

AN ANALYSIS ON DIGITAL PERSONAL DATA PROTECTION BILL, 2022

Author: Samriddhi Singh, pursuing B.A.,LL.B.(Hons.) from ICAI Law School, Hyderabad

ABSTRACT

The Digital Personal Data Protection Bill, 2022 is a landmark legislation aimed at safeguarding personal data in the digital age. With the increasing use of technology, personal data has become a valuable commodity and is vulnerable to unauthorized access, misuse, and exploitation. The bill aims to address these issues by providing a comprehensive framework for the protection of personal data.

The bill defines personal data as any information that relates to an individual and can be used to identify them. It covers a wide range of data, including but not limited to, names, addresses, financial information, health information, and biometric data. The bill also lays down strict guidelines for the collection, storage, processing, and dissemination of personal data by data controllers and processors.

The bill establishes a data protection authority to oversee the implementation of the provisions of the bill and to address the grievances of individuals. The authority has the power to investigate, enforce, and impose penalties for violations of the bill. In addition, the bill provides for the right of individuals to access, rectify, and erase their personal data, and to object to its processing. It also provides for the right to data portability, allowing individuals to transfer their personal data from one controller to another.

This paper provides a comprehensive analysis of the Digital Personal Data Protection Bill, 2022. The paper discusses the key provisions of the bill and their implications for individuals and organizations. It also highlights the challenges in implementing the provisions of the bill and the need for a robust enforcement mechanism.

In conclusion, the Digital Personal Data Protection Bill, 2022 is a step in the right direction toward protecting personal data in the digital environment and ensuring the privacy rights of individuals. This Essay provides a valuable resource for policy-makers, organizations, and individuals to understand the provisions of the bill and its implications for personal data protection.

Introduction

¹The Digital Personal Data Protection Bill, 2022 is a proposed legislation in India that aims to protect the personal data of individuals. The bill seeks to establish a framework for collecting, storing, and processing personal data and provide individuals with rights over their personal data.

Under the bill, companies will be required to obtain consent from individuals before collecting their personal data and will be required to disclose the purposes for which the data will be used. The bill also establishes a Data Protection Authority, which will be responsible for enforcing the provisions of the bill and for handling complaints related to processing personal data.

The bill also includes provisions for data localization, which would require certain types of data to be stored within India's borders, and *the right to be forgotten*, which would allow individuals to request the deletion of their personal data. The bill also mandates that organizations get individuals' explicit consent before collecting, using, or disclosing sensitive personal data, such as financial information and medical records.

Overall, the Digital Personal Data Protection Bill, 2022 represents an attempt by the Indian government to address concerns about the protection of personal data in the digital age and to give individuals greater control over their personal information.

Why Data Protection Is Necessary

Data protection is important because it helps to ensure that personal information is kept secure and private. Personal information can include a wide range of data, such as name, address, date of birth, financial information, and medical records. When this type of information is collected and stored by organizations, it is important to have appropriate safeguards in place to protect it from unauthorized access, use, or disclosure. Data protection helps to protect the privacy of individuals and can also help to prevent identity theft and other types of cybercrime.

¹Harsh Walia†, Digital Personal Data Protection Bill 2022: Juxtaposing the Old and the New, 2022 SCC OnLine Blog Exp 86, (January 18, 2023, 9:26 AM), <https://www.sconline.com/blog/post/2022/12/16/digital-personal-data-protection-bill-2022-juxtaposing-the-old-and-the-new/#:~:text=The%202022%20Bill%20envisages%20that,time%20of%20notifying%20such%20jurisdictions>

The Data Protection Board of India (Board) is a body that has been set up under the Personal Data Protection Bill, 2019 (PDPB) to regulate the processing of personal data in India. The Board is responsible for the overall supervision of the implementation of the PDPB, including the development of guidelines and codes of conduct, the handling of complaints, and the enforcement of the provisions of the Personal Data Protection Bill. It is composed of a Chairperson and six other members, who are appointed by the Central Government. The Chairperson and members of the Board are required to have expertise in the field of data protection and related laws. The Board is empowered to exercise all the powers and functions conferred upon it by the Personal Data Protection Bill and to perform such other duties and functions as may be prescribed by the Central Government.

