Legislative Brief

The Draft Digital Personal Data Protection Bill, 2022

The Draft Digital Personal Data Protection Bill, 2022 was released by the Ministry of Electronics and Information Technology for public feedback on November 18, 2022.

Saket Surya
saket@prsindia.org

Omir Kumar
omir@prsindia.org

December 30, 2022

Highlights of the Bill

- The Bill will apply to the processing of digital personal data within India where such data is collected online, or collected offline and is digitised. It will also apply to such processing outside India, if it is for offering goods or services or profiling individuals in India.
- Personal data may be processed only for a lawful purpose for which an individual has given consent. Consent may be deemed in certain cases.
- Data fiduciaries will be obligated to maintain the accuracy of data, keep data secure, and delete data once its purpose has been met.
- The Bill grants certain rights to individuals including the right to obtain information, seek correction and erasure, and grievance redressal.
- The central government may exempt government agencies from the application of provisions of the Bill in the interest of specified grounds such as security of the state, public order, and prevention of offences.
- The central government will establish the Data Protection Board of India to adjudicate non-compliance with the provisions of the Bill.

Key Issues and Analysis

- Exemptions to data processing by the State on grounds such as national security may lead to data collection, processing and retention beyond what is necessary. This may violate the fundamental right to privacy.
- The Bill accords differential treatment on consent and storage limitation to private and government entities performing the same commercial function such as providing banking or telecom services. This may violate the right to equality of the private sector providers.
- The central government will prescribe the composition, and manner and terms of appointments to the Data Protection Board of India. This raises a question about the independent functioning of the Board.
- The Bill does not grant the right to data portability and the right to be forgotten to the data principal.
- The Bill requires all data fiduciaries to obtain verifiable consent from the legal guardian before processing the personal data of a child. To comply with this provision, every data fiduciary will have to verify the age of everyone signing up for its services. This may have adverse implications for anonymity in the digital space.

PART A: HIGHLIGHTS OF THE BILL

Context

Personal data is information that relates to an identified or identifiable individual. Businesses as well as government entities process personal data for delivery of goods and services. Processing of personal data allows understanding preferences of individuals, which may be useful for customisation, targeted advertising, and developing recommendations. Processing of personal data may also aid law enforcement. Unchecked processing may have adverse implications for the privacy of individuals, which has been recognised as a fundamental right.[1] It may subject individuals to harm such as financial loss, loss of reputation, and profiling.

Currently, India does not have a standalone law on data protection. The usage of personal data is regulated under the Information Technology (IT) Act, 2000.[2,3] It has been observed that this framework is not adequate to ensure the protection of personal data.[1] In 2017, the central government constituted a Committee of Experts on Data Protection chaired by Justice B. N. Srikrishna to examine issues relating to data protection in the country. The Committee submitted its report in July 2018.[4] Based on the recommendations of the Committee, the Personal Data Protection Bill, 2019 was introduced in Lok Sabha in December 2019.[5] The Bill was referred to a Joint Parliamentary Committee which submitted its report in December 2021.[2] In August 2022, the Bill was withdrawn from Parliament. In November 2022, the Ministry of Electronics and Information Technology released the Draft Digital Personal Data Protection Bill, 2022 for public feedback.[6]

