NATIONAL LAW UNIVERSITY, DELHI

December 14, 2022

Shri Alkesh Kumar Sharma
Secretary, Ministry of Electronics and Information Technology,
Electronics Niketan, 6, CGO Complex,
Lodhi Road, New Delhi- 110003

Subject: Submission of Comments on the proposed draft of Digital Personal Data Protection Bill, 2022

Dear Shri Alkesh Kumar Sharma,

The *National Law University Delhi* (NLU Delhi), established by 'The National Law University Delhi Act, 2007' (Act No. 1 of 2008 National Capital Territory of Delhi) is a public funded university established by the Government of NCT of Delhi on the initiative of the High Court of Delhi. The Chief Justice of India is a visitor of the University and the Chief Justice of the High Court of Delhi is the Chancellor of the University. The *Centre for Communication Governance* (CGG) was established by the University in 2013 to contribute to improved governance and policy making, and to ensure that Indian legal education establishments engage more meaningfully with information technology law and policy. CCG is the only academic research centre dedicated to working on information technology law and policy in India.

CCG regularly engages with various institutions such as the Ministry of External Affairs, the Ministry of Law and Justice, and the Competition Commission of India, and seeks to support the executive and judiciary with research on legal, technical and regulatory aspects in the course of their decision-making on issues relating to information technology law and policy.

As part of our work, and given how critical it is to provide policymakers with well-researched and useful material, we are submitting our response to the proposed Digital Personal Data Protection Bill, 2022. We are thankful to the MeitY for giving us the opportunity to comment on this draft Bill and commend the MeitY for adopting a public and consultative approach to this process.

For any further information or input please reach out to the Executive Director of the Centre for Communication Governance, NLUD - Jhalak M. Kakkar at jhalak.kakkar@nludelhi.ac.in

With best wishes,
Sincerely yours,

15/12/2022

Professor (Dr.) Harpreet Kaur
Vice Chancellor (I/c)

Encl: Comments on the proposed draft Digital Personal Data Protection Bill, 2022

CENTRE FOR COMMUNICATION GOVERNANCE AT NATIONAL LAW UNIVERSITY DELHI

COMMENTS TO THE MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY ON THE DRAFT DIGITAL PERSONAL DATA PROTECTION BILL, 2022[1]

nludelhi.ac.in | ccgdelhi.org | ccg@nludelhi.ac.in

[1] Authored by Joanne D'Cunha, Priyanshi Dixit, Srishti Joshi, Sachin Dhawan, and Shashank Mohan. Reviewed and edited by Jhalak M. Kakkar.

Introduction

The Centre for Communication Governance would like to thank the Ministry of Electronics and Information Technology ('MeitY') for the opportunity to provide inputs on the Digital Personal Data Protection Bill, 2022 ('DPDP Bill'). We appreciate the efforts of MeitY in drafting a data protection bill that is clear and accessible. However, the proposed framework does not provide comprehensive protection of privacy rights and redressal of harms for data principals.

Our submission highlights the following five fundamental concerns with the DPDP Bill: (i) Does not safeguard the privacy of data principals, (ii) Absence of key data protection principles, (iii) Excessive reliance on delegated legislation, (iv) Lack of independence and regulatory powers for the DPBI, and (v) Imposition of onerous burdens on data principals.

1. **Does not safeguard the privacy of data principals:** At the outset, we would like to highlight that the DPDP Bill does not place the right to privacy of the data principal at the centre of its objectives. The Supreme Court in *Puttaswamy* has explicitly recognized the right to privacy of individuals. Consequently, a data protection law should be rights-centric and drafted with the intention of protecting privacy and empowering individuals to meaningfully exercise this right. Instead, by focusing on removing barriers from data processing activities, the Bill dilutes the rights of data principals, limits the understanding of harm, and eases obligations of data fiduciaries. For example, the preamble focuses on processing data in a manner that recognises the right to data protection alongside the need to lawfully process data. This is a significant departure from previous iterations of the Bill. To clarify its intent the Bill should go further and explicitly state that (i) the right to privacy is a fundamental right in India and (ii) it seeks to protect the informational privacy of individuals, much like earlier versions of the Bill.

2. **Absence of key data protection principles:** Universally recognised data protection principles such as collection limitation, purpose limitation, and openness are not adequately reflected in the framework of the DPDP Bill. To ensure a privacy focused data protection regulation, it is crucial for the Bill to be grounded in strong principles that enshrine the rights of individuals. The A.P. Shah Committee in 2012 examined numerous international privacy practices and principles and recommended the incorporation of national privacy principles in any privacy legislation. These principles have been further referred to by the Supreme Court in *Puttaswamy*. The

explanatory note accompanying the Bill features a few of these principles but it is important for all of them to be included within the data protection legislation itself. We thus recommend that core data protection principles are incorporated in the text of the Bill.

3. **Excessive reliance on delegated legislation:** Delegating rule making power to the government is necessary to provide flexibility, accommodate future circumstances, and prevent laws from becoming obsolete. However, the DPDP Bill does so without providing any legislative guidance or criteria for the framing of such delegated legislation to the government. Having guidelines set out precisely in the text of the Bill will not only help data principals but also the government in their rule-making power. This ties in with the government's goal of ensuring comprehensibility of the law for citizens as expressed in the explanatory note released alongside the Bill. Therefore, the DPDP Bill must articulate foundational principles, safeguards, and criteria to guide the framing of delegated legislation within the text of the Bill.

4. **Lack of independence and regulatory powers for the DPBI:** The DPDP Bill envisions the Data Protection Board of India ('DPBI') as only a quasi-judicial body. This is a departure from the previous versions of the Bill where a regulatory authority was envisaged. Data protection is a technical subject that necessitates the establishment of an expert regulator composed of individuals with the necessary expertise and regulatory capacity to exercise various regulatory powers. To ensure effective data protection, it may be crucial for the DPBI to have regulatory powers, especially for subject areas such as determining the grounds for non-consensual grounds of processing personal data.

   The DPBI's functions are further diminished by its lack of independence. The government will determine many aspects of its operation and functioning such as the appointment and removal of its members. As a result, the DPBI may not be well positioned to take decisions which are independent of government considerations.

   We recommend that the Bill establish a board with independent regulatory and adjudicatory powers. Such a body will be well positioned to serve the best interests of data principals.

5. **Imposition of onerous burdens on data principals:** Many provisions of the DPDP Bill discourage and disincentivise data principals from exercising their rights. For instance, data principals are burdened with unforeseen consequences while

exercising their basic right to withdraw consent for processing data. Many data principals who would otherwise have exercised this choice will now refrain from doing so, due to the uncertainty about what the 'consequences' of such withdrawal could entail.

Additionally, before proceeding with their grievances against data fiduciaries, data principals have to jump through several hoops. They have to ensure that they are fulfilling several duties or risk paying a hefty penalty. The DPBI may at various stages dismiss complaints due to insufficient grounds or demerits. Even when a data principal is successful in establishing a valid claim, the DPBI cannot impose penalties on a data fiduciary without establishing that the non-compliance is 'significant' in nature. The Bill does not provide the DPBI with powers to provide any compensation to data principals. Thus, a data protection regulation whose enforcement mechanism that disadvantages data principals in these ways will not be able to effectively fulfil its objectives. Additionally, the Bill specifically imposes duties and penalties on data principals, which will only further hinder them from exercising their rights. We recommend that i) duties of data principals be removed from the Bill; ii) the DPBI should be able to impose penalties for even non-significant non-compliance; and iii) the DPBI should be empowered to provide sufficient compensation to data principals.

Executive Summary

Below, we provide a summary of the key clauses of the DPDP Bill.

Chapter 1

Need for a more inclusive definition of harm: The DPDP Bill defines harm to mean bodily harm, distortion or theft of identity; or harassment; or prevention of lawful gain or causation of significant loss. The current definition of harm as per Clause 2(10) may be limited in its scope and does not adequately encompass harms across the spectrum of physical, mental, psychological, and financial harm. Further, the definition does not include harms that may arise from privacy violations such as loss of autonomy and self-determination. The DPDP Bill should incorporate a wider and inclusive definition for harm, that accounts for non-tangible, non-quantifiable and, future forms of privacy related harm.

Category of sensitive personal data is absent: The category of sensitive personal data is missing compared to previous versions of the Bill. The rationale behind categorising certain categories of personal data such as biometric data in this manner is to provide a higher standard of protection as it may involve greater risks due to its sensitive nature. Therefore, it may be beneficial for the Bill to consider re-incorporating this category to ensure that more sensitive forms of data receive appropriate protection.

Graded approach to age of a child and parental consent: The DPDP Bill defines a child to be eighteen years of age. By doing so, the Bill requires that any child that accesses internet services below the age of 18, will require verifiable parental consent. This may restrict a child's ability to use the internet even for educational purposes. In order to allow children to exercise agency and autonomy in their access to the internet and related services, a graded approach to parental consent may be considered. Through this approach, parental consent can be required depending on the potential risk associated with the services provided. This may enable children to use internet services that do not pose risks to them more freely while also ensuring their protection through parental consent where required.

Chapter 2

Incorporate stronger obligations for Data Fiduciaries: Chapter 2 of the Bill provides for the obligations of data fiduciaries. Clauses 6 and 7 of the Bill lay down the obligation of the data fiduciary to provide notice and seek consent from the data principal prior to processing any data. However, compared to the previous iterations of the Bill, these have been significantly diluted. We recommend that in addition to the itemised notice requirements to the data principal under Clause 6, the notice should specify additional details for the data principal based on data retention, updated notifications, information regarding sharing of personal data with any third party, and ensuring specific notice in addition to a general notice be given to the data principals. Additionally, we recommend that the parameters for consent under Clause 7 (free, specific, informed and unambiguous) be clearly defined as articulated in previous iterations of the Bill.

Reliance solely on consent to allow data processing could be insufficient due to information asymmetry in favour of the data fiduciary. Along with improved consent mechanisms, it becomes important to address this challenge by ensuring that other universally recognised data protection principles are incorporated explicitly under the law. Unlike the previous iterations of the bill, the DPDP Bill significantly digresses from the inclusion of the core privacy principles that were developed by the Organisation for Economic Co-operation and Development (OECD) and then subsequently recognised in privacy frameworks across the globe. The addition of these principles would ensure fair and lawful data processing after consent is provided. Thus, we recommend that Clause 9 of the Bill explicitly incorporate key data protection principles of purpose limitation, storage limitation, and accountability within the general obligations of all data fiduciaries. Clause 9 also requires that a data fiduciary have appropriate technical and organisational measures. We recommend that these measures are privacy friendly and that the provision specifically incorporate privacy by design and default policy requirements along with procedural guidelines.

Deemed consent should be defined and be based on specific safeguards: Clause 8 allows processing of personal data based on deemed consent and lays down certain grounds under which such processing can take place. However, the provision is unclear about how deemed consent will function in practice. For example, it does not clarify which other obligations of the data fiduciary will cease to apply in the case of deemed consent. The previous iterations of the Bill expressly stated that the obligation of notice would be exempt in cases of non-consensual data processing.

