

DATA PROTECTION REGULATION BY PERSONAL DATA PROTECTION BILL IN INDIA: BEARING ON BUSINESS INDIA

ASMITA MAHALE¹, MADHAVI DAMLE², ABHIJIT CHIRPUTKAR³, PRASANNA KULKARNI⁴, TRUPTI
BHOSALE⁵

Symbiosis Institute of Digital and Telecom Management, Symbiosis International (Deemed University)

Lavale, Pune, Maharashtra, India ^{1,2,3,4}

Symbiosis School of Banking and Finance, Symbiosis International (Deemed University)

Lavale, Pune, Maharashtra, India ⁵

asmita.mahale2123@sidtm.edu.in¹

*mdamle@sidtm.edu.in²

abhijitchirputkar@sidtm.edu.in³

pkulkarni@sidtm.edu.in⁴

trupti.bhosale@ssbf.edu.in⁵

Abstract - Data privacy is essential to individuals to protect their personal information as it is sensitive to external abuse and threats. Safeguarding personal information is crucial for preserving potential exposure and maintaining trust between individuals; defining the information they want to be exposed to and business organisations; use this information. Using this information must safeguard individuals beyond intimidation or fear by businesses or external entities, who must adhere to legal standards and guidelines regarding data collection, storage, and usage. This paper highlights the critical aspects of the Personal Data Protection Bill (PDPB) on the Indian landscape and its impact on businesses. The technology law in India and the latest supreme court decision on PDPB have been discussed, which will pave and share the implications for individuals and businesses operating in India as the significance of data privacy and protection. The study re-inspects key terms and terminologies defined for India while visiting Global Data Protection Regulations (GDPR) adaptation is discussed. We examine how the PDPB will alter the privacy framework for businesses, the impact of critical data on data localisation, and the business's reaction to the cost of compliance. While the privacy of individuals is at issue, this research is particularly pertinent to the millions of people globally whose information is accessible over the internet.


Keywords: General Data Protection Regulation (GDPR), Personal Data Protection Bill (PDPB), Data protection, Data Privacy, Technology law

INTRODUCTION

Personal information about individuals may be collected and analysed for various reasons. Pooled datasets allow for faster trend detection and more precise targeting. While data can be helpful, the unpredictable and unrestrained use has raised worries about one's individual's privacy. Concerns include the centralisation of records, the summarising of entities, improved monitoring, and the consequent destruction of human liberty. This freedom resulted from a landmark Supreme Court decision in which the "right to privacy" was recognised as a "Fundamental right". India cannot be far behind in refining the eminence of life and imparting a sagacity of privacy and security to its people. The Supreme Court of India specified that the "right to privacy is protected as an integral part of the right to life and personal liberty guaranteed by Article 21 of the Constitution and as part of the freedoms guaranteed by Part III".

When it comes to establishing genuinely ethical standards, there is always room for improvement, even though many businesses have established privacy protection policies. The power of privacy legislation that is designed to protect an individual's personal information is growing on a worldwide scale. Countries in Northern Europe were the first to institute a system of this kind to protect personal data. From the beginning of the 1970s onward, it could be found in every area of the planet. In the beginning, this method was primarily used to encrypt information that was reasonably safe, such as who owns a vehicle or how many children a person had. When more information travels across international borders, there is a greater chance that victims of identity theft and other forms of financial crime may be affected. Because of this, society has demanded the establishment of an appropriate policy concerning this matter.

In today's modern times, the collecting of data for a variety of purposes has grown familiar. Google is constantly gathering information for the benefit of its users, who may gain access to relevant details



simply by visiting the relevant websites. Facebook is also responsible for the collection and dissemination of information. Also, other organisations are taking part in this activity. Using data currently being collected for marketing and analysing user behaviour in the context of the company's sector can help businesses improve their current financial standing. The development of fair information policies and procedures is a must for businesses. Training of users is required prior to the collection of any personally identifiable information.

Hackers have made public the contents of many debits and credit card information and sold it to criminals and other parties with questionable morals. Even though this trend has significantly increased the likelihood of sensitive information being exposed, people worldwide are increasingly flocking to social networking sites as a means of communication and breaking down conventional geographical borders. They do this even though these sites significantly increase the likelihood of exposing sensitive information. The precise location of the data-storing servers, which are kept hidden from the general public, is unknown. Do we have any idea where the primary server for Facebook is located? On other occasions, unauthorized persons have gained access to sensitive material, disclosing millions of previously kept private files. The collection of private information is carried out in this manner. Regrettably, from the beginning, policymakers paid little attention to ensuring the privacy of information about individuals.