Key Features

- **Applicability:** The Bill will apply to the processing of digital personal data within India where such data is: (i) collected online, or (ii) collected offline and is digitised. It will also apply to the processing of personal data outside India, if it is for offering goods or services or profiling individuals in India. Personal data is defined as any data about an individual who is identifiable by or in relation to such data. Processing has been defined as an automated operation or set of operations performed on digital personal data. It includes collection, storage, use, and sharing.
- **Consent:** Personal data may be processed only for a lawful purpose for which an individual has given consent. A notice must be given before seeking consent. Notice should contain details about the personal data to be collected and the purpose of processing. Consent may be withdrawn at any point in time. Consent will be deemed given where processing is necessary for: (i) performance of any function under a law, (ii) provision of service or benefit by the State, (iii) medical emergency, (iv) employment purposes, and (v) specified public interest purposes such as national security, fraud prevention, and information security. For individuals below 18 years of age, consent will be provided by the legal guardian.
- **Rights and duties of data principal:** An individual, whose data is being processed (data principal), will have the right to: (i) obtain information about processing, (ii) seek correction and erasure of personal data, (iii) nominate another person to exercise rights in the event of death or incapacity, and (iv) grievance redressal. Data principals will have certain duties. They must not: (i) register a false or frivolous complaint, (ii) furnish any false particulars, suppress information, or impersonate another person in specified cases. Violation of duties will be punishable with a penalty of up to Rs 10,000.
- **Obligations of data fiduciaries:** The entity determining the purpose and means of processing, called data fiduciary, must: (i) make reasonable efforts to ensure the accuracy and completeness of data, (ii) build reasonable security safeguards to prevent a data breach and inform the Data Protection Board of India and affected persons in the event of a breach, and (iii) cease to retain personal data as soon as the purpose has been met and retention is not necessary for legal or business purposes (storage limitation). The storage limitation requirement will not apply in case of processing by government entities.
- **Transfer of personal data outside India:** The central government will notify countries where a data fiduciary may transfer personal data. Transfers will be subject to prescribed terms and conditions.
- **Exemptions:** Rights of the data principal and obligations of data fiduciaries (except data security) will not apply in specified cases including prevention and investigation of offences, and enforcement of legal rights or claims. The central government may, by notification, exempt certain activities from the application of provisions of the Bill. These include: (i) processing by government entities in the interest of the security of the state and public order, and (ii) research, archiving, or statistical purposes.
- **Data Protection Board of India:** The central government will establish the Data Protection Board of India. Key functions of the Board include: (i) monitoring compliance and imposing penalties, (ii) directing data fiduciaries to take necessary measures in the event of a data breach, and (iii) hearing grievances made by affected persons. The central government will prescribe: (i) composition of the Board, (ii) selection process, (iii) terms and conditions of appointment and service, and (iv) manner of removal.
- **Penalties:** The schedule to the Bill specifies penalties for various offences such as: (i) up to Rs 150 crore for non-fulfilment of obligations for children and (ii) up to Rs 250 crore for failure to take security measures to prevent data breaches. Penalties will be imposed by the Board after conducting an inquiry.

PART B: KEY ISSUES AND ANALYSIS

Exemptions to the State may have adverse implications for privacy

Bill: Clauses 2(18), 8 and 18

Personal data processing by the State has been given several exemptions under the Bill. As per Article 12 of the Constitution, the State includes: (i) central government, (ii) state government, (iii) local bodies, and (iv) authorities and companies set up by the government. We discuss certain issues with these exemptions below.

The Bill may enable unchecked data processing by the State, which may violate the right to privacy

The Supreme Court (2017) has held that any infringement of the right to privacy should be proportionate to the need for such interference.[1] The exemptions may lead to data collection, processing, and retention beyond what is necessary. This may not be proportionate, and may violate the fundamental right to privacy.

The Bill empowers the central government to exempt processing by government agencies from any or all provisions, in the interest of aims such as the security of the state and maintenance of public order. None of the rights of data principals and obligations of data fiduciaries (except data security) will apply in certain cases such as processing for prevention, investigation, and prosecution of offences. The Bill does not require government agencies to delete personal data, after the purpose for processing has been met. Using the above exemptions, on the ground of national security, a government agency may collect data about citizens to create a 360-degree profile for surveillance. It may utilise data retained by various government agencies for this purpose. This raises the question whether these exemptions will meet the proportionality test.

For interception of communication on grounds such as national security, in *PUCL vs Union of India (1996),* the Supreme Court had mandated various safeguards including: (i) establishing necessity, (ii) purpose limitation, and (iii) storage limitation.[7,8] These are similar to the obligations of data fiduciaries under the Bill, the application of which has been exempted. The Srikrishna Committee (2018) had recommended that in case of processing on grounds such as national security and prevention and prosecution of offences, obligations other than fair and reasonable processing and security safeguards should not apply. It observed that obligations such as storage limitation and purpose specification, if applicable, would be implemented through a separate law. India does not have any such legal framework.

In the United Kingdom, the data protection law enacted in 2018, provides similar exemptions for national security and defence.[9] However, actions such as bulk processing of personal datasets by government agencies for intelligence and law enforcement activities are regulated under the Investigatory Powers Act, 2016.[10] A warrant for such action is issued by the Secretary of State (i.e., Home Minister), which requires prior approval by a Judicial Commissioner. Necessity and proportionality for such actions must be established. Data retention beyond the period of warrant is restricted. This law also provides for parliamentary oversight.

Processing without consent for preventing dissemination of false statements of fact

The Bill specifies "preventing dissemination of false statements of fact" as one of the public interest purposes for deemed consent. This raises the question about the need for such a ground. It may be argued that any harm or adverse implication due to such dissemination is already covered under grounds such as prevention of incitement of offence, public order, and security of the state. Mere expression or dissemination of false statements of fact may not be an offence under any law. The Supreme Court (2015) has held that speech can be limited on the grounds under the Constitution when it reaches the level of incitement.[11] Other forms of speech even if offensive or unpopular remain protected under the Constitution.[11]

Whether consent requirement should apply where government agencies provide commercial services

The Bill provides that consent will be deemed to have been obtained for processing of data to provide benefits and services by the State and its instrumentalities. Consent requirement provides individuals control over the extent of data collection and processing. Government and public sector utilities owned by it provide various services to individuals such as health, banking, telecom, and electricity. Thus, government health departments and companies such as SBI, BSNL, and state discoms need not take consent from individuals for processing their data. The question is whether this is appropriate.

