aapti institute

To:

The Ministry of Electronics and Information Technology, (Government of India)

Electronics Niketan, 6, CGO Complex,

Lodhi Road, New Delhi - 110003

15 December 2022

We thank the Ministry of Electronics and Information Technology for the opportunity to provide feedback on the Digital Personal Data Protection Bill 2022. The process of consultation is a necessary and welcome one. We hope that this spirit of transparency and due process is continued in the framing of future legislations by the Ministry.

The growth in digitalization in the country has transformed dynamics around collection and use of personal data for products and service delivery, urgently raising the need for a robust data protection legislation that secures individual privacy and frames digital rights, while promoting the broader value of data. However, we believe that the 2022 Bill falls short on providing certainty through its framework, encoding strong data protection principles in the law, establishing reliable checks and balances, and complying with the Puttaswamy judgement towards securing the right to privacy.

At Aapti Institute, we believe in the potential of technology and responsible use of data for deriving immense societal value. Our research is thus rooted in equity, empowerment, and security and agency of individuals as they negotiate with technology. Our detailed submission below builds off our philosophy on balancing the use of data in favor of society with individual rights. We hope that this bill will go through transparent iterations - to realize an ecosystem that supports the data economy and firmly protects the right to privacy.

Our high level comments can be summarized in the following five points:

1. As the country's primary data protection legislation being released after the Puttaswamy judgement of 2017, the Bill falls short on incorporating the framework on the right to privacy in its preamble and provisions.
2. The simplified approach to the language of the Bill retains ambiguity in drafting on various provisions and operates on a limited data taxonomy that shall raise complications in implementation.

3. Vague wording in granting wide exemptions to the government has resulted in dilution of individual rights and the data protection principles acknowledged in the explanatory note accompanying the Bill.
4. There is a need for establishing greater checks and balances in the framework proposed by the bill to secure independence within regulatory and adjudicatory processes.

Drawing from this, the attached table presents an in-depth, section wise analysis of the Digital Personal Data Protection Bill 2022.

For any further questions, please contact us at astha@aapti.in or avani@aapti.in.

We look forward to engaging further on this issue,

Astha Kapoor

Co-founder, Aapti Institute

<note to reader: This cover letter was not submitted, owing to the format of the feedback portal>

Aapti's Comments

Section	Relevant Content	Critique
S. 2(10)	Definitions: "harm", in relation to a Data Principal, means - (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;	1. The bill truncates the scope of this definition by omitting the inclusion of mental harm, surveillance that is not reasonably expected, etc. 2. Further, it adds broad terms such as 'harassment' or 'causation of significant losses' with little indication to the standard of thresholds that will be followed in their determination. 3. In the absence of a data taxonomy, other harms may also arise from the processing of data that can straddle the line between personal and non-personal data which the Bill does fails to account for. For instance, the risk re-identification from datasets.
S. 2	Sub-section (5): Data fiduciary and sub-section (7) Data processor	The lines between a data fiduciary and a data processor are not well delineated and can lead to complications in practice. The law needs to provide for specific details on their obligations and differences, including - 1. The test to establish specific relationships and obligations of the two entities, considering the vague delineation on who decides the purpose of data processing, and who conducts such processing on their behalf, 2. Breaches in performance of obligations by the data processor and the question of establishing negligence. 3. Clarity on the expectation of the fiduciary to maintain oversight on

		the processor, and the standards around the same.
S. 4	Sub-section (1): Application on data collected online or subsequently digitised; Sub-section (3)(a): non-automated processing of data;	1. There has been little justification for limiting the individual's right to protect data to that which is digital, collected online, and is processed through automated means. 2. Not only does this raise confusion on definitions and scope of 'digital' and 'online', but the process also fails to account for lack of regulation on physical copies of digital data that could be collected offline. 3. For instance, what kind of rights can an individual exercise towards the protection of printed copies of digital bank statements shared with their chartered accountant? Details and inferences drawn from this without digitization may be shared with third parties for unintended purposes.
S. 4	Sub-section (3)(d): Data in record for 100+ years	No justification has been provided for the 100-year limitation period for protection of personal data under this act. This could lead to the dilution of an individual's rights over their data after their death, such as the right to erasure or the rights of the data principal's nominee. There is no reference for similar provisions in the previous versions of the bill, or in corresponding data protection legislations such as the GDPR.

