Draft Personal Data Protection Bill 2022:

Comments from eGovernments Foundation

17th December, 2022.

Introduction

The "Right to Privacy" was read into Art. 21 of the Constitution of India by the Supreme Court of India in 2017, vide its judgment in *Justice K.S. Puttaswamy (Retd.) vs Union of India and Ors.*[1] ***("Puttaswamy case").*** The Supreme Court has further elaborated on the Right to Privacy in subsequent cases, notably in *Justice K.S. Puttaswamy and Anr vs Union of India and Ors*[2] ***("Aadhar case")*** and *Navtej Singh Johar vs Union of India*[3] ***("Navtej Singh Johar case")***.

Situating the Right to Privacy in Art. 21 has the effect of making legal tests, established in Supreme Court jurisprudence, applicable to the Right, its regulation, and any proposed derogations from it[4]. Specifically with respect to the Right to Privacy, the Supreme Court has established that a restriction or derogation is permissible if it satisfies the following four-fold test:

1. **Legality:** the act leading to restriction or derogation of the Right must be authorised by law.
2. **Legitimate Aim / Purpose:** the act leading to restriction or derogation must seek to achieve some specific objective; this objective cannot itself be unlawful / *ultra vires*, and the act must have some rational connection with the objective.
3. **Proportionality:** the act leading to restriction or derogation must be proportionate, i.e. the extent of intrusion into privacy should be commensurate with the potential need or benefit of the intrusion. This is generally interpreted to mean that, given a choice between different measures, the least intrusive measure should be adopted.
4. **Adequate Safeguards**: there should be suitable measures (guidelines, checks and balances, monitoring mechanisms, etc.) to ensure that the above three requirements are being adhered to, and that in the event that they are not, the act leading to restriction or derogation is also ceased or prohibited from continuing.

Following the *Puttaswamy* case, in August 2017, the Government of India constituted a Committee of Experts on a Data Protection Framework for India, under the chairmanship of Justice (Retd.) B.N. Srikrishna **("Srikrishna Committee"**). The Committee was mandated to make recommendations on a draft law that would address the Right to Privacy and data protection in India. The Committee conducted extensive consultations, and submitted its report (including a draft bill) in July 2018[5].

---

[1] Writ Petition (Civil) No. 494 of 2012, (2017) 10 SCC 1
[2] Justice K.S Puttaswamy & Anr. v. Union Of India & Ors. [W.P No 494 of 2012] https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf
[3] AIR 2018 (SC) 4321
[4] *Maneka Gandhi vs Union of India,* (1978) 1 SCC 248
[5] https://prsindia.org/policy/report-summaries/free-and-fair-digital-economy

The Srikrishna Committee Report and Draft Bill covered a number of key elements necessary to establish and operationalise the Right to Privacy and data protection:

- **Data Principal ("DP") and Data Fiduciary ("DF")**: The Committee established that an individual to whom a given piece of data pertains is a principal, and that persons or organisations using that data owe a fiduciary duty to them. This was an important development, given that the global norm is to consider such individuals "data subjects", and the users of the "data controllers". This approach is consistent with recognising the Right to Privacy as a fundamental right of each individual.

- **Consent-based and Non-consent-based Processing:** The Committee established a general norm, that data fiduciaries can process data principals' data only on the basis of informed and meaningful consent. At the same time, the Committee recognised that there were legitimate grounds for non-consent-based processing, and established the specific circumstances under which this would be possible[6]. This approach is consistent with the four-fold test established in the *Puttaswamy* case.

- **Rights of the Data Principal:** The Committee recognised that certain rights are inherent in the concept of a Data Principal. Specifically, these include the right to access, confirm, and correct one's own data; the right to know if one's data is being used, and to object to certain uses; the right to data portability (from one fiduciary to another); and the right to have data deleted, sometimes known as the "right to be forgotten".

Over the past 54 months, the Draft Bill proposed by the Srikrishna Committee has gone through several waves of discussion and modification, culminating in the Draft Digital Personal Data Protection Bill of 2022[7] (**"DPDP Bill"**).