On the other hand, due to the worldwide scope of the issue, the authorities' commitment to reason and justice in data processing has grown. The cultural impact of the internet can now be felt in India, not to mention the rest of the world. Consequently, the likelihood of sensitive data being stolen has increased. That might make it easier for dishonest people to steal money from financial institutions. Technology is developing at a breakneck pace in India.

The federal government allocates a considerable portion of its budget to various e-government programs. India's information technology (IT) and allied services sector cannot continue expanding at the current rate. We know that the outsourcing market is presently worth sixty billion dollars and will expand to two hundred and twenty-five billion dollars by 2020. As a direct consequence of this modification, the risk of data loss, which might ultimately result in a breach of privacy, has increased. The legislation does not consider Native Americans' unique circumstances in any way. The willingness of individuals in India to divulge their personal information is a critical factor in determining the development of the country's commercial sector.

These agencies have implemented data security best practices to reassure their constituents that the confidentiality of their personal information would be maintained during any electronic transactions with government bodies. Recent months have seen a rise in the focus directed at data security in the context of international data transfers. Customers based in countries other than India typically have more stringent standards for data security. Even though there are a variety of advantages to outsourcing to India, businesses are concerned about the safety of their data when it is sent to India for processing.

1. Indian state of Privacy of Personal Information

This year, India is expected to become the latest major economy to enact comprehensive data privacy legislation. "The Information Technology Act of 2000" safeguarded the personal Information of India's 1.4 billion people. Even though the act has been revised several times, the public and private sectors agree that India now requires separate personal data privacy laws. Furthermore, Indian officials are working to align the country's data protection legislation with global best practices. The PDPB represents a significant step for India in achieving its obligations under Article 51, of the Constitution of India, by giving the equivalent amount of security to personal data supplied by other countries.

Data is a national asset that can be used to unlock the power of data for India by establishing the necessary data infrastructure and governance systems. While the PDP Bill emphasises the creation of sandboxes to foster new ideas and activities, the ongoing need to develop sound data-managing legislation, standards, and optimal practices should not be overlooked.

Several pieces of legislation, such as the Indian "Telegraph Act" (1885) , "the Indian Contract Act" (1872) , "the Special Relief Act" (1963), "the Public Financial Institutions Act" (1983), "the Consumer Protection Act" (1986), "the Credit Information Companies (Regulations) Act" (2005), and "the Information Technology Act" (2000), have been enacted to improve the situation. These pieces of legislation were passed to rectify the situation. "The Information Technology (Amendment) Act" of 2008 introduced the idea of "sensitive personal information" and made "Body Corporate" legally responsible for the safety of this type of data. Because of this strategy, the safeguards are now far more reliable.



2. Rationale

The PDPB must address data privacy and protection concerns as India is developing a data-driven ecology spanning public and private segments. This Bill will legalise privacy, penalise violators, reduce data fraud and misuse, establish a centralised data source, and educate individuals by making them mindful of the authority of their permission. These measures would prevent other countries from widely exploiting individuals' personal information.

UNDERSTANDING THE CONCEPT OF PRIVACY

There are a variety of ways to understand the concept of privacy. The answer will change depending on whom it is asked and how they interpret privacy. There is a preponderance of structuralist, individualist, and integrative points of view. By looking at confidentiality through the prism of social interactions, a structuralist perspective is taken. A person's level of privacy may be measured by the extent to which other people's senses and monitoring technologies cannot get information about them, as well as their mental state and other details about themselves. A scholar put out the idea that confidentiality and anonymity are intertwined. A common assertion made from a structuralist point of view is that individuals feel better at ease disclosing personal information when such information is disguised. Maintaining Individuals' dignity and venerability to the external world is an individualistic way of looking at the world, and privacy is a means through which individuals may exert some control over disclosing their personal information. One possible definition of privacy is disclosing the assertions of individuals, groups, or institutions to third parties. Having control over one's information and making one's own choices independently are two more meanings of privacy.

A comprehensive definition of privacy is necessary in order to account for the existence of rights and interests. From an individual's fundamental rights, It is clear from Reiman's description that this method results from a combination of structuralist and individualist principles. When examined through the lens of an integrative definition of privacy, while privacy may be regarded as a substantial contributor to society; when viewed through the lens of an integrative definition of privacy.

In India, the concept of privacy is not generally accepted; it varies from person to person and area to area, depending on the typical social structure in certain areas. In addition, the gender of the individual might have a significant impact on how they see their own space in some regions of India. Women who adhere to the "Purdah" custom in some parts of India would rather keep to themselves and stay concealed at home. As a result of a series of legal rulings, the term "purdah" has come to be interpreted as including essential characteristics of decent behaviour and humility. Outside of residential complexes, one should not behave in such a manner. Yet, there are circumstances in which it is permissible to do purdah, with the understanding that one's privacy will be compromised.

