The Dialogue™

INFORM ENGAGE IDEATE

28TH JANUARY, 2022

IMPLEMENTING INDIA'S DATA PROTECTION REGIME

VIRTUAL STAKEHOLDER CONSULTATION REPORT

DRAFTED BY: KAMESH SHEKAR

TABLE OF CONTENTS

INTRODUCTION

The Dialogue has been at the forefront of the discourse on India's envisioned data protection regime, answering some of the crucial and challenging policy questions for making the Indian digital sphere secure and lucrative at the same time. As part of this effort towards having a nuanced data protection regime for India, we at the Dialogue hosted a consultation on "Implementing India's Data Protection Regime: taking stock and way forward" on January 28, 2022. We were delighted to have **Justice BN Srikrishna (Retd.), Judge, Supreme Court of India and Chairperson of the Expert Committee on Data Protection Framework, and, Dr. Amar Patnaik, Hon'ble Member of Parliament Rajya Sabha and Member of Joint Parliamentary Committee on Personal Data Protection Bill**, as the keynote speakers. The expert panel included- Atul Bist, Senior AVP and Head - Technology, Media, Telecom & Electronics Manufacturing at Invest India, GoI; Ashish Agrawal, Vice President & Head of Public Policy at NASSCOM; Beni Chugh, Research Manager of Future of Finance Initiative at Dvara Research; Aadya Misra, Senior Associate of Technology, Media & Telecommunications at Spice Route Legal; Ameya Ashok Naik, Head of Policy at eGovernance Foundation; Eunice Lim, Senior Manager of Policy-APAC at BSA Alliance; Nishant Singh, Ministry of External Affairs; Prof. Graham William Greenleaf, UNSW and Vinay Kesari, Setu. The event was moderated by Deeksha Bharadwaj, Political Correspondent, The Hindustan Times and Kazim Rizvi, Founding Director, The Dialogue.

This consultation followed Chatham house rules; therefore, the views and observations have been summarised and not attributed to any speakers in this report. The views summarised in this report are personal and do not represent views of speakers' organisation or of The Dialogue.

Section 2 of the report discusses the concerns with the envisioned data protection regime raised by the panellists, followed by the way forward. Section 3 of the report will tabulate critical points raised during the panel discussion to the clauses in both the draft Personal Data Protection Bill, 2019 (PDP Bill) and the Joint Parliamentary Committee's (JPC) report on the bill.

KEY TAKEAWAYS

Some of the critical points raised during the discussion are listed below:

The Data Protection Authority (DPA) must have 50% independent members comprising industry personnel, academicians, researchers, etc. The selection committee must have a judge.

The DPA must branch out into state-level data protection authority to tackle state-level matters.

The roadblock in compliance with data localisation is the ambiguity in provision where specifics like transit data being processed offshore or fully local are unclear.

Consent management is the only way to implement a key data protection principle, i.e., purpose limitation. But from a business perspective, it is difficult for data fiduciaries to educate individuals in a diverse country like India to have informed consent.

The consent management problem could turn into opportunities for start-ups to bring innovation in regulatory technologies. One such innovation discussed during the consultation was the consent manager.

Parameters, clearer definitions, and safeguards for state exemption from the PDP Bill must be fleshed out. From an implementation perspective, there is a need for a transparent and proportionate process by the agencies exempted from the bill, as there is no ability to seek compensation.

Non-Personal Data (NPD) must be separated from the PDP Bill and considered differently, where personal data has the protection of fundamental rights needing to meet higher standards while NPD doesn't have this requirement.

The implementation of the measures should be phased out, covering different aspects of data security like hardware regulation.

Considering data principals below 18 years as a child, the PDP Bill contradicts the status-quo as guardians are digital migrants while gen z children are digital natives who understand technology better.