The comments provided below reflect our understanding of how the DPDP Bill corresponds to the standards established by the Supreme Court, which are currently the highest authority of law on privacy and data protection in India. We use the Srikrishna Committee's draft bill as a reference point to understand how these standards can be translated into legislation. The comments also reflect our experience, as an entity that supports local governments with providing public services and welfare to residents.

[6] (i) where processing is relevant for the state to discharge its welfare functions,
(ii) to comply with the law or with court orders in India,
(iii) when necessitated by the requirement to act promptly (to save a life, for instance), and
(iv) in employment contracts, in limited situations (such as where giving the consent requires an unreasonable effort for the employer).

[7] https://www.meity.gov.in/content/digital-personal-data-protection-bill-2022

Summary of the Bill

The DPDP Bill may be summarised as follows:

Chapter	Sections	Key Subject Matter in Section
1	1-4	Commencement; Applicability; Definitions of key terms
2	5-11	Grounds for processing PD (Notice & Consent; Deemed Consent); General obligations of DF; Additional obligations in certain cases
3	12-16	Rights of DP (information, correction, erasure, grievance redressal, nomination); Duties of DP
4	17-18	Transfer of PD outside India; Exemptions to Chapters 2 & 3 (automatic exemptions, exemptions by notification)
5	19-25	Data Protection Board (composition, functions, powers and processes, appeals, financial penalties that the board may impose).
6	26-30	Rule-making powers, amendment powers, amendments to existing laws that will be effected by the DPDP Bill
Schedule 1		Details of non-compliance events and associated penalties.

Key Feedback Points

1. Right to Privacy

The Right to Privacy of individuals finds no explicit mention in the Bill. The Supreme Court, in the Puttaswamy judgment, had recommended the right to privacy be enshrined within a legislative instrument. The previous version of the Bill[8] gave due importance to this right. As it forms the primary basis for the existence of this law, the explicit mention of the Right to Privacy in the processing of the digital personal data is crucial. Suitable language was already used in the 2019 Draft Bill, and we recommend that the same be included in the present Bill as well.

[8] Draft Personal Data Bill (2019):
"*...to provide for protection of the privacy of individuals relating to their personal data, specify the flow and usage of personal data, create a relationship of trust between persons and entities processing the personal data, protect the rights of individuals whose personal data are processed, to create a framework for organisational and technical measures in processing of data, laying down norms for social media intermediary, cross-border transfer, accountability of entities processing personal data, remedies for unauthorised and harmful processing, and to establish a Data Protection Authority of India for the said purposes…*"
"*WHEREAS the right to privacy is a fundamental right and it is necessary to protect personal data as an essential facet of informational privacy;*
AND WHEREAS the growth of the digital economy has expanded the use of data as a critical means of communication between persons;
AND WHEREAS it is necessary to create a collective culture that fosters a free and fair digital economy, respecting the informational privacy of individuals, and ensuring empowerment, progress and innovation through digital governance and inclusion and for matters connected therewith or incidental thereto."

2. Limitation of Scope to Digital Personal Data

Sec. 4(3) of the Bill restricts the application of the law to digital personal data, excluding *inter alia* personal data that is in paper or offline format as well as non-automated processing of personal data.

While the exclusion of non-personal data (which had been included in the 2019 Draft Bill) is a welcome step, that will bring greater clarity, the rationale for excluding offline and non-automatedly-processed personal data is unclear.

First, the possibility of unlawful collection, use, or disclosure of personal data exists even in the case of manual processing or recording.

Second, paper records may be digitised on various occasions and in various forms; for instance, a photograph of a document may be shared on email or Whatsapp; this image in turn may be converted to a text record (e.g. by use of OCR technology). If there is a rationale for making protections applicable to such image or derived record, yet not to the original record, this should be articulated and debated.

3. Definition of Lawful Purpose

Sec. 5 of the Bill provides the grounds for processing of digital personal data. Lawful purpose, in this section, is defined as "*...any purpose which is not expressly forbidden by law.*"

This is inconsistent with the principles of legality, legitimate purpose, and proportionality as laid down in the *Puttaswamy* case, and against the globally-recommended practice of data minimisation[9]. Data collection, processing, sharing etc. should be restricted to specific and well-defined purposes, with each such purpose having specific legislative backing. Without such specificity, the tests of legitimate purpose and proportionality are difficult to apply.

