Legislative Brief

The Digital Personal Data Protection Bill, 2023

The Digital Personal Data Protection Bill, 2023 was introduced in Lok Sabha on August 3, 2023.

Saket Surya
saket@prsindia.org

August 4, 2023

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 in India.
- Personal data may be processed only for a lawful purpose upon consent of an individual. Consent may not be required for specified legitimate uses such as voluntary sharing of data by the individual or processing by the State for permits, licenses, benefits, and services.
- 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 on 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 does not regulate risks of harms arising from processing of personal data.
- The Bill does not grant the right to data portability and the right to be forgotten to the data principal.
- The Bill allows transfer of personal data outside India, except to countries notified by the central government. This mechanism may not ensure adequate evaluation of data protection standards in the countries where transfer of personal data is allowed.
- The members of the Data Protection Board of India will be appointed for two years and will be eligible for re-appointment. The short term with scope for re-appointment may affect the independent functioning of the Board.

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. Use of personal data is regulated under the Information Technology (IT) Act, 2000.[2,3] 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, a Draft Bill was released for public consultation.[6] In August 2023, the Digital Personal Data Protection Bill, 2023 was introduced in Parliament.[7]

Key Features

- **Applicability:** The Bill applies 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 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 wholly or partially 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 after obtaining the consent of the individual. A notice must be given before seeking consent. The 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 not be required for 'legitimate uses' including: (i) specified purpose for which data has been provided by an individual voluntarily, (ii) provision of benefit or service by the government, (iii) medical emergency, and (iv) employment. For individuals below 18 years of age, consent will be provided by the parent or 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, and (ii) furnish any false particulars 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, (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, (iii) inform the Data Protection Board of India and affected persons in the event of a breach, and (iv) erase personal data as soon as the purpose has been met and retention is not necessary for legal purposes (storage limitation). In case of government entities, storage limitation and the right of the data principal to erasure will not apply.
- **Transfer of personal data outside India:** The Bill allows transfer of personal data outside India, except to countries restricted by the central government through notification.
- **Exemptions:** Rights of the data principal and obligations of data fiduciaries (except data security) will not apply in specified cases. These include: (i) prevention and investigation of offences, and (ii) enforcement of legal rights or claims. The central government may, by notification, exempt certain activities from the application 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. Board members will be appointed for two years and will be eligible for re-appointment. The central government will prescribe details such as the number of members of the Board and the selection process. Appeals against the decisions of the Board will lie with TDSAT.
- **Penalties:** The schedule to the Bill specifies penalties for various offences such as up to: (i) Rs 200 crore for non-fulfilment of obligations for children, and (ii) 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 7, 17, Chapter II, Chapter III

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. There may be certain issues with such exemptions.

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] Exemptions for the State 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, the Supreme Court (1996) had mandated various safeguards including: (i) establishing necessity, (ii) purpose limitation, and (iii) storage limitation.[8,9] 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.[4] 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.[10] 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.[11] 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.

Whether overriding consent for purposes such as benefit, subsidy, license, and certificates is appropriate

The Bill overrides consent of an individual where the State processes personal data for provision of benefit, service, license, permit, or certificate. It specifically allows use of data processed for one of these purposes for another. It also allows use of personal data already available with the State for any of these purposes. Hence, it removes purpose limitation, which is one of the key principles for protection of privacy. Purpose limitation means data should be collected for specific purposes, and should be used only for that purpose.[4] The question is whether such exemptions are appropriate.

Since data taken for various purposes could be combined, this could allow profiling of citizens. On the other hand, if consent were required, individuals would have the autonomy and control over collection and sharing of their personal data.