DATA PROTECTION SCENARIO IN INDIA

The privacy of users' Personal Data is an ancient concept. A prior version of the application focused on privacy and was built around being user-friendly. The focus was on privacy so users could control their privacy and personal data. Many other countries have also collaborated to develop governing structures for the international movement of personal data.

Although there are instances where privacy concerns may clash, the Indian Supreme Court's ruling in 2012 established that the right to privacy is safeguarded as an essential component of the right to personal liberty and life under Article 21. And it is also a part of the freedoms guaranteed by Part III of the Constitution".

In 2012, a petition was submitted to the Indian Supreme Court claiming that sharing sensitive information through the Aadhaar system encroach upon an individual's right to privacy. In response, the Supreme Court reaffirmed the fundamental right to privacy protected by the Indian Constitution in the well-known "Puttaswamy v. State of Kerala case Anr v Union of India & Ors (WP (Civil) No. 494 of 2012)", establishing a similar circumstance. On Aug. 24 2017, the "Supreme Court's nine-judge bench" solidly declared that the "right to privacy" is an elementary right of the people in India. According to the Supreme Court of India, "the right to privacy is secured by the Indian Constitution as an essential feature of the right to life and personal liberty under Article 21. The Supreme Court also stated that privacy of information and personal details protection is crucial to the right to privacy¹". Over the past few years, India has taken significant steps to enhance its data protection scenario. In 2017, the Indian government

¹ HARISH SURYAVANSHI, "India's Personal Data Protection Bill ('PDP Bill'), 2018: Brief Introduction, Key Provisions and Comparison with GDP".

set up a committee to draft a comprehensive data protection law for India. The committee submitted its report in 2018, which led to the introduction of the Personal Data Protection Bill (PDPB) in 2019. The PDPB aims to protect the privacy of personal data and establish a regulatory framework for its collection, storage, and processing.

In December 2019, the PDPB with parliamentary committee's review, released its report on July 2020. The bill has been under discussion and revision since then, and a new draft bill is expected accepted in the Indian Parliament in the near future.

In the meantime, the Indian government has taken other measures to improve data protection, such as launching the National Cyber Security Policy in 2013, establishing the Computer Emergency Response Team (CERT-In) in 2004, and introducing guidelines for intermediaries to ensure safe and responsible use of online platforms.

Overall, India's data protection scenario has been evolving, and critically viewed for its protection of privacy in the country. The new data protection law, once enacted, is expected to significantly enhance the existing regulatory framework, and establish India as a leader in data protection. This affects not just the local businesses but international business, intermediaries, market research firms, policy makers as well as the individuals.

1. Announcement of the PDP Bill

The PDPB was announced on Jul. 27 2018, with the account of the Committee of Experts, Justice B. N. Srikrishna. The Committee was designed by the Indian Government's Ministry of Electronics & IT to design a law for data protection in India. PDPB specifies how the government and business companies established in India and overseas process individuals' personal data.

The "Personal Data Protection Bill" (PDPB) is anticipated as the data protection law in India that will assist in regulation while the processing and storage of personal data by individuals, companies, and the government. Here are some key facts about the proposed bill:

- i. Scope: The PDPB applies companies who use this data for commerce while operating within India or those offering goods or services to individuals in India. It also applies to data fiduciaries (those who collect and process personal data) and data processors (those who process personal data on behalf of data fiduciaries).
- ii. Personal data categories: The PDPB categorizes the data into three categories - "critical personal" data, "sensitive personal" data, and "general personal" data. Here, the critical personal data and sensitive personal data are subject to stricter rules for processing due to their nature.
- iii. Consent: The PDPB requires data fiduciaries to obtain the informed and explicit consent of individuals for the collection, processing, and transfer of their personal data.
- iv. Data localization: The PDPB mandates that depending on the classification certain categories of data be stored within Indian boundaries, and the transfer of such data outside India is subject to specific conditions.
- v. Enforcement: The PDPB establishes a Data Protection Authority (DPA) as the primary regulator responsible for overseeing the implementation and enforcement of the law.
- vi. Penalties: The PDPB provides for substantial penalization for non-compliance with the law, including fines of up to around four percent of a company's global turnover.
- vii. Exemptions: The PDPB provides certain exemptions for certain types of data processing activities, such as those for journalistic, academic, artistic, or literary purposes.
- viii. Parliamentary review: The PDPB has been referred to a parliamentary committee for review and revision, and a new draft bill is expected to be tabled in the Indian Parliament soon.