[9] ISO 2011 - *Data minimization: minimizing the personal information, which is processed and the number of privacy stakeholders and people to whom personal information is disclosed or who have access to it.*
GDPR - Principle No. 3 - *'Data minimization: personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.'*

4. Itemised Notice

Sec. 6(1) of the Bill mandates that DFs shall provide DPs with itemised notice in clear and plain language, containing a description of personal data sought to be collected,and the purpose of processing of such personal data.

While notice as provided for under the previous version of the Bill included more fields of information,[10] many of these fields are addressed in subsequent sections of the Bill. In order to be more closely aligned with the principles of legality and legitimate purpose, such notice should include the legal basis and authority that underlies the data collection or processing as well. That is, for each item of data requested from or obtained about the DP, the purpose for processing and the legal instrument that gives that particular DF the mandate and authority to collect / process that data.

Sec. 6(2) further requires DFs to provide itemised notice for PD collected and consented to be used prior to this law. This is as a welcome step that will bring greater transparency and awareness; to the extent that there are costs associated with identifying such data and communicating with the corresponding DPs, it could incentivise DFs to stop storing data they do not actively require. However, in order to achieve this objective, the Bill should include a time limit within which this provision must be complied with.

---

[10] Draft PDP Bill 2019, Sec. 7: "*(1) Every data fiduciary shall give to the data principal a notice, at the time of collection of the personal data, or if the data is not collected from the data principal, as soon as reasonably practicable, containing the following information, namely:—*
(a) the purposes for which the personal data is to be processed;
(b) the nature and categories of personal data being collected;
(c) the identity and contact details of the data fiduciary and the contact details of the data protection officer, if applicable;
(d) the right of the data principal to withdraw his consent, and the procedure for such withdrawal, if the personal data is intended to be processed on the basis of consent;
(e) the basis for such processing, and the consequences of the failure to provide such personal data, if the processing of the personal data is based on the grounds specified in sections 12 to 14;
(f) the source of such collection, if the personal data is not collected from the data principal;
(g) the individuals or entities including other data fiduciaries or data processors, with whom such personal data may be shared, if applicable;
(h) information regarding any cross-border transfer of the personal data that the data fiduciary intends to carry out, if applicable;
(i) the period for which the personal data shall be retained in terms of section 9 or where such period is not known, the criteria for determining such period;
(j) the existence of and procedure for the exercise of rights mentioned in Chapter V and any related contact details for the same;
(k) the procedure for grievance redressal under section 32;
(l) the existence of a right to file complaints to the Authority;
(m) where applicable, any rating in the form of a data trust score that may be assigned to the data fiduciary under sub-section (5) of section 29; and
(n) any other information as may be specified by the regulations."

5. Consent Managers

Sec. 7(6) creates a category of DFs known as consent managers, who will support DPs and other DFs in managing, reviewing, and withdrawing consent for collection, processing, and sharing of PD.

In a country like India, where access to internet remains limited for many social and economic groups, this is a welcome innovation that will help the "next half billion"[11] manage their online presence and data in safer and more effective ways.

6. Deemed Consent

Sec. 8 of the Bill establishes the grounds on which data can be processed without consent from a DP, using the legal fiction of "deemed consent" to address what was described as non-consent-based processing in previous drafts of the Bill.

To the extent that the grounds for such processing remain largely similar to those mentioned in previous drafts, this is a reasonable provision. However, the grounds mentioned under **Secs. 8(8) and 8(9)** are much broader than in previous drafts, and create grounds for ambiguity. The grounds for processing on the basis of deemed consent should remain specific, limited, and narrow.

A related point is that the Bill does not extend the requirement to provide notice (u/**Sec. 6**) to instances of data collection or processing with deemed consent. This is an inconsistency; even when the grounds for processing is deemed consent, there must still be a lawful basis and legitimate purpose, and only specific data related to such purpose can be collected and processed. As such, the requirement for itemised notice should be maintained even for cases of processing on the grounds of deemed consent.