CRITICAL POINTS ON ENVISIONED DATA PROTECTION REGIME

In 2019, the Personal Data Protection Bill 2019 was introduced in the parliament after Justice B.N Srikrishna committee submitted its report in 2018. After two years of deliberation over the Personal Data Protection bill, 2019 (PDP Bill), the Joint Parliamentary Committee (JPC) tabled its report and draft Data Protection Bill, 2021 (DPB), in the 2021 winter session of the parliament. As we are moving close to having data protection legislation in India, the expert panel discussed the various concerns with India's envisioned data protection regime as follows.

With India's rapid technological advancements and digitalisation, the panellists highlighted the need for a robust data protection regime. They marked that 86% (1 billion) of Indian use smartphones, whereas 3 internet subscribers every second were added in the past 5 years. While they marked that government has a crucial role in enhancing digitalisation through increasing connectivity, providing incentives and a conducive regulatory environment, the panellists also flagged the importance of advancing cyber security and the industry behind it.

2.1. DELIBERATIONS ON THE ROLE OF DATA PROTECTION AUTHORITY

The PDP Bill provides a contour for setting up a Data Protection Authority who will protect the interest of data principal, formulate rules, functions, penalty and boundaries for data fiduciary and processor, supervise compliance to the bill, and perform an adjudicatory role in matters of informational privacy. The DPA is envisioned to be appointed by a select committee as defined in the PDP Bill, and Cabinet Secretary chairs this Committee. The Secretary from the Ministry of Legal Affairs and a secretary from the Ministry of Electronics and Information Technology (MeitY) are also members. Along with these members from the executive, other members are also executive appointees. While the executive could make the appointment of the members of the Data Protection Authority, the panel stressed the need for the appointment of independent members (50%) comprising industry personnel, academicians, researchers etc.

The JPC has suggested changes to the DPA's selection committee in the report and DPB, including the Attorney General and three other members nominated by the Central Government (an independent expert from relevant fields, Director of an IIM and the Director of an IIT). However, responding to JPC's recommendation on having the Attorney General (AG) as part of the DPA selection committee, some panellists highlighted that AG couldn't be considered an independent member in practice; instead suggested having a judge. Besides, the panel cautioned that the central government's binding order over DPA is no longer merely a policy question but spread to all aspects of the framework, which may hamper the functional independence of the DPA.

Despite getting the structural foundation of independence straight, the panellist pointed out that the DPA will hit various roadblocks as it comes into force, because technology evolves faster than the regulations. The panellists highlighted the importance of having accountability, transparency, and a robust institutional capacity in DPA to keep up with technological developments and sectoral differences. Some panellists

discussed international experiences such as the United States' Federal Trade Commission (FTC) and Consumer Financial Protection Bureau's (CFPB) prevalence-based approach to inform India's DPA in capacity building. FTC and CFPB maintain a complaints database that looks into grievances and highlights issues that might become systemic issues in their published reports. Besides, in terms of enforcement, the panellists suggested that DPA must adopt responsive regulation - tools of punitive punishments that scale and are proportionate to the breaches.

On the other hand, some of the panellists specified the importance of having a state-level data protection authority as (a) states collect data under different state-level laws, which are not ideal for central DPA to govern (b) single DPA at the central level will be overwhelmed and would lack the capacity to tackle complaints from state data principals (c) the trust in the DPA will erode if we have single central-level DPA with no room for state-level representation. Besides, the panellists hinted at the possibility of having state-level authorities like in the case of the RTI Act, where every administrative unit and office is mandated to designate a separate central and state public information officer.

2.2. CROSS BORDER DATA FLOWS

The PDP Bill places certain restrictions on transferring sensitive and critical data outside India with strict data location requirements. Clause 33 and 34 of the PDP Bill places data localisation mandate for critical data and data mirroring mandate for sensitive data. Panellists emphasised that the seamless flow of data across the border is crucial to enable innovation, economic proliferation, and competition. From a business perspective, some panellists pointed out the potential roadblocks in compliance with data localisation due to ambiguity in provision where specifics like data in transit, data being processed offshore or fully local are unclear. In addition, panellists cautioned that data localisation would increase the compliance burden for the businesses and have a disproportionate impact on start-ups as they are not ready while big tech has a background with GDPR compliance. While cross border data transfers can be useful for businesses, from the perspective of the harm, it was also stated that there is a need to hold data fiduciaries accountable to data breaches in bilateral treaties through which cross border data transfers take place. They highlighted how a citizen claims action against data stored offshore is still nebulous in cross border data transfer settings. Moreover, there is also a need to understand how DPA can enforce data protection on data that is not backed up within the country.