S. 6	Notice for consent	The notice for consent mechanism prescribed under the Bill may prove to be ineffective for the following reasons - 1. Consent fatigue, where individuals are de-sensitized to the risks of sharing personal data due to a remarkably high number of requests, 2. Lack of the technical literacy to make informed choices on the data shared and the purposes of its processing, There is a need to look at alternatives for effective consent mechanisms, and the adoption of an advisory role for the consent manager may benefit the individual's capacity to meaningfully engage with consent. Here, creative and engaging formats for consent should be incentivized (such as a comic format for communication of terms). Additionally, principles may be borrowed from various data stewardship models for consent facilitation. By acting as an intermediary that facilitates consent and decision-making for the data principle, a data steward can bridge the digital divide and bolster user agency on personal data.
S. 6	Notice – Sub-section (1): "clear and plain language"; Sub-section (2): notice for data collected before the commencement of this Act	The standard on 'clear and plain language' for the notice may not be enough to provide users with clarity on what sort of data is being collected and the purposes it is used for. The details mandated to be included in the notice have also been reduced

		compared to previous iterations and the fair processing notice as articulated in the GDPR. The Bill does not mandate inclusion of terms on data sharing, storage limitations etc. Thus, significantly reducing informed choice and decisional autonomy for the data principal. Additionally, the timelines and obligations for data collected before the commencement of act have been defined in unclear terms of "as soon as is reasonably practicable". A definite implementation period must be provided for to ensure compliance, as under the GDPR and previous versions of this Bill.
S. 7(4)	Withdrawal of consent - "The consequences of such withdrawal shall be borne by such Data Principal."	The broad imposition of this burden on the principal could lead to excessive "consequences" on the principal without clarity on standards. Hypothetically, charges could be levied on a data principal to effectuate withdrawal of their consent under the pretext that the withdrawal requires the fiduciary to undertake further action. Further, such a provision risks acting as a deterrent to the exercise of the principal's right to withdraw.
S. 7(5)	Exemption on processing withdrawal - "unless such processing without the Data Principal's consent is required or authorized under the provisions of this Act or any other law."	The provision dilutes the data principal's right to consent revocation and data deletion and muddles the principle of storage limitation. Such continued use of data beyond withdrawal for broadly defined authorized purposes is doubly harmful in the context of deemed consent. This is because the processing happens without

		the explicit consent of the data principal, where additionally, there is ambiguity on whether they shall be notified or given the right to withdraw the same (discussed above under Section 7(4)).
S. 7(6)	Consent Manager	While the inclusion of consent managers in the Bill is good, there needs to be some clarity in the rules governing such consent managers. "Accessible, transparent, interoperable" while good principles to abide by are not robust enough and require elaboration. Adding an additional layer in the absence of clear governance guidelines can add to consent fatigue and complicates implementation of this framework for a population with limited digital literacy. Adding an advisory function to the CM's role to facilitate consent is worth exploring in this context, as in the case of various data stewardship models that encourage user agency and informed choice. Additionally, pre-existing sectoral frameworks for CMs, such as the Account Aggregators in the banking sector and the Health Information Exchange under ABDM, would have to be harmonized with the law in terms of the role and fiduciary duties assigned.
S. 8(1)	Deemed Consent	Deeming consent beyond the specified use based on a 'reasonable expectation' standard muddle the purpose limitation principle in data protection.

		This subjective standard varies from person to person, and may be ineffective in a country where digital literacy rates vary widely among differently placed communities. Additionally, with no explicit requirement to provide notice on the purpose or fact of collection, a data principal may remain uninformed on the processing or sharing of their data. This takes away from their decisional autonomy over personal data. In the past, the automatic adoption of ABHA Health ID for users of the COWIN vaccination portal or the Aarogya Setu Application raised concerns around agency and consent. The creation of ABHA without the explicit consent of the data principal was specious in itself; made worse with the complication in the right to withdraw consent when it is deemed. Such practices also lead to inaccurate inferences on the actual uptake for public welfare schemes. Finally, no judicial oversight or reasoned decision-making provision has been provided for deemed consent, leaving little recourse for challenging the use of personal data beyond active and explicit consent.
S. 8(7)	Deemed consent in employment	Non-consensual processing of an employee's data by her employer risks violating an employee's privacy and enables the use of surveillance technologies that allow employers to take screenshots and monitor videos. Such law governing the personal data of an employee must be phrased in their

		favor, especially considering the power dynamics of an employer-employee relationship. The provision also raises questions on its applicability around newer forms of workplace relationships in the gig economy. Without clarity, we risk large scale abuse of worker data where individuals continue to face a loss of agency in work.
S. 8(8)(d)	Deemed consent for credit scoring	It is not clear where an allowance on data processing for credit scoring finds its origin, with no precedence in past versions of the law or corresponding legislations from the EU or Singapore. Additionally, there is little justification or jurisprudence on including 'credit scoring' as a 'public interest' purpose. Processing data for credit scoring on deemed consent is even more harmful with the increased adoption of AI-based systems that find empirical relationships between new factors including social media profiles to activities such as what is eaten and worn. Such an expanded scope of the data made relevant for use has serious implications for privacy and the financial wellbeing of individuals in the absence of explicit consent.
S. 8(8)(e)	Deemed consent for "operation of search engines for processing of publicly available data"	Allowances for deeming consent for data available on search engines must account for the risk of accessing data not intended for public availability and the resultant implications for the principal's privacy.