We recommend that the provision clarify the rationale for allowing data processing through deemed consent. We also recommend that the Bill specifically allow for notice to be a mandatory obligation for all data processing under deemed consent barring a few circumstances like medical emergencies, where it would be absolutely impossible to provide a notice. Additionally, since Clause 8 impinges on the choice and autonomy of individuals we recommend that any processing of personal data based on deemed consent should follow the test of necessity and proportionality which should be explicitly laid down in the provision.

Processing of children's data should follow a graded approach: The DPDP Bill allows for the processing of children's data solely on the basis of verifiable parental consent. Imposing such a condition would limit access to online services for children and teenagers impacting their ability to access information and the overall development of the child.

However, the objective of the law should be to balance the right of the child to access the internet with their data protection interests. So, we recommend that the mechanism for verifying parental consent should ensure that it follows the principles of collection limitation and purpose limitation. For example, verification via government IDs should be permitted under extremely limited circumstances; Unlike the previous iterations of the Bill, the DPDP Bill does not specifically state that any processing of children's data will take place based on the best interests of the child. This principle has been mandated by the United Nations Convention on Child Rights and as India has adopted the convention, the Bill should require that any decisions regarding a child be bound by it. Additionally, the Bill should provide for instances where data fiduciaries can allow self-verification of the child's age for services that have no risk of harm to the child.

Chapter 3

Inclusion of duties burden the data principal: The inclusion of duties for the data principal as per Clause 16 significantly dilutes the rights based framework of the Bill. The clause places the onus on the data principal to provide correct information to the data fiduciary. Imposing penalties in case of non-compliance with the duties will disincentivise data principals and limit their ability to seek any redressal or invoke their rights under the Bill. We recommend that the entire provision on duties, i.e., Clause 16 should be deleted.

Wider application of rights of the data principal: The DPDP Bill has limited the applicability of the right to erasure of data principals. We recommend that the Bill should ensure that the right to erasure should include seeking discontinuation of processing their data by withdrawing consent for the collection, use or disclosure of the same. This should be based on certain safeguards whereby an independent authority established under the Bill would balance the implementation of this right with the right to freedom of speech and expression and the right to information.

Further, we recommend that the DPDP Bill should include the right to data portability and the right against direct marketing in order to ensure that data principals can exercise true autonomy over their personal data.

Chapter 4

Wide exemptions and declining safeguards: Clause 18(2) provides broad exemptions from the provisions of the Bill for the purpose of State interests such as sovereignty, integrity and security of India, maintenance of public order and crime prevention. The purposes listed in these clauses may be open to wide interpretation and could justify extremely wide uses of personal data by the State without any data protection obligations. These wide exemptions undermine the right to privacy of data principals and it is crucial that such limitations of the right to privacy adhere to the tests of legality, necessity, and proportionality as laid down by the Supreme Court in *Puttaswamy*.

Therefore, specific safeguards that have been laid down clearly by the Supreme Court, should be incorporated into Clause 18(2).

Vague criteria for exempting Data Fiduciaries: Clause 18(3) allows the central government to exempt by notification certain data fiduciaries from specific provisions of the Bill. The Bill does not articulate any guidelines for such an exemption and it is unclear what criteria will be used to make such determinations. Also, there is no justification for exempting fiduciaries from obligations such as ensuring accuracy, data retention requirements or protections afforded to children's data.

To the extent that they are retained, Clause 18(3) must include clear and relevant criteria for determining when a data fiduciary will be eligible for exemption. Also the rationale for doing so must be provided in the ensuing notifications.

Chapter 5

Independence and role of the Data Protection Board of India: The DPDP Bill provides for the establishment of the Data Protection Board of India ('DPBI'). The strength, composition, process of selection, terms and conditions of appointment and service, and removal of members of the DPBI will be entirely determined by the central government. The DPBI is envisaged to be digital by design, whereby most functions will be carried out digitally. The Chief Executive will manage the affairs of the Board. Their appointment and terms and conditions of service will be determined by the central government.

The institutional design of the DPBI has been considerably weakened in the DPDP Bill in comparison to the previous versions of the Bill. Now the Executive will solely determine the composition of the board, the process of selection of board members and other matters via its rule-making power. Similarly, marking a big shift from previous iterations the DPBI is no longer a regulator and has not been designed as a quasi-judicial body which could have significant implications for safeguarding user rights. It is recommended that in order to ensure the independence of the DPBI from the Executive, appointments should be made through a Selection Committee with adequate judicial representation. Finally, the 'digital by design' framework must be optional and not mandatory, so as to account for the digital access gap.

Chapter 1: Preliminary

Definitions

Child

Clause 2(3): Clause 2(3) defines a child as an individual who has not completed eighteen years of age. A concern that may arise with such a strict definition is that it has a blanket approach to the age of consent and therefore, in determining the obligations of a data fiduciary. According to Clause 10(1) of the DPDP Bill, any processing of personal data belonging to children below the age of 18 will require verifiable parental consent, irrespective of the type and purpose for collection.

Concerns: This may heavily restrict a child's access to internet services for both educational and entertainment purposes.

Recommendations: Lowering the age of who is considered a child, along with a graded approach to parental consent may be beneficial in order to further children's agency and choice while also providing them with adequate protection.

The GDPR defines 16 as the age above which children are deemed capable of giving consent.[2] This standard has also been followed by Sri Lanka which has set the age of a child as below 16.[3] Similarly, in Singapore, the Personal Data Protection Commission has provided guidance asking organisations to consider if a child has "*sufficient understanding of the nature and consequences of providing consent*".[4] Since organisations have made it a practice to require children's consent below the age of 13, the Commission also observed that 13 could be deemed a "*practical rule of thumb*".

[2] Article 8, Regulation (Eu) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>

[3] Section 56, Personal Data Protection Act, No. 9 of 2022, Parliament of the Democratic Socialist Republic of Sri Lanka <https://www.parliament.lk/uploads/acts/gbills/english/6242.pdf>

[4] 'Advisory Guidelines on the Personal Data Protection Act for Selected Topics' 53–54 <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Selected-Topics/Advisory-Guidelines-on-the-PDPA-for-Selected-Topics-17-May-2022.ashx?la=en>.

Children use internet services for educational, informational, and entertainment purposes, which can be hampered by requiring strict parental consent for every given use. However, this does not mean that parental consent should be exempted entirely without any alternative measures in place. There is growing consensus that a consent-based mechanism for children may not be adequate, both in terms of protecting children and accommodating for evolving levels of maturity and experiences.[5] As a result, it may be necessary for regulation to provide varying degrees of protections to children.

Frameworks such as the UK Information Commissioner's Office's ('ICO') Gillick competence test have begun to recognise that children have different capacities which ultimately influence their ability to exercise control over their online decisions.[6] In order to avoid relying entirely on parental consent, the Children's Online Privacy Protection Act ('COPPA') adopts a risk-based approach to determine the need for parental consent based on the potential risk involved in the provision of a service.[7] Therefore, commercial services that do not specifically share personal data would not require parental consent. In order to find a balance between protecting children while enabling their participation online, recent literature suggests such a 'sliding-scale' approach to the age of consent.[8] This may enable children to use internet services more freely as services that pose a higher risk could necessitate parental consent, while a child's consent would suffice for safer activities. However, in order to actualise this, it may be necessary to lower the age of who is considered a child under Clause 2(3). By doing so, a tailored approach to parental consent may be further considered.

Harm

Clause 2(10): Clause 2(10) defines 'harm' to mean (a) any bodily harm; or (b) distortion or theft of identity; or (c) harassment; or (d) prevention of lawful gain or causation of significant loss. The understanding of harm in the DPDP Bill is significantly limited

[5] Gerison Lansdown, 'Can You Hear Me? The Right Of Young Children To Participate In Decisions Affecting Them' <https://bibalex.org/baifa/Attachment/Documents/114976.pdf> accessed 5 December 2022.

[6] Information Commissioner's Office, 'What Is Valid Consent?' (2021) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent> accessed 5 November 2022.

[7] Federal Trade Commission, 'Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business' (June 2017) <https://www.ftc.gov/business-guidance/resources/childrens-online-privacy-protection-rule-six-step-compliance-plan-your-business#chart> accessed 5 December 2022.

[8] Lauren A Matecki, 'Update: COPPA Is Ineffective Legislation! Next Steps For Protecting Youth Privacy Rights In The Social Networking Era' (2010) 5 Northwestern Journal of Law and Social Policy 369.

compared to the 2019 Bill and 2018 Bill. These Bills, in comparison, encompassed harms that ranged from physical, mental, psychological, and financial harm.

Concerns:

1] The definition of harm does not include privacy-based harm i.e., direct harm occurring from the loss of privacy by breach or misuse of personal data. It does not consider harms that may arise due to loss of autonomy or self-determination.

2] Further, the definition is not broad or clear enough to indicate how it will apply to non-tangible, non-quantifiable, or new forms of harm that might arise as a result of technological developments.

3] Also, the framing of Clause 2(10) through the use of the term 'means' may indicate that it will be interpreted to mean those harms that may arise from the ones listed in the clause. The DPDP Bill has moved away from the 2019 Bill which uses the term 'includes' allowing it to be more expansive in nature. A listing out of harms should not be the aim of the provision.

Recommendations:

1] Harm should include harms that arise out of privacy violations.

2] The protections offered by a data protection legislation may benefit from a more flexible framework that can act as guidance to interpreting harm, especially as it relates to the application of many provisions across the Bill.[9] As a result, it may be necessary for the definition of harm to be sufficiently wide so as to account for the numerous risks that may arise out of data processing. For instance, apart from the definition including mental or psychological harms, it should also indicate specific harms towards children or individuals that might be differently abled. It may be further useful for the provision to include the nature of harms that may arise out of unauthorised State access.[10]

[9] Dvara Research, 'Initial Comments on the Personal Data Protection Bill 2019' (2020) <http://www.dvara.com/research/wp-content/uploads/2020/01/Initial-Comments-on-the-Personal-Data-Protection-Bill-2019.pdf> accessed 5 December 2022.

[10] Software Freedom Law Centre, 'A Ready Reckoner on Proposed Data Protection Laws in India: Comparative Analysis' (25 November 2022) <https://sflc.in/ready-reckoner-proposed-data-protection-laws-india-comparative-analysis> accessed 5 December 2022.

Finally, an indicative list of harms can provide guidance to even adjudicatory bodies and aid them in grievance redressal. Therefore, it may be useful for the DPDP Bill to incorporate a definition that can cover existing and potential forms of physical, mental, psychological, financial and privacy harm to allow for a wider and more inclusive consideration of harm.

Personal data

Clause 2(13): Clause 2(13) defines personal data to mean any data about an individual who is identifiable by or in relation to such data.

