Legislative Brief

The Personal Data Protection Bill, 2019

The Personal Data Protection Bill, 2019 was introduced in Lok Sabha on December 11, 2019, and was referred to a Joint Parliamentary Committee for detailed examination.

Recent Briefs:

Three Labour bills on Industrial Relations, Social Security and Occupational Safety
September 21, 2020

The Banking Regulation (Amendment) Bill, 2020
September 14, 2020

Anurag Vaishnav
anurag@prsindia.org

Manish Kanadje
manish@prsindia.org

October 5, 2020

Highlights of the Bill

- The Bill provides a framework for safeguarding the privacy of personal data of individuals (data principals) which is processed by entities (data fiduciaries).
- Processing can only be done for a specific purpose, after obtaining consent of the data principal. Such consent is not required in case of a medical emergency or by the State for providing benefits or services.
- The Bill provides the data principal with certain rights. These include the right to correct their data, confirm whether the data has been processed, or to restrict its continued disclosure.
- The Bill allows exemptions from many of its provisions when the data is processed in the interest of national security, or for prevention, investigation or prosecution of offences.
- Sensitive personal data such as financial and health data, can be transferred abroad, but should also be stored within India.
- The Bill sets up a national-level Data Protection Authority (DPA) to supervise and regulate data fiduciaries.

Key Issues and Analysis

- Personal data processed for prevention, detection, investigation and prosecution of an offence is exempted from most provisions of the Bill. Such an exemption may be too broad.
- The State does not need to obtain a person's consent to process their data for providing a service. Thus, in case of commercial services, public sector entities (which are part of the State) are treated differently from their private sector competitors.
- Mandatory local storage of sensitive personal data has certain advantages such as ease and speed of access to data for law enforcement agencies. However, it may also lead to additional infrastructure costs on data fiduciaries.
- Fiduciaries are required to inform the DPA of a data breach only where such breach is likely to cause harm to the data principal. This may lead to fiduciaries under-reporting breaches in order to protect their market reputation.
- It is not necessary for the adjudication officer to have a background in law. This officer has to judge cases related to the right to be forgotten, and may not have the requisite knowledge of Constitutional law.

PART A: HIGHLIGHTS OF THE BILL

Context

Personal data pertains to characteristics, traits or attributes of identity, which can be used to identify an individual.[1] In recent years, it has been observed that entities (both businesses and governments) are increasingly making use of large volumes of personal data for decision making.[2] Data protection is the process of safeguarding this usage of personal data through policies and procedures to ensure minimum intrusion of privacy of an individual.

In August 2017, the Supreme Court held that the right to privacy is a fundamental right of Indian citizens.[3] It also held that informational privacy, or privacy of personal data and facts, is essential to the right to privacy. However, currently there is no legislation which provides a comprehensive framework for protecting the right to privacy of Indian citizens. In India, usage of personal data or information of citizens is currently regulated by the Rules notified under the Information Technology (IT) Act, 2000.[4] These Rules specify security safeguards for data collection, disclosure and transfer of information for entities processing the data.

A Committee of Experts (Chairperson: Justice B.N. Srikrishna) set up by the government to study issues related to data protection and digital economy in India submitted its report in July 2018.[5] The Committee noted that the IT Rules (2011) have not kept pace with the development of digital economy. For instance: (i) the definition of sensitive personal data under the Rules is narrow, and (ii) some of its provisions can be overridden by a contract.

Along with its report, the Expert Committee also recommended a draft Personal Data Protection Bill to specify norms of data processing for entities using personal data. Further, it recommended setting up a regulatory body to ensure compliance with the legislation. The Personal Data Protection Bill, 2019 is based on the recommendations of the Expert Committee and the suggestions received from various stakeholders.[6] The 2019 Bill seeks to: (i) protect the privacy of individuals with respect to their personal data, (ii) create a framework for processing such personal data, and (iii) establish a Data Protection Authority for these purposes.

