Reserve Bank Information Technology Pvt Ltd

Analysis of Personal Data Protection Bill (2019)

Abstract

This document presents a detailed analysis of the significant provisions of the Personal Data Protection Bill (2019). It also lists down changes from the 2018 draft of the same bill.

Author

Shikha Pathak, Policy Research Analyst, ReBIT

The original text of the Personal Data Protection Bill (2019) is available here:
http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

Contents

Executive summary

The Personal data protection bill, 2019 aims to create a robust framework for privacy protection, by upholding the rights of the data owner. The bill also makes way for "digitally enabled consent", which ensures that consent is given real time and the choice to revoke content is always present to the data owner.

The Right to Privacy was established as a fundamental right in the KS Puttaswamy case after which a committee was formed under the chairmanship of Justice Sri Krishna to draft the Data Protection Bill, 2018. To address the shortcomings of the 2018 draft and make the privacy framework more dynamic and suitable for the needs of the fast changing digital age, it was opened for comments from public, privacy experts and academia. The Personal Data Protection Bill 2019 is the consequent result of these contributions. It was cleared by the Union Cabinet in December 2019, and is currently awaiting review by the Joint parliamentary committee.

The Personal Data Protection Bill 2019 is drafted with three major objectives- first; to secure more rights for the data owner and second; to ensure that consent is unbundled, clear and provided real time. The third major concern addressed in the bill is around data localization. This had stirred a debate and many corporates demanded that government needs to adopt a fine balance between commerce and privacy. The current bill addresses this concern of data localisation and relaxes the norms for cross border data transfer. Though the transfer of critical data is still primarily banned, exemptions in this clause for health and emergency service have been introduced.

The role of the Data Protection authority and that of the data protection officer remains unchanged. The draft bill emphasises the need to incorporate privacy by design principle which has to be certified by regulation. The 2019 bill also introduces "consent manager" an entity regulated by the Data Protection Authority that can enable end users to gain, withdraw, review and manage consent through it. Transparency in processing and emphasis on consent are consistently emphasised upon in the bill.

Overall, the bill is a step ahead in the country's privacy laws. Its approach is more balanced unlike that of the 2018 draft which imposed blanket bans on cross border transfer of data. The significance of consent and rights of data principal are also more pronounced in the new draft bill. However, exemptions granted to certain government agencies have stirred a controversy and may warrant further elaboration.

Introduction

In 2017, Ministry of Information and Technology (MEITY), had constituted a committee of experts under the chairmanship of the retired Supreme Court judge, Justice BN Srikrishna. The committee spearheaded the formulation of the first draft of the Personal Data Protection Bill, in July 2018. ReBIT research team had prepared a detailed analysis, which can be read here.

Since then, the Government of India had solicited comments from public, various ministries and key stakeholders with the objective to address the lapses in the 2018 draft Data Protection bill to work towards a stronger data protection law with privacy and consent as cornerstone. The result was the revised Personal Data Protection (PDP) Bill, which was cleared by the Union Cabinet on December 4, 2019.

The bill has now been referred to a Joint selection committee and will be presented for the parliament's approval in the monsoon session.

Scope and Applicability

This act shall apply to processing of personal data which has been collected, shared or processed within the territory of India.

It shall also apply to processing of personal data by state, any Indian company, any citizen of India or any person or body incorporated under Indian law. It will apply to data fiduciaries and data processors not present in India, but processing data in connection to any business carried on in India, or in connection with any activity involving profiling of data principals. The act will not apply to the processing of anonymized data.

Most of the definitions of the terms data fiduciaries, data processors and anonymized data remain unchanged in the Personal Data Protection Bill, 2019. However, they have covered in the next section for readers' convenience.

Legal Definitions

The relationship of trust between data principal and data fiduciary remains unchanged. The following are definitions of important terms[1], as elaborated in the draft:

Anonymization in relation to personal data, means such irreversible process of transforming or converting personal data to a form in which a data principal cannot be identified, which meets the standards of irreversibility specified by the Authority

Data Fiduciary means any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data

Data Processor means any person, including the State, a company, any juristic entity or any individual, who processes personal data on behalf of a data fiduciary

Data Principal means the natural person to whom the personal data relates

Data Auditor means an independent data auditor referred to in section 29 who may assign a rating in the form of a data trust score to the data fiduciary. The authority may direct the data fiduciary to conduct a data audit by appointing a data auditor where it is of the view that data fiduciary is processing personal data in a manner that can cause harm to the data principal.