Recommendations: Our submissions on Clause 2(13) deal with the concept of identifiability. We appreciate that the DPDP Bill includes individuals that are identified but also identifiable through personal data. The adoption of a wider definition will facilitate a comprehensive application of the law. It may be further beneficial to clarify that a data principal can be identified/identifiable through both direct and indirect means. This ensures that the definition includes within its ambit the possibility of identification through the combination of various types of information.[11]

Based on the spectrum of identifiability, a growing body of literature indicates that there may not be a need for separate classification of data. This approach is advocated alongside adopting a risk-based approach for the definition of personal data.[12] The proponents of this approach - scholars Paul Schwartz and Daniel Solove, suggest that the spectrum of personal information may be divided into three categories.[13] Information can be about an identified person – where the person has been identified; an identifiable person – when specific identification can be possible; or a non-identifiable person – an unidentified person where there is only a remote risk of identification. Therefore, instead of regulating personal data based on categories, such an approach would provide 'different regimes' of regulation for each category based on the potential risk associated with identification of an individual. However, given that the data protection framework in India is still

[11] Information Commissioner's Office, 'Can We Identify an Individual Indirectly from the Information We Have (Together with Other Available Information)?' (5 December 2022) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/can-we-identify-an-individual-indirectly/>.

[12] Paul Schwartz and Daniel Solove, 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information' (2011) 86 New York University Law Review <https://scholarship.law.berkeley.edu/facpubs/1638/> accessed 5 December 2022.

[13] ibid.

developing, it may be of value to first begin by classifying certain categories of data which require additional protection, separately.[14]

The 2019 Bill included the category of sensitive data which is missing from the DPDP Bill. In our previous comments to the White Paper Of The Committee Of Experts On A Data Protection Framework For India, we highlighted that when considering special categories of data such as sensitive data, it's important to understand the reason for such classification and why many jurisdictions have afforded it higher protections.[15] The GDPR is one regulation that provides some insight about why these specific types of data have been included as a separate category. Recital 51 of the GDPR states that "*Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms*". This rationale has stemmed from the approach taken by the GDPR's predecessor. It suggested that the need to regulate particular categories of data in a different way stems from the presumption that misuse of these data could have more severe consequences on the individuals fundamental rights, such as the right to privacy and non-discrimination.[16]

In comparison to the approach taken by the DPDP Bill, the 2019 Bill rightly considered the need for the category of sensitive data along with a higher standard of obligations for data fiduciaries. As a side note, Clause 11(1) which deals with additional obligations for Significant Data Fiduciaries ('SDFs') lists the 'sensitivity' of data as a factor for determining SDFs. In addition to the benefit of affording higher protections to certain types of data, defining sensitive data within the text of the DPDP Bill may aid the central government to select SDFs. Therefore, to protect personal data that may be exposed to higher risks, the DPDP Bill should reconsider the inclusion of sensitive personal data.

General Comments

Missing provisions

[14] Centre for Communication Governance, 'Comments to the White Paper of the Committee of Experts on a Data Protection Framework for India'.(2018)

[15] ibid.

[16] Article 29 Data Protection Working Party, 'Advice Paper on Special Categories of Data ("Sensitive Data")' <https://www.pdpjournals.com/docs/88417.pdf> accessed 8 December 2022.

Anonymisation and re-identification: Amongst many other definitions, the DPDP Bill no longer includes the terms anonymisation, anonymised data or re-identification. At the outset, it may be necessary for the Bill to include these terms in order to acknowledge the risks of re-identification after anonymisation. It is important for a data protection regulation to provide data fiduciaries with guidance on anonymisation to adhere to necessary data security measures in ensuring adequate data protection. Although non-personal data will fall outside the ambit of a personal data protection regulation, the government is considering policies to govern non-personal data and the type of de-identification techniques used will determine how data is categorised into personal and non-personal data.[17]. As the challenges with anonymisation are now well known, scholars such as Schwartz and Solove (discussed above) have suggested risk-based approaches to address the risk of re-identification. Further, it is also important to recognise that re-identified data should once again be afforded protections under a data protection regulation. As a result, we recommend that the DPDP Bill define concepts such as anonymisation, anonymised data, de-identification and re-identification.

[17] Yianni Lagos, 'Taking the Personal out of Data: Making Sense of De-Identification' (2014) 48 Indiana Law Review 187.

Chapter 2: Obligations of data fiduciary

Notice

Clause 6: We appreciate that the Bill recognises the importance of notice and the need to ensure ease of access to notice in any language specified in the Eighth Schedule to the Constitution of India. Clause 6 of the DPDP Bill provides for the obligations of the data fiduciary to provide an itemised notice before seeking consent from the data principals. It defines notice to be a separate document or a part of the same document through which data is collected. This definition also includes notice to be an electronic form besides a separate document. It leaves any other forms of notice to be included through subsequent rules.

Concerns: The DPDP Bill substantially misses out on providing a detailed list of contents that the notice should contain, the lack of which would directly negatively impact informed and meaningful consent.

Recommendations: Ensuring that the itemised notice contains detailed information would significantly improve the data principal's knowledge of the use or processing of their personal data and facilitate informed decisions.[18] The previous iterations of the Bill rightly listed all the requirements that should accompany a detailed notice provided by the data fiduciary.[19] We suggest that the method for the issuance of notice mentioned under Clause 6 should also identify other details that should form a part of the notice provided by a data fiduciary:

1. Information regarding any third party data processors who would collect or process data on the behalf of the data controller
2. The data principal should be notified if the data controller updates/changes its data processing or collection
3. The data principal should be informed of the duration for which the data is being retained by the data fiduciary.
4. Data fiduciary should ensure that notice is provided to each individual in addition to any general notice that may be provided on their website / platform.

[18] Daniel Susser, 'Notice After Notice-and-Consent: Why Privacy Disclosures Are Valuable Even If Consent Frameworks Aren't' (2019) 9 Journal of Information Policy 37.

[19] Clause 7 of the Personal Data Protection Bill, 2019; Clause 8 of Personal Data Protection Bill, 2018.

5. Contact details of the data fiduciary and the Data Protection Officer of the data fiduciary wherever applicable
6. The mechanism and procedure to withdraw consent

The aforementioned requirements for notice should be read in tandem with consent. Once the data principal consents to the processing of personal data based on the notice, it should not be assumed that the decision is binding for all processing (besides the stated purpose) that would be taken on behalf of the data principal.[20]

Privacy policies often contain a provision which allows the data fiduciary/processor to unilaterally amend them.[21] In some cases, they will offer to notify users of the amendments before or after the fact, but many policies simply state that by continuing to use the service, the user accepts the amendments. Thus, point 2 would ensure that this is done through specific consent of the data principal. We have also addressed this issue in our comments on Clause 7 (consent).

Further, storage limitation is an important data protection principle that ensures that the data collected is only retained until it meets the purpose for which it was collected.[22] Previous iterations of the Bill emphasised the principle of storage limitation and mandated the disclosure of such data retention period under notice. The DPDP Bill ensures compliance with this principle by the data fiduciary (under Clause 9(6)) - we have made our recommendations regarding this in the subsequent chapters. However, in addition to such compliance requirements, it is also important to ensure that data principals are informed of the period of retention of their personal data with the data fiduciary or what parameters are in place to make such a decision about retention. This requirement should also be met by the data processors - not solely data fiduciaries.

Additionally, since the DPDP Bill ensures that significant data fiduciaries appoint a Data Protection Officer, it should also ensure that such details are provided through the notice. This would enable the data principal to easily access and proceed through any issues that may arise after their data is collected by the data fiduciary. Such a requirement is currently

[20] John Sebastian and Aparajito Sen, 'Unraveling the Role of Autonomy and Consent in Privacy' [2020] Indian Journal of Constitutional Law.

[21] Logan Koepke, '"We Can Change These Terms at Anytime": The Detritus of Terms of Service Agreements' (*Medium*, 19 January 2015) <https://medium.com/@jlkoepke/we-can-change-these-terms-at-anytime-the-detritus-of-terms-of-service-agreements-712409e2d0f1> accessed 16 December 2022.

[22] ICO, Guide to GDPR, 'Principle (e): Storage Limitation' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/>.

under the provision of consent, Clause 7(3), and should be included under Clause 6 as a notice requirement. In a similar vein, this should also apply to informing data principals of the mechanisms in place for withdrawal of consent. The scope and importance of withdrawal of consent is addressed in the next section of our comments on Clause 7 (consent).

Clause 7(9) of the DPDP Bill places the onus on the data fiduciary to ensure that the notice given and consent provided by the data principal is in accordance with DPDP Bill. In this light, it is recommended that in addition to a general detailed notice, the data fiduciary demonstrates compliance by providing individual notices to each data principal.

Consent

Clause 7: Clause 7(1) of the Bill provides for the obligation of the data fiduciary to obtain consent from data principals for a 'specified purpose' for the processing of their personal data. It defines 'specified purpose' as the purpose mentioned in the notice given by the data fiduciary to the data principal. Accordingly, it lays down that consent should be free, informed, specific and unambiguous. It also states that consent should be given by the data principal by a clear affirmative action.

Recommendations:

1] Establish clear parameters of consent: While previous iterations of the data protection bill defined what each of these parameters would mean - the DPDP Bill does not do so. Leaving the compliance with these parameters open to interpretation by the data fiduciary would allow expansive grounds of data processing which might solely be in the interest of the data fiduciary. This provision should ensure that the mechanism of obtaining consent is in cognizance of data principals' autonomy over their personal data and follows the principle of purpose limitation. For example, the previous iterations of the Bill expressly stated that 'informed consent' would mean consent obtained as per proper compliance with the notice requirement under the previous draft Bill. Thus, this provision should lay down an established legally binding consent mechanism as was seen in the previous iterations of the Bill.

The JPC had recommended that the requirement of consent should "*reflect the idea that the consent of data principal has to be obtained by specifying the conduct and context*

explicitly without circumvention of law and without any kind of implicit inferences".[23] The ambiguous language of the provision fails to meet these concerns. Therefore, we recommend that for ease of compliance and in the interest of data principals - these terms must be backed by an explanation as to how one is to interpret what consent stands for. We also emphasise on the need to clarify that where a data fiduciary seeks consent for multiple purposes, consent must be specific to each of those purposes.

2] Withdrawal of consent: We appreciate that the DPDP Bill in Clause 7(4) recognises (i) the importance of consent withdrawal and (ii) the necessity of ensuring that withdrawal of consent should be as easy as giving consent. However the provision states that the consequences of such withdrawal of consent shall be borne by the data principal. It is important to note that with, the data principal should not face any consequences for withdrawal of consent - such withdrawal should only lead to termination of data processing of the personal data in question.

However, Clause 7(5) of the DPDP Bill allows perpetuation of processing of personal data after withdrawal of consent, i.e., data processing without consent if it is required under this Act or any other law. The inclusion of broad grounds for allowing data processing after withdrawal of consent under 'any other law' is vague and would open various other grounds for non-consensual data processing. This also lacks clarity as to whether the grounds for such perpetual processing would be similar to the grounds mentioned under Clause 8 (deemed consent).

The provision should be amended to exclude 'required under any other law' as a ground for continuing data processing after withdrawal of consent. We recommend that in cases where the data fiduciary is required to retain data under this Bill, the data principal should be informed in writing of the reasons as to why such retention is taking place.

