Submission for the public consultation on the Digital Personal Data Protection Bill, 2022

Introduction

We welcome the Ministry of Electronics & Information Technology's attempt to create a comprehensive digital personal data protection framework for India as well as the opportunity to participate in the public consultation process. We also appreciate the need to strike an appropriate balance between protecting individuals' fundamental right to privacy – particularly in light of the rapid datafication of all aspects of personal, societal and economic life – and enabling digital personal data's enormous potential for transformational governance, innovation and economic growth.

Keeping this in mind, we have organised our inputs under 5 themes that address major components of this legislation. Each theme covers detailed comments for relevant clauses, covering the departure from the rights based approach, excessive exemptions, weakened protections and the effectiveness of the proposed Data Protection Board.

1. Lack of a rights-based approach

The purpose of DPDP, 2022, as drafted:
"to provide for the processing of digital personal data in a manner that recognizes both the right of individuals to protect their personal data and the need to process personal data for lawful purposes, and for matters connected therewith or incidental thereto".

Comments: This stated purpose of the bill implies a rights-based approach to data protection. However, the bill confers only the following rights to a data principal:

- right to information about personal data, (Section 12)
- right to correction and erasure of personal data, (Section 13)
- right to grievance redressal, and (Section 14)
- right to nominate, (Section 15)

It does not recognise a more specific fundamental right to the protection of personal data. This is in contrast to global best practices adopted by jurisdictions like the European Union (EU). In its subject matter and objectives, the EU's General Data Protection Regulation (GDPR) contains:

Article 1 (2) "This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data."

This is also a break from the former Personal Data Protection Bill, 2019 draft that acknowledged: *"the right to privacy is a fundamental right and it is necessary to protect personal data as an essential facet of informational privacy".*

The framing and elaboration of this bill's purpose via specific clauses is therefore not in keeping with the spirit of the K S Puttaswamy (Retd.) v Union of India judgement[1] where Justice D.Y. Chandrachud stated:

[1] K S Puttaswamy vs Union of India judgement

"Privacy is a constitutionally protected right which emerges primarily from the guarantee of life and personal liberty in Article 21 of the Constitution. Elements of privacy also arise in varying contexts from the other facets of freedom and dignity recognised and guaranteed by the fundamental rights contained in Part III;"

The judgement also went on to clarify that, "A law which encroaches upon privacy will have to withstand the touchstone of permissible restrictions on fundamental rights."

This sentiment was also reflected in the Justice Srikrishna committee report[2], which stated:

"The right to privacy has been recently recognised as a fundamental right emerging primarily from Article 21 of the Constitution, in Justice K.S. Puttaswamy (Retd.) v. Union of India. To make this right meaningful, it is the duty of the state to put in place a data protection framework which, while protecting citizens from dangers to informational privacy originating from state and non-state actors, serves the common good. It is this understanding of the state's duty that the Committee must work with while creating a data protection framework."

Taking a rights-based approach can empower data principals and create duties for the Data Protection Board and data fiduciaries to build capacity to protect rights under the law. The bill instead takes a compliance-based approach which imposes obligations on both data principals and fiduciaries, whose non-fulfilment attracts penalties. In the absence of recognising personal data protection as a right, data principals lose remedies, especially in cases of infringement made by the state itself against the fundamental right to privacy. Going by the doctrine of *Ubi jus ibi remedium*, only when there is a legal right is there a remedy.

Suggestion: Recognise the protection of personal data as a means to safeguard the fundamental right to privacy in the stated purpose of the bill.

2. Excessive exemptions and lack of clarity

Section 8. (2) A Data Principal is deemed to have given consent to the processing of her personal data if such processing is necessary: for the performance of any function under any law, or the provision of any service or benefit to the Data Principal, or the issuance of any certificate, license, or permit for any action or activity of the Data Principal, by the State or any instrumentality of the State;

Section 18. (1) The provisions of Chapter 2 except sub-section (4) of section 9, Chapter 3 and Section 17 of this Act shall not apply where:
(a) the processing of personal data is necessary for enforcing any legal right or claim;
(b) the processing of personal data by any court or tribunal or any other body in India is necessary for the performance of any judicial or quasi-judicial function;
(c) personal data is processed in the interest of prevention, detection, investigation or prosecution of any offence or contravention of any law;

Section 18 (3) The Central Government may by notification, having regard to the volume and nature of personal data

[2] Justice Srikrishna committee report

processed, notify certain Data Fiduciarie or class of Data Fiduciaries as Data Fiduciary to whom the provisions of Section 6, sub-sections (2) and (6) of section 9, sections 10, 11 and 12 of this Act shall not apply

Comments: These provisions violate the criteria laid down by the Justice Srikrishna committee, following the K S Puttaswamy (Retd.) v Union of India[3] judgement, on exemptions to meet the bounds of proportionality. They are reproduced below:

1. "Exemptions must be proportionate and necessary in the interest of the security of the state and pursuant to a law that meets the test of constitutionality.
2. Restrictions on privacy must be proportionate and narrowly tailored to the stated purpose.
3. Obligations on maintaining security safeguards in processing personal data will remain with the agency collecting such data and no exemption to the same will be provided."[4]

The exceptions fail on these grounds. Proportionality requires that "there be a reasonable relationship between the objective which is sought to be achieved and the means used to achieve that end"[5].

