

MEMBERS' REFERENCE SERVICE

LARRDIS

LOK SABHA SECRETARIAT

NEW DELHI



LEGISLATIVE NOTE

For the use of Members of Parliament

NOT FOR PUBLICATION

No.34 /LN/Ref./Dec/2022

THE DIGITAL PERSONAL DATA PROTECTION BILL, 2022

- ❖ The Centre on 3rd August, 2022 withdrew the [Personal Data Protection \(PDP\) Bill, 2019](#) to replace it with a new bill with a 'comprehensive framework' and 'contemporary digital privacy laws'.
- ❖ The new Bill "[The Digital Personal Data Protection Bill 2022](#)" has been circulated for public comments by 17th December, 2022.
- ❖ Over the years, rapid technological advances have led to large volumes of data being generated through various activities.
- ❖ Data is becoming more and more valuable and skills and opportunities for retrieving different types of personal data are evolving extremely fast.
- ❖ Unauthorized, careless or ignorant processing of personal data can cause great harm to persons and to companies this required need for protection of personal data

Brief History of the Bill:

- ❖ On 24th August, 2017 a nine Judge Constitutional Bench of the Supreme Court in the matter of [Justice K.S. Puttaswami and another Vs. Union of India](#) [WP 494 of 2012] while delivering its judgment, declared "privacy" as a fundamental right under article 21 of the Constitution.
- ❖ Consequent to the Supreme Court declaring "privacy" as a fundamental right under article 21 of the Constitution and calling for bringing out a robust data protection regime, the Government, in July, 2017, constituted a "Committee of Experts on Data Protection" chaired by Justice B.N. Srikrishna to examine the issues relating to data protection
- ❖ The Personal Data Protection Bill, 2019 was introduced in the Lok Sabha on 11.12.2019 and the same day it was referred to Joint Committee on 'The Personal Data Protection Bill, 2019'.
- ❖ The Joint Committee on Personal Data Protection Bill, 2019, headed by Shri P.P. Chaudhary, MP, presented their report on 16.12.2021.

Prepared by Shri Abhishek Thakur, Assistant Research Officer under the supervision of Shri S.H. Baite, Director (23034536) and Shri Pulin Bhutia, Joint Secretary (2303 4656/5396) of Lok Sabha Secretariat.

I. Background

Over the years, rapid technological advances have led to large volumes of data being generated through various activities, and increasing reliance of businesses on data-driven decision making. Large-scale collection and usage of data by the government for provision of State benefits have also been enabled. One example of this is the biometric identification and verification system of Aadhaar that enables the government to ensure targeted delivery of State benefits, such as subsidies. Data is becoming more and more valuable and skills and opportunities for retrieving different types of personal data are evolving extremely fast.

Therefore, unauthorized, careless or ignorant processing of personal data can cause great harm to persons and to companies. To ensure that personal data is secure, it's important to know what data is being processed, why it's being processed and on what grounds. In addition, it is also important to identify which safety and security measures are in use. The need for protection of personal data is required to be understood in this context.

II. Objective of the Bill

The objective of the Digital Personal Data Protection Bill, 2022 is 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.

Salient Features of the Bill

1. Definitions under the DPDP Bill

- Data Fiduciary: Any person who alone or in conjunction with other persons determines the purpose and means of the processing of Personal Data.
- Data Principal: 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.
- Personal Data: Any data about an individual who is identifiable by or in relation to such data.

2. Applicability of the DPDP Bill

- The DPDP Bill will apply to the processing of Personal Data collected within the territory of India where: (i) such Personal Data is collected from Data Principals online; and (ii) such Personal Data collected offline, is digitized.
- The DPDP Bill will also apply to processing of Personal Data outside of India, if such processing is in connection with profiling people in India or offering goods and services to Data Principals in India. Profiling here means "any form of processing of Personal Data that analyses or predicts aspects concerning the behaviour, attributes or interests of a Data Principal."
- The DPDP Bill does not apply to: (i) non-automated processing of Personal Data; (ii) offline Personal Data; (iii) Personal Data processed by an individual for any personal or domestic purpose; (iv) Personal Data about an individual that is contained in a record that has been in existence for at least 100 years.

3. Obligations of Data Fiduciaries

- Seek Consent: Personal Data can only be processed with consent or deemed consent. When seeking consent, or as soon as it is reasonably practicable, Data Fiduciaries must give the users a notice that describes what Personal Data will be collected and for what purpose. The consent given by the Data Principals must be freely given, specific, informed and unambiguous indication of the Data Principal's agreement to the processing of its Personal Data for the specified purpose. Data Fiduciaries cannot seek consent for anything that will infringe the provisions of the DPDP Bill. The contact details of a data protection officer must be mentioned when seeking consent.
- Withdrawal of Consent: Users should have their right to withdraw consent at any time with the same ease as they were able to give consent.
- No Conditional Services: If a Data Fiduciary has a contract with a user to deliver a service or good, the same cannot be made conditional on the consent to the processing of any Personal Data not necessary for performing that contract.
- Accuracy of Data: Data Fiduciaries are required to make reasonable efforts to ensure that Personal Data processed by or on behalf of the Data Fiduciary is accurate and complete, especially if the Personal Data is to be used to make a decision that affects the Principal or if it is to be disclosed to another Data Fiduciary.
- Notifying Data Breaches: In the event of a Personal Data breach, the Data Protection Board and the concerned Data Principals must be notified in such manner as may be prescribed.
- Retention of Personal Data: A Data Fiduciary must cease to retain Personal Data, or remove the means by which the Personal Data can be associated with particular Data Principals, as soon as it is reasonable to assume that the purpose

for which such Personal Data was collected is no longer being served by its retention and retention is no longer necessary for legal or business purposes.