General Comments

Notice and Consent: As pointed out in our past comments, it is important to acknowledge that in the age of Big Data it is difficult to obtain meaningful consent from data principals. Thus, relying on consent as the only ground for data processing presents unique challenges. Consent is often obtained in the form of standard form contracts where there is a power imbalance or information asymmetry in favour of the data

[23] Recommendation 33, Seventeenth Lok Sabha, 'Report of the Joint Committee on The Personal Data Protection Bill, 2019'.

controller who is obtaining the consent.[24] Therefore, the law should provide substantive safeguards to ensure that the contractual nature of consent is not misused to work around the implementation of data protection principles.[25]

In our recommendations to the 2018 Bill, we had highlighted that the existing consent-based mode should be strengthened with more substantive law.[26] In this regard, reiterating our recommendations to the White Paper of the Committee Of Experts on A Data Protection Framework For India - consent should be unbundled, and separated in the context of collection of data that is used for different purposes, as well as data that is not necessary for the service in question.[27] The GDPR has adopted a similar approach wherein - it sets mandatory 'unbundling' of consent[28] in the following contexts: (i) separation of consents for each item requiring consent, not one overall consent;[29] and (ii) separation of consents from the collection of any other information not necessary for the performance of the contract.[30]

Consent Managers: Clause 7(6) and 7(7) of the DPDP Bill constitutes the provisions through which data principals may give, manage, review or withdraw consent through consent managers. Consent managers have been defined as data fiduciaries that enable data principals to give, manage, review and withdraw their consent through an accessible, transparent, and interoperable platform. This definition is in consonance with the definition of the term under the previous iterations of the Bill.

However, there is also potential for significant harm to the data principal given the sensitive nature of the service that is provided in such cases. It is also important to recognise that there may be sensitive data with a higher degree of risk associated with them, that is being dealt with by such consent managers. The Bill does not provide any safeguards or procedures for the provision of such a service. For example, in situations

[24] Centre for Communication Governance, 'Comments on the Data Protection Bill, 2019'.

[25] ibid.

[26] Kritika Bhardwaj, 'Preserving Consent Within Data Protection In The Age of Big Data' (2018) 5 NLUD Student Law Journal 100.

[27] 'Comments on the Data Protection Bill, 2019' (n 24).

[28] Graham Greenleaf, 'Data Protection: A Necessary Part of India's Fundamental Inalienable Right of Privacy – Submission on the White Paper of the Committee of Experts on a Data Protection Framework for India' [2018] UNSW Law Research Paper No. 18-6.

[29] Article 7(2), GDPR (n 2).

[30] Article 7(4), GDPR (n 2).

where consent managers are handling health data, there may be specific safeguards needed as opposed to handling low-risk personal data. We recommend that the concept of a consent manager is discussed in greater detail, and an appropriate mechanism that takes into consideration the security of and potential for harm to the data principal is put in place, if required.

Key issues with consent managers are - to recognise that there may be sensitive data with higher risk of harm that is being dealt with by consent managers. Owing to that there should be specific safeguards in place. There should be more clarity on the details of the functionality and mechanism of consent managers be put into place.

The DPDP Bill rightly places the onus on the data fiduciary to prove that the notice provided and consent obtained from the data principal is in accordance with the law. However, the implementation of this clause would only have a positive impact on the rights of the data principals if the parameters of consent are defined under the law as suggested above.

Deemed Consent

Clause 8: Clause 8 of the DPDP Bill states the grounds under which a data principal would be 'deemed' to have given consent for the data processing. This provision is premised considering situations wherein it would be impracticable or inadvisable to seek consent.[31]

Concerns: The Bill does not define what constitutes 'deemed' under this Clause. Based on previous iterations of the Bill, it could be interpreted as processing of data without the obligation of providing notice to the data principal. However, the 2018 Bill and the 2019 Bill were clear on the exemption of notice under certain circumstances where processing of data took place without consent. Additionally, the provision does not include appropriate safeguards/qualifiers prior to allowing processing of personal data based on deemed consent.

Recommendations: The DPDP Bill should clearly define 'deemed' consent. Since notice is an important obligation to protect the rights of the data principals - the

[31] Ministry of Electronics and Information Technology, 'Explanatory Note to Digital Personal Protection Bill, 2022' <https://www.meity.gov.in/writereaddata/files/Explanatory%20Note-%20The%20Digital%20Personal%20Data%20Protection%20Bill%2C%202022.pdf>.

requirement of notice should not be exempt for all types of data processing under deemed consent. Further, the entire provision should indicate that the processing will be fair and reasonable keeping in mind balancing of rights of data principals with any requirement of non-consensual data processing. Thus, we recommend that the following be considered in order to give effect to non-consensual processing of data:

1] Requirement of notice: The DPDP Bill is silent on whether the deemed consent provision exempts data fiduciaries from having to provide notice. In this regard, we recommend that the requirement of notice should be applied to a few categories of deemed consent based data processing. Notice is an important safeguard in terms of informing data principals about the type of data that might be collected and for what purpose, even without obtaining consent.[32] For example, the requirement of notice can be exempted for Clauses 8(4) (emergency) to 8(6) (medical emergencies or disasters) but would be valid in the case of 8(1), 8(2) (compliance under any law), 8(7) (employment related activities), 8(8) (mergers, credit scoring, etc.).

2] Data processing under 'public interest' is unclear:

'Public interest' has been defined under Clause 2(18) and the Bill is unclear whether there is an overlap in the understanding of what constitutes public interest under Clause 8(8) and Clause 2(18). Thus, we recommend that data processing under Clause 8(8) should not be phrased as 'public interest' given the overlap of the term within the Bill itself.

Additionally, previous iterations of the Bill explicitly included 'whistleblowing' as a ground under this Clause. Therefore, in light of a probability arising wherein data is processed for whistle blowing purposes, we recommend that Clause 8(8) should also include it as one of the grounds for data processing based on deemed consent.

3] Processing of publicly available personal data: Further, it is important to note that processing publicly available personal data may not always be a reasonable purpose. This is because in the absence of a data protection regime, personal data that should not have been made public may have been shared. In these cases, it is not appropriate to continue using this information. We suggest adding a caveat to Clause 8(8)(f) to address this issue.

[32] 'Comments on the Data Protection Bill, 2019' (n 24).

4] Proportionality for State use of deemed consent: As stated above relying on consent would not be valid for all types of data processing - there needs to be a qualifying test based on the grounds of necessity and proportionality to enable such processing. The clause currently relies on identifying when it would be 'necessary' to process data without the consent of the data principal. As suggested in our comments for the 2018 Bill under Clause 8(2) for the State to qualify data processing under the necessity test, each individual function of the State should be tested to see not only if it is necessary for the State to undertake the processing, but also if it is necessary to do so without the consent of the data principals. For this purpose, the requirements of proportionality must be expressly inserted as merely a legal requirement to part with personal data (whether for a service, benefit, or otherwise) will not be sufficient to meet the tests established by the Supreme Court in *Puttaswamy I*.[33] It must be established that less intrusive alternatives will not meet the desired aim of the legislation. [34]

5] Power to include additional grounds should be limited: Clause 8(9) of the Bill lays down that the central government would be allowed to include additional grounds for data processing under deemed consent for a fair and reasonable purpose after considering certain parameters under Clause 8(9)(a) to (c). However, this clause is ambiguous and gives wide powers to the central government to allow non-consensual data processing. In this regard, it becomes important to refer to the Supreme Court's decision in *Puttaswamy I*, wherein it recognised informational self-determination and autonomy as the foundation of the right to privacy. Thus, we recommend that the clause be amended to ensure that any processing of data without obtaining informed and meaningful consent should be strictly necessary and proportionate.

General Obligations

Clause 9: Clause 9 of the Bill provides the obligations that the data fiduciary needs to comply with while processing personal data. We appreciate that this provision places the responsibility of ensuring compliance of obligations by the data processor and the data fiduciary.

Concerns: The listed obligations under this clause are vague and unclear. Additionally, unlike the previous iterations of the Bill, the data protection principles have not been incorporated under these obligations for data fiduciaries.

[33] *K.S. Puttaswamy v. Union of India* (2017) 10 SCC 1 (hereinafter "Puttaswamy I").

[34] Ibid.

Recommendations: We recommend that the clause lay down specific requirements to enforce privacy friendly technical and organisational measures. Further, we also recommend that the Bill incorporates data protection principles of purpose limitation, storage limitation, accountability, fair and reasonable processing as reaffirmed by the Supreme Court in *Puttaswamy I*.[35] Additionally, the exceptions to ceasing retention of personal data must not include vague grounds of 'business purposes'.

1] Inclusion of privacy by design and default: Clause 9(3) states that the data fiduciary and the data processor shall have the appropriate technical and organisational measures in place to ensure compliance with the Act. There must be additional obligations in place to ensure that the interest of data principals is proactively protected. We recommend that the Bill lays down specific privacy by design and default policy requirements along with procedural guidelines.[36] The requirement for adopting a privacy by design policy was suggested by the Srikrishna Committee Report stating that it establishes technical and organisational measures in a manner ensuring compliance with the law by minimising or eliminating adverse impacts on privacy.[37] In addition to this, as suggested by us in our comments to the 2018 Bill, this should also include a privacy by default standard that ensures that the most privacy-protective legal option should be presented to users as the default. [38]

2] Principles based approach to obligations: Unlike the previous iterations of the Bill, the DPDP Bill does not lay down a broader requirement for fair and reasonable data processing. Any data protection regulation should follow a principle based approach.[39] The processing of data should be fair such that it does not cause harm to the privacy of the data principal even after consent is given.[40]

---

[35] Committee of Experts under the Chairmanship of Justice B.N., 'A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians' (2018) <https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf> accessed 25 October 2022.

[36] 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default'.

[37] Committee of Experts under the Chairmanship of Justice B.N. (n 35) 60.

[38] Graham Greenleaf, 'GDPR-Lite and Requiring Strengthening – Submission on the Draft Personal Data Protection Bill to the Ministry of Electronics and Information Technology (India)' [2018] UNSW Law Research Paper No. 18-83.

[39] Committee of Experts under the Chairmanship of Justice B.N. (n 35).

[40] ICO, Guide to GDPR 'Principle (a): Lawfulness, Fairness and Transparency' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-

Further, the obligation of the data fiduciary should also include the storage limitation principle.[41] Although such a requirement is present under Clause 9(6), it also provides the data fiduciary with an option to "*remove the means by which the personal data can be associated with particular data principals*". Since there is no explanation as to what the latter obligation could come to mean, it could be interpreted in different ways by the data fiduciaries to escape the obligation to delete the data stored with them. On the other hand, this could mean that the data fiduciary could choose to de-identify/anonymise data by removing identifiers from the dataset. In such instances, the DPDP Bill is not equipped to deal with issues arising out of such de-identification/anonymisation. Further, this lays down 'business purposes' as a ground to bypass the obligation to delete stored data. This ground is too broad and would bring under its ambit any data processing activity in the interest of the data fiduciary resultantly being detrimental to the rights of the data principal. In most cases, it would be in the interest of the data fiduciary to retain data for any business purpose listed by them in their interest - this obligation would in effect be redundant against the protection of privacy of the data principals. Thus, we recommend that this clause be amended to ensure that the storage limitation principle is placed in accordance with the interests of data principals.