Key Features

- **Definitions:** Personal data is data which pertains to characteristics, traits or attributes of identity, which can be used to identify an individual. The Bill classifies certain categories of personal data as sensitive personal data. This includes financial data, biometric data, caste, religious or political beliefs, or any other category of data as specified. The Bill defines data fiduciary as the entity or individual who decides the means and purpose of processing personal data, and data principal as the individual to whom the data relates. The Bill governs the processing of personal data by: (i) government, (ii) Indian companies, and (iii) foreign companies dealing with personal data of individuals in India.
- **Grounds for processing personal data:** The Bill allows processing of personal data of an individual by an entity only after taking consent of the individual. However, in certain circumstances, personal data can be processed without consent. These include: (i) if required by the State for providing service or benefit to the individual, (ii) legal proceedings, or (iii) to respond to a medical emergency.
- **Obligations of data fiduciary:** Any processing by a data fiduciary can only be done for a specific purpose. Further, the data fiduciary will be subject to data collection and storage limitations. This means that only as much data can be collected as required for the specified purpose, and data cannot be stored for longer than what is necessary for the purpose. Additionally, fiduciaries must also undertake certain transparency and accountability measures such as: (i) implementing security safeguards (by encrypting data and preventing unauthorised access), and (ii) instituting grievance redressal mechanism to address user complaints.
- **Social media intermediaries:** The Bill defines these to include intermediaries which enable online interaction between users and allow for sharing of information. All such intermediaries with users above a threshold, and whose actions can impact electoral democracy or public order, will have to provide a voluntary user verification mechanism for users in India.
- **Rights of the individual:** The Bill provides the individual (or data principal) with certain rights. These include the right to: (i) confirm from the fiduciary on whether their data has been processed, (ii) seek correction of inaccurate, incomplete, or out-of-date personal data, (iii) seek erasure of personal data which is no longer necessary for the purpose it was processed, and (iv) restrict continuing disclosure of their data by a fiduciary, if it is no longer necessary for the purpose or consent is withdrawn.
- **Data Protection Authority (DPA):** The Bill sets up a Data Protection Authority which may: (i) take steps to protect interests of individuals, (ii) prevent misuse of personal data, and (iii) ensure compliance with the Act. It will consist of a chairperson and six members, with at least 10 years' expertise in the field of data protection, information technology or public administration.

- **Grievance redressal:** Under the Bill, a data principal may raise a complaint of contravention of provisions of this Act which has caused or is likely to cause harm to them. The data fiduciary must resolve such a complaint in an expeditious manner (within 30 days). If the data principal is not satisfied with the manner in which the complaint is resolved, they may file a complaint to the DPA.
- The DPA can initiate an enquiry based on the complaint and provide for a penalty or compensation. If the data principal or data fiduciary is not satisfied with the decision, they can file an appeal before the Appellate Tribunal. An appeal against any order of the Tribunal will go to the Supreme Court.
- **Transfer of data outside India:** Sensitive personal data may be transferred outside India for processing if explicit consent is provided for the same by the individual, and subject to certain additional conditions. However, a copy of such sensitive personal data should also be stored in India. Certain personal data notified as critical personal data by the government can only be processed in India.
- **Exemptions:** The central government may exempt any of its agencies from the provisions of the Act: (i) in the interest of security of state, public order, sovereignty and integrity of India and friendly relations with foreign states, or (ii) for preventing incitement to commission of any cognisable offence (where arrest can be made without warrant) relating to the above matters. Processing of personal data is also exempted from provisions of the Bill for certain other purposes such as: (i) prevention, investigation, or prosecution of any offence, (ii) personal or domestic purpose, or (iii) journalistic and research purposes. However, such processing must be for a specific, clear and lawful purpose.
- **Offences and penalties:** Processing or transferring personal data in violation of the Bill is punishable with a fine of 4% of the worldwide annual turnover of the fiduciary, subject to a minimum of Rs 15 crore. Failure to conduct a data audit is punishable with a fine of 2% of the worldwide annual turnover, subject to a minimum of five crore rupees. Re-identification and processing of de-identified personal data (where identifiers are removed) without consent is a punishable offence with imprisonment of up to three years, or fine, or both. A court will take cognizance of an offence only on a complaint by the DPA.
- **Sharing of non-personal data and anonymised personal data with the government:** The central government may direct data fiduciaries to provide it with any: (i) non-personal data and (ii) anonymised personal data (where it is not possible to identify data principal) for better targeting of services.

PART B: KEY ISSUES AND ANALYSIS

Processing of personal data may cause harm, but also has certain advantages

The White Paper by the Expert Committee (2017) noted that there are several benefits of collecting and analysing personal data from individuals.[7] For instance: (i) healthcare data from a number of individuals such as details of hospital visits can be used by health care providers to make diagnostic predictions and treatment suggestions, (ii) location data of an individual can be used for monitoring traffic and improving driving conditions, (iii) financial transactions data can be used to improve fraud detection. Companies are also making use of personal data for providing better services to their customers. For example, a mobile application based taxi service can make personalised booking suggestions by using personal data of previous trips of a user. Processing of personal data can generate new market opportunities in a developing country such as India.