Currently, India uses the Mutual Legal Assistance Treaty in Criminal Matters ("MLAT") as a mechanism for retrieving data and information for the approved investigation process. Panellists highlight the MLAT process to be broken and froth with delay, justifying the data mirroring requirement to gain data access in an agile fashion. They regard data localisation provisions within data protection regulation can safeguarding our data without trade partners' involvement. Moreover, from a market perspective, they envision making India a data storage hub through a data localisation mandate. Responding to this, a panellist stated that to make India a data behemoth, some of the provisions in the PDP bill have to be cleaned, and gold standards of privacy have to be adopted.

On the other hand, some panellists discussed means to enable cross border data transfer through sharing the international experience of being part of multilateral arrangements like the APEC Cross-Border Privacy Rules (CBPR) System. But it was highlighted that these arrangements are country-specific, cautioning that recognising, for example, APEC CBPR would make India lose chances to trade with the European Union as the Court of Justice of the European Union has struck it as inadequate under their recital 67.

2.3. CONSENT AND CONSUMER PROTECTION

As India's data protection regime bedrocks on a consent-based approach, panellists highlighted the importance and roadblocks to having informed consent. The PDP Bill mandates that personal data shall be processed only after obtaining consent from data principals 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 PDP Bill places the burden of proof over the data fiduciaries to show that the data principal has given their consent. From a business perspective, panellists highlighted that it would be challenging for data fiduciaries to educate individuals in a diverse country like India to have informed consent.

Still, at the same time, some panellists mentioned that consent management is the only way to implement one of the key principles of data protection, i.e., purpose limitation. It was discussed that the consent management problem could turn into opportunities for start-ups to bring innovation in regulatory technologies. One such innovation discussed during the consultation was consent manager (a techno-legal solution for managing consent). The PDP 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.

Besides, panellists highlighted a big win in consumer protection as Clause 62 in the JPC version of the Bill, i.e DPB, allows consumers to file grievances and seek compensation from the DPA. From the experience of the Consumer Protection Act, they highlighted that a line to the regulators, like in the case of Clause 62, is a good development as it gives a higher chance of grievance redressal.

2.4. STATE EXEMPTION

Clause 35, the most contested provision of the PDP Bill, provides a blanket exemption to the government from the applicability of the PDP Bill. The panellists highlighted that this clause stands contrary to the triple test (proportionally, legality and necessity) laid down under Puttaswamy judgment I. It was cautioned that all power and no accountability is a sour mix where the state can use public order and national security to take away individuals' data. So, the panellists emphasised the need for parameters, clearer definition, and safeguard for state exemption from the Bill. Where definitions such as in the interest of "sovereignty and integrity", "security of the State," "friendly relations with foreign states," "public order" remain broadly defined. From an implementation perspective, some panellists highlighted the need for a transparent and proportionate process by the agencies exempted from the bill, as there is no ability to seek compensation.

Besides, it was highlighted that the right to informational privacy is a fundamental right, but the way the bill is being drafted changes that narrative to seem like the government is providing these rights by exempting itself from the PDP bill.

2.5. NON-PERSONAL DATA (NPD)

Clause 91(1) of the PDP Bill allows the government to make any policy for the digital economy, provided it doesn't govern personal data. Besides, Clause 91(2) mandates the data fiduciaries and data processors to share non-personal data with the government to frame policies and enable targeted service delivery for the digital economy. Additionally, DPB widened the scope of the PDP Bill to govern both personal and non-personal data, with less clarity on how the regulator will effectively regulate, how companies will comply, and how individuals will exercise the rights granted to them.