The principle of accountability does not echo in this clause. According to this principle the data fiduciary should not only have safeguards for data protection and compliance of the law in place but also should be able to demonstrate such compliance when sought for.[42] We recommend that the obligation of the data fiduciary should include accountability measures such as record keeping obligations and periodic assessments.

Processing of Children's Data

Clause 10: This provision lays down specific obligations of data fiduciaries in relation to processing of children's data. It broadly allows for data processing of children only through 'verifiable parental consent' and under the conditions that such processing (i) does not cause 'harm' to the child nor does it undertake (ii) tracking or behavioural monitoring of children or targeted advertising directed at children. Under Clause 10(4), a

transparency/#:~:text=In%20general%2C%20fairness%20means%20that,also%20about%20whether%20you%20should.>.

[41] ICO, Guide to GDPR (n 22).

[42] ICO, Guide to GDPR, 'Accountability Principle' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accountability-principle/>.

data fiduciary can be exempted from parental consent as well as allowed tracking or behavioural monitoring of children or targeted advertising directed at children.

Concerns: The provision does not include the best interest principle which is essential to ensure that any processing of children's data would only be for the benefit of the child. Further, the provision does not state whether the data fiduciary will be required to verify the child's age and lacks clarity on the safeguards for verifiable parental consent.

Recommendations: The provision should include the best interest principle based on the United Nations Convention on the Rights of the Child (UN-CRC). Clause 10(1) should state that the data fiduciary would allow for self-verification of the child's age. Additionally, mechanisms for verifiable parental consent should also follow the purpose limitation and collection limitation principle. Further, the DPDP Bill should ensure that on attaining majority, there is an option provided to the child to opt-out of any data processing consented to by the parent. Thus, the clause significantly misses out on the following key factors:

The Best Interests Principle: Previous iterations of the Bill, explicitly stated that the processing of children's data should be based on the best interests of the child. The UNCRC recognises the best interest principle to be crucial in all actions concerning children. Further, since India has adopted the UN-CRC it is legally bound to adhere to the best interest principle throughout its regulatory framework.[43]

The UK ICO, in its code of practice explains the interaction of the best interest principle with data protection stating that the best interests of child users in all aspects of design of online services, should mean compliance with the "*lawfulness, fairness and transparency*" principle, and proper account of Recital 38 of the GDPR.[44] Therefore, it is important to establish the best interest parameter in the parent legislation that would institute the very legality of data processing of children.

[43] Article 253, Constitution of India, 1950.

[44] Recital (38) Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.

Verifiable parental consent: The DPDP Bill seeks verifiable parental consent for any processing of personal data of children. Since the definition of child under Clause 2(3) sets the age of consent at 18 - this would limit access to all online services for children and teenagers. It is important to balance the right to privacy of children with their right to access online services. In light of our recommendation made for Clause 2(3) under Chapter 2, there should not be a blanket age of consent. For example, the Singapore Personal Data Protection Commission suggests that although the blanket age of consent could be 13 years, the onus should be on the data fiduciary to determine whether a particular service would require specific parental consent or any other appropriate steps to effectuate services based on the consent of the child itself.

The Bill should ensure that laying down mechanisms for verifiable parental consent would be limited to the purpose limitation and data minimisation principle. For example, the UK GDPR Code of Practice lays down various methods of verification - while requiring 'hard identifiers' such as government IDs in only extremely limited circumstances and only for a valid justification based on risk and accessibility assessments.[45]

Child should be allowed to give consent on his own behalf: As opposed to the previous iterations of the Bill,[46] the DPDP Bill does not state that the age of the child will be verified prior to determining parental consent. According to this clause before processing 'any' children's data the data fiduciary should obtain verifiable parental consent in such manner as may be prescribed.

It is important to note that in certain cases it would be valid to proceed with data processing of children through self-verification mechanisms that simply confirm the age of the child. For example, an application providing text-book-like math learning services with no risk of profiling. To enable such practices, the DPDP Bill must allow for an option in the parent act itself where consent of the child would also be a ground for data processing - however make it subject to specified rules.

An additional point to note is, given that the Bill currently requires that processing of personal data is made contingent on parental consent, it is necessary that upon attaining

[45] UK ICO, 'ICO Codes of Practice, Age Appropriate Application' <https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/3-age-appropriate-application/>.

[46] Clause 16 (2) of Personal Data Protection Bill, 2019 stated that "The data fiduciary shall, before processing of any personal data of a child, verify his age and obtain the consent of his parent or guardian, in such manner as may be specified by regulations."

majority children are given the option to withdraw or opt-out from the digital services in question. Children's right to opt-out upon attaining majority has expressly been recognised by the Supreme Court of India in *Puttaswamy I*[47], and given effect to in *Puttaswamy II*.[48]

Allowing exceptions with safeguards: Clause 10(4) of the DPDP Bill should include language mirroring the best interest clause. If certain data fiduciaries are being exempted from these obligations, then such exemption should be based on data processing that would necessarily benefit the child. Thus, the premise for allowing exceptions to this provision should be based on what would benefit the child while ensuring adherence to fair information principles.

Additional obligations of Significant Data Fiduciaries

Clause 11(1): Clause 11(1) states that the central government may notify any data fiduciary or class of data fiduciaries as a 'Significant Data Fiduciary' based on an assessment of relevant factors. The clause lists a few factors such as volume and sensitivity of data, risk of harm to the data principal amongst others and additionally, any other factors that may be considered necessary.

Concerns: There are two primary concerns that may arise from a reading of this provision. First, there is little clarity as to the procedure in which the assessment of these factors will take place and no guiding thresholds or criteria within such factors to ensure objectivity to any determination. Further, the discretion provided to the central government is too wide as it can carry out these assessments as well as establish additional factors.

Additionally, when a data fiduciary is being notified as an SDF, such notification should clearly mention the relevant factors that were taken into consideration prior to such decision.

Recommendations: The previous iterations of the Bill listed additional factors such as turnover of the data fiduciary and the use of new technologies for processing of personal data. We recommend that these factors should be included in the current Bill since it would set a general yet relevant ground for future determination of factors in line with

[47] Puttaswamy I (n 33) para 633.

[48] K.S. Puttaswamy v. Union of India (2019) 1 SCC 1 (hereinafter 'Puttaswamy II'), paras 391.2, 512.2.

developing technologies. There should also be accompanying guidance as to how any of these listed factors would be assessed. For instance, the Bill should also provide adequate clarity on what would primarily entail when determining 'volume and sensitivity of personal data' under Clause 11(1)(a).

Chapter 3: Rights and Duties of Data Principal

Right to erasure

Clause 13: Clause 13 of the DPDP Bill recognises the right of the data principal to seek (i) correction of their data and (ii) erasure of their data once the purpose for which it was collected/processed is met. However, as opposed to the previous iterations of this Bill, it bases the invocation of the right to erasure on the condition that it can only be sought if the personal data in question is not needed for any other legal purpose.

Concerns: The provision is vague in terms of stating that the right to correction and erasure would be implemented based on applicable laws and subsequent rules. Further, unlike the previous iterations of the Bill the scope of the right to seek discontinuation of processing of personal data has been eliminated. For data principals to exercise true autonomy over their personal data the scope of this right should be expanded.

Recommendations: This provision should include safeguards to guard against the risk of over removal of personal data. Clause 20 of the 2019 Bill included a proviso stating that any order for the discontinuation of disclosure/processing of personal data should be balanced with the freedom of speech and expression, and the right to information. We recommend that the Bill include such safeguards. In addition, an independent authority should be empowered to evaluate right to erasure requests on a case by case basis.

Further, Clause 13(2)(d) lays down a condition for exercising the right to erasure stating that the right can be invoked unless data is required for legal purposes. We recommend that the accessibility of the right to erasure should not be restricted in this way.

Missing Rights

1] Right to data portability: Data portability helps give individuals back control over their personal data. It is premised on informational self-determination and autonomy which are the guiding factors of a data protection framework in the interest of data principals. Data portability allows individuals to move their data across different service providers which can help reduce the costs associated with switching between providers. Data fiduciaries should not be exempted from data portability requirements based on any technical infeasibility. In consonance with our recommendations to the White Paper Of The Committee Of Experts On A Data Protection Framework For India, it would allow

users to switch to services with more privacy friendly policies.[49] This would contribute to the start-up ecosystem that is on the rise in India and prove beneficial in presenting a level playing field for new entrants. Thus, it would promote innovation and competition in the market. Further, in line with the JPC recommendation the application of this right should not be limited to data processed by automated means.

2] The right to object to processing for the purpose of direct marketing

We have suggested the inclusion of this right in our comments to the previous iterations of the Bill.[50] Since the DPDP Bill allows for processing of data based on 'deemed consent', it should also have safeguards in place for such processing. This should be in addition to exercising this right by withdrawal from consensual processing of personal data. If a data principal is only post facto aware of their data being used for purposes they had not consented to, they should be given the right to opt-out of such processing.[51]

Duties of the data principal

Clause 16: Clause 16 suggests that Data Principals must ensure that they are in compliance with all laws in the country prior to invoking any of the rights mentioned under the framework.

Concerns: The imposition of duties, along with penalties under Schedule 1 - would put data principals at a disadvantage and be a clear disincentive for them to invoke their rights.

Recommendations: We recommend the deletion of Clause 16. The dearth of digital literacy in India already creates an imbalance in the way the digital ecosystem is accessed and how the rights under a data protection framework are understood and invoked. Placing duties on data principals will further exacerbate this gap. This clause places the onus on data principals under Clause 16(2) and 16(3) to ensure that the information provided by them is not false or leads to impersonation. In the Indian digital ecosystem, where data principals accessing services would not be aware of methods to ensure that they are submitting the right information - there could be a genuine mistake in providing

[49] Centre for Communication Governance (n 14).

[50] 'Comments on the Data Protection Bill, 2019' (n 24).

[51] Graham Greenleaf (n 38); Centre for Communication Governance (n 14).

the right information to the data fiduciary. Thus, placing such a burden through duties and imposing penalties in case of non-compliance would prove detrimental to their very access to redressal under this framework.

The Srikrishna Committee Report states that the goal of the State with regard to a data protection law is to put in place a framework which protects citizens from harms arising out of information sharing.[52] Further, in order to effectuate rights arising out of such a framework it is important to ensure that access to redressal mechanisms is smooth and inclusive. Including mandatory compliance with such duties hinders this process and goes against the nature of a data protection framework. For a framework that focuses on individual's right to privacy and enabling necessary lawful processing of data - imposing such duties clubbed with penalties would be overstepping the role of a data protection framework. Thus, we recommend that the entire provision on the duties of the data principle should be withdrawn.

[52] Committee of Experts under the Chairmanship of Justice B.N. (n 35).

Chapter 4: Special Provisions

Transfer of personal data outside India

Clause 17: Clause 17 states that the central government may after an assessment of factors considered 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.

