


PUBLISHED 13/07/2023

Recommendations to the Digital Personal Data Protection Bill, 2022

By FTI Consulting and Law Offices of Panag & Babu





Shri Ashwini Vaishnaw
Ministry of Electronics and Information Technology
Government of India

Subject: Comments and recommendations on the Digital Personal Data Protection Bill 2022 published by the Ministry of Electronics and Information Technology on November 18, 2022 for public consultation.

Dear Sir

FTI Consulting and the Law Offices of Panag & Babu (**PBLaw**) jointly presented to the Ministry of Electronics and Information Technology (**MeitY**) a submission containing the recommendations to the draft Digital Personal Data Protection Bill, 2022 (**DPDP Bill**) in January 2023, as a part of the public consultation process initiated by MeitY.

The Government of India is also contemplating an overhaul of the existing technology laws in the form of the Digital India Act, 2023 (**DIA**) which is also being viewed as an opportunity to revisit certain aspects of the DPDP Bill such as, without limitation, the protection of children's data, automated decision-making.

In light of these developments in the tech regulatory landscape, FTI Consulting and PBLaw co-hosted a multi-stakeholder roundtable discussion in April 2023 to collate feedback from the business leaders and policy thinkers on the DPDP Bill and the DIA for the purpose of submitting it to MeitY. This engagement with the stakeholders led to a collective raising of logical questions, which through discourse resulted in finding meaningful and constructive solutions to bridge the lacunae in the draft legislation in a future proof manner.

In light of the above, we hereby submit suggestions and recommendations on the draft legislations, which we have added in **blue** in the existing draft of recommendations which was submitted to MeitY in January 2023, for ease of reference.

We look forward to future opportunities to discuss the specific issues highlighted hereinbelow as we move forward with this consultation process. In the meantime, if you have any questions, please do not hesitate to contact us.

Sincerely

FTI Consulting and Law Offices of Panag & Babu

Key Concerns and Recommendations

Digitalization has led to large-scale transformations across multiple aspects of businesses and governance alike, providing opportunities for value creation, and allowing for data-driven policymaking. At the heart of this digitization is the use of data for innovation and provision of services to consumers and citizens.

Enabling the accountable exchange of data between different stakeholders in the data ecosystem is important for realizing the positive economic and social potential of data usage. Any framework to govern data should take into consideration rapid changes in the marketplace, technologies and consumer and business preferences. In this context, the following areas of concern emerge from the DPDP Bill.

CHAPTER 1: PRELIMINARY

DESCRIPTION	RECOMMENDATION
<p>1 Section 1(2) : Implementation of the DPDP Bill</p> <p>The Joint Parliamentary Committee (JPC) Report that contained recommendations for the phased implementation of Personal Data Protection Bill, 2019 (2019 Bill) envisaged an approximate period of two years to be provided from the date of notification of the 2019 Bill. However, the DPDP Bill does not contain any timeline for implementation and Section 1(2) of the DPDP Bill states that the Bill will come <i>“into force on such date as the Central Government may by notification in the Official Gazette appoint.”</i></p>	<p>We recommend that the DPDP Bill clearly specify a timeline for the implementation of the various provisions contained within it. This would provide stakeholders with clarity regarding imminent next steps to align their operations to the DPDP Bill and allow an adequate amount of time to implement the obligations set out in the DPDP Bill.</p>
<p>2 Section 2(10): Harm</p> <p>The definition of ‘harm’ under the DPDP Bill includes any of the following in relation to a Data Principal¹: <i>“a. any bodily harm; b. distortion or theft of identity; c. harassment; or d. prevention of lawful gain or causation of significant loss.”</i></p>	<p>The DPDP Bill should</p> <ul style="list-style-type: none"> (i) harmonize the definition of harm with that of Personal Data breach² that includes the requirement of a notification to the Data Protection Board (Board) and the affected Data Principals, and (ii) clarify whether this reporting would fall under the jurisdiction of the Indian Computer Emergency Response Team or the Data Protection Board or both.

DESCRIPTION

RECOMMENDATION

3 Section 2(13): Classification of Data

Under the DPDP Bill, all data is included under the broad ambit of Personal Data.³ The DPDP Bill does not categorize data into sensitive or critical Personal Data.