At the same time, it is necessary to balance the objective of promoting the digital economy with the protection of personal data. As of March 2020, 687 million people use internet in India, as compared to nearly 200 million five years ago.[8] Due to this rapid increase, users may not have the experience and expertise to understand the potential for misuse of their personal data. Unregulated and unrestricted use of personal data can lead to discrimination and harm for users. They generally have limited control over their data.[8] They may not know the extent of data collection or its purpose. Besides harm to individuals, such incidents may also have implications for electoral democracy and public order. For example, in 2018, it was revealed that personal data of 87 million Facebook users (including 5 million Indians) was shared with a private company, Cambridge Analytica through a third-party application. This data was used for profiling persons to show them targeted advertisements around the United States presidential election in 2016. Considering such potential for misuse, it also becomes necessary to have a framework for protection of personal data.

For this purpose, the Bill puts restrictions on data fiduciaries which aim to process personal data, such as processing only for a specific purpose, limitations on data collection and data retention, and requirement of consent. However, it also offers certain exemptions for promoting innovation in form of a sandbox. Further, purposes such as credit scoring and operation of search engines are exempted from the requirement of consent.

Broad exemptions for processing for prevention and detection of offences

Bill: Clauses 36(a), 3(20)

Under the Bill, fiduciaries are subjected to certain obligations such as: (i) specifying the purpose of data collection, (ii) ensuring that the processed data is complete and not misleading, and (iii) ensuring that data is not retained beyond the necessary period. Further, fiduciaries are required to report personal data breaches to the DPA if they may cause harm to the data principal. However, fiduciaries are exempted from all of these obligations while processing personal data for prevention, detection, investigation and prosecution of any offence; the only requirement is that such processing must be done for a specific, clear and lawful purpose. This implies that a fiduciary may collect more data than necessary for the purpose and retain it for a period longer than necessary. Further, the individual will not have rights over their data. It may be argued that for the prevention or investigation of offences, a data principal's consent cannot be taken for processing of their data. However, it is unclear why other obligations will not apply.

Further, the Bill provides these exemptions without adequate safeguards. For example, the Indian Telegraph Rules, 1951 under the Indian Telegraph Act, 1885 allow for the interception of telephone calls for purposes such as national security. However, an exemption order under the Rules can only be made by the Home Secretary of the central or state government.[9] Further, the intercepted records have to be destroyed within six months unless they are required for functional purpose.[10] Such safeguards are absent in the Bill.

The Expert Committee (2018) had argued that prevention, detection, investigation, and prosecution for a contravention of law are essential State functions.[5] It recommended that these activities should be exempted from certain provisions of the Bill. However, such exemption should be proportionate to the interests being achieved. The question is whether exempting a fiduciary from most of the provisions of the Bill for this purpose without adequate safeguards is proportionate to the intended purpose.

Distinction between State and private entities providing similar service

Bill: Clause 12(a)

The Bill prohibits all fiduciaries, including the State, from processing personal data without the consent of the data principal. However, in certain cases, processing of personal data is permitted without the consent of the individual. These include processing personal data for: (i) providing any service or benefit to the data principal by the State, (ii) issuing licenses or permits to the data principal, (iii) legal proceedings, or (iv) responding to a medical emergency. It is not clear why the State is not required to take consent of the data principal for providing them with any service or benefit.

The Expert Committee (2018) had stated that there is an imbalance of power between the individual and State if the State is the only provider of a service or benefit.[5] This means that the data principal does not have a choice to refuse consent if he needs the benefit or service. In such a situation, the idea of requiring consent is meaningless. Hence, the State should be allowed to process personal data without consent for providing any service or welfare benefit.

However, it is unclear why such an exemption is extended to all services provided by the State (including commercial services). For example, an insurance company created by an Act of Parliament will fall under the definition of the State under Article 12 of the Indian Constitution. Under the Bill, this company can process personal data of its customers without obtaining their consent. However, its competitors in the private sector would need to obtain consent of the customers before processing their data. Thus, the provision results in differential treatment towards public and private entities providing a similar service.