Concerns: The 2019 Bill included conditions that guided the selection of countries by the central government, albeit for the transfer of sensitive personal data only. However, Clause 17 does not include any such considerations when determining such countries. Clause 17 also provides the central government with power to whitelist countries in accordance with "*terms and conditions as may be specified*". However, it does not provide clarity as to how the assessment of adequacy for whitelisting will be carried out.

Recommendations: It is necessary to include a broad framework for assessment of adequacy within the text of the law. Therefore, it may be useful for Clause 17 to include factors such as "*adequate level of protection, alignment with applicable laws and international agreements, effectiveness of the enforcement by authorities with appropriate jurisdiction*" as was laid down in the 2018 Bill. Further, we reiterate our comments to the White Paper Of The Committee Of Experts On A Data Protection Framework For India in which we suggested that reliance could be placed on adequacy assessments by other regulators and international data protection authorities, whose standards are considered sufficiently rigorous.[53] This will promote sound decision making by the central government and guard against arbitrariness.

Exemptions

Clause 18(1)(a) and (b): Clause 18(1) (a) and (b) relate to entities processing data to enforce legal claims, or courts, tribunals and other bodies performing judicial and quasi-judicial functions. The clause exempts these entities from certain provisions such as obligations of data fiduciaries (except complying with safety measures), rights and duties of data principles, and cross border data transfers.

[53] Centre for Communication Governance (n 14).

Concerns: These exemptions are too wide and can apply to any situation in which a legal right or claim is being enforced. In particular, quasi-judicial functions should not be given a blanket exempt.

Recommendations: In order to ensure that the purposes of the clauses are fulfilled in a manner that balances the right to privacy with these essential state functions it may be necessary for appropriate rules to be framed to govern the processing of data in these circumstances. But the rules should specify that in certain cases the right to privacy should nonetheless prevail. For instance, rules contained in the Juvenile Justice (Care and Protection of Children) Act, 2015, or rules against publication of the names of survivors of sexual assault should continue to prevail.

It may be beneficial to apply separate standards to parties directly involved in judicial proceedings, and others such as witnesses. In the case of criminal proceedings, we recommend that different standards may be necessary while dealing with personal data of the accused and victims, particularly in cases of sexual violence.

Clause 18(2): Clause 18(2) states that the central government, through notification, may exempt the provisions of this Act to *any instrumentality* of the State for three purposes, (i) in the interests of sovereignty and integrity of India, security of the State, friendly relations with foreign States, (ii) to maintain public order or (iii) to prevent incitement to any cognizable offence relating to any of these.

Concerns: Clause 18(2) lacks safeguards unlike the corresponding provisions in the 2019 Bill and the 2018 Bill. While even the provisions in the previous Bills were insufficient, they still included a layer of safeguards prior to providing exemptions. There is also little clarity in the Bill as to how "*instrumentalities of the State*" must be interpreted. Further, the purposes listed in Clause 18(2) may be interpreted to be wide enough to potentially justify a plethora of State action.

Consequently, this removes the application of any data protection obligations on the State. This significantly impacts the right to privacy. Further, there is no clear rationale behind an exemption from data security measures, compared to Clause 18(1) which maintains this requirement.

Recommendations: We recommend that the tests of legality, necessity, and proportionality laid down by the Court in *Puttaswamy I* and *Puttaswamy II* be introduced into the language of the Bill and guide the exemptions under this chapter, to

ensure protection of the right to privacy. The Bill would benefit from including safeguards to Clause 18(2) that constitutionally satisfy the requirements laid down by the Court, in order to adequately protect the right to privacy.

Decline in Safeguards: We begin our submissions for Clause 18(2) by highlighting that the current version of the Bill offers the widest exemption to the State for the various listed purposes, compared to earlier versions of the Bill. The 2019 Bill required that as long as it was considered *"necessary and expedient"* to fulfil the purposes in the clause, the exemptions were permitted. Further, any additional procedural safeguards such as requiring reasons for such exemptions were to be provided in writing. This is not to say that the conditions within the 2019 Bill provided sufficient safeguards, however, it still did require adherence to some conditions prior to providing exemptions. As mentioned above, there is no such procedure or safeguard in the provisions of the DPDP Bill. Comparatively, the 2018 Bill had stronger conditions by requiring that the exemptions would be permitted only if it were *"authorised by a law made by Parliament, in accordance with the procedure established by such law, and necessary and proportionate."* However, even the 2018 Bill exempted the State from a significant portion of the Bill and needed better safeguards.

Safeguards are a constitutional necessity: Fundamental rights including the right to privacy are not absolute in nature. However, courts have established that certain safeguards need to be adhered to when limiting the right to privacy. Unfortunately, Clause 18 lacks these safeguards. We draw from our comments on previous Bills to highlight the importance of relevant safeguards to protect the right to privacy.[54]

The Supreme Court's judgement on the right to privacy, in *Puttaswamy I*,[55] locates the right to privacy in Article 21, as well as across all the fundamental rights under Part III of the Indian Constitution. The Court provided some guidance by identifying the tests of lawfulness, legitimate state aim, and proportionality to be met in order for any violation of privacy to be permissible.

Further, when read in conjunction with *Puttaswamy II*,[56] the Court further expanded this test. The Court noted that the proportionality test itself consists of four parts:

[54] 'Comments on the Data Protection Bill, 2019' (n 24); Centre for Communication Governance (n 14).

[55] Puttaswamy I (n 33).

[56] Puttaswamy II (n 48).

i. "*A measure restricting a right must have a legitimate goal (legitimate goal stage).*

ii. It must be a suitable means of furthering this goal (suitability or rationale connection stage).

iii. There must not be any less restrictive but equally effective alternative (necessity stage).

iv. The measure must not have a disproportionate impact on the right holder (balancing stage)."[57]

These tests may also be considered when looking at Clause 18(4). Clause 18(4) exempts any State authority from deletion of data after use, indicating that the personal data may be stored for an indefinite period. Such an exemption has not previously featured in any of the earlier versions of the Bills. This is in clear contravention with the principles of data minimisation and purpose limitation, as there is no purpose or objective provided within the clause to justify such an extended period of retention. Clause 18(4) may further allow for such data to be used for numerous purposes beyond which was given during collection of data and may contribute to function creep. Therefore, any potential violation of privacy will need to meet the tests laid down in *Puttaswamy I* and *II*. Finally, it is important to note that the use of the term 'instrumentality' of the State is vague and should be defined to provide clarity to the application of Clause 18(2).

Clause 18(2)(b): Clause 18(2)(b) exempts the application of the Bill for research, archiving or statistical purposes, if the personal data is not to be used to take any decision specific to a data principal and such processing is carried on in accordance with standards specified by the Board.

Concerns: We recognise that these purposes are necessary to further ease of access to data for public benefits and as a result warrants some exemptions from data protection compliances. However, completely exempting the application of the Bill may allow for entities to justify the use of personal data without safeguards, as long as it can be associated with the purposes under the clause.

Recommendations: It may be beneficial for Clause 18(2)(b) to incorporate certain conditions to be fulfilled prior to permitting such an exemption. But the Central Government should not be empowered to exempt the application of the entire Bill.

[57] Ibid para 148.

A crucial departure from the 2019 Bill is that the DPDP Bill removes all preconditions that were necessary to claim exemptions under this provision. For instance, it permitted exceptions if compliance with the provisions hindered resources or decisions made on personal data used would not impact a data principal. The purposes under the clause may not have a justifiable objective in excluding certain provisions of the Bill. For example, there are no clear reasons to exempt provisions that aim to protect children's personal data, to prevent data principals from the knowledge that their personal data is being utilised for public benefits or allowing them to enforce their rights against risks of misuse. Similarly, the exemption from requiring that such use of personal data without adequate data security may pose data and storage security risks to the individual and potentially jeopardise the sanctity of the very data being used for the purposes listed in the clause.

To protect against unnecessary exemptions and misuse of personal data, there must be qualifiers within the provision to prevent harm. Additionally, the application of certain provisions of the Bill such as data retention requirements and children's data protection should be retained. These additional safeguards would limit the misuse of this provision for purely profit making undertakings, and ensure that the interests of individual data principals and the public benefit are balanced.

Clause 18(3): Clause 18(3) permits the central government to issue a notification that would exempt data fiduciaries who process personal data of a certain volume and nature from providing notice, ensuring accuracy, meeting data retention requirements, specific children's data protections, obligations of SDFs and even the data principal's right to access information about themselves.

Concerns: Similar to Clause 18(2)(b), this clause does not justify the exemption from some of these data protection obligations that would otherwise be crucial for a data principal's personal data protection. There is also no clear criteria based on which these data fiduciaries would be exempted from these clauses.

Recommendations: It is important for Clause 18(3) to list intelligible criteria to exempt data fiduciaries. Also it is important to retain the application of certain necessary provisions of the Bill. Further, reasons for why these data fiduciaries are exempted should be provided within the notification issued by the central government. Finally, clause 18(3) should incorporate the safeguards of necessity and proportionality contained in Puttaswamy I and II.

The clause is vague about how the characteristics of volume and nature will be interpreted for such exemption and may be based on subjective criteria set out by the central government. Any conditions that will be considered for such determination should be included within the text of the law to ensure clear legislative intent to guide the application of such provisions and prevent arbitrariness in the selection of fiduciaries. Further, much like Clause 18(2)(b), irrespective of the kind of data fiduciaries that the clause will be applied to, there are no clear reasons to exempt provisions that focus on children's personal data - specifically to protect children from harm, ensuring accuracy or even data retention requirements. Therefore, we reiterate that there must be qualifiers within the provision to protect against unjustifiable exemptions and that reasons for granting exemptions must be provided. Further, it may be necessary to reconsider the extent of provisions that the clause exempts.

General comments

Missing provisions

Journalistic, Artistic and Literary Purpose:

The DPDP Bill does not contain a provision that provides journalistic purposes with an exemption from certain compliance obligations within the Bill. This provision in the 2019 Bill was included in section 36(e). It allowed for exemptions from requiring consent, children's data protections, rights of a data principal, transparency and accountability measures except data security measures and cross border data transfers, on the condition that data for journalistic uses was processed with a lawful purpose. The Bill also lacks an exemption for artistic and literary purposes. Clause 18 should thus contain an exemption for journalistic, artistic and literary purposes.

Chapter 5: Compliance Framework

Data Protection Board of India

Clause 19: Clause 19 provides for the establishment of the Data Protection Board of India ('DPBI'). The strength, composition, process of selection, terms and conditions of appointment and service, removal of members of the DPBI will now be entirely determined by the central government. The DPBI is now envisaged to be digital by design, whereby most functions will be carried out digitally. The Chief Executive will manage the affairs of the Board whose appointment and terms and conditions of service will be determined by the central government.

Concerns: The independence of the DPBI has been considerably weakened in the DPDP Bill. Now the Executive will solely determine the composition of the board, the process of selection of board members and other matters via its rule-making power. The 'Chief Executive' provision may also facilitate Executive influence. Finally, the 'digital by design' framework may need to be amended to account for the lack of digital literacy and accessibility.