Doing away with specific classifications of Personal Data that existed in the older drafts of the data privacy bills would mean that all Personal Data, irrespective of the sensitivity of the information, will be treated in the same manner and the actions that are to be taken when non-critical Personal Data is collected and processed will be the same for critical/sensitive Personal Data.

In light of the above comment, MeitY should:

- define clearly discernable and narrowly worded definitions to categorize Personal Data and offer greater protection to Personal Data that is categorized as critical/sensitive such as health data and financial data.
- envisage a framework wherein the compliance with obligations under the DPDP Bill gets triggered in accordance with the category of Personal Data that is affected by a potential breach or any other violation of the DPDP Bill.
- ensure that the consequences for non-compliance/violation of the DPDP Bill are related to the category of Personal Data in a risk-commensurate manner and the risk of harm by the breach of sensitive categories of Personal Data.

CHAPTER 2: OBLIGATIONS OF DATA FIDUCIARY

DESCRIPTION	RECOMMENDATION
<p>4 Section 5: Grounds for Processing of Personal Data</p> <p>While the DPDP Bill explicitly states that Personal Data can only be processed in accordance with the DPDP Bill, for a lawful purpose,⁴ the DPDP Bill does not expressly include contractual necessity as a ground for processing Personal Data.</p>	<p>We recommend that the ‘fulfilment of contractual obligation’ along with model contractual obligations for data processing pursuant to a contract are incorporated in Chapter 2 as valid / statutorily recognized grounds for the processing of Personal Data.</p>
<p>5 Section 8: Deemed Consent</p> <p>As per the draft DPDP Bill, Personal Data should only be processed for a lawful purpose for which the Data Principal has given or is deemed to have given consent. However, the factors mentioned under Section 8 of the DPDP Bill state that consent of a Data Principal will be ‘deemed’ in certain situations, including for the maintenance of public order, purposes related to employment and in legitimate interest exercised in public interest.</p>	<ul style="list-style-type: none"> — While we commend the convenience it offers to businesses that process data for the purposes identified in Section 8 of the DPDP Bill, we recommend including specific circumstances where consent may not be deemed. This can include instances where Personal Data is of a child, criminal records of a person used outside of law enforcement, etc. — The DPDP Bill should be prescriptive about the ‘safeguards against misuse of any deemed consent’ to ensure that it is not used to the detriment of the data principal’s rights therein. — The principles of proportionality and purpose limitation should strictly apply to any processing of data under deemed consent. — The DPDP Bill should prescribe a graded approach for the processing of Personal Data basis deemed consent, such that in some industries like finance and health, Personal Data be processed under deemed consent for the benefit of the Data Principal. However, processing basis such deemed consent should be strictly limited to the purpose for which the data was collected, which can also be prescribed by sectoral regulators like RBI.

DESCRIPTION

RECOMMENDATION

- We recommend that the DPDP Bill should provide for a tiered consent approach such as implied consent (in terms of contractual obligations), explicit informed consent (for processing of sensitive Personal Data) and deemed consent (for public interest purposes).
- The government should implement guidelines which facilitate privacy by design, for example:
 - At the consumer facing end: the user interface of a platform should be user friendly and should make it easier for Data Principals to understand and give consent after fully comprehending what they are consenting to. To give effect to this recommendation, the DPDP Bill can prescribe certain key information which must be communicated to the Data Principals at the time of taking their consent akin to as prescribed under the extant Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
 - The DPDP Bill should elaborate upon ways in which the data subject can provide consent efficiently without undergoing consent fatigue which can be counterproductive to informed consent envisaged under the DPDP Bill.

DESCRIPTION

RECOMMENDATION

6 Section 9(4): Adoption of Reasonable Security Safeguards

The DPDP Bill imposes upon the Data Fiduciary⁵ and the Data Processor⁶ the duty to protect Personal Data in its possession or under its control by taking reasonable security safeguards to prevent Personal Data breach. However, the DPDP Bill fails to provide guidelines as to what constitutes ‘reasonable security safeguards.’