Optional reporting of breaches may lead to a conflict of interest

Bill: Clause 25(1)

Under the Bill, data fiduciaries are required to inform the DPA of any breach of personal data only where such a breach is likely to cause harm to the data principal. The Bill defines a data breach as any unauthorised or accidental disclosure, alteration or loss of access to personal data. The Bill defines harm to include financial loss, loss of reputation, or withdrawal of a service. Giving a data fiduciary the discretion of determining whether a data breach needs to be reported to the DPA may lead to a conflict of interest.

The Expert Committee (2018) noted that all personal data breaches are not of equal gravity.[5] To avoid notification of relatively low impact breaches, only such breaches which may harm the data principal should be notified to the DPA. Such selective reporting of data breaches will ensure that the DPA is not burdened with many notifications of low impact breaches. However, fiduciaries may have an economic interest in downplaying the impact of a data breach to protect their market reputation. For instance, in June 2019, it was reported, that an American multinational company did not report a personal data breach stating that only demonstration data was leaked.[11] Note that the DPA may conduct data audits of a fiduciary on instances of personal data breach, among other things.[12] Therefore, reporting of such instances may affect the fiduciary's data trust score.

Further, it may be argued that a data principal could choose to trust a fiduciary that has fewer instances of data breaches as such a fiduciary may be perceived safer compared to others. In such a scenario, optional reporting of data breaches by the fiduciary may deprive the individual of the information they would use while making a future choice about trusting their data with a fiduciary.

Grievance redressal process under the Bill

A complaint can only be raised if there is a possibility of harm to the data principal

Bill: Clause 32(2)

Under the Bill, a data principal may make a complaint of contravention of any of the provisions of the Act to the data fiduciary, if such contravention has caused or is likely to cause harm to them. If the data principal is not satisfied with the manner in which the complaint is resolved, they may file a complaint to the DPA. It could be questioned why a complaint cannot be made for mere violation of the rights of the data principal or any other violation of the Act. For instance, if a data fiduciary mines personal data of a user without their consent for commercial gains, it may not necessarily cause harm to the user. However, in order to raise a complaint in such cases, the user would be required to demonstrate the possibility of harm to them.

Adjudication Officer for the exercise of right to be forgotten may not have the necessary expertise

Bill: Clauses 20(1), 20(2), 20(3), 62(3)

The Bill provides certain rights to the data principal with respect to their personal data. Under the right to be forgotten, the data principal can restrict continuing disclosure of personal data which is no longer necessary for the purpose or if the consent is withdrawn. The right can be exercised only after an order by an adjudicating officer appointed by the DPA (an expert in the field of data protection, law or information technology). The officer determines whether the exercise of this right violates the right to freedom of speech and expression or the right to information of any other citizen. The question is whether this adjudicating officer would be competent enough to make this decision. These matters are typically interpreted by higher judiciary since they involve questions related to constitutional rights. However, the Bill allows the appointment of an adjudication officer who may be an expert in the field of data protection or information technology, and not in law. Therefore, such an officer may not have the expertise to decide upon matters related to the exercise of the right to be forgotten.

Storage of sensitive personal data within the country

Advantages and disadvantages of storing sensitive personal data locally

Bill: Clause 33(1)

The Bill states that sensitive personal data (such as health data or financial data) of individuals can be transferred abroad, but a copy should be stored within India. The central government has the power to classify additional categories of data as sensitive personal data in consultation with the DPA and the sectoral regulator. The Expert Committee (2018) noted that local storage of sensitive personal data has certain advantages such as: (i) ease and speed of access to data for law enforcement agencies for investigation, (ii) building digital infrastructure and data processing ecosystem in the country, and (iii) preventing foreign surveillance of Indian citizens.[5] It recommended that a serving copy of all personal data should be stored in India.

However, the Committee also noted that local storage of sensitive personal data may also have certain disadvantages. Domestic enterprises often avail foreign infrastructure such as cloud computing for storing data. Therefore, mandatory local storage may lead to additional costs on data fiduciaries. Further, it may discourage some data fiduciaries from investing in India, due to the additional infrastructure costs involved with processing data in India. The requirement of local storage for sensitive personal data can also lead to fragmentation of data into sensitive and non-sensitive personal data, which can be an added compliance burden for fiduciaries.