Recommendations: Hence, it is recommended that the provisions relating to the composition, tenure, and eligibility of members of the DPBI should not be left to executive rule-making. They should be codified in the DPDP Bill itself. Additionally, the appointment of the members of the DPBI should be made by a Selection Committee, the composition of which should be balanced with representation from the Executive, Judiciary, and technical experts. To ensure further clarity regarding the role and powers of the Chief Executive, we recommend that the role of the Chief Executive is codified in the DPDP Bill. We also recommend transitioning to a digital DPBI gradually or providing the option to file complaints physically. Our recommendations on Clause 19 are set out in greater detail below.

1] Make the DPBI independent

The effectiveness of a data protection regime is contingent not only upon the existence of a legal framework that safeguards privacy and liberty but also upon the establishment of an independent adjudicatory body. In *Union of India v. R. Gandhi*[58], the Supreme Court

[58] Union of India v. R. Gandhi 25 (2010) 11 SCC 1.

stated that tribunals must be constituted in a manner that inspires the confidence of the public in their ability and independence.[59]

Independence of an adjudicatory body from the Executive in particular is key, for several reasons. It is tasked with supervision of both private and public data fiduciaries. Furthermore, the Executive and its instrumentalities may commonly be opposite parties in proceedings before the DPBI. Clause 21(1) of the DPDP Bill provides that the DPBI shall function as an independent body. However, achieving independence may be challenging given that the central government has significant influence over the institutional and functional design of the DPBI, with no judicial oversight.

The organisational structure of a regulator impacts the extent of such independence from the Executive.[60] In this vein, the composition of the DPBI and the Selection Committee of the DPBI are of critical importance.

A] Composition of the DPBI:

Previous iterations of the Bill have clearly laid down the strength, composition of the DPBI, and the Selection Committee tasked with selecting members for the DPBI (previously Data Protection Authority ('DPA')). With a total strength of six whole-time members and the Chairperson, the qualifications of the DPA were also provided under the 2019 Bill. The 2021 Bill also proceeded to clarify that one out of the six members would be an expert in law; further, it stated that qualifications for members would be prescribed.

We would like to reiterate our comments to the 2019 Bill wherein we had recommended that the Chairperson should be a former judge of the Supreme Court, at least two members should be from legal background, at least one member should be a former secretary or additional secretary of the MeitY. We also recommend a minimum age (35 years) and experience requirement (10 years) in data protection, information technology, data management, data science, data security, cyber and internet laws, public administration, national security or related subjects. The DPDP Bill should be amended to include these details in the parent legislation, rather than leaving them to be prescribed through delegated legislation.

[59] Ibid.

[60] Christopher Carrigan and Lindsey Poole, 'Structuring Regulators: The Effects of Organizational Design on Regulatory Behavior and Performance' 41.

B] Composition of the Selection Committee:

Under the 2018 Bill, the Selection Committee comprised the Chief Justice of India (CJI) or another Judge of the Supreme Court, the Cabinet Secretary and a subject-matter expert appointed by the CJI and the Cabinet Secretary. This composition reflected the well-balanced amalgamation of the Judiciary, Executive and an independent technical expert, as proposed by the Srikrishna Committee Report.[61] Marking a departure from the 2018 Bill, subsequent Bills have witnessed the inclusion of more Executive influence and representation in the Selection Committee. Under the 2019 Bill, the Selection Committee consisted of the Cabinet Secretary and the Secretaries of the Ministry of Law & Justice (Legal Affairs) and MeitY. The 2021 Bill included the Attorney General, an independent expert and directors of an IIT and IIM to be nominated by the central government.

The DPDP Bill does not provide for the formation of a Selection Committee. Members will now be selected by the Executive through delegated legislation. This contradicts established judicial precedent, according to which the DPBI is a quasi-judicial body[62] whose members must be appointed independently.[63] Consequently, we strongly recommend that appointments to the DPBI be made through a well-balanced Selection Committee. The Selection Committee should include the following members: (a) the CJI or a judge nominated by the CJI, (b) the Minister of Electronics and Information Technology, (c) the leader of opposition in Lok Sabha, and (d) two independent experts nominated by the CJI.

Moreover, the Supreme Court has clarified, in the following cases, the indispensability of the presence of a judicial member in Selection Committees to tribunals or administrative bodies that perform quasi-judicial functions.

---

[61] Committee of Experts under the Chairmanship of Justice B.N. (n 35).

[62] The Supreme Court has held in the case of *National Securities Depository Limited v. Securities and Exchange Board of India* [(2017) 5 SCC 517] that the three requisites necessary to characterise the act of an administrative body as quasi-judicial are: (i) There must be legal authority; (ii) This authority must be to determine questions affecting the rights of subjects; and (iii) There must be a duty to act judicially. As per the provisions of Chapter 5 of the DPDP Bill and the aforementioned test, the powers vested in the DPBI are quasi-judicial.

[63] The Constitution Bench in Supreme Court *Advocates-on-Record Assn. v. Union of India* [(2015) AIR 2015 SC 5457] held that there is a compulsory need for the exclusion of the Executive over quasi-judicial bodies discharging responsibilities akin to Courts. The absence of a procedure for the appointment of members of the DPBI and the exclusive power of the Executive to make appointments to the DPBI would be against the constitutional scheme inasmuch as they could be considered an encroachment by the executive over such quasi-judicial bodies. This would also violate the principles of separation of powers and independence of the judiciary.

The Supreme Court in the recent case of *Rojer Mathew v. South Bank India Ltd. & Ors,*[64] held that there is a "*compulsory need for exclusion of control of the Executive over quasi-judicial bodies of Tribunals discharging responsibilities akin to Courts*." In this case, the court held that the search-cum-Selection Committee (as envisaged under the rules to the Finance Act 2017) which made appointments of member, vice president and president was predominantly made by the nominees of the central government and there was only token representation of the Chief Justice or his nominees in the Committee, which impinged on the independence of the Judiciary. The court held that the search-cum-Selection Committee as envisaged in the Rules was against the constitutional scheme inasmuch as it diluted the involvement of Judiciary in the process of appointment of members of tribunals which is in effect an encroachment by the Executive on the Judiciary. This was considered to be excessive interference by the Executive on the appointment of members and presiding officers of the statutory Tribunal. Such influence or control on judicial appointments was held to be detrimental to the independence of the Judiciary.

In the case of *S.P. Sampath Kumar v. Union of India,*[65] the Supreme Court held that the composition of the Selection Committee to appoint the members of the tribunal under the Administrative Tribunals Act, 1985 should compulsorily have a judicial member to save the provision from being held invalid. The court held that the appointment of members to the tribunal should be made by the Executive only after consultation with the CJI of India. Alternatively, the court also held that a High-Powered Selection Committee headed by the CJI of India or a sitting Judge of the Supreme Court or High Court nominated by the CJI of India, may be constituted to make such appointments. This was held as necessary to ensure independence and impartiality of the tribunal as in many cases the litigant would be the government and any bias in the adjudication process would render the tribunal ineffective. Clause 19 makes appointment of the members of the DPBI the sole prerogative of the government and would go against the ruling of the court. In light of the abovementioned catena of cases the absence of a judicial member in the selection process for the Board will render the DPDP Bill open to constitutional challenge.

To emphasise the need to have judicial representation in the selection process for such bodies, we have included a brief comparison of the composition of other Selection Committees to regulatory bodies.

[64] *Rojer Mathew v. South Bank India Ltd. & Ors.* 2019 (15) SCALE 615.

[65] *S.P. Sampath Kumar v. Union of India* 1987 (1) SCC 124.

The Competition Act

Section 9 - Selection Committee for Chairperson and Members of Commission

(1) The Chairperson and other Members of the Commission shall be appointed by the Central Government from a panel of names recommended by a Selection Committee consisting of:

(a) the Chief Justice of India or his nominee (Chairperson)
(b) the Secretary in the Ministry of Corporate Affairs
(c) the Secretary in the Ministry of Law and Justice
(d) two experts of repute who have special knowledge of, and professional experience in international trade, economics, business, commerce, law, finance, accountancy, management, industry, public affairs or competition matters including competition law and policy.

The Lokpal and Lokayuktas Act

Section 4 - Appointment of Chairperson and Members on recommendations of Selection Committee

(1) The Chairperson and Members shall be appointed by the President after obtaining the recommendations of a Selection Committee consisting of:

(a) the Prime Minister (Chairperson);
(b) the Speaker of the House of the People;
(c) the Leader of Opposition in the House of the People;
(d) the Chief Justice of India or a Judge of the Supreme Court nominated by him;
(e) one eminent jurist, as recommended by the Chairperson and Members referred to in clauses (a) to (d) above, to be nominated by the President.

Securities and Exchange Board of India Act

Section 15M: Qualification for appointment as Presiding Officer or Member of Securities Appellate Tribunal

(1A) The Presiding Officer of the Securities Appellate Tribunal shall be appointed by the Central Government in consultation with the Chief Justice of India or his nominee.

Telecom Regulatory Authority of India Act, 1997

Section 14B. Composition of Appellate Tribunal

(2) The selection of Chairperson and Members of the Appellate Tribunal shall be made by the Central Government in consultation with the Chief Justice of India.

Finally, international standards are increasingly emphasising the importance of independent data protection authorities. Under the GDPR, Article 52 creates a special provision to ensure the independence of the members of the supervisory authorities. It requires all DPAs in the EU to act with 'complete independence' when carrying out their duties. Similarly, the Paris Principles require appointees to human rights bodies to be qualified, pluralistic and outside the government in addition to having financial independence for its funding from the government.[66] Data privacy being a critical human rights concern makes the Paris Principles relevant to the functioning of national data protection authorities. Furthermore, the OECD Privacy Guidelines highlight the necessity of the authority to function in a manner devoid of influence which may sway the objectivity, integrity and professional judgement of their decisions.[67]

The requirement of establishing an independent DPBI is also crucial in order to fulfil the GDPR's 'adequacy' requirement for India to be qualified to receive and process personal data from the EU.[68] This will be determined through a finding by the European Commission that a third country or an international organisation has adequate safeguards and mechanisms to ensure that the data protection regime is equivalent to that within the EU. Given the concerns of the DPDP Bill in its current form, it could hamper India's chance of meeting the adequacy requirements under the GDPR and could suffocate the ability of Indian industries to extend services to the European markets.[69]

2] Provide clarity about the role of the Chief Executive

[66] A/RES/48/134. National institutions for the promotion and protection of human rights, General Assembly (20 December 1993).

[67] OECD, Supplementary explanatory memorandum to the revised recommendation of the council concerning guidelines governing the protection of privacy and transborder flows of personal data (2013) . In OECD, The OECD Privacy Framework (pp. 19 - 38). Paris: OECD.

[68] Article 45, GDPR (n 2).

[69] Dvara Research (n 9) 11.

A new addition to the 2022 Bill is the appointment of a 'Chief Executive' by the central government, to manage the affairs of the Board. The terms and conditions of service of the Chief Executive will be determined by the central government. With no clarity on the role of the Chief Executive within the DPBI, the independence of the board stands to be further diluted.