Overall, the PDPB is expected to significantly enhance the existing data protection regime in India and establish a comprehensive regulatory framework for the collection, storage, and processing of personal data.

2. Proposed PDPB

The PDPB represents a fundamental change in the legislative edifice for data protection. The anticipated legislation hopes to be a complete act. The "natural person who owns the data of individuals" is defined as the Data Principal. The phrase "Data Fiduciaries" refers to "any person, including the State, a firm, any legal body, or any individual who, alone or in collaboration with others, determines the purpose and means of personal processing data." In compliance with the PDPB, Data Fiduciaries have an obligation to Data Principals to guarantee that the data acquired is utilised responsibly.

Data collection is only permitted with the persons' informed permission. Section 12 of the PDP Bill delves into the more important topic of consent. Section 12 of the PDPB states that the permission must be explicit and unambiguous and that the Data Principal should be able to withdraw it without difficulty. Section 12 of the PDPB makes notice and consent obligations under the PDPB further detailed than the "Sensitive Personal Data Rules, 2011". There is a realistic paradigm for obtaining unambiguous consent from the Data Principal. The PDPB has a broader characterisation of data that is not restricted to sensitive personal data, as is the case with the Sensitive Personal Data Rules, 2011.

Apart from emphasising individual discretion, the PDPB takes a right-based attitude to the Data Principal's privacy protection. Data Principals have the right to confirm if the Data Fiduciaries utilised the correct data and the right to make changes in the data held by Data Fiduciaries if it is wrong. The "right to be forgotten", a fundamental right in the digital sector, has been included as an indispensable Data Principal right. The PDPB establishes a background for data protection rights for persons by enumerating a collection of rights for the Data Principal, which might be equated with worldwide best practices².

3. Nuances in the Bill

The primary concern is determining when a person or an enterprise/company can share this Data with different platforms for analysis and how data privacy will be safeguarded. These apprehensions necessitate building a legal body to shield individuals' privacy, protect their data, and prevent data breaches. To make this sure, the Central Government of India engrained an assembly by Justice B. N. Srikrishna to scrutinise the disputes which are currently existing and create a data protection body which addresses individuals' data privacy. The PDPB's goal is to ensure that the country's digital economy rises and citizens' personal data are safe³.

A noteworthy change in the Indian setting is the regulatory obligation positioned on the state apparatus to establish the "data governance regulatory framework". By starting privacy as a fundamental right, the judiciary has imposed the necessity to provide a regulatory and organised background. The degree to which the Indian prototype adopts the General Data Protection Regulation (GDPR) based concepts of privacy regulation is an indicator of regulatory alignment with the EU⁴.

4. Earlier steps taken for Data Privacy

Previous data protection law has been fragmented across the EU as different nations added to the core principles included in the original directive of 1995. Some countries amended the demand notice of violations and punishment, while some nations, such as Spain, were fined severely and frequently. France, for example, virtually never could impose any penalties. As a result, the scenario exists where businesses operating around the region are confronted with a legal quagmire of conflicting perspectives on data protection⁵.

The government of the EU took significant measures to strengthen the protection of data and privacy rules present in the EU. On that basis, there was the creation of the GDPR, which was put into action on May 27 2016, swapping the Data Protection Directive (1995/46/EC). Eventually, the GDPR was implemented on May 25 2018. The motivation for implementing GDPR was to permit the citizens of the EU to fend off others from putting their personal data to the wrong use and putting their privacy at risk. This wrongful use of data, especially by marketing and sales firms, increased significantly in the digital era. The provisions of the PDPB, like the GDPR, have extensive consequences for domestic and international businesses that handle personal data⁶.

² R. Bailey, V. Bhandari, S. Parsheera, and F. Rahman, "Comments on the (Draft) Personal Data Protection Bill, 2018," 2018.

³ R. G. Singh and S. Ruj, "A Technical Look At The Indian Personal Data Protection Bill," May 2020, [Online]. Available: <http://arxiv.org/abs/2005.13812>

⁴ D. M. Prasad and S. C. Menon, "The Personal Data Protection Bill, 2018: India's regulatory journey towards a comprehensive data protection law," *International Journal of Law and Information Technology*, vol. 28, no. 1, pp. 1-19, Jun. 2020, doi: 10.1093/ijlit/eeee003.

⁵ C. Tankard, "What the GDPR means for businesses," *Network Security*, vol. 2016, no. 6, pp. 5-8, Jun. 2016, doi:10.1016/S1353-4858(16)30056-3.