[11] https://www.omidyarnetwork.in/insights/innovating-for-the-next-half-billion

7. Obligation of DF to ensure data quality

Sec. 9(2) of the Bill creates an obligation on DFs, to take reasonable efforts to ensure completeness and accuracy of PD if it is likely to be used to make decisions that will affect the DP to whom it pertains, or if it is likely to be shared with other DFs.

This is a welcome move, and it is also appropriately phrased ("reasonable efforts"). It should be read in conjunction with **Sec. 9(3)**, which obliges DFs to implement appropriate technical and organisational measures to ensure adherence with the Bill/Act as a whole.

Depending on existing practices and levels of capacity, as well as the volume of PD handled, different DFs may require greater amounts of time and investment to achieve these outcomes. Subsequent rules and guidelines may seek to address prioritisation and provision of time periods for compliance with this obligation.

8. Obligation of DF to notify in case of PD breach

Sec. 9(4) of the Bill obliges DFs to adopt reasonable security safeguards to prevent data breaches.

Sec 9(5) further requires a DF to notify the Data Protection Board as well as every affected DP in the event of any breach of PD.

This is consistent with the principle of adequate safeguards as discussed in *Puttaswamy*, and is a necessary measure to enable both government agencies and DPs to take adequate measures to respond and mitigate harm in case of such breaches. As above, it should be read in conjunction with **Sec. 9(3)**, and the Government of India may consider establishing standard processes and mechanisms for such reporting, especially to enable DFs with limited resources or capacity to comply with this obligation.

A related matter is that while **Sec. 25** of the Bill (read with **Schedule 1**) lays down financial penalties around security lapses and breaches, there is no provision for compensation to affected DPs. Read together with the narrowed definition[12] of harms in **Sec. 2(10)**[13], this limits the range of remedies available to a DP affected as a result of such breaches. This gap may be addressed in the present Bill; it can also be addressed in delegated legislation, or through other legislations.

[12] The PDP Bill, 2019,Sec 3(20):
"harm" includes—
(i) bodily or mental injury;
(ii) loss, distortion or theft of identity;
(iii) financial loss or loss of property;
(iv) loss of reputation or humiliation;
(v) loss of employment;
(vi) any discriminatory treatment;
(vii) any subjection to blackmail or extortion;
(viii) any denial or withdrawal of a service, benefit or good resulting from an evaluative decision about the data principal;
(ix) any restriction placed or suffered directly or indirectly on speech,movement or any other action arising out of a fear of being observed or surveilled;"

[13] **Sec 2(10)** defines harms as
""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."

9. Obligation of DF to anonymise or delete PD

Sec. 9(6) of the Bill obliges DFs to delete or anonymise PD "as soon as" the purpose for its retention (as identifiable / PD) can be reasonably assumed to longer be served by such data, and such retention is not required for other legal or business purposes.

This is broadly consistent with the "Right to be Forgotten" as envisaged by the Srikrishna Committee, and is a welcome move. The definition of "business purposes" remains vague, and it would be helpful if acceptable business purposes in the context of this clause were to be specified.

The rationale for exempting instrumentalities of the State from this provision is unclear. We discuss this further in our comments on Sec. 18, below.

10. Right of DP to information

Sec. 12 of the Bill gives a DP the right to seek, from any DF, information about what PD of said DP this DF may have collected, processed, or shared, along with certain details (the categories of data, who it was shared with, etc.)

This is an excellent provision, and the primary mechanism that compensates for the narrowing of the Notice requirement in **Sec. 6**. It is entirely consistent with the idea of a DP as an individual having ultimate control over their PD and its use and dispositions.

In order to be more consistent with the principles of legality and legitimate aim/purpose, as also with the globally-recommended practice of purpose limitation, the information required to be shared by the DF under this provision should extend to the purpose of processing, and the legal basis / authority for such processing.

Further, the provision of information must be initiated by the DF themselves under certain circumstances, notably when making changes to (updating / deleting) PD.

- In cases where the grounds for processing is consent, any such changes, when not initiated by the DP, must be made with the consent of the DP as well; for this, the DF must notify the DP of such changes and the basis for making them.
- In cases where the grounds for processing is deemed consent, the DF should still notify the DP of such changes and the basis for making them.
- In either event, the DF must maintain an auditable and non-repudiable log of all such changes, so that it is possible to trace when and why a change was made, and potentially to reverse changes (short of deletion) in case they are later found to be erroneous.