		In the past, crucial personal data has been indexed on search engines like Google with the 2019 Aadhar leaks. These incidences point to an alarming need for reconsideration on this provision.
S. 8(9)	Deemed consent for "any fair and reasonable purpose as may be prescribed after taking into consideration - "	With a dilution of the Puttaswamy Test for encroaching on a data principle's right to privacy, the Bill resorts to a paternalistic approach for the government to prescribe purposes for deeming consent. The provision instead relies on outweighing interests over adverse effects and indefinite thresholds of 'reasonable expectation.'
S. 9(6)	Fiduciary obligations on data retention - "reasonable to assume"	The phrasing of the provisions muddles purpose limitation with vague terms such as 'reasonable to assume' and inclusion of 'business purposes. Additionally, there is little clarity on the standards and review mechanisms in this regard, leaving the Fiduciary itself to put in place a "procedure to redress grievances" (Section 9(8)).
S. 10	Children's data - Verifiable parental consent No targeted advertising/monitoring	Obtaining verifiable parental consent for processing data of all users under 18 shall raise complications in implementation. Basing a child's experience access to the internet on a parent or legal guardian also works on the assumption of a benevolent relationship, which may not exist for all children on all matters. This affects the child's autonomy and the

		ability to access information through the Internet. Borrowing jurisprudence from India's Juvenile Justice Act, EU's GDPR, or USA's Children's Online Privacy Protection Rule, this age limit should be reconsidered for 13-16 years. The process also hints at adding KYC requirements to online platforms such as social media, which has often been critiqued for being impractical and raising privacy concerns.
S. 11(1)	"Assessment of relevant factors, including"	The listed factors relevant for classification as a significant data fiduciary have been reduced with the adoption of more broad ranging powers for determination. In the absence of a detailed data taxonomy, the factors specified, such as sensitivity of data processed also become obscure. Overall, there is limited guidance on the scope of executive powers to notify for 'other factors as it may consider necessary', which risks to arbitrary classification of Fiduciaries.
S. 12	Right to information	There needs to be regulation on the format in which data is to be provided to the data principal as well as the timeline this shall follow. As evidenced by the experience of drivers in the gig economy, this stands to reduce the judicial burden on questions on worker's rights to access

		data, for instance, and secures more meaningful agency to the principal.
S. 12	Right to data portability	The explicit statement of right to data portability under the PDP has been removed with the new Bill. Additionally, the obligations around the principal's right to information limit access to mere confirmation, summaries, and details on data sharing, with no provision to request the entirety of the personal data collected by any entity. This hampers the principal's ability to port their data even manually. The right to portability must be re-instated in a meaningful manner as it is key to ensure that users are not locked into specific digital ecosystems and have freedom of choice.
S. 14	Right to grievance redressal	The Bill provides little guidance on the grievances that may be raised, the standard of proof to be followed for them, or the enforcement mechanism. While the manner for filing complaints shall be prescribed at a later point, there is need for clarity on the standards for grievances especially considering a principal's 'duty to not raise frivolous complaints' (Section 16(2)). The law lays down no specific mechanisms to ensure grievance redressal mechanisms are truly accessible. This is made worse with the limited access provided under the law to one's own data (Section 12). Finally, there is a need to establish clear standards on how effectiveness of

		grievance redressal will be evaluated and monitored.
S. 16	Duties of data principals	The bill states a duty to not register 'frivolous complaints' with the Fiduciary or the Board, thus defining the standards in vague terms. Similarly, the right to erasure has been made subject to the production of 'verifiably authentic documents' with no prescription on what that shall entail. Considering the power asymmetries between an individual data principal and the often large scale data processors/fiduciaries, the Bill risks harm by attaching broadly defined duties that the principal can be penalized for (u/ section 25 r/w schedule 1).
S.17	Transfer outside India	The Bill allows the executive immense discretion in notifying the select countries that data may be transferred to. There is a need to lay down some guiding principles that place limits and checks on the executive's power in this regard to ensure that the decisions are made for public interest in a right's preserving manner. Here, the Bill may borrow from the factors laid down under the GDPR for cross-border data sharing such as thresholds for adequacy and trustworthiness.
S. 18		The blanket non-applicability of the mandate to not retain data beyond the

	Exemptions ss (4) state exempted from data deletion	intended use for any processing by state its instrumentality comes with little justification. This raises concerns about an individual's right to privacy and reduces their agency over how their data is used. There is a need to instate a limit to the state's power in this regard, with guidance on what situations the data may be retained in and the notification mechanism for its subsequent use, where required.
S. 19	Data Protection Board	The new Bill dilutes the authority of the Board to mere review and grievance redressal body, taking away all functions around standard setting and regulation. This presents a gap in the data protection framework for a strong unifying authority on sectoral regulations and harmonized implementation. In the proposed law, the rule making power has been delegated to the central government as opposed to an independent expert body. This potentially takes away from the objectivity in the framework that is further muddled in the absence of a process of public consultation and parliamentary debate. Additionally, the composition of the Board along with the qualifications of members, and process for removal of chairperson and members should be legislative action, not executive action to ensure independence of the institution.
S. 30(2)	Amendment to RTI Act	

		The amendment to the RTI Act further hampers an individual's ability to access their own data, considering the limited scope of the right to information clause.