- Appointing a Data Protection Officer: Data Fiduciaries must publish the business contact information of a Data Protection Officer, if applicable, or a person who is able to answer on behalf of the Data Fiduciary, the Data Principal's questions about the processing of its personal data in a format, as may be prescribed.
- Grievance Redressal Mechanism: Data Fiduciaries must have in place a procedure and effective mechanism to redress the grievances of Data Principals.

4. Processing Children's Data

Data Fiduciaries must obtain verifiable parental consent, before any Personal Data of a child is processed. Data Fiduciaries shall not undertake any processing of Personal Data that is likely to cause harm to a child.

5. Rights of Data Principals

- Right to Information: The Data Principal has the right to know: (i) if a Data Fiduciary is processing or has processed their Personal Data; (ii) if yes, a summary of the Personal Data being processed and the processing activities undertaken by the Data Fiduciary; (iii) the identities of all those with whom Personal Data has been shared along with the categories of Personal Data so shared.
- Right to Correction and Erasure of Personal Data: The Data Principal has the right to request for correction and erasure of its Personal Data in accordance with the applicable laws and in such manner as may be prescribed. Erasure requests can be denied if data is necessary to be retained for legal purposes.

- Right of Grievance Redressal: Data Principals have the right to register a grievance with a Data Fiduciary.

6. **What is Deemed Consent?**

A Data Principal is deemed to have given consent to the processing of its Personal Data if such processing is necessary for the following purposes: (i) when the Data Principal voluntarily provides their data to the Data Fiduciary and it is reasonably expected that they would provide such Personal Data; (ii) when the state or its agencies need to perform any function under any law, provide any service or benefit to the Data Principal, or issue any certificate, license, or permit for any action or activity of the Data Principal; (iii) for compliance with any judgment or order issued under any law; (iv) for responding to a medical emergency involving a threat to the life or immediate threat to the health of the Data Principal or any other individual; (v) for taking measures to provide medical treatment or health services to any individual during an epidemic, outbreak of disease, or any other threat to public health; (vi) for taking measures to ensure the safety of, or provide assistance or services to any individual during any disaster, or any breakdown of public order; (vii) for the purposes related to employment, including prevention of corporate espionage, maintenance of confidentiality of trade secrets, intellectual property, classified information, recruitment, termination of employment, provision of any service or benefit sought by a Data Principal who is an employee, verification of attendance and assessment of performance; (viii) for the sake of public interest and for any fair and reasonable purpose as may be prescribed.

7. **Transfer of Personal Data outside India**

Data Fiduciaries can transfer Personal Data outside of India to countries or territories that have been approved by the central government in accordance with such terms and conditions as may be specified.

8. Data Protection Board of India ("DPBI")

The DPDP Bill provide for establishment of the DPBI, an independent body, to *inter alia*, determine non-compliance with the provisions of the DPDP Bill and impose appropriate penalties. In the event of a Personal Data breach, the DPBI can direct the Data Fiduciary to adopt any urgent measures to remedy such breach or mitigate any harm caused to Data Principals.

9. Penalties and Offences

The DPDP Bill prescribes the following penalties for non-compliance under the DPDP Bill:

Subject Matter of Non-Compliance	Penalty
Failure to take reasonable security safeguards to prevent Personal Data breach.	Upto Rs. 250 Crores
Failure to notify the Board and affected Data Principals of a personal data breach.	Upto Rs. 200 Crores
Non-fulfilment of additional obligations in relation to processing data of children.	Upto Rs. 200 Crores
Non-fulfilment of additional obligations of Significant Data Fiduciary.	Upto Rs. 150 Crores
Violation of user duties	Upto Rs. 10,000
For all other non-compliances under DPDP Bill	Upto Rs. 50 Crores

While the DPDP Bill has retained and modified some of the provisions from the earlier draft legislations, there are certain fresh provisions as well that are sought to be introduced. A data protection legislation has been in the works for many years now and the trajectory of data protection in India has taken many turns and it will be interesting to see these draft legislations culminate into the final law of the land.

References:

- i. https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Protection%20Bill%2C%202022_0.pdf
- ii. <https://www.meity.gov.in/writereaddata/files/Explanatory%20Note-%20The%20Digital%20Personal%20Data%20Protection%20Bill%2C%202022.pdf>
- iii. https://www.meity.gov.in/writereaddata/files/Notice%20-%20Public%20Consultation%20on%20DPDP%202022_1.pdf
- iv. https://www.meity.gov.in/writereaddata/files/MeitY_AR_English_2021-22.pdf P20
- v. <https://indianexpress.com/article/explained/explained-economics/india-draft-digital-privacy-law-data-protection-laws-8279199/>
- vi. <https://thewire.in/rights/data-protection-bill-2022>
- vii. http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf
(English)
- viii. [Report of the Joint Committee on the Personal Data Protection Bill, 2019](#)