⁶ Poulami Sen, "EU GDPR and Indian Data Protection Bill: A comparative study." [Online]. Available: <https://gdpr-info.eu/art-1-gdpr/>



SIGNIFICANT COMPONENTS OF THE PDP BILL

1. Classification of Data

Data is classified as health, biometric, genetic, or financial. Definition of "Personal Data": "information about or relating to a natural person who is directly or indirectly identifiable based on any characteristic, trait, attribute, or other feature of such natural person's identity, or any combination of such features, or any combination of such features with any other information." The "sensitive personal data" includes "health information, financial information, sex life, sexual orientation, biometric information, genetic information, caste or tribe, and political or religious belief or affiliation, which requires additional safeguards." Critical personal data is another category of data to be defined.

2. Stakeholders

The Data Principal is a "person who owns the data." The definition of a "Data Fiduciary" is "any person, including the state, a company, any legal entity, or any individual who, alone or in collaboration with others, determines the purpose and means of personal processing data." A "Data processor" is an entity that "processes data for data fiduciary or a third party and is responsible for protecting an individual's data." The other entities include autonomous auditors who are responsible for the audit of the data. An entity, "Data Protection Authority of India (DPAI)", institutes procedures and takes legal decisions.

3. Reasons for Collection of Data

A data fiduciary must collect, disclose, share, and process personal data for explicit, rational, and lawful purposes. The data fiduciary must identify and define such purpose before data collection and disclose it to the "Data Principal". The data processing by the Data fiduciary should be fair and reasonable. In particular, an organisation that processes personal data must process the personal data fairly and reasonably while respecting the data principal's privacy. The data fiduciaries must collect as little and as little data as possible following the "collection limitation" requirements.

The Data fiduciary must notify the Data Principal formerly to collect and process the data. The notice will include the reason for the collection, a form for consent, the type of data collected, and evidence about any cross-border transfers. A data fiduciary must make sure that data is correct, complete, and not deceptive. Consent, which must be obtained before data processing, will be freely given, informed, specific, and unambiguous. The processing of sensitive data would necessitate the data principal's explicit consent. Explicit consent requires the data fiduciary to inform the Data principal about "the sensitivity of personal data, the reason for such collection, and the potential consequences".

The processing of data about children would be done to protect children's rights. The Data fiduciary will authenticate the child's age and acquire consent from the guardian. There is a prohibition from conducting activities that may endanger children's privacy, such as profiling and target-based advertising⁷.

4. Right to Confirmation and Access

The data protection framework enables the data subject various rights, with "the right to confirmation and access, the right to correction and erasure, the right to data portability, and the right to be forgotten". The "Data Subject" can request to "update, alter, correct, erase or prevent or limit further disclosure" of their data.

5. System Design

The data fiduciary must take the essential measures to implement "privacy by design", transparency and security safeguards. Transparency means "the disclosure of steps taken to protect personal data, and security safeguards include the use of appropriate de-identification, encryption mechanisms, integrity protection, and access control mechanisms". The type and size define significant Data Fiduciaries and the severity of data being processed by a data fiduciary or processed by a class of data fiduciaries". Each social media company designated as a "Significant Data fiduciary" will be responsible

⁷ "Data Privacy Day 2022: Indian Personal Data Protection Bill 2019's benefits and effect on the industry | The Financial Express," Data Privacy Day 2022: Indian Personal Data Protection Bill 2019's benefits and effect on the industry | The Financial Express, Jan. 28, 2022. <https://www.financialexpress.com/industry/technology/data-privacy-day-2022-indian-personal-data-protection-bill-2019s-benefits-and-effect-on-the-industry/2418894/>. (Accessed Dec. 09, 2022).

for validating the account of India-based users⁸. And this will enforce the functions of the systems into its evolution.

DISCUSSION

1. Framework and Consent

Indian organisations would have undertaken GDPR compliance only if they provided goods/services to EU citizens, tracked EU citizens' behaviour, or had an establishment in the EU. If the organisations are already GDPR compliant, one of the noteworthy variances between the GDPR and the PDPB is data localisation requirements regarding critical and sensitive data. Another challenge is that the definition of critical data is not yet comprehensive. Implementing the framework will require much effort from the organisation. Most organisations that deal with end-user data have begun to analyse the provisions of the Bill and carry out assessments to understand the gap between current practices and requirements. However, since the Bill may change, organisations are at present not implementing any significant changes. Fundamental measures such as creating a policy and its impact are being studied⁹.

2. Comparison of PDPB and GDPR

The PDPB was proposed for India and has been inspired by GDPR. GDPR and PDPB share many similarities and only a few differences.