It is recommended that the managerial powers of this rank should be clarified so as to ascertain the scope of powers vested in the individual. This will also help in understanding the extent of control the Executive may exercise over the operational and functional workings of the DPBI, vicariously through the Chief Executive.

3] Modify the adoption of the Digital by Design framework

We welcome the push to create a digital by design DPBI. However, such a design raises certain concerns. Accessibility to the internet and digital literacy is not widespread in India. Also, no adjudicatory body has yet been completely digital in design and functioning. For these reasons, the government's ambitious attempt should perhaps be revised to include a delayed hybrid model that initially focuses on setting up the physical presence of the DPBI and then builds its digital presence. In the alternative, the Bill should clarify that complainants will always have an option to file complaints with the DPBI physically if they wish to do so.

We recommend that the DPBI establish a physical presence in the country first and then gradually transition into going digital. Or in the alternative, provide both methods of filing complaints simultaneously, digital and physical. We also recommend that the DPBI have a timeline for prioritising administrative and adjudicatory functions in its first few years of operation.[70] During this time, it can also focus on adopting practices which will help it to gradually transition into a fully digital body. As the DPBI is anticipated to handle a large volume of complaints, building internal capacity will be crucial before adopting a final design with no precedent.

Functions of the Board

Clause 20: Clause 20 provides for the adjudicatory functions of the Board, chiefly consisting of determining non-compliance, imposing penalties, issuing directions, and directing data fiduciaries to adopt urgent measures to remedy personal data breaches.

[70] Srikara Prasad and others, 'Implementing the Personal Data Protection Bill': 12.

Concerns: Previous iterations of the Bill provided the DPBI clearly demarcated functions with the focus also on protecting the interests of data principals, preventing misuse of personal data in addition to ensuring compliance with the provisions of the Bill. Furthermore, other functions of the DPBI which the central government could previously prescribe through subsequent Rules, have been modified to now empower the central government to assign the DPBI any other functions by an "*order published in the Official Gazette*" and not through Rules. The central government is empowered to also assign the DPBI any other functions not just under the provisions of the Bill, but also under any other law. Without a clear mandate of protecting the interests of data principals, the extent of Executive control over the DPBI without judicial oversight, may work in detriment to having a board that is independent in its functioning.

Process to be followed by the Board to ensure compliance with the provisions of the Act

Clause 21: Clause 21 provides the grievance redressal mechanism which shall be followed by the DPBI to ensure compliance with the provisions of the Bill.

Concerns: In previous iterations of the Bill, the grievance redressal process consisted of the DPA, Adjudicatory Officer, Inquiry Officer and an Appellate Tribunal. Under the 2022 Bill, the DPBI absorbs all the powers without any clear demarcation in roles between the different parties (as they were in the previous versions of the Bill) involved in adjudication and investigation. Appeals against the order of the DPBI now lie to an appropriate High Court.

Clause 21(2) provides that the DPBI may take action against a complaint that is brought before it by an affected person, or on a reference made to it by the Central or a State Government, or in compliance with the directions of any court or in case the data principal is in non-compliance with their duties under the Bill. What is unique about this clause is that the DPBI has been empowered to now take suo-moto cognizance of a case of non-compliance against the data principal (for not adhering to duties), however, this power has not been extended to the DPBI taking suo-moto cognizance of cases against a data fiduciary.

Under Clause 21(3), the Board is now authorised to conduct proceedings relating to complaints by individual members or groups of members. There is no legislative clarity

on the standards that will be employed to determine which matters will be handled by individual members and which by groups of members.

Constituting an added layer of scrutiny of the complaint before it proceeds for inquiry, Clause 21(4) now empowers the DPBI to make a determination as to the merits of a complaint before the process of inquiry commences. At this stage, the DPBI determines whether there are sufficient grounds for proceeding with inquiry. In the event the Board determines that there are insufficient grounds, it may close such proceedings.

With individual members also being authorised to conduct proceedings, the prospect of an individual member dismissing a complaint after ascertaining its merits is concerning. At this juncture, the qualification and expertise of a single board member to make such a determination is critical. With no requirement for deliberation with other members of the board or an advisory committee, the provision fails to provide any safeguards against the abuse of discretion by a single member.

Clause 21(5) provides that the DPBI can inquire into the "*affairs of any person*" to ascertain compliance with the provisions of the Bill. While the Bill mentions that the DPBI shall carry out these functions following the rules of natural justice, it is unclear as to how it will carry out an investigation into determining the legitimacy of the "*affairs of any person*" making the complaint. Similarly, this clause does not provide clarity as to who will be the subject of such investigation, given 'person' includes a wide variety of legal entities including an individual.[71] This provision should clarify that such an investigation shall be initiated against a data fiduciary.

Clause 21(11) provides that at the conclusion of the inquiry if the Board determines that non-compliance by a person is not significant, it may close such inquiry. If the Board determines that the non-compliance by the person is significant, it shall proceed in accordance with Section 25 of the Bill. The Bill does not lay down how the DPBI will make the determination of how significant the non-compliance is, given that the term significant has not been defined under the Bill. This also implies that there is no penalty for non-significant non-compliance under the DPDP Bill.

Constituting another hurdle for a complaint to be addressed by the DPBI, under Clause 21(12) if at any stage after receipt of a complaint, the Board determines that the complaint is devoid of merit, it may issue a warning or impose costs on the complainant. The

[71] Clause 2(12), DPDP Bill 2022.

provision of imposing costs in addition to the possibility of imposing a penalty for making a frivolous complaint could significantly disincentive complainants from pursuing a grievance given the prospect of stiff financial penalties. Especially when the Bill does not provide the DPBI with powers to award compensation to data principals.

Recommendations: Clause 16 provides that individuals must ensure that they are in compliance with all laws in the country.. We have strongly recommended that Clause 16 be withdrawn from the DPDP Bill as it would constitute a clear disincentive for the data principals to invoke their rights. Building on this recommendation, we also suggest that under Clause 21(2) the DPBI should not be empowered to determine non-compliance with duties under Clause 16. This would once again act as a deterrent for data principals to invoke their rights under the Bill and seek redressal of their grievances from the DPBI.

While the DPBI has been empowered to initiate proceedings against a data principal for non-compliance, there is no scope for the DPBI to take suo-moto action against non-compliance by data fiduciaries. It is important that under Clause 21(2) the DPBI should be empowered to take suo-moto action against a data fiduciary for non-compliance.

To ensure legislative clarity Clause 21(3) should lay down the standards for determining which matters will be handled by individual members and which by groups of members. Factors such as extent of harm caused, including the number of data principals affected, and number of instances of non-compliance by data fiduciaries should be taken into account when making such determinations. This would provide scope for more extensive deliberations being made. Similarly, the concern highlighted under Clause 21(4) can be addressed by ensuring that clear safeguards are provided to ensure complaints being scrutinised by individual members have some level of oversight and accountability.

In its current form Clause 21(5) is vague. It is crucial that the provision specifies that it only applies to data fiduciaries.

Under Clause 21(11) 'significance' should not be a factor for determining penalties. Therefore, it is recommended that upon the conclusion of the inquiry, the DPBI should have the powers to impose penalties in any complaint purely based on the merits of the case.

Voluntary Undertaking

Clause 24: Clause 24 provides for the power of the Board to accept voluntary undertakings related to any compliance matter under the Act from any person at any stage.

Concerns: This provision may allow companies to circumvent formal proceedings and qualifies as another provision which could potentially hamper the prospect of data principals and their rights being protected under the DPDP Bill.

Recommendations: We recommend that Clause 23 should be removed as it may help data fiduciaries circumvent formal proceedings before the DPBI.

Financial Penalty

Clause 25: Clause 25 provides that the DPBI may impose a financial penalty on the data fiduciaries on the conclusion of the inquiry. The DPBI may do so if it is of the opinion that non-compliance is 'significant'.

Concerns: Once again, the term 'significant' has not been defined which gives the DPBI wide discretion to interpret it." It is also concerning that the DPBI may choose not to levy any penalty on data fiduciaries if their non-compliance is not significant.

Recommendations: To emphasise our recommendation for Clause 21(11), the 'significance' or 'non-significance' of non-compliance should not be a qualifier to determine penalties. Rather, the DPBI should be empowered to ascertain the merits of each case before them and accordingly impose penalties following such deliberations.

Chapter 6: Miscellaneous

Power to make Rules

Clause 26: Clause 26 relates to the powers of the central government to make Rules to carry out the provisions of the Act.

Concerns: While consistent with the 2019 Bill, the DPDP Bill does not provide a detailed list of all the rule-making powers of the central government. Similarly, the DPDP Bill does not contain the precondition for previous publication of the Rules before the notification of the Rules by the central government, which was included under the 2021 Bill. The lack of specificity in the clause could result in vast regulatory power being vested in the central government.

Recommendations: It is recommended that the clause should list out the core areas on which the central government can make Rules, with the precondition that prior publication of the Rules shall be made before the notification of the Rules.

Amendments

Clause 30: Clause 30 seeks to amend the IT Act, 2000 and the RTI Act, 2005. Clause 30(2) proposes a new amendment to Section 8(1)(j) of the RTI Act.

Section 8(1) of the RTI Act provides for exemptions from disclosure of information by the government. Section 8(1)(j) of the RTI Act allows for the information commissioner to determine if personal information about administration officials can be released in the greater public interest. However, the proposed amendment through Clause 30(2) now provides that there shall be no obligation on the public information officer to give any citizen information which is related to personal information. Similarly, the proviso to Section 8(1)(j) has also been omitted therefore further diluting the RTI Act. This proviso created an exception that prevented public information officers from denying information to any person, which could not be denied to the Parliament or a State Legislature.

Concerns: Clause 30(2) will have a deleterious impact on the right of the public to know and access information about public officials. Since 'personal information' is not defined in the Right to Information Act, it can be expansively interpreted by information officers to deny requests for information even in situations where there might be a public interest component.

Recommendations: Allow data principals to seek compensation. To this end, reinstate the compensation provision contained in the 2019 Bill. Also, Clause 30(2) should be deleted.

General Comments

Missing Provisions

Rule-making powers: Marking a departure from the 2019 Bill, the 2022 Bill has no provision which empowers the DPBI to make regulations under the Act. Under Clause 94 of the 2019 Bill, the DPA was empowered to make regulations consistent with the provisions of the Act and Rules made thereunder, with the previous approval of the central government. The matters in respect of which the regulations were to be made were of administrative and procedural nature. While the 2019 Bill through its Memorandum on Delegated Legislation notes that it is not practicable to list out all possible powers in the proposed Bill itself, not providing any scope for the DPBI to make regulations is concerning. The current institutional and functional design of the DPBI envisions the body as an adjudicatory body and not a regulator. It is crucial for the DPBI to be given regulatory powers to make regulations, given it will have the technical expertise and be better positioned to exercise this function instead of the central government. This is particularly necessary because data protection is a technical subject and requires an expert regulator to be equipped to deal with necessary complexities.