Sec. 91 – which enables the Central Government to request entities to convert personal data into anonymized data for their own use.

In September this year, the Ministry of Electronics and Information Technology, constituted an expert committee to deliberate over a data governance framework for the regulation of 'non-personal data'. Till the report of this expert committee is published, it would not be appropriate for the PDP Bill, 2019 to include government access to non-personal/ anonymised data. The expert committee must invite recommendations from the public and give civil society an opportunity to comment on privacy rights related issues with anonymised/ non-personal data.

On the point of requesting anonymised and non-personal data by the Central Government from any data fiduciary, this may be an onerous demand on data fiduciaries. Applying anonymisation standards, specially for start-ups and SMEs may be a cumbersome task. There aren't any safeguards appended to this provision. What if a data fiduciary does not properly anonymise personal data? Or shares non-personal data which can easily be turned into personally identifiable data by combining various data points? The Bill does not provide safeguards for such situations in the interest of privacy rights of data principals.

7. **Transparency in Data Sharing and the Concept of Consent Managers (Sec. 17, 21, and 23 of the Bill)**

Sec. 17(3) of the PDP Bill, 2019, gives rights to data principals to access, in one place, the identities of data fiduciaries with whom their personal data has been shared by any (other) data fiduciary. This potentially enables data principals to review the entities with whom their personal data has been shared by one particular data fiduciary. This right has been added under the clause for the right to confirmation and access (this right was contained in Sec. 24 of the Srikrishna Bill).

This bolsters the rights framework in the PDP Bill, 2019. Data principals shall have the right to know about all the entities which are processing/ sharing their personal data. This, clubbed with the right to withdraw consent enhances the rights of the data principals in terms of their informational privacy.

The PDP Bill, 2019, also introduces the concept of 'consent managers' [See Sec. 21(1) and 23] which was not present in the Srikrishna Bill. The term Consent Managers is not defined in the definitions clause of the Bill, but is defined under an explanation to Sec. 23 as – a data fiduciary which enables a data principal to gain, withdraw, review and manage their consent through

an accessible, transparent and interoperable platform. All consent management platforms are to be registered with the DPA [See Sec. 23(5)].

From a reading of the definition of consent managers, it seems like the PDP Bill, 2019 has introduced the concept of 'consent dashboards' as recommended by the Srikrishna Committee in its report. On the face of it consent management tools/ consent dashboards may help in reducing consent fatigue, but they might bring up fresh privacy challenges. A trail of metadata generated by consent dashboards might help create a detailed profile of an individuals user engagement online. Specially, when such management tools are required to be registered with the DPA, metadata generated by these tools may assist in profiling of citizens.

8. **Definitions of Personal and Sensitive Personal Data [Sec. 3(28) and (36) of the Bill]**

The PDP Bill, 2019 has expanded the definition of personal data to include inferred data. Sec. 3(28) includes - *"... and shall include any inference drawn from such data for the purpose of profiling".*

Including inferred data for the purpose of profiling in the definition of personal data is a positive move as this will give the right to data principals to request data fiduciaries for such data as well (See Sec. 17 of the Bill).

The PDP Bill, 2019 has taken off 'passwords' from under the purview of sensitive personal data. This may be for the reason for easy transfer of such data outside India when read in conjunction with the data localisation clauses – Sec. 33 and 34 of the Bill.

9. **Privacy by Design Policy (Sec. 22 of the Bill)**

The PDP Bill, 2019 introduces a concept of a privacy by design policy. Every data fiduciary is required to prepare a privacy by design policy and have it certified by the DPA. There is a requirement on each data fiduciary to publish this privacy by design policy once it has been certified by the DPA.

10. **Removal of offences for obtaining, transferring, or selling of personal/ sensitive personal data (Sec. 90 and 91 of the Srikrishna Bill)**

Offences for obtaining, transferring or selling of personal/ sensitive personal data have been removed from the PDP Bill, 2019 as compared to the Srikrishna Bill.

[There are other changes in the PDP Bill, 2019, like – removal of an obligation on data fiduciaries to demonstrate adherence to the Bill {Sec. 11(2) of the Srikrishna Bill}; SPD has been removed from the employer processing exception {Sec. 13(1) of the PDP Bill, 2019}; there is strict mandate now for data protection officers to be located in India {Sec. 30(3) of the PDP Bill, 2019}; and there is an exemption from certain clauses of the Bill for regulatory sandboxes (Sec. 40 of the PDP Bill, 2019). We will cover all these in our detailed analysis of the Bill.]