Further, as noted above, various DFs may require time and support to bring their systems and processes in line with this requirement. Subsequent guidelines and rules may consider prioritisation of specific categories of DFs, setting timelines for compliance, and creation of such support mechanisms.

11. Right of DP to correction, erasure, and grievance redressal

Sec. 13 of the Bill gives a DP the right to seek updation or correction of their PD, as also erasure of their PD (as long as retention is not required for some legal purpose).

Sec. 14 further gives the DP the right to "readily-available means" of registering a grievance with a DF, and to escalate such complaints to the Data Protection Board in case they do not receive a satisfactory response within 7 days.

These provisions are consistent with the concept of a Data Principal as having ultimate control over their PD, its use and dispositions. They embody some of the rights of the DP envisaged by the Srikrishna Committee.

Sec. 13 forms a comprehensive set with Secs. **9(2)** and **9(6)**. The intent of **Sec. 14** would be better served if a corresponding obligation (to provide grievance redressal mechanisms, to communicate information about such mechanisms to DPs, etc.) were to be added u/**Sec. 9** as well.

12. Right of DP to nominate

Sec. 15 of the Bill gives the DP the right to nominate an individual who may, in the event of the death of incapacity of the DP, exercise the rights of the DP over their data.

This is a laudable innovation in this draft of the Bill. It is consistent with the "Right to be Forgotten"[14] – one might even describe it as the right of the DP to be remembered, on terms defined by the DP. It is a well-founded provision, which recognises the fact that individuals leave a "digital legacy" (e.g. on social media, on search engines), and that it is the right of each individual to determine what they want this legacy to be.

While the provisions of the "Right to be Forgotten" as envisaged in previous drafts are not included within the scope of the Bill, the right to nominate would allow for implementation of posthumous rights over data protection and privacy of the DP.

[14] Section 20 of the PDP Bill, 2019.
"(1) The data principal shall have the right to restrict or prevent the continuing disclosure of his personal data by a data fiduciary where such disclosure—
(a) has served the purpose for which it was collected or is no longer necessary for the purpose;
(b) was made with the consent of the data principal under section 11 and such consent has since been withdrawn; or
(c) was made contrary to the provisions of this Act or any other law for the time being in force."

13. Right of DP to data portability

This was included in previous drafts of the Bill[15], and has been dropped from the current draft. The rationale for this exclusion is not clear, as the concept of a Data Principal should extend to being able to move their PD from one DF to another. A provision to this effect should be incorporated into the present Bill.

14. Exemptions to instrumentalities of the State

Sec. 18(2a) grants the Central Government the power to, by notification, exempt from application of any provisions of this law, the processing of PD by an 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.*"

Such a provision has been consistently criticised in previous drafts of the Bill[16]. As the prevailing law is the *Puttaswamy* judgment, even exemptions to any instrumentality of the State must comply with the four-fold test laid down there.

A blanket exemption provision as envisaged in this section will be *ultra vires*; in the event that the Bill is adopted, this provision is likely to be challenged in court and struck down. A more specific and rigorous procedure for exemptions may be specified. The exemption under **Sec. 18(1c)**[17] may also be made subject to this specific procedure.

---

[15] Sec 19 of the PDP Bill, 2019;
"(1) Where the processing has been carried out through automated means, the data principal shall have the right to—
(a) receive the following personal data in a structured, commonly used and machine-readable format—
(i) the personal data provided to the data fiduciary;
(ii) the data which has been generated in the course of provision of services or use of goods by the data fiduciary; or
(iii) the data which forms part of any profile on the data principal, or which the data fiduciary has otherwise obtained; and
(b) have the personal data referred to in clause (a) transferred to any other data fiduciary in the format referred to in that clause."

[16] Personal Data Protection Bill: Exemptions for government agencies worry experts - The Economic Times

[17] Sec. 18(1) states that "*The provisions of Chapter 2 (except sub-section (4) of section 9), Chapter 3, and Section 17 of this Act shall not apply where:* …(c) *personal data is processed in the interest of prevention, detection, investigation or prosecution of any offence or contravention of any law.*"

15. Specific Exemptions to Secs. 6, 9(6), and 12

Sec. 18(3) enables the Government of India to, by notification, exempt any DF from the obligation to provide notice u/**Sec 6**, delete or anonymise data u/**Sec. 9(6)**, and/or to provide information about data collected, processed, or shared with DPs u/**Sec. 12**.