The Srikrishna Committee (2018) had observed that there is an imbalance of power between the individual and the State if the State is the only provider of a service or benefit.[4] A data principal does not have a choice to refuse consent if he needs the benefit or service.[4] In such a situation, the idea of requiring consent is meaningless.[4] However, it is unclear why such an exemption has been extended to all services provided by the State, including commercial services.

The Bill accords differential treatment towards public and private entities performing the same function

As discussed above, a government company can process the personal data of its customers without obtaining their consent, and it may retain the data for an unlimited period. However, its competitors in the private sector would have to comply with these requirements. Thus, these provisions will result in differential treatment towards public and private entities performing the same function. This may violate the right to equality protected under Article 14 of the Constitution.

Implications of exemption from data fiduciary obligations

For certain public interest purposes such as national security and law enforcement, the consent requirement would be meaningless due to the covert nature of such actions. However, it may be argued that other principles should continue to apply to safeguard privacy. As these obligations do not apply, a data breach at the National Crime Records Bureau or the Unique Identification Authority of India need not be reported as per the mechanism under the Bill. Data collected by police for the investigation and prosecution of one offence may be utilised for other purposes. Similarly, where personal data is processed to enforce legal rights or claims (for example, the right to food under the National Food Security Act, 2013), the obligation to ensure the accuracy and completeness of data will not apply. The rights of the data principal including the right to seek correction of personal data and the right of grievance redressal will also not apply. Thus, the Bill does not provide an individual with any recourse, where legal rights may be denied based on the processing of inaccurate data. Such recourse may have to be provided in the specific laws.

Bill may not ensure independence of the Data Protection Board of India

Bill: Clauses 19, 20 and 21(1)

The Bill requires the central government to set up the Data Protection Board of India. It provides that the Board will function as an independent body. The composition, terms of appointment, and manner of removal of the members will be prescribed by the central government. The question is whether these details should be provided in the principal legislation to ensure the independence of the Board.

Key functions of the Board include: (i) determining non-compliance with provisions of the Bill, (ii) imposing penalties, and (iii) directing data fiduciaries to adopt necessary measures in case of a data breach. Often, government entities may be subject to such investigations, as they process a significant amount of personal data. This may raise questions whether the Board will be able to function independently in such matters.

The Personal Data Protection Bill, 2019 sought to provide for an independent Data Protection Authority. The details such as composition, manner and terms of appointment were specified in the Bill itself.[12] Acts establishing regulators such as the Telecom Regulatory Authority of India and the Competition Commission of India also specify such details.[13,14] In particular, they assure the term of service and restrict removal only on certain grounds such as abuse of position, conviction for an offence, unsound mind, and insolvency. Under the RTI Act, 2005, while the term of the members of the Central Information Commission may be prescribed by the central government, other details such as a selection committee to recommend appointments, qualification, and manner of removal have been specified in the Act.[15]

Right to data portability and the right to be forgotten not provided

The Bill does not provide for the right to data portability and the right to be forgotten. The 2018 Draft Bill and the 2019 Bill introduced in Parliament had sought to provide for these rights.[16,17] The Joint Parliamentary Committee, examining the 2019 Bill, recommended retaining these rights.[2] General Data Protection Regulation (GDPR) of the European Union also recognises these rights.[18] The Srikrishna Committee (2018) observed that a strong set of rights of data principals is an essential component of a data protection law.[4] These rights are based on principles of autonomy, transparency, and accountability to give individuals control over their data.[4]

Right to data portability: The right to data portability allows data principals to obtain and transfer their data from data fiduciary for their own use, in a structured, commonly used, and machine-readable format. It gives the data principal greater control over their data and can facilitate the migration of data from one data fiduciary to another. One possible concern has been that access to such information may reveal trade secrets of the data fiduciary.[4] The Srikrishna Committee (2018) had recommended that to the extent it is possible to provide the information without revealing such trade secrets, the right must be guaranteed.[4] The Joint Parliamentary Committee had observed that trade secrets cannot be a ground to deny data portability, and it may only be denied on the ground of technical feasibility.[2]

Right to be forgotten: The right to be forgotten refers to the right of individuals to limit the disclosure of personal data on the internet.[4] The Srikrishna Committee (2018) observed that the right to be forgotten is an idea that attempts to instil the limitations of memory into an otherwise limitless digital sphere.[4] However, the Committee also highlighted that this right may need to be balanced with competing rights and interests. Exercise of this right may interfere with someone else's right to free speech and expression and the right to receive information.[1] Its applicability may be decided on factors such as the sensitivity of the personal data to be restricted, the relevance of the personal data to the public, and the role of the data principal in public life.[1]

Additional provisions for children

Bill: Clauses 2(3) and 10

Additional obligations apply to processing data of children. We discuss issues with these provisions below.