An outline of what constitutes ‘reasonable security safeguards’ must be defined and provided under the DPDP Bill prior to being set out in the rules framed thereunder to enable companies to take necessary steps to be compliant with the security obligations as soon as the DPDP Bill becomes effective. Regulatory requirements for security measures that are to be followed by Data Fiduciaries and Data Processors as set out in the GDPR⁷ and California Consumer Privacy Act (CCPA) may be referred to and adopted. Additionally, the DPDP Bill should afford some degree of safe harbour that would mitigate risk of penalty should a Data Fiduciary be in compliance with the reasonable security measures required when a Personal Data breach occurs.

7 Section 9 (5): Personal Data Breach Reporting Obligations

As per the DPDP Bill, Data Fiduciaries and Data Processors are required to notify the Board and each impacted Data Principal about all Personal Data breaches, regardless of the risk of harm. However, it is essential to note that this could distract businesses from incident response at a critical time when they need to focus on stopping the breach. Such a flood of notifications could also overwhelm the Board, making it difficult for it to concentrate its resources on the most significant incidents. This could lead to inefficient and ineffective responses, thus, putting impacted Personal Data at greater risk. It is essential that there exist better clarity and guidance on how, when, or what information must be included when notifying the Board and the Data Principal about Personal Data breaches.

We recommend that the DPDP Bill:

- Should prescribe different timelines for reporting of breach of Personal Data to the Board based on the severity of the breach that has occurred and the potential harm to the Data Principal that would occur due to such a breach. [The CERT-In Directions of 2022⁸](#) and [the CERT-In Rules⁹](#) currently provide timelines for reporting cybersecurity incidents. The timelines under the DPDP Bill should complement the obligations prescribed by CERT-In while being Personal Data-centric.
- Except for incidents of a greater magnitude or a pre-determined threshold, the DPDP Bill should require only Data Fiduciaries (not Data Processors who often don’t have the necessary context) to notify the Board and Data Principals. Data Processors, however, should be required to notify the impacted Data Fiduciary within a stipulated time frame in the event of a Personal Data breach.
- Ensure that the timeline for giving notice regarding a breach aligns with global best practices (within 48-72 hours).

DESCRIPTION

RECOMMENDATION

- Implement guidelines and processes to ensure that a Data Fiduciary provides all necessary information when notifying the Board and the Data Principal regarding a Personal Data breach.
- Given that the CERT-IN Directions, 2022 prescribe that a notice be sent to the CERT-IN to report cybersecurity incidents, sending out a notice of breach under the DPDP Bill as well would be a duplication of the notification obligations. Hence, the DPDP Bill should clarify that how the notification of breach obligations would work where a breach falls under the jurisdiction of both CERT-IN and the Board.

8 Section 10: Processing Children's Data

The DPDP Bill retains the age of consent at 18 years. Multiple stakeholders have previously called for reducing the age of consent to protect the agency and privacy of teenagers and adolescents on the internet.

We recommend that the DPDP Bill should:

- Take a two-pronged approach to consent when it comes to Data Principals that are children. Guardian consent should be required for younger Data Principals under 13 years of age, but the consent of teenagers (aged 13-17), rather than that of their guardians, should be acceptable. This will help maintain appropriate oversight over young children who cannot yet provide consent while affording sufficient autonomy and privacy for older, teenage Data Principals.
- Include clear metrics to consider when data processing will be considered 'harmful' to children.
- Provide certain exceptions if profiling, tracking, and behavioral monitoring are in the best interest of the child or necessary to provide the digital service. However, all profiling, tracking, and behavioral monitoring must be done only with the explicit consent of the lawful guardian of the child.
- Provide that any processing of Personal Data of children should only be done in the interest of children (and what comprises 'interest of children' must be statutorily prescribed).
- Not require parental consent to be taken for educational platforms or for age-appropriate online games which do not require any financial transactions to the extent that such platforms do not engage in behavioral monitoring, targeted advertisements, and profiling of children's data.

DESCRIPTION

RECOMMENDATION

9 Section 11: Significant Data Fiduciary

The DPDP Bill allows the Central Government to notify a Data Fiduciary or class of Data Fiduciaries, as Significant Data Fiduciaries based on the volume, nature of Personal Data they process, etc., and imposes additional obligations on such Significant Data Fiduciaries. While this appears to be a provision that can be used to classify small Data Fiduciaries and exempt them from onerous obligations, there is nothing in the DPDP Bill to ensure safekeeping of a Significant Data Fiduciary's interest.