Some illustrative examples are the ends listed in Section 8(8) for public interest. They breach the rule of law principles by the executive arm of the state:

- Credit scoring
- Recovery of debt
- Mergers, acquisitions, any other similar combinations or corporate restructuring transactions in accordance with the provisions of applicable laws;

And section 8(9) also casts a wide net on state discretion : "for any fair and reasonable purpose as may be prescribed" with fewer specific considerations.

Some of the tasks are routine functions of the state in the principal-agent relationship. Such a relationship should not be superseded just because the party delivering on it is the state.

Suggestion: Narrow the scope of exceptions using principles of proportionality. Key protections such as data breach notifications (Section 9. (5)) should not be denied to Data Principals in situations listed in 18. (1) a. or 18. (1) b. Processing of personal data for enforcement of legal claims or by any court and tribunal should be held to the same standard of safety as significant data fiduciaries and an exemption only reduces the accountability of the State, while increasing chances of harm for Data Principals who may be affected due to non-compliance of basic data protection obligations by the State.

Section 18. (2) a The Central Government may, by notification, exempt from the application of provisions of this Act, the processing of personal data: by any instrumentality of the State in the interests of sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order or preventing incitement to any cognizable offence relating to any of these

Comments: As highlighted above, these provisions violate the criteria laid down by the Justice Srikrishna committee, following the K S Puttaswamy (Retd.) v Union of India judgement, on exemptions to meet the bounds of proportionality, which state that "Exemptions must be proportionate and necessary in the interest of the security of the state and pursuant to a law that meets the test of constitutionality."

[3] K S Puttaswamy (Retd.) v Union of India
[4] Justice SK report
[5] Principle of proportionality, Halsbury's Law of England

Suggestion: Narrow down the scope of exemptions in line with the recommendations of the Srikrishna committee and establish a system of checks and balances to oversee claims for exemptions.[6]

Section 17. Transfer of personal data outside India The Central Government may, after an assessment of such factors as it may consider 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.

Comments: The draft legislation does not provide clear guidance or criteria for the consideration of the Union government in this clause. The criteria is left to the Central government itself to be specified under its rule making power. The uncertainty around the clause could create difficulties and costs that could hamper businesses and investments.

Suggestion: The bill should specify the basis on which cross-border transfer may be permissible. An example may be taken from GDPR which lays down clear provisions and regulations including 'adequacy decisions' and 'appropriate safeguards' for processing and transfer of personal data to third countries.[7]

3. Regulatory jurisdiction and Independence of the Data Protection Board

Section 19. (1) The Central Government shall, by notification, establish, for the purposes of this Act, a Board to be called the Data Protection Board of India. The allocation of work, receipt of complaints, formation of groups for hearing, the pronouncement of decisions, and other functions of the Board shall be digital by design.

Comments: The above clause 19.1 suggests that functions of the board shall be digital by design, including receipt of complaints.

Suggestion: We suggest that the Bill specify the Board's compliance with standard accessibility provisions of government services whereby an offline or paper mode of filing complaints also be made available as 50% of the population do not have access to online facilities[8]

Section 19. (2) The strength and composition of the Board and the process of selection, terms and conditions of appointment and service, and removal of its Chairperson and other Members shall be such as may be prescribed

Section 19. (3) The chief executive entrusted with the management of the affairs of the Board shall be such individual as the Central Government may appoint and terms and conditions of her service shall be such as the Central Government may determine

Comments: Clauses 19.2 and 19.3 suggest that the Data Protection Board may not have sufficient independence in working as a regulator. An OECD report[9] on governance of regulators suggests a few

---

[6] A parallel of such a system in place is the Foreign Intelligence Surveillance Act of 1978 (FISA) which oversee requests for surveillance warrants against foreign spies inside the United States by federal law enforcement and intelligence agencies.