Consent Manager means a data fiduciary which enables a data principal to gain, withdraw, review and manage his consent through an accessible, transparent and interoperable platform. Such an entity will be registered with the Authority in such manner and subject to such technical, operational, financial and other conditions as may be specified by regulations.

[1] Please refer to the Personal Data Protection Bill (2019), Chapter 1, Section 3 for all definitions.

Definition of Sensitive Personal Data

Sensitive personal data means which may reveal, be related to, or constitute

Financial data
Health data
Official identifier
Sex life
Sexual orientation
Biometric data
Genetic data
Transgender status
Intersex status
Caste or tribe
Religious, political belief or affiliation
Data categorized as sensitive under section 15
Passwords has been removed from the definition of sensitive personal data.

Important aspects of the bill

Rights of data principal

The data principal has a right to confirm from the data fiduciary whether the personal data collected has been processed. If requested, the data fiduciary is bound to provide a clear summary of such information in a concise, comprehensible form.

Further, the data principal has right to correction and erasure in case the personal data being processed is incorrect or misleading. In case the data fiduciary fails to correct, update, complete or erase such data, the data fiduciary is bound to provide justification for rejecting the request, in writing.

In case the data fiduciary corrects, updates, completes or erases the personal data, He/she is also bound to take all necessary steps to notify the same to all relevant authorities and stakeholders.

Privacy by design

The bill stipulates that the data fiduciary must submit its privacy by design policy to the authority for certification within the period and manner specified by regulation.

This policy should contain the organizational best practices, obligations of data fiduciary, technology used and legitimate business interests along with accounting for the interests of the data principal. It should also contain steps taken to protect privacy from the point of collection of personal data to its deletion.

Transparency in data processing

The data principal may give or withdraw his consent to the data fiduciary through a consent manager. A consent manager is a data fiduciary which enables data principal to gain, withdraw, review and manage his consent through an accessible, transparent and interoperable platform. However, the consent manager has to be registered with the authority. If a data principal makes a request via a consent manager, it is deemed to be made directly to the data fiduciary.

The emphasis on consent is one of the most significant changes in this bill. While strengthening consent is primary for enabling a stronger privacy framework, noted data privacy experts recommend[2] that it is also important that consent be provided or withdrawn at the time of transfer of data, unlike the current practice wherein bundled consent is sought in a single instance, in ambiguously drafted policies which are difficult to understand for the user.

Consent manager addresses this concern as it enables users to permit and revoke consent instantaneously, at the time of data transfer. This is also the foundation principal of account aggregator ecosystem. The account aggregators act as third party consent brokers, and seek consumer's consent, hence acting as a bridge and facilitating the movement of financial data between Financial Information users (FIUs) and Financial Information Providers (FIPs).

[2] https://www.livemint.com/opinion/columns/opinion-a-new-framework-for-consent-to-ensure-data-privacy-1565111736679.html

Classification of data fiduciaries as significant

Data fiduciaries may be notified as "significant" based on volume of data, sensitivity of data processed, turnover, risk of harm resulting from processing, use of technology and other relevant factors.

The 2019 bill adds that any social media intermediary with users above such threshold or is likely to have significant impact on electoral democracy shall be notified as a significant data fiduciary. Every significant data fiduciary based or working in India must voluntarily verify their accounts in manner prescribed by the authority. The methods of voluntary identification and verification of social media users will be prescribed by central government via notification.

The bill defines a "Social media intermediary" as any intermediary that primarily enables online interaction between users and allows the creation, upload, sharing, modification and dissemination of information for commercial, business transactions, providing internet access or for online encyclopedias and e mail services.

Data transfer restrictions

The bill stipulates that sensitive personal data may be transferred outside India for processing, but shall continue to be stored in India. However, critical personal data shall only be processed in India.

Earlier in 2018, in line with the previous draft of the Personal Data Protection Bill, RBI had released a notification[3] detailing the storage of payment data system advising all system providers to ensure that data relating to payment systems is stored only in India. This included Customer data, Mobile numbers, email, Aadhaar number, PAN number, Payment sensitive data, Payment credentials and other transaction data.