We strongly recommend that the threshold for determination of a Data Fiduciary as a Significant Data Fiduciary be kept high. The EU NIS Directive¹⁰, which similarly seeks to target the key data processing actors, specifically applies to operators providing essential services, such as energy, transport, financial market infrastructure, etc., and digital service providers, such as search engines, cloud computing services, and online marketplaces.

Such a targeted approach may also be considered in the regulations issued under the DPDP Bill to identify Significant Data Fiduciaries.

CHAPTER 4: SPECIAL PROVISIONS

DESCRIPTION

RECOMMENDATION

10 Section 17: Cross Border Data Flows

The DPDP Bill recognizes the concept of trusted jurisdictions i.e., nations where Personal Data (of all kinds) may be transferred. It is, however, not clear if it is intended to be similar to the adequacy mechanism under the GDPR. Further, there is no clarity on the criteria on which the countries will be evaluated before being allowed to process Personal Data belonging to Indian nationals. The lack of clarity concerning the whitelist of countries to which Personal Data may be transferred, raises concerns pertaining to the legal status of cross-border transfers before such a list of countries is published. Additionally, the DPDP Bill does not recognize other grounds for overseas transfers, such as contract clauses, certifications, code of conduct and others.¹¹

- The DPDP Bill should explicitly recognize a valid contract (to ensure the Data Principal has enforceable rights and effective legal remedies) as grounds for permitting cross-border transfer of Personal Data to any jurisdiction as long as the Data Principal is made aware of the potential risk of such transfer and explicitly consents to such transfer of their data. **Standard contractual clauses can be prescribed which are to be used before any data transfer to a foreign entity, and which are enforced with a strengthened mechanism.**
- The factors that the Central Government will consider prior to allowing data transfers to other jurisdictions must be clearly elucidated in the DPDP Bill to avoid ambiguity and executive overreach. **A predictable framework-based approach should be adopted (i.e., the process/criteria for whitelisting one country over the other should be available in public domain).**

DESCRIPTION

RECOMMENDATION

- In case a country is blacklisted, the DPDP Bill should prescribe the way forward in terms of what steps would be required for it to be removed from the blacklist, how much time would be given to allow companies to transfer data out of that jurisdiction for business continuity measures and transition outside that blacklisted jurisdiction.
- Additionally, it is proposed that alternate data transfer mechanisms such as certifications, prescribing codes of conduct, etc. can be used to allow cross-border transfer of Personal Data as were contemplated in the Data Bill 2019¹².
- Instead of a country-based approach, the DPDP Bill can prescribe certain standards/ parameters for companies to meet, before they are eligible to receive Personal Data from India. Companies can be rated for the level of data protection that they comply with/ follow, similar to ESG rating. This could also be in the form of certification which is earned by entities who meet the prescribed standards of data protection.
- In order to allow an easier cross- border flow of non-sensitive Personal Data for the purposes of increasing the ease of doing business in India, the DPDP Bill could also prescribe a tiered or graded approach. This would involve categorizing Personal Data into sensitive Personal Data such as financial and health data, and non-sensitive Personal Data. The blacklisting/ whitelisting approach could be used depending on the type of Personal Data that is being transferred.
- Government and industry organizations can collaborate to prepare a ready reckoner to ease compliance by smaller players like startups.

DESCRIPTION

RECOMMENDATION

11 Section 18: Exemptions granted to Data Fiduciaries by Central Government

Under this section, the Central Government is given the power to exempt certain Data Fiduciaries from the applicability of the DPDP Bill and in the processing of certain specific Personal Data.

To remove the potential arbitrariness of this section and reduce the unchecked power conferred on the Central Government, the process and the criteria to qualify for such exemptions and the categories of Data Fiduciaries (especially body corporates) that are entitled to such exemptions should be made more specific in the DPDP Bill.