The Bill does not regulate harm arising from processing of personal data

The Bill does not regulate risks of harms arising out of processing of personal data. The Srikrishna Committee (2018) had observed that harm is a possible consequence of personal data processing.[4] Harm may include material losses such as financial loss and loss of access to benefits or services.[4] It may also include identity theft, loss of reputation, discrimination, and unreasonable surveillance and profiling.[4] It had recommended that harms should be regulated under a data protection law.[4]

The Personal Data Protection Bill, 2019 had defined harm to include: (i) mental injury, (ii) identity theft, (iii) financial loss, (iv) reputational loss, (v) discriminatory treatment, and (vi) observation or surveillance not reasonably expected by the data principal.[12] The 2019 Bill required data fiduciaries to take measures to prevent, minimise, and mitigate risks of harm.[13] These included undertaking evaluation of these risks in impact assessments and audits.[13] It also granted the data principal the right to seek compensation from data fiduciary or data processor, where the data principal has suffered harm.[14] The Joint Parliamentary Committee, examining the 2019 Bill, had recommended retaining the provisions regarding harm arising from processing of personal data.[2] General Data Protection Regulation (GDPR) of the European Union also regulates risks of harm and provides for compensation to the data principal in the event of harm.[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 provided for these rights.[16,17] The Joint Parliamentary Committee, examining the 2019 Bill, recommended retaining these rights.[2] GDPR 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. It may facilitate the migration of data from one data fiduciary to another. One possible concern has been that it 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 the right 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 their 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]

Adequacy of protection in case of cross-border transfer of data

Bill: Clause 16 (1)

The Bill provides that the central government may restrict the transfer of personal data to certain countries through a notification. This implies the transfer of personal data to all other countries without any explicit restrictions. This question is whether this mechanism will provide adequate protection.

The aim of the regulation of transfer of personal data outside India is to safeguard the privacy of Indian citizens.[2] In the absence of robust data protection laws in another country, data stored there may be more vulnerable to breaches or unauthorised sharing with foreign governments as well as private entities. The 2019 Bill required that for certain categories of data, transfer to a country should be allowed only if it provides for adequate level of protection.[19] The 2022 Draft Bill took a different approach, with the central government notifying countries where any personal data may be transferred.[20] Both these mechanisms require a case-by-case evaluation of the standards in every country to which data may be transferred. The mechanism to restrict countries selectively does not require such exhaustive evaluation.

Shorter appointment term may impact independence of the Board

Bill: Clause 20 (2)

The Bill provides that members of the Data Protection Board of India will function as an independent body. Members will be appointed for two years and will be eligible for re-appointment. A short term with the scope for re-appointment may affect independent functioning of the Board.

Key functions of the Board are monitoring compliance, carrying out investigations, and adjudging penalties. In case of Tribunals, the Supreme Court (2019) had observed that short-term along with the provisions of re-appointment increases influence and control of the Executive.[21] Regulatory authorities with adjudicatory role such as the Central Electricity Regulatory Commission and the Competition Commission of India have a term of five years under respective Acts.[22,23] In case of TRAI, the term of appointment is three years. [24] The term of appointment to SEBI is five years, specified through Rules.[25]

Additional provisions for children

Bill: Clauses 2 (f) and 9

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

Definition of child different from other jurisdictions

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.[26,27] GDPR of the European Union sets this age at 16, member countries may lower it up to 13.[28] The Srikrishna Committee (2018) had recommended that while determining the age of consent for children, certain factors should be considered. These include: (i) minimum age of 13 and maximum age of 18, and (ii) a single threshold for ensuring practical implementation.[4] It also observed that 18 years may be too high from the perspective of the full autonomous development of a child.[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.[29]

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 help avoid instances of children giving false declaration. However, this may reduce anonymity in the digital sphere.

Lack of clarity on what constitutes detrimental to well-being of a child

The Bill provides that data fiduciary will not undertake any processing which has detrimental effect on well-being of child. The Bill has not defined detrimental effect. It has also not provided any guidance for determining such effect.