The primary distinction is that both frameworks take diverse approaches to sensitive and critical personal data. The EU permits cross-border data transfers to non-E.U. Countries or firms under GDPR if the commission determines that the transfers provide 'adequate' protection. These transfers will not require any special permission. Adequate would mean "the nature of the data, law and enforcement in non-EU countries/territories, international relations, and the commitment of data fiduciaries to data security and safeguarding are all criteria for an adequate level of protection." The PDPB imposes more restrictions on data transfer across borders. For data categorised as sensitive personal data, DPPI would sanction the transfer of a party to a location extending the border of the country and decide whether such a transfer is adequately protected.

Another significant distinction is that the PDPB and GDPR take different methods of reporting breaches in data privacy. In the PDPB, the data fiduciaries must account for the data breaches straight to the DPA. The severity of the harm will be considered, and the necessary action will be taken. The "Data controller" must inform the "Data principal" directly of any data breach. The data subject has more power under GDPR¹⁰.

The PDPB defines a Significant Data fiduciary, which is not in the GDPR. The PDPB has the idea of a consent manager. A consent manager is basically defined as "an entity that manages and updates all consent records provided by the data principal."

GDPR and PDPB have provisions protecting children's personal data during processing. According to the PDPB, anyone under 18 is considered a child in India. Before data processing, the PDPB requires age verification and consent from the authorised guardian. Conducting profiling, targeted advertising, or other actions that may endanger children is prohibited under PDP, but the GDPR does not mention such a restriction.

Both frameworks have different definitions and approaches regarding Data principal rights. According to the PDP Bill, if a Data Fiduciary is not gathering personal data straight from the data principal, it must reveal the source of such data. While in contrast, GDPR requires data controllers to provide "the source of the collection, the purpose for which the data will be used, the categories of data obtained, the further recipient of this data, with any other relevant information. If the data controller uses "profiling,

⁸A. Burman, "Will a GDPR-Style Data Protection Law Work For India?," Carnegie India. <https://Carnegieindia.Org/2019/05/15/Will-Gdpr-Style-Data-Protection-Law-Work-for-India-Pub-79113>. (Accessed Dec. 09, 2022).

⁹ J. Andrew and M. Baker, "The General Data Protection Regulation in the Age of Surveillance Capitalism," *Journal of Business Ethics*, vol. 168, no. 3, pp. 565-578, Jan. 2021, doi: 10.1007/s10551-019-04239-z.

¹⁰ "View: How Personal Data Protection Bill is expected to change the way privacy is perceived and practised," *The Economic Times*. <https://economictimes.indiatimes.com/opinion/et-commentary/view-how-personal-data-protection-bill-is-expected-to-change-the-way-privacy-is-perceived-and-practised/articleshow/88530207.cms> (accessed Dec. 09, 2022).

automated decision-making, or behavioural analysis", the data subject has the "right to request" information about it under GDPR. Such a provision does not exist in the PDPB¹¹.

According to GDPR, if a "Data controller" wants to utilise the personal data for uses other than those it was collected or intended for, then the Data controller should inform the data subject of the intention of processing and other related information. The PDPB contains no provision for such additional processing. The data subjects do have the decision not to participate in "profiling and automated decision-making" in GDPR, but there are no such provisions available in the PDPB.

GDPR provides the data principals with the "right to restrict" and the "right to object". Instead of deletion, the data principal may limit his processing. The Data subjects can object to the processing under GDPR at any time. In place of the right to restrict, the PDPB provides the "right to be forgotten." PDPB has a trust score, whereas the GDPR has a fiduciary data certificate.

3. Current Status

The Government of India has taken a significant step in withdrawing the PDPB after four years of its proposal since many issues were identified that were relevant yet beyond the scope of modification. There were 81 amendments and 12 recommendations given by the Joint Parliament commission. PDPB faced considerable resistance from privacy, civil society activists, and extensive technology firms like Facebook and Google. The tech companies had issues with "Data localisation", while the activists had problems with government agencies being given specific exemptions. The postponements in implementing the Bill have been condemned by stakeholders who say that India, one of the world's prime internet markets, is not equipped with a rudimentary agenda to shield citizens' privacy. "The retraction of the Data Protection Bill, 2019, is worrying because a deferred regulation is being discarded." An executive director of Delhi-based digital rights organisation Internet Freedom Foundation says, "It is not about getting a perfect law, but it is about getting a law at this point. It has been close to 10 years since the (Justice) A P Shah Committee report on privacy, five years since the Puttaswamy judgement (right to privacy) and four years since the (Justice B N) Srikrishna Committee's report – they all gestured earnestness for a data protection law and surveillance reforms. Every day that passes results in more injury and harm."

