The Dialogue™
INFORM ENGAGE IDEATE

THE PERSONAL DATA PROTECTION BILL, 2019

RIGHTS - BASED CONSIDERATIONS

Kamesh Shekar

RIGHTS-BASED CONSIDERATIONS

1. Introduction

India's Personal Data Protection Bill 2019 ("PDP 2019") is at the cusp of enactment as Joint Parliamentary Committee (JPC) tabled its report in the 2021 winter session. The objective and reason for enacting this Bill dates to 24th August 2017 when the Supreme Court of India delivered its judgement on Justice K.S Puttaswamy and others vs Union of India, declaring privacy as a fundamental right under Article 21 of the Indian Constitution. The judgement also directed the Government of India to bring in a robust data protection regime for the country to safeguard the informational privacy of the citizens.

The PDP Bill 2019 takes a consent-based approach as a privacy default and vests certain rights in the hands of the data principles. The Bill also provides a contour for setting up a Data Protection Authority (DPA) who will protect the interest of data principals by performing an adjudicatory role and providing a grievance redressal mechanism to solve disputes related to privacy matters (amongst other roles).

As India moves closer towards enacting a nuanced data protection regime, it is essential to deliberate on some of The Bill's rights-based considerations to weed out unintended consequences and have a comprehensive regime. Some of the pertinent elements under rights-based considerations discussed in this primer are the consent-based approach taken by the Bill, citizen rights held by the Bill, and the grievance redressal mechanism provided by the Bill.

2. Key provisions and our recommendations

2.1. Consent-based approach

The Bill mandates that personal data shall be processed only after obtaining consent from data principles at the commencement of its processing and provides reasonable purposes (determined by DPA) for data fiduciaries to process personal data without the consent of the data principal. Besides, The Bill places the burden of proof over the data fiduciaries to show that the data principal has given their consent and the legal responsibility on data principals for withdrawing consent without any valid reasons. In addition, to enable data principals to exercise their consent, the Bill introduces a new category of business called consent managers who must register with the DPA in such a manner and subject to such technical, operational, financial, and other conditions as may be specified by regulations.

This show that consent is the bedrock on which the Bill has been constructed. But at The Dialogue, we believe that The Bill over relies on consent, despite consent being criticised as means for obtaining legitimacy for data processing. Without other bases for processing, we expect it can cause demand-side and supply-side issues, as discussed below.

Demand-side issues: Individuals may receive innumerable privacy notifications causing consent fatigue; this issue was considered and acknowledged by the Justice Srikrishna committee report. But The Bill adds to the consent fatigue by requiring more information to

be provided in a privacy notice. Besides, it is reported that data fiduciaries use dark patterns to manipulate data principals to obtain consent through playing with their cognitive abilities and bounded rationality. Adding to this, with consent managers incorporated into the process, it will be challenging to trace the origination of dark pattern usage in terms of whether it was instituted by data fiduciary or consent manager or both in symbiosis. Besides, providing a technological solution in form consent manager for technological problems (i.e., to contain/manage consent for legitimising data processing or sharing) is suboptimal and burdensome because some data principals already lack awareness and access to the technological processes.

Supply-side issues: While The Bill list out factors to be considered before determining the reasonable purposes for non-consensual data processing, it doesn't have 'processing pursuant to a contract' and 'other reasonable purposes determined by the data fiduciary', which means any additional legitimate business reasons for processing data as to be approved by the DPA. This makes the data processing mechanism complex, less agile and increases the operational burden for both data fiduciaries and DPA and, in turn, might slow down innovations.

Our Recommendations

- The bill must layout better means and ways to obtain consent, which is inclusive, less tiresome, less manipulative, and efficient.
- We recommend that, the Bill should allow data fiduciaries to determine what rea-sonable purposes are, instead of such purposes being specified by the DPA.

2.2. Rights of the Data Principal

The Bill vests a couple of rights in the hands of the data principles and mandates DPA to safeguard the same through regulation under various provisions in the Bill. The below infographic (figure 1) illustrates the rights of the data principal provided under The Bill