CHAPTER 5: COMPLIANCE FRAMEWORK

DESCRIPTION

RECOMMENDATION

12 Section 19: Constitution of the Data Protection Board of India

Without the mention of the basic qualifications, the power to determine the composition, members and governance of the Board that replaces the Data Protection Authority, is entirely at the Central Government's discretion. While these factors are still to be established, failure of giving out any criteria in the DPDP Bill is a step back from the previous data protection bills. This ambiguity would also raise questions regarding the efficiency and independence of the Board. Given that the Central Government and its instrumentalities are major Data Fiduciaries, the Central Government's role in the governance, establishment, and its involvement in the functions of the Board must be expressly set out and ringfenced by way of documentation of such functions and powers in the DPDP Bill and the rules thereunder.

In the interest of the Board functioning independently, the DPDP Bill should set out certain factors based on which decisions pertaining to the formation of the Board would take place. In the interest of transparency and to assure the stakeholders of the absence of any undue influence, various bodies and individuals like industry experts and judges should be involved in setting up the Board.

DESCRIPTION

RECOMMENDATION

13 Section 20 (3): Functions of the Data Protection Board of India

The Board is vested with the power to direct a Data Fiduciary to adopt any urgent measures in order to remedy breach of Personal Data and to mitigate any harm caused to the Data Principal. The DPDP Bill potentially gives the Board unlimited authority to set security measures for a Data Fiduciary in cases of breach of Personal Data.

- Consistent with other provisions of the DPDP Bill, this provision should be amended to limit the remedies and mitigation measures to only those which are ‘reasonable’ in relation to the risk posed by the breach of Personal Data. These measures should be prescriptive only, with the implementation of certain measures being made purely at the discretion of the Data Fiduciary.
- The Board should act as a nodal agency which facilitates conversation amongst various sectoral and cross-sectoral regulators, as well as state governments to take their inputs on data protection as they have better knowledge about the nuances of the industry/ jurisdiction they govern, such as RBI for data privacy in fintech, Ministry of Information and Broadcasting for data privacy over OTT platforms, MeitY for data protection in online gaming sector and protection of children’s data.
- In order to reduce the enforcement burden on the regulators, sector- specific self-regulatory organizations/bodies can also be constituted to assist and increase compliance amongst fintech companies and startups.
- A child data protection expert should be made a part of the Board to represent children’s interests specifically, to prevent any misuse of the agency granted to the parents/ guardians to consent to children’s data being processed.

SUSHMITA DAS

Senior Director - Legal Tech
FTI Consulting
sushmita.das@fticonsulting.com

PRASANTO ROY

Managing Director
FTI Consulting
prasanto.roy@fticonsulting.com

AKASH KARMAKAR

Partner
Law Offices of Panag & Babu
akash@pblawoffices.com

The views expressed herein are those of the author(s) and not necessarily the views of FTI Consulting, Inc., its management, its subsidiaries, its affiliates, or its other professionals. FTI Consulting, Inc., including its subsidiaries and affiliates, is a consulting firm and is not a certified public accounting firm or a law firm.

FTI Consulting is an independent global business advisory firm dedicated to helping organizations manage change, mitigate risk and resolve disputes: financial, legal, operational, political & regulatory, reputational and transactional. FTI Consulting professionals, located in all major business centers throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges and opportunities. © 2023 FTI Consulting, Inc. All rights reserved. [fticonsulting.com](https://www.fticonsulting.com)

Endnotes

¹“Data Principal” means the individual to whom the Personal Data relates and where such individual is a child includes the parents or lawful guardian of such a child.

²“Personal Data Breach” means any unauthorized processing of Personal Data or accidental disclosure, acquisition, sharing, use, alteration, destruction of or loss of access to Personal Data, that compromises the confidentiality, integrity, or availability of Personal Data.

³“Personal Data” means any data about an individual who is identifiable by or in relation to such data.

⁴“Lawful purpose” means any purpose which is not expressly forbidden by law.

⁵“Data Fiduciary” means any person who alone or in conjunction with other persons determines the purpose and means of processing of Personal Data.

⁶“Data Processor” means any person who processes Personal Data on behalf of a Data Fiduciary.

⁷ 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) [2016]

⁸ Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet.

⁹ The Information Technology (The Indian Computer Emergency Response Team and Manner of performing functions and duties) Rules, 2013

¹⁰ Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union

¹¹ Update: As per several recent reports (as of April 2023), the government is mulling a blacklisting-based approach where data transfers will be permitted to all countries unless specifically prohibited by the government.

¹² Personal Data Protection Bill, 2019