The government is contemplating enhancing the prearranged new form of the "Information Technology Act" and permitting cross-border data flows only to "trusted geographies". "The rationale is that the data should be warehoused in a region that the Indian government trusts and that data should be reachable in the event of a crime," the government official explained. Conferring to senior government officials, "the new data protection Bill will abandon some JCP recommendations, such as including trusted hardware and limited storage of personal data within India's borders. Instead, it will incorporate these concepts into the greater agenda for the Internet ecosystem, which will replace the Information Technology Act of 2000". The PDPB happens to be "compliance intensive"¹².

The adorned Bill will be easier to comply with. The Minister of State of IT said, "This will soon be swapped by a comprehensive framework of global standard laws, including digital privacy laws, for contemporary and future challenges and catalyse PM Narendra Modi's vision of India Techade"¹³.

THE IMPLICATIONS OF PDPB ON BUSINESS


1. Responding to Data Localisation

Data localisation requirements can become a huge operational challenge for organisations. They must ensure that the cloud servers' hosting locations are in India and that the data is not going outside India. However, it defeats the entire purpose of having data on the cloud and overcoming the availability challenges. These access issues could prove to be a significant barrier to multinational firms. However,

¹¹ B. Marr, "How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read," *Forbes*, May 21, 2018. <https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/> (accessed Dec. 09, 2022).

¹² S. Barik, "Explained: Why the Govt has withdrawn the Personal Data Protection Bill, and what happens now," *The Indian Express*, Aug. 04, 2022. <https://indianexpress.com/article/explained/explained-sci-tech/personal-data-protection-bill-withdrawal-reason-impact-explained-8070495/> (accessed Dec. 14, 2022).

¹³ B. R. & PTI and @bsindia, "Govt withdraws Data Protection Bill, 2021, will present new legislation," *Govt withdraws Data Protection Bill, 2021, will present new legislation | Business Standard News*, Aug. 03, 2022. https://www.business-standard.com/article/economy-policy/centre-withdraws-personal-data-protection-bill-2019-to-present-new-bill-122080301226_1.html (accessed Dec. 09, 2022).



most Indian brands may not have troves of SPD on foreign soil. Cloud service providers have already started introducing regions in India to enable their customers to comply with data localisation requirements. Ex. AWS and Azure have local instances in India.

2. Dealing with the Cost of compliance

Considering the bigger picture, once a data protection bill comes into the picture and starts levying fines on organisations, it will be way more expensive than investing money in compliance initiatives initially. It may be an initial challenge for small-scale and medium-scale organisations. If they have exposure to GDPR, things might look easier on their part. Small and medium organisations are likely to be hit the most. They usually do not have sufficient skills and know-how to address IT and security risks, which may mean an additional burden. However, this will open up opportunities for the services sector to serve such clients and to get them on the green with the requirements of the Data Privacy law once approved.

CONCLUSION

After four years of its proposal, the Government of India has taken a significant step in withdrawing the PDPB since many relevant issues were identified that were beyond the scope of modification. There were 81 amendments and 12 recommendations given by the Joint Parliament commission. PDPB faced considerable resistance from privacy, civil society activists, and extensive technology firms like Facebook and Google. The tech companies had issues with "Data localisation", while the activists had problems with government agencies being given specific exemptions. The postponements in implementing the Bill have been condemned by stakeholders who say that India is one of the world's prime internet markets and is not equipped with a rudimentary agenda to shield citizens' privacy. "The retraction of the Data Protection Bill, 2019, is worrying because a deferred regulation is being discarded." An executive director of Delhi-based digital rights organisation Internet Freedom Foundation says, "It is not about getting a perfect law, but it is about getting a law at this point. It has been close to 10 years since the (Justice) A P Shah Committee report on privacy, five years since the Puttaswamy judgement (right to privacy) and four years since the (Justice B N) Srikrishna Committee's report – they all gestured earnestness for a data protection law and surveillance reforms. Every day that passes results in more injury and harm."

The government is contemplating enhancing the prearranged new form of the "Information Technology Act" and permitting cross-border data flows only to "trusted geographies". "The rationale is that the data should be warehoused in a region that the Indian government trusts and that data should be reachable in the event of a crime," the government official explained. Conferring to senior government officials, "the new data protection Bill will abandon some JCP recommendations, such as including trusted hardware and limited storage of personal data wit. Rather than being an independent entity, the new PDPB will be integrated into a broader agenda for the Internet ecosystem that will supersede the 2000 Information Technology Act. Although the PDPB requires significant compliance efforts, the updated Bill will be easier to comply with. According to the Minister of State for IT, the PDPB will soon be replaced by a comprehensive framework of laws of global standards, including digital privacy laws, to address current and future challenges and support PM Narendra Modi's vision for India Techade in India's borders.