The panellists suggested that NPD must be separated from the PDP Bill and considered differently, where personal data has the protection of fundamental rights needing to meet higher standards while NPD doesn't have this requirement. But a panellist mentioned that it is difficult to separate data into non-personal and personal data, especially in financial data; hence it is hard to have separate jurisdictions. Besides, it was also observed that while the inclusion of NPD has bypassed the long parliamentary process, it is important to address key concerns related to it.

From an implementation perspective, it was highlighted that having privacy regulation and promotion of NPD for industry growth under a single regulator could cause a lot of conflicts and issues.

2.6. CHILDREN'S PERSONAL DATA

The definition of a 'child' under both the PDP Bill and DPB is any data principal below 18 years of age. Panellists cautioned that considering data principals below 18 years as a child, the PDP Bill contradicts the status-quo, as guardians are digital migrants while gen z children are digital natives who understand technology better. In addition, a panellist pointed out that consent managers should be allowed to aid guardians in managing children's consent through the Bill.

Besides, it was flagged that age bracketing 18 years will cause market implications for those data fiduciaries whose user base predominantly is teenagers.

2.7. SOCIAL MEDIA INTERMEDIARIES

While the DPB does not contain any provision regarding treating social media intermediaries as publishers, the JPC report contains a recommendation to this effect. The report proposes that digital platforms acting as intermediaries should be construed as publishers of the content hosted on their platform. Cautioning this move, panellists mentioned that breaking safe harbour and imposing a higher standard on platforms isn't always valid and adequate, as laws shouldn't take the direction of pre-censorship.

2.8. HARDWARE REGULATION

In the JPC's version of the Bill, i.e., DPB, Clause 49(2)(o) was included to regulate hardware manufacturers, which collect data from digital devices. In consultation, it was noted that the bill should take a phased out implementation of the measures covering different aspects of data security like hardware regulation.

SUMMARY OF CONSULTATION: CLAUSE-WISE

Provision is PDP Bill	Change in DPB/JPC Report	Key points highlighted by panellists	Way forward discussed by panellists
DATA PROTECTION AUTHORITY			
Clause 42 - Composition and qualifications for appointment of Members.	Inclusion of Attorney General (AG) and three other members nominated by the Central Government (an independent expert from relevant fields, Director of an IIM and the Director of an IIT) to the select committee.	AG couldn't be considered an independent member in practice.	While the executive could make the appointment of the members of the Data Protection Authority, there is a need for the appointment of independent members (50%) comprising industry personnel, academicians, researchers etc. A Judge in the place of the Attorney General should be appointed to have independence.
Clauses 86 - Power of Central Government to issue directions.	The power of the central government expanded to all aspects and frameworks of DPA under this clause.	Expansion of the central government's power may hamper the functional independence of the DPA.	
Clause 42(1) – DPA comprises a chairperson and not more than 6 members Clauses 50 - DPA must set the standards and codes of practice for data handle/use.		To keep up with technological developments and sectoral differences, DPA must have robust institutional capacity.	International experiences such as the United States Federal Trade Commission (FTC) and Consumer Financial Protection Bureau's (CFPB) prevalence-based approach can inform India's DPA in capacity building. DPA must adopt responsive regulation - tools of punitive punishments that scale and proportionate to the breaches.
Clause 41 – Establishment of DPA for India.		Single central-level DPA is problematic because (a) states collect data under different state-level laws, which are not ideal for central DPA to govern (b) single DPA at the central level will	There is a possibility of having state-level authorities like in the case of the RTI Act, where every administrative unit and office is mandated to designate a separate central and state public information officer.