[7] Chapter 5 – Transfers of personal data to third countries or international organisations - General Data Protection Regulation (GDPR)

[8] Internet Adoption in India - ICUBE 2020

[9] Being an Independent Regulator | OECD

best practices after studying 48 public regulators in 26 countries in order to reduce undue political influence and ensure independence.
Suggestion: A few of these best practices that can be incorporated:

1. The Chairperson of the Board should either be appointed by Parliament or through a search committee rather than the Central Government
2. The Act itself should lay down specific guidelines on factors to be considered (technical expertise, reputational standing, independence) by the search or selection committee in appointing the members of the Board.
3. There should be a minimal cooling off period for members before and after taking up a post on the Data Protection Board in terms of joining a particular firm within the industry, in order to ensure there is minimal conflict of interest.
4. Budget for the function of the Data Protection Board should be for a long period (multi-annual) rather than an annual budget, decided by the relevant Ministry.

Section 9. (5) In the event of a personal data breach, the Data Fiduciary or Data Processor as the case may be, shall notify the Board and each affected Data Principal, in such form and manner as may be prescribed.

Section 20. (3) The Board may, in the event of a personal data breach, direct the Data Fiduciary to adopt any urgent measures to remedy such personal data breach or mitigate any harm caused to Data Principals.

Comments: Clauses 9.5 and 20.3 suggest that the Board will potentially handle reports of all breaches, irrespective of the size of the firm, the data they handle and the likelihood of the harm and enormity of the breach, on an equal footing. In terms of reporting and redressal, a smaller firm, not classified as a Significant Data Fiduciary, with a breach of personal data of a single individual could be placed on par with breaches of far wider scope to cause harm. This would place enormous demands on the capacity of the Data Protection Board (DPB) to address all breaches.

Suggestion: We recommend outlining a tiered regulatory approach where data breaches by significant data fiduciaries who handle a large volume of data and operate in sensitive sectors have more stringent clauses in terms of reporting the breach. The reported breaches of significant data fiduciaries should be redressed on a higher priority level by the Board compared to non-significant data fiduciaries.

4. Definitional and classification issues

Section 11. (1) The Central Government may notify any Data Fiduciary or class of Data Fiduciaries as Significant Data Fiduciary, on the basis of an assessment of relevant factors, including:
(a) the volume and sensitivity of personal data processed;
(b) risk of harm to the Data Principal;
(c) potential impact on the sovereignty and integrity of India;
(d) risk to electoral democracy;
(e) security of the State;
(f) public order; and
(g) such other factors as it may consider necessary;

Comments: Clause 11.1 suggests that the central government will have wide discretion in notifying a data fiduciary at any point in time. This could lead to vast regulatory uncertainty for firms, with regards to being compliant. Regulatory uncertainty can prove detrimental to the business environment, as firms

would be unable to plan clearly for any additional obligations on significant data fiduciaries after being classified as one.

Suggestion: The bill should only use well-defined criteria such as annual turnover, market revenue, number of users to classify a firm as a significant data fiduciary, in order to provide regulatory certainty to firms. The defined criteria should adopt metrics that help tie a risk based approach to the scope and pervasiveness of harm. For example, the European Union's Digital Markets Act (DMA) designates a platform as a 'gatekeeper' based on objective quantitative metrics (annual turnover, number of users), in addition to clearly defined qualitative metrics arising from assessing the platform's scope for harm. We also recommend removing sub-points (d), (f), (g) of clause 11.1 in order to reduce the ambit of discretion in classifying any data fiduciary as significant.

Section 2. (13) defines 'personal data' as any data about an individual who is identifiable by or in relation to such data.

Comments: The definition of personal data can be more comprehensive to cover criteria of being identified, directly or indirectly, in a more clear way. Such data is also sensitive and the Personal Data Protection Bill, in Section 2(36), for example, listed xii relevant items (reproduced below).

Section 2(36) "sensitive personal data" means such personal data, which may, reveal, be related to, or constitute—
(i) financial data;
(ii) health data;
(iii) official identifier;
(iv) sex life;
(v) sexual orientation;
(vi) biometric data;
(vii) genetic data;
(viii) transgender status;
(ix) intersex status;
(x) caste or tribe;
(xi) religious or political belief or affiliation; or
(xii) any other data categorised as sensitive personal data under section 15

GDPR too has a wider definition of personal data that bring in the direct and indirect clause:

"Article 4(1) 'personal data' as any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;"

An illustration of where a safeguard may be missing is, for example, A's personal information could be traced using Information from F, her parents. In such an instance, Section 2(13) may not protect A from being joined to information F consented to provide.

Suggestion: Expand the definition of personal data to restrict direct or indirect identification.

5. Weakened protections and burden on the principal

Section 12 The Data Principal shall have the right to obtain from the Data Fiduciary: (1) the confirmation whether the Data Fiduciary is processing or has processed personal data of the Data Principal; (2) a summary of the personal data of the Data Principal being processed or that has been processed by the Data Fiduciary and the processing activities undertaken by the Data Fiduciary with respect to the personal data of the Data Principal; (3) in one place, the identities of all the Data Fiduciaries with whom the personal data has been shared along with the categories of personal data so shared; and (4) any other information as may be prescribed.