The proposed PDPB is a significant step in India's data protection and privacy enhancement. India is advancing digitisation, and a robust and competent data protection law is critical. Implications of the PDPB are correctly stated in a statement by the EU upon its introduction of the PDPB, "with the new law in place, India will join the growing global trend of convergence in this area. This is certainly true for the Asia-Pacific region, where countries such as Japan, Korea, and New Zealand have enacted data protection laws based on these principles. Still, it is also true for many other parts of the world. As a leading global economy and the world's largest democracy, India's support for high levels of data protection would serve as a critical example of a growing demand for international privacy standards."

The Bill, has constraints regarding data localisation and implementation. Although the initial rationale behind implementing localisation was that Indian people's data must not be used for any criminal activities and should be locally available in case of any investigation. The broader idea of data protection and privacy in the Indian context must be considered for successful implementation whenever this Bill or its amendments is passed as law.

REFERENCES

- [1] HARISH SURYAVANSHI, "India's Personal Data Protection Bill ('PDP Bill'), 2018: Brief Introduction, Key Provisions and Comparison with GDP".
- [2] Bailey R., V. Bhandari, S. Parsheera, and F. Rahman, "Comments on the (Draft) Personal Data Protection Bill, 2018," 2018.
- [3] Singh R. G., S. Ruj, "A Technical Look At The Indian Personal Data Protection Bill," May 2020, [Online]. Available: <http://arxiv.org/abs/2005.13812>
- [4] Prasad D. M. and S. C. Menon, "The Personal Data Protection Bill, 2018: India's regulatory journey towards a comprehensive data protection law," *International Journal of Law and Information Technology*, vol. 28, no. 1, pp. 1-19, Jun. 2020, doi: 10.1093/ijlit/aaaa003.
- [5] Tankard C., "What the GDPR means for businesses," *Network Security*, vol. 2016, no. 6, pp. 5-8, Jun. 2016, doi:10.1016/S1353-4858(16)30056-3.
- [6] Poulami Sen, "EU GDPR and Indian Data Protection Bill: A comparative study." [Online]. Available: <https://gdpr-info.eu/art-1-gdpr/>
- [7] "Data Privacy Day 2022: Indian Personal Data Protection Bill 2019's benefits and effect on the industry | The Financial Express," *Data Privacy Day 2022: Indian Personal Data Protection Bill 2019's benefits and effect on the industry | The Financial Express*, Jan. 28, 2022. <https://www.financialexpress.com/industry/technology/data-privacy-day-2022-indian-personal-data-protection-bill-2019s-benefits-and-effect-on-the-industry/2418894/>. (Accessed Dec. 09, 2022).
- [8] Burman, "Will a GDPR-Style Data Protection Law Work For India?," *Carnegie India*. <https://Carnegieindia.Org/2019/05/15/Will-Gdpr-Style-Data-Protection-Law-Work-for-India-Pub-79113>. (Accessed Dec. 09, 2022).
- [9] Andrew J. and M. Baker, "The General Data Protection Regulation in the Age of Surveillance Capitalism," *Journal of Business Ethics*, vol. 168, no. 3, pp. 565-578, Jan. 2021, doi: 10.1007/s10551-019-04239-z.
- [10] *Economic Times Article*, "View: How Personal Data Protection Bill is expected to change the way privacy is perceived and practised," *The Economic Times*. <https://economictimes.indiatimes.com/opinion/et-commentary/view-how-personal-data-protection-bill-is-expected-to-change-the-way-privacy-is-perceived-and-practised/articleshow/88530207.cms> (accessed Dec. 09, 2022).
- [11] Marr B., "How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read," *Forbes*, May 21, 2018. <https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/> (accessed Dec. 09, 2022).
- [12] Barik S., "Explained: Why the Govt has withdrawn the Personal Data Protection Bill, and what happens now," *The Indian Express*, Aug. 04, 2022. <https://indianexpress.com/article/explained/explained-sci-tech/personal-data-protection-bill-withdrawal-reason-impact-explained-8070495/> (accessed Dec. 14, 2022).
- [13] *Business Review Article & PTI and @bsindia*, "Govt withdraws Data Protection Bill, 2021, will present new legislation," *Govt withdraws Data Protection Bill, 2021, will present new legislation | Business Standard News*, Aug. 03, 2022. https://www.business-standard.com/article/economy-policy/centre-withdraws-personal-data-protection-bill-2019-to-present-new-bill-122080301226_1.html (accessed Dec. 09, 2022).