The 2019 Personal data protection bill has now relaxed the norms and laid down the conditions for cross border transfer of personal data on the condition that explicit consent is given by the data principal for such transfers and that -

[3] Storage of Payment System Data, 2018, Reserve Bank of India, https://m.rbi.org.in/Scripts/FAQView.aspx?Id=130

Transfer is made subject to standard contractual clauses / intra group scheme approved by authority, provided it makes provision for:
Effective protection of rights of data principal
Liability of data fiduciary for the harm caused for non-compliance
The central government after consultation with authority has allowed such transfer to another country or international organization, on the basis that:
Such data has adequate protection under international agreements
Such data will not affect enforcement of laws by authorities with relevant jurisdiction

Conditions for critical data transfer

According to the bill, critical personal data[4] shall only be processed in India. The only exemptions in this regard are when such processing is related to emergency or health services or where such transfer doesn't affect the security and strategic interests of the country.

Since payments system data is user's personal data and some of such data is sensitive personal data, the regulations related to their processing and storage will have to be revised keeping in mind explicit consent and rights of data principal.

Exemptions granted in data transfer

The central government has the power to exempt any agency of the government from the application of the act in interest of:

Sovereignty and security
Preventing incitement to commission of cognizable offenses, public order
Friendly relations with foreign states
prevention, detection, investigation and prosecution of contraventions of law
Processing for legal proceedings
Research, archiving and statistics
Personal/domestic purpose
Journalistic purpose
manual processing by small entities

[4] "critical personal data" means such personal data as may be notified by the Central Government to be the critical personal data.

Regulatory Infrastructure

In the draft Data Protection Bill (2018), the central government had notified about the creation of a Data Protection authority and the appointment of a Data Protection officer. It was recommended that a selection committee be formed to appoint its chairman. The 2019 privacy draft notes that the Cabinet secretary shall be the chairperson of the selection committee. The committee will include:

- Secretary to GOI in Ministry dealing with legal affairs
- Secretary to GOI in Ministry dealing with electronics and information technology.

The role of a data protection officer remains unchanged. The authority or the enquiry officer as the case may be will have same powers as vested in a court under Code of Civil Procedure 1908.[5]

Grievance Redressal

In case of violation, a data principal may raise a grievance:

- With a data protection officer in case of a significant data fiduciary
- Officer designated in case of other data fiduciaries

It is suggested that any grievance raised must be solved in expeditious manner and no later than 30 days The 2019 bill further adds that where the complaint is not resolved in period specified or data principal is not satisfied with the grievance redressal, or in case the data fiduciary has rejected to entertain the complaint; the data principal may file a complaint to the authority. As in the draft data protection bill 2018, in case the data principal is aggrieved by any order made by the data protection authority, he/she can file an appeal with the Appellate Tribunal. The functions and role of the Appellate Tribunal remain unchanged, orders passed by it are to be executed as a decree. An appeal will lie with the Supreme Court only on substantial question of law.

[5] Code of Civil Procedure 1908, http://legislative.gov.in/sites/default/files/A1908-05.pdf

STAY CONNECTED

Reserve Bank Information Technology Pvt. Ltd
https://rebit.org.in

LinkedIn
https://www.linkedin.com/company/reserve-bank-information-technology-pvt-ltd

Twitter
https://twitter.com/reservebankit

Email
communications@rebit.org.in

ABOUT REBIT

Reserve Bank Information Technology Private Limited (ReBIT), has been set up by the Reserve Bank of India to serve its IT and cybersecurity needs and to improve the cyber resilience of the Indian banking industry.

DISCLAIMER

This document is intended for general informational purposes only and does not take into account the reader's specific circumstances, and may not reflect the most current developments. ReBIT disclaims, to the fullest extent permitted by applicable law, any and all liability for the accuracy and completeness of the information in this document and for any act or omissions made based on such information. ReBIT does not provide legal, regulatory, audit or tax advice. Readers are responsible for obtaining such advice from their own legal counsel and other licensed professionals. The views, thoughts, and opinions expressed in this document belong solely to the author, and not necessarily to ReBIT.

Subscribe to ReBIT's Cyber Pulse Monthly Newsletter
https://rebit.org.in/newsletter