Taking verifiable parental consent may require verification of everyone's age on digital platforms

The Bill requires all data fiduciaries to obtain verifiable consent from the legal guardian before processing the personal data of a child. To comply with this provision, every data fiduciary will have to verify the age of everyone signing up for its services. It will be needed to determine whether the person is a child, and thereby

obtain consent from their legal guardian. This may have adverse implications for anonymity in the digital space. Currently, several data fiduciaries require a declaration from users that they are above the minimum required age to give consent. As there is no verification beyond a declaration, a child may give a false declaration and use the services. The way to get past this gap is to require proof of age, which will compromise anonymity.

Definition of child different from other jurisdictions

Data fiduciaries have certain additional obligations to minimise harm to children. While it is an accepted principle that the processing of a child's data should be subject to greater protection, there are differences in how different jurisdictions define a child for giving consent for the processing of personal data. Under the Bill, a child has been defined as a person below 18 years of age. In USA and UK, persons above the age of 13 can give consent for the processing of personal data.[19,20] GDPR of the European Union sets this age at 16, member countries may lower it up to 13.[21] The Srikrishna Committee (2018) had recommended that while determining the age of consent for children, factors such as the minimum age of 13 and maximum age of 18 and a single threshold for ensuring practical implementation, should be taken into account.[4] It noted that from the perspective of the full autonomous development of a child, 18 years may be too high.[4] However, to be consistent with the existing legal framework, the age of consent should be 18 years.[4] Under the Indian Contract Act, 1872, the minimum age to sign a contract is 18.[22]

Definition of 'harm'

Bill: Clause 2(10)

The Bill defines harm in relation to a data principal as: (i) any bodily harm, (ii) distortion or theft of identity, (iii) harassment, or (iv) prevention of lawful gain or causation of significant loss. We discuss certain issues with the above definition below.

The definition of harm may be narrow

The Personal Data Protection Bill, 2019 specified the following types of harm: (i) mental injury, (ii) loss of reputation or humiliation, (iii) discriminatory treatment, (iv) blackmail or extortion, (v) any observation or surveillance not reasonably expected by the data principal, and (vi) restriction of speech, movement, or any other action arising out of fear of being observed or surveilled.[23] The 2022 Draft Bill does not include these. The Joint Parliamentary Committee (JPC) recommended adding 'psychological manipulation that impairs the autonomy of the individual' to the list of harms in the 2019 Bill.[2] The 2022 Draft Bill does not provide for such harm. It is unclear whether the term 'harassment' included in the 2022 Draft Bill will include the types of harm discussed above. The JPC also recommended empowering the central government to prescribe other types of harms.[2] It reasoned that there may be considerations to identify new types of harms in the future. The Bill does not provide for such powers to the central government.

Lack of clarity on what constitutes a significant loss

Under the Bill, harm includes prevention of lawful gain or causation of significant loss. It is unclear what constitutes a significant loss. The Bill does not provide any guidance on determining the significance of loss.

Key differences between various drafts of the Data Protection Law

Table 1: Comparison of various drafts of the Data Protection Law

The Draft Personal Data Protection Bill, 2018	The Personal Data Protection Bill, 2019	Recommendations of the Joint Parliamentary Committee	The Draft Digital Personal Data Protection Bill, 2022
Scope and Applicability			
▪ Processing of personal data: (i) within India, (ii) also outside India if it is for business carried on, systematic offering of goods and services, or profiling individuals, in India	▪ Expands the scope under the 2018 Bill to include anonymised personal data	▪ Expands the scope under the 2018 Bill to include processing of non-personal data and anonymised personal data	▪ As compared to the 2018 Bill, removes the reference to business carried in India; also, does not cover offline personal data and non-automated processing
Reporting of data breaches			
▪ Fiduciary to notify the Data Protection Authority about a data breach, which is likely to cause harm, the Authority will decide whether to notify data principals or not	▪ Same as 2018 Bill	▪ All breaches, regardless of potential harm, must be reported to the Authority, within 72 hours	▪ Every personal data breach must be reported to the Data Protection Board of India and each affected data principal
Exemptions from provisions of the Bill for the security of the state, public order, prevention of offences etc.			
▪ Processing must be authorised pursuant to a law, and in accordance with the procedure established by law, and must be necessary and proportionate	▪ The central government, by order, may exempt agencies where processing is necessary or expedient, subject to certain procedure, safeguards, and oversight	▪ Adds that order should specify a procedure, which is fair, just, and reasonable	▪ The central government may exempt by notification; does not require any procedure or safeguards to be specified