		be overwhelmed and would lack the capacity to tackle complaints from state data principals (c) the trust in the DPA will erode if we have single central-level DPA with no room for state-level representation.	
CROSS BORDER DATA FLOWS			
Clause 33 - Prohibition on the processing of sensitive personal data and critical personal data outside India Clause 34 - Conditions for transfer of sensitive personal data and critical personal data.	Under Section 34(1) of the Bill, the Committee has recommended that for transfers pursuant to the contract or intra-group scheme (for purpose of transfer of sensitive personal data) outside of India, it must now be approved by the DPA in consultation with the Central Government.	From a business perspective, roadblocks in compliance with data localisation due to ambiguity in provision where specifics like data in transit, data being processed offshore or fully local are unclear. Data localisation would increase the compliance burden for the businesses and have a disproportionate impact on start-ups as they are not ready while big tech has a background with GDPR compliance. Bilateral treaties through which cross border data transfers are enabled doesn't hold data fiduciaries accountable to data breaches. Legitimate case behind the data localisation mandate is (a) the need for data access in an agile fashion, (b) to have certainty and stability in cross border data transfers through adequacy measures etc., (c) to develop India as a data storage hub.	To make India a data behemoth, some of the provisions in the PDP bill has to be cleaned, and golden standards of privacy as to be adopted. The international experience of enabling cross border data flows by taking part in multilateral arrangements like the APEC Cross-Border Privacy Rules (CBPR) System was discussed to inform India's case.
CONSENT AND CONSUMER PROTECTION			
Clause 11 - Consent necessary for processing of personal data Clause 12 - Grounds for processing of personal data without consent in certain cases.		From a business perspective, it would be challenging for data fiduciaries to educate individuals in a diverse country like India to have informed consent. At the same time, consent management is the only way to implement one of the key principles of data protection, i.e., purpose limitation.	One such innovation discussed during the session was the techno-legal solution for managing consent i.e. consent managers, which is also contoured under the Bill.

		On the bright side, the consent management problems could turn into opportunities for start-ups to bring innovation in regulatory technologies.	
STATE EXEMPTION			
Clause 35 - Power of Central Government to exempt any agency of Government from the application of PDP Bill.	JPC recommended incorporation of just, fair, reasonable and proportionate procedure to be introduced for the exemption process to safeguard the individual's right to privacy.	This clause stands contrary to the triple test (proportionally, legality and necessity) laid down under Puttaswamy judgment I. All power and no accountability is a bad mix where the state can use public order and national security to take away individuals' data.	There is a need for parameters, clearer definition, and safeguard for state exemption within the Bill. Process followed by the agencies exempted from the bill must be transparent and proportionate.
NON-PERSONAL DATA (NPD)			
Clause 91(1) - Government to make any policy for the digital economy, provided it doesn't govern personal data. Clause 91(2) - Mandates the data fiduciaries and data processors to share non-personal data.	Expansion of scope to govern both personal and non-personal data (NPD).	Having privacy regulation and promotion of NPD for industry growth under a single regulator could cause a lot of conflicts and issues. It is difficult to separate data into NPD and personal data, especially in financial data; hence it is hard to have separate jurisdictions.	NPD must be separated from the PDP Bill and considered differently, where personal data has the protection of fundamental rights needing to meet higher standards while NPD doesn't have this requirement.
CHILDREN PERSONAL DATA			
'Child' under the PDP Bill remains any data principal below 18 years.		Contradicts the status-quo as guardians are digital migrants while gen z children are digital natives who understand technology better. Age bracketing 18 years will cause market implications for those data fiduciaries whose user base predominantly is teenagers.	Consent managers should be allowed to aid guardians in managing children's consent through the Bill. The definition of "Child" within the data protection regulation must be congruent with international best practices by reducing the age bracket to 13 years.
SOCIAL MEDIA INTERMEDIARIES			
	JPC report proposes that digital platforms acting as intermediaries should be construed as publishers.	Breaking safe harbour and imposing a higher standard on platforms isn't always valid and adequate, as laws shouldn't take the direction of pre-censorship.	

HARDWARE REGULATION			
	Clause 49(2)(o) – Regulating hardware manufacturers, which collect data from digital devices.		The bill should take a phased out implementation of the measures covering different aspects of data security like hardware regulation.

The Dialogue™

INFORM ENGAGE IDEATE

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 technology and devel-opment issues. The Dialogue™ has been ranked as the world's Top 10 think- tanks to watch out for, by the Think-Tank and Civil Societies Programme (TTCSP), University of Pennsylvania in their 2020 and 2021 rankings.

https://thedialogue.co