Comments: The clause omits the right to data portability that allowed the data principal to receive in a structured format all the personal data they had provided to the data fiduciary and data that the data fiduciary generated on the data principal while processing for provisioning of its services.

Suggestion: To add a clause that confers on the data principals the right to receive the personal data concerning them in a structured format and have the right to transmit that data to another controller without hindrance. This will promote competition between data fiduciaries and protect consumer welfare.

Section 16.2 A Data Principal shall not register a false or frivolous grievance or complaint with a Data Fiduciary or the Board.

Comments: This clause along with the penalty on data principals in Schedule 1 could result in a chilling effect that discourages individuals from exercising the rights provided by this Act. This has also been raised as a concern[10] under RTI where multiple requests have been discarded by public authorities on the grounds that these were "frivolous".

Suggestion: Failure on the part of the data principal to adhere to this clause should not attract a financial penalty. Moreover, clear grounds should be stated by authorities for dismissing a complaint as frivolous.

Section 6. (1) On or before requesting a Data Principal for her consent, a Data Fiduciary shall give to the Data Principal an itemised notice in clear and plain language containing a description of personal data sought to be collected by the Data Fiduciary and the purpose of processing of such personal data.

Comments: The notice omits the duration or time period for which the data will be processed. This is an important safeguard that finds mention in GDPR, for example:

In Article 14 (2) In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject :

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

Suggestion: To add a clause that reflects the notice informs the data principal the duration for which the information will be processed and if that is not possible, a criteria that will be used to determine the duration.

---

10 https://thewire.in/government/govt-denied-information-under-rti-on-frivolous-grounds-during-2020-21-cic-analysis

Section 6. (2) Where a Data Principal has given her consent to the processing of her personal data before the commencement of this Act, the Data Fiduciary must give to the Data Principal an itemised notice in clear and plain language containing a description of personal data of the Data Principal collected by the Data Fiduciary and the purpose for which such personal data has been processed, as soon as it is reasonably practicable.

Comments: A clear specification of implementation timeline or criteria to arrive at what is "reasonably practicable" is important here to ensure it is implemented and complied with. Ambiguity from "as soon as it is reasonably practicable" can be subject to discretion, leaving room for copping out of complying.

Suggestion: Add clear timelines for notice for processing personal data collected before the commencement of the law.

Section 7. (1) Consent of the Data Principal means any freely given, specific, informed and unambiguous indication of the Data Principal's wishes by which the Data Principal, by a clear affirmative action, signifies agreement to the processing of her personal data for the specified purpose.

Comments: This provision is silent on the granularity of consent. When Data Fiduciaries offer multiple services, not all collected personal data needs to be processed for each offering. A data fiduciary should be able to unbundle personal data required for each service and offer to a data principal an option to give granular consent for each service and the relevant data required for it. This also operationalises the principle of data minimisation which states that a data fiduciary should acquire only that personal data which is essential for delivering the service or fulfilling the function requested by the data principal.

This is also a norm later clarified under GDPR[11]:

"Recital 43 clarifies that consent is presumed not to be freely given if the process/procedure for obtaining consent does not allow data subjects to give separate consent for personal data processing operations respectively (e.g. only for some processing operations and not for others) despite it being appropriate in the individual case. Recital 32 states, "Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them" .

The Justice Srikrishna committee report, meanwhile, laid down the principle of data minimisation. Data minimisation was also an important feature of the former draft bill, with Section 6 stating:

6. the personal data shall be collected only to the extent that is necessary for the purposes of processing of such personal data".

The former draft bill thus imposed a limitation on both the purpose and collection of personal data, that this bill does not.

Suggestion: Add a provision of granular consent, and define its usage for the sub-section. The bill should include a clause that specifies a limitation on data collection as well as purpose.

[11] GDPR, recital 43 with regards to European Data Protection Board

Section 8. (1) A Data Principal is deemed to have given consent to the processing of her personal data if such processing is necessary: in a situation where the Data Principal voluntarily provides her personal data to the Data Fiduciary and it is reasonably expected that she would provide such personal data;

Comments: Reasonable expectations could have wider implications. The illustration is too specific to cover the ambit of what amounts to reasonably expected.

Suggestion: Include a clear definition of what reasonable expectations mean here.

Section 21. (2) At any stage after receipt of a complaint, if the Board determines that the complaint is devoid of merit, it may issue a warning or impose costs on the complainant

Suggestion: In clause 21.2, we recommend that the word 'devoid of merit' be changed to 'frivolous', in order to ensure that there are no adverse incentives imposed on complainants, where the complaint did possess some merit but not enough to reach a successful conclusion.