Sec. 18(4) further exempts any instrumentality of the state from the obligation to delete or anonymise data u/**Sec. 9(6)**.

The above exemptions create inconsistency with the principles of Legitimate Aim/Purpose and Proportionality, as well as with the globally-recommended best practices of data minimisation[18] and purpose limitation[19].

Provisions of notice, anonymisation, and deletion should apply to all DFs, including all instrumentalities of the State. This is even more true of the requirements u/**Sec. 12**, to provide information to DPs about what data about them is held, processed, or shared. As noted above, Sec. 12 is one of the most important provisions in this Bill, and allowing exemptions to its terms will dilute the entire scheme of the Bill itself.

Where there are considerations of scale, allowances may be made in terms of the mode, timelines, etc. Provision of notice, obligations to delete or anonymise PD, and provide information on what PD is stored, processed, or shared are essential for DPs to exercise agency and control over their data, and no such exemption should be made.

[18] ISO 2011 - *Data minimization: minimizing the personal information, which is processed and the number of privacy stakeholders and people to whom personal information is disclosed or who have access to it.*
GDPR - Principle No. 3 - *'Data minimization: personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.'*

[19] GDPR, Principle No. 2 - *'Purpose limitation: personal data shall be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.'*

16. Data Protection Board

Sec. 19 of the Bill presents the structure and composition of the Data Protection Board.

The section reserves the Board's composition and functioning to be prescribed by future rules created by the Government of India. This is not ideal; given the role and powers of the Board, it is worth presenting these details in the Bill itself, so that they may be debated in Parliament and amended as necessary. This will also enhance the legislative standing of the Board – a key consideration, given the primacy given in *Puttaswamy* to the legal basis for decisions that affect privacy.

In any event, when formulating such rules, the independence of the Board should be of paramount importance. This could be achieved, for instance, by including experienced members from the fields of data protection, information technology, data management, data science, data security, cyber and internet laws, etc., who are not on the payroll of the Government of India, or not otherwise closely affiliated with the State.

The term in office of members, their terms of service, and the process of selection should be published in advance, and then adhered to during that term. More broadly, globally recommended best practices on institutional and regulatory independence may be studied and incorporated in creating the Board.

Sec. 21 of the Bill lays out the processes to be followed by the Board in order to ensure Compliance with provisions of the Bill/Act.

One provision that may be considered as part of this section is requiring reporting by DFs (or by some sub-category of DFs) to the Board. This can again be paired with inclusion of a suitable section in Chapter 2 of the Bill. The Board can use these reports as a basis for identifying cases that require inquiry. This will incentivise DFs to adopt suitable processes and safeguards as needed to ensure compliance with the Bill/Act.

About eGovernments Foundation

Headquartered in Bengaluru, Karnataka, eGovernments Foundation (**eGov**) is a non-profit that leverages the power of digital public goods to enhance local government capacity to deliver public services and welfare to their residents.

eGov was founded in 2003 as a collective of technologists, strategists, and policy professionals committed to solving societal challenges. We are problem-solvers and responsible builders of communities and ecosystems, motivated by a sense of responsibility for making countries better and improving the lives of our fellow people.

We work on three strategic pillars: public digital platforms, enabling policies, and open ecosystems. We believe that technology is only an enabler; to have a sustainable impact at scale, we tap into the collective energy of the ecosystem to enact enabling policies, understand local needs, and build local capacity to solve local problems.

We work with different stakeholders in the ecosystem to catalyse this collective energy. Our impact framework is based on the contribution of digital public infrastructures to transform the experience of living and working for each stakeholder.

For more information about eGov, please visit our website www.egov.org.in

The above comments were prepared by:

1. Manish Srivastava, Chief Technology Officer
2. Ameya Ashok Naik, Head of Policy & Advocacy
3. Brinda Lashkari, Associate (Data Policy)