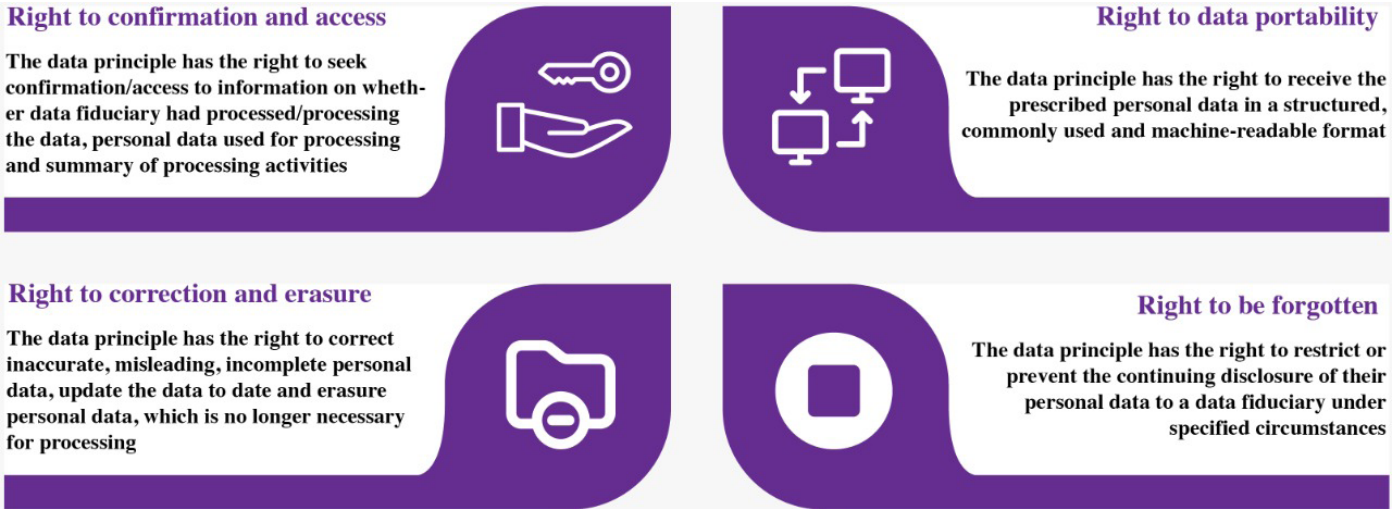

Figure 1: Rights of the Data Principal

The Bill provides that the data principal can exercise their rights (except the right to be forgotten, which it needs adjudicating officer's order) through reaching out to the data fiduciaries directly or through the consent managers. The data fiduciaries must comply with the request, do the needful on a nominal fee, and provide written refusal to the data principal in case of denial. The data principal also has the right to file a complaint with the DPA against the refusal within the specified duration.

Under The PDP Bill 2019, any data principal who has suffered harm due to violation of any provision under The Bill has the right to seek compensation from the data fiduciary or the data processor as the case may be. This shows that The Bill provides for a private right of action, which creates various issues.

Issues with private rights of action: A private right of action will lead to burdensome enforcement under the laws, with no practical limits on the numbers or frequency of complainants. Further, the inconsistencies in interpretation of private rights of action provisions will lead to wide discretionary powers at the hands of the adjudicating officer. Moreover, enforcement regimes that provide for private rights of action and classes of data fiduciaries incentivise plaintiffs to strategically target defendants who are known or perceived to be solvent. In The Bill's context, this means that complainants are likely to target "deep pocket" parties, including large-scale data processors such as cloud service providers and telecom service providers. Besides, the consent managers are not held liable for their actions under The Bill.

Our Recommendations

- The ability of data principals to individually or as a class claim compensation from data processors and data fiduciaries should be removed.
- The DPA should be the exclusive authority to prosecute claims under The Bill.
- The liability of data processors on the grounds of "negligence" should also be limited as they only act on the directions of data fiduciaries.
- Liability structure for consent managers must be instituted.

2.3. Grievance management system

The Bill mandates data fiduciary to institute an effective grievances mechanism to redress data principals' complaints efficiently in a speedy manner. In that regard, The Bill seeks the data fiduciaries to appoint a data protection officer (in the case of significant data fiduciary) or any designated officer (in case of data fiduciary) for dispute management.

Issue of Multiple grievance management: Currently, there are multiple forms of grievance redressal portals for entities and consumers to lodge their complaints with the regulator/ policymakers. For instance, each financial sector regulator has its own ombuds, there is Cyber Appellate Tribunal under IT Act, The Bill envisages setting up an appellate tribunal etc. As grievance in the technology sector would tick the box of multiple tribunals and ombuds, the current disjointed way of operating grievance might become obsolete, confusing, and onerous. This would also cause regulatory uncertainty, where the regulator/policymaker might deny redressal to a particular grievance stating this doesn't fall within their ambit.

Our Recommendations

We suggest a calibrated hierarchical grievance redressal mechanism with horizontal and vertical coordination (between different elements of the system) and agility proofing. Borrowing inference from the responsive regulation framework, we suggest the below steps for grievance management:

- **Step 0**: To find the designated portal for lodging a dispute through interactive voice response (automated voice response system)
- **Step 1**: Get the dispute redressed through reporting it to the data fiduciaries, pro-cessors, and consent managers themselves
- **Step 2**: Reach out online dispute resolution (a mediated litigant dispute resolution framework facilitated through online platforms)
- **Step 3**: Reach out the appellate tribunal (set up under the PDP Bill) if step 2 fails

The Dialogue is a public-policy think-tank with a vision to drive a progressive narrative in India's policy discourse. Founded in 2017, we believe in facilitating well-researched policy debates at various levels to help develop a more informed citizenry, on areas around tech-nology and development issues.

The Dialogue was ranked amongst the Top-Ten think-tanks in the world to watch out for by the Think-Tank Civil Societies Programme, Lauder Institute, University of Pennsylvania, in their 2020 and 2021 ranking index.

Email: info@thedialogue.co
Website: www.thedialogue.co

The Dialogue™

INFORM ENGAGE IDEATE