Exemption from notice for consent may not be appropriate

Bill: Clauses 5, 6, 17 (3)

The Bill empowers the central government to notify certain data fiduciaries or classes of data fiduciaries including startups from certain obligations. This must be done with due regard to volume and nature of personal data. One of the obligations which may be exempted is notice for consent. The requirement to seek free and informed consent will continue to apply in case of these entities. However, if there is no obligation to provide notice regarding nature of data collected and purpose of processing, it may be argued that a data principal will not be able to provide informed consent.

Drafting issue

Bill: Clauses 27 (1) (e), 36

Clause 27 (1) (e) refers to the sub-section (2) of Clause 36, however, Clause 36 does not have any sub-sections.

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 Digital Personal Data Protection Bill, 2023
Scope and Applicability			
▪ Processing of personal data: (i) within India, (ii) outside India if it is for business carried on, offering of goods and services, or profiling individuals, in India	▪ Expands the scope under the 2018 Bill to cover certain anonymised personal data	▪ Expands the scope under the 2018 Bill to include processing of non-personal data and anonymised personal data	▪ does not cover offline personal data and non-automated processing
Reporting of data breaches			
▪ Fiduciary to notify the Data Protection Authority about a breach which is likely to cause harm, the Authority will decide whether to notify the 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, in prescribed manner
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
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
Harm from processing of personal data			
▪ Harm includes monetary loss, identity theft, loss of reputation, and unreasonable surveillance ▪ Data fiduciaries to take measures to minimise and mitigate risks of harm ▪ Data principal has a right to seek compensation in the event of harm	▪ Same as 2018 Bill	▪ The central government should have powers to prescribe additional harms	▪ Not provided

The Draft Personal Data Protection Bill, 2018	The Personal Data Protection Bill, 2019	Recommendations of the Joint Parliamentary Committee	The Digital Personal Data Protection Bill, 2023
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; ▪ TDSAT has been designated as the 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 ▪ The central government may restrict of personal data to certain countries through notification

Sources: The Draft Personal Data Protection Bill, 2018; The Personal Data Protection Bill, 2019 and the Digital Personal Data Protection Bill, 2023 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. The Digital Personal Data Protection Bill, 2019, as introduced in Lok Sabha.
8. Rule 419A, The Indian Telegraph Rules, 1951 issued under Section 7 (2) of the Indian Telegraph Act, 1885.
9. People's Union for Civil Liberties (PUCL) vs Union of India, Supreme Court of India, December 18, 1996.
10. Chapter 3, Data Protection Act, 2018, United Kingdom.
11. Part 6, 7, and 8, Investigatory Powers Act, 2016, United Kingdom.
12. Clause 2 (20), Clause 2 (38), Clause 15, The Personal Data Protection Bill, 2019, as introduced in Lok Sabha.
13. Clause 22, Clause 23, Clause 26, Clause 27, The Personal Data Protection Bill, 2019, as introduced in Lok Sabha.
14. Clause 64, The Personal Data Protection Bill, 2019, as introduced in Lok Sabha.
15. Recital 75, Article 82, General Data Protection Regulation of European Union.
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. Clause 33 and 34, The Personal Data Protection Bill, 2019, as introduced in Lok Sabha.
20. Clause 17, The Draft Digital Personal Data Protection Bill, 2022, Ministry of Electronics and Information Technology, November 18, 2022.
21. Rojer Mathew versus South Indian Bank Ltd & Ors., 2019 (369) ELT3 (S.C.), Supreme Court of India, November 13, 2019.
22. Section 89, The Electricity Act, 2003.
23. Section 10 (1), The Competition Act, 2002.
24. Section 5 (2), The Telecom Regulatory Authority of India Act, 1997.
25. Rule 3 (2), The SEBI (Terms and Conditions of Service of Chairman and Members) Rules, 1992.
26. Children's Online Privacy Protection Rule ("COPPA"), Federal Trade Commission, USA, as accessed on December 6, 2022.
27. Guide to Data Protection, Information, Information Commissioner's Office, United Kingdom, as accessed on December 6, 2022.
28. Article 8, General Data Protection Regulation, European Union.
29. Section 11, The Indian Contract Act, 1872.