Unlike other countries, penalties for offences includes imprisonment

Bill: Clause 82

Under the Bill, re-identification of de-identified personal data without the consent of such data fiduciary or data processor is punishable with imprisonment for a term of up to three years or a fine of up to two lakh rupees, or both. The Bill defines de-identification of personal data as removal or concealing of identifiers from data, so that the data principal cannot be directly identified. By re-identification, this process is reversed. All other contraventions under the Bill (including obtaining, transferring or selling personal data of an individual without consent) attract a monetary penalty, while the offence of re-identification of de-identified personal data could lead to imprisonment. Note that jail terms are not provided for any offence or contravention in the Privacy Act of Canada as well as the General Data Protection Regulation (GDPR) in the European Union.[2,13]

Comparison of the Bill with international data protection laws

There are several provisions in the Bill that differ from international data protection laws. The Bill differs from the laws in the European Union, Australia and Canada with respect to the presence of provisions related to social media intermediaries and non-personal data, which are absent in other jurisdictions. The definition of sensitive personal data does not include financial data in the data protection laws of the above jurisdictions.

Further, most jurisdictions do not have an imprisonment term for violation of the law. The European Union's GDPR provides the user with certain additional rights which are not present in the proposed Indian legislation. For example, the 'right to object' which enables the individual to object to processing of their data for profiling or direct marketing purposes. Table 1 outlines some of the provisions in the proposed Bill which differ from international laws.

Table 1: International comparison of data protection and privacy laws

Country	European Union	Australia	Canada	India (proposed Bill)
Sensitive personal data	▪ Does not include financial data, passwords.	▪ Does not include financial data, passwords.	▪ Not defined separately.	▪ Includes financial data, health data, does not include passwords.
Local storage of data	▪ Not mandatory.	▪ Not mandatory. ▪ Sector-specific mandates, e.g., for health data.	▪ Not mandatory.	▪ Local copy of sensitive personal data mandatory; exclusive local storage of critical personal data mandatory.
Cross border transfer of data	▪ Permitted if the receiving country has adequate standards of data protection (assessed by the European Commission).	▪ Permitted if the processing entity has taken steps to ensure that the recipient does not breach country's privacy principles.	▪ Permitted if the processing entity uses contractual or other means to ensure comparable level of protection.	▪ Permitted (for some data) if approved by the regulator or prescribed by the government.
Exemptions	▪ Public and national security, defence, judicial proceedings, domestic, journalistic, research and employment purposes.	▪ Defence and intelligence agencies, federal courts, political parties, small businesses, journalistic and employment purposes.	▪ No blanket exemptions. ▪ Specific exemptions from seeking consent, such as for journalistic purposes, are allowed.	▪ Sovereignty and integrity, national security, friendly relations, public order, prevention and prosecution of offences, research and journalistic purposes, sandbox.
Penalties	▪ Up to EUR 20 million, or 4% of previous year's worldwide annual turnover, whichever is higher. ▪ No jail term.	▪ Up to AUD 2.1 million. ▪ No jail term except disclosure of information obtained during an emergency.	▪ Up to CAD 1,00,000. ▪ No jail term.	▪ Up to Rs 15 crore, or 4% of previous year's worldwide annual turnover. ▪ Imprisonment for re-identification of de-identified personal data (up to 3 years).

Sources: European Union - The General Data Protection Regulation, 2016; Australia - The Privacy Act, 1988; Canada - The Privacy Act, 1985; The Personal Information Protection and Electronic Documents Act, 2000; The Personal Data Protection Bill, 2019; PRS.

1. Section 3(28), The Personal Data Protection Bill, 2019.
2. The General Data Protection Regulation 2016, European Union.
3. Justice K. S. Puttaswamy Vs. Union of India, Supreme Court, Writ Petition (Civil) 494 of 2012, August 24, 2017.
4. Information Technology (Reasonable security practices and sensitive personal data or information) Rules, 2011.
5. "A Free and Fair Digital Economy", Report of the Committee of Experts under the Chairmanship of Justice B. N. Srikrishna, July 2018.
6. Statement of Objects and Reasons, The Personal Data Protection Bill, 2019.
7. "White Paper of the Committee of Experts on a Data Protection Framework for India", November 2017.
8. "Draft Empowerment and Protection Architecture", NITI Aayog, August 2020.
9. PUCL Vs. Union of India, Writ Petition (Civil) 256 of 1991, Supreme Court, December 18, 1996.
10. Rule 419(A), The Indian Telegraph Rules, 1951.
11. "Cybersecurity giant Symantec plays down unreported breach of test data", The Guardian, June 13, 2019.
12. Section 29, The Personal Data Protection Bill, 2019.
13. The Personal Information Protection and Electronic Documents Act, 2000, Canada; The Privacy Act, 1985, Canada.