The Draft Personal Data Protection Bill, 2018	The Personal Data Protection Bill, 2019	Recommendations of the Joint Parliamentary Committee	The Draft Digital Personal Data Protection Bill, 2022
Right to Data Portability and Right to be Forgotten			
▪ Data principal will have the right to data portability (to obtain data in interoperable format), and right to be forgotten (to restrict disclosure of personal data over internet)	▪ Provided for both rights	▪ Provided for both rights	▪ Not provided
Regulator			
▪ Provides for establishing: (i) the Data Protection Authority of India to regulate the sector, and (ii) the Appellate Tribunal.	▪ Same as 2018 Bill	▪ Same as 2018 Bill	▪ Provides for the Data Protection Board of India, whose primary function is to adjudicate non-compliance; no Appellate Tribunal
Transfer of personal data outside India			
▪ Every fiduciary to store at least one serving copy of personal data in India ▪ May be transferred outside India, if consent provided, to certain permitted countries or under contracts approved by the Authority ▪ Certain critical data can be processed only in India	▪ A copy of sensitive personal data should remain in India ▪ Certain sensitive personal data may be transferred only if explicit consent provided, no restriction on other personal data ▪ On critical personal data, same as 2018 Bill	▪ Adds that sensitive personal data will not be shared with foreign agencies or government, without prior approval of the central government	▪ Removes sensitive and critical personal data classification ▪ Provides that personal data may be transferred to countries notified by the central government, subject to prescribed terms and conditions

Sources: The Draft Personal Data Protection Bill, 2018 and The Draft Digital Personal Data Protection Bill, 2022 released by the Ministry of Electronics and Information Technology; The Personal Data Protection Bill, 2019 as introduced in Lok Sabha; Report of the Joint Parliamentary Committee on the Personal Data Protection Bill, 2019; PRS.

1. Justice K.S. Puttaswamy (Retd) vs. Union of India, W.P. (Civil) No 494 of 2012, Supreme Court of India, August 24, 2017.
2. Report of the Joint Committee on the Personal Data Protection Bill, 2019, December 2021.
3. The Information Technology Act, 2000.
4. 'A Free and Fair Digital Economy Protecting Privacy, Empowering Indians', Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, July 2018.
5. The Personal Data Protection Bill, 2019, as introduced in Lok Sabha.
6. The Draft Digital Personal Data Protection Bill, 2022, Ministry of Electronics and Information Technology, November 18, 2022.
7. Rule 419A, The Indian Telegraph Rules, 1951 issued under Section 7 (2) of the Indian Telegraph Act, 1885.
8. People's Union for Civil Liberties (PUCL) vs Union of India, Supreme Court of India, December 18, 1996.
9. Chapter 3, Data Protection Act, 2018, United Kingdom.
10. Part 6, 7, and 8, Investigatory Powers Act, 2016, United Kingdom.
11. Shreya Singhal vs Union of India, Writ Petition (Criminal) No. 167 Of 2012, Supreme Court of India, March 24, 2015.
12. Chapter IX, The Personal Data Protection Bill, 2019, as introduced in Lok Sabha.
13. Chapter II: Telecom Regulatory Authority of India, The Telecom Regulatory Authority of India Act, 1997.
14. Chapter III: Competition Commission of India, The Competition Act, 2002.
15 Chapter III: Central Information Commission, The Right to Information Act, 2005.
16. Clause 26, The Personal Data Protection Bill, 2018, as released by Ministry of Electronics and Information Technology.
17. Clause 19, The Personal Data Protection Bill, 2019, as introduced in Lok Sabha.
18. Article 20, General Data Protection Regulation, European Union.
19. Children's Online Privacy Protection Rule ("COPPA"), Federal Trade Commission, USA, as accessed on December 6, 2022.
20. Guide to Data Protection, Information, Information Commissioner's Office, United Kingdom, as accessed on December 6, 2022.
21. Article 8, General Data Protection Regulation, European Union.
22. Section 11, The Indian Contract Act, 1872.
23. Clause 3(20), The Personal Data Protection Bill, 2019, as introduced in Lok Sabha.