What the Digital Personal Data Protection Bill Has To Say About The Protection Of Personal Data

This Act aims to create rules for the processing of digital personal data in order to respect both the need to process personal data for legal purposes and individuals' right to data protection.²Section 2(13) of the act says about the term "Personal data" which refers to any information that can be used to identify an individual and Section 2(14) says about the term "Personal data breach" which refers to any unauthorized processing of personal information or an unintentional acquisition, sharing, use, alteration, destruction, or loss of access to personal information that jeopardizes the privacy, integrity, or accessibility of personal information.

The Digital Personal Data Protection Bill, 2022 lays out several provisions aimed at protecting personal data in India. Some of the key sections related to the protection of personal data include:

1. Collection and Processing of Personal Data: This section lays out the rules for the collection and processing of personal data by data fiduciaries, including obtaining consent from individuals, purpose limitation, and storage limitation.

²"The Digital Personal Data Protection Bill, 2022" S.2, https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Protection%20Bill%2C%202022_0.pdf (January 5, 2023)

2. **Rights of Data Principals:** This section outlines the rights of individuals with respect to their personal data, including the right to access, correct, delete, and portability of their data.
3. **Data Auditing and Certification:** This section requires data fiduciaries to conduct regular audits of their data protection practices and to obtain certifications from accredited data protection agencies.
4. **Data Protection Officers:** This section requires data fiduciaries to appoint a Data Protection Officer to oversee the organization's data protection practices and to serve as a point of contact for individuals seeking to exercise their rights.
5. **Data Localization:** This section requires data fiduciaries to store certain categories of personal data on servers located within India.
6. **Cross-Border Data Transfers:** This section regulates the transfer of personal data to foreign countries, including the requirement for data fiduciaries to enter into data transfer agreements with foreign entities and to obtain the prior approval of the government.
7. **Penalties and Remedies:** This section outlines the penalties for non-compliance with the provisions of the Bill, including monetary fines, imprisonment, and compensation for harm suffered by individuals as a result of a data breach.
8. **Establishment of a Data Protection Authority:** This section establishes the Data Protection Authority, an independent body responsible for overseeing the implementation of the provisions of the Bill and for ensuring the protection of personal data in India.


Disadvantages of Digital Personal Data Protection Bill 2022

It also has several disadvantages that may impact businesses and individuals alike.

The major disadvantages of the bill are the-

1. **Cost of compliance-** Businesses will need to invest in new systems and processes to ensure they are in compliance with the bill's requirements. This can be a significant

financial burden for small and medium-sized enterprises (SMEs) that may not have the resources to make these changes.

2. **Limited innovation:** Strict regulations on data collection and usage may impede innovation in the tech industry, as companies may be hesitant to develop new products and services that could run afoul of the law.
 3. **Privacy concerns:** Some people may be concerned that the bill could be used to restrict their privacy rights and enable government surveillance and also individuals may be hesitant to share personal information with organizations and businesses that they perceive as untrustworthy.
 4. **Administrative burden:** Businesses may face significant administrative burdens to comply with the regulations set forth in the bill. The bill may also lead to increased bureaucracy and administrative burden for businesses, as they will need to comply with the regulations set out in the bill. This could lead to delays in the processing of personal data and could impede the efficiency of businesses.
- 
5. **Infringement of freedom of speech:** The bill may restrict freedom of speech and expression by regulating content online, which would be an infringement of the fundamental rights of citizens.
 6. **Complex Regulations:** The bill may be difficult for businesses and organizations to understand and comply with, leading to confusion and potential non-compliance.
 7. **Increased Government Surveillance:** The bill may lead to increased government surveillance as they will have more power to access and monitor personal data in the name of protecting it.

8. Lack of International Harmonization: The bill may not be in line with the data protection laws of other countries, which could create difficulties for companies operating in multiple jurisdictions.
9. Limited scope: The bill may not cover all types of personal data, which could leave some individuals vulnerable to data breaches and other privacy violations.
10. Confusion among individuals about their rights and responsibilities regarding their personal data, could lead to a lack of trust in digital platforms and services.

Overall, while the Digital Personal Data Protection Bill 2022 aims to protect personal data, it may also have negative consequences for businesses and individuals. It is important for lawmakers to carefully consider the potential drawbacks of the bill before implementing it.

Elements to Be There In The Personal Data Protection Bill

It is important to note that any legislation related to personal data protection should include strong measures to safeguard individual's personal information, including measures to prevent misuse and unauthorized access to personal data. Additionally, it is important for individuals to be aware of their rights and for organizations to be held accountable for any breaches of personal data protection laws.

However, there are certain key elements that are generally considered important for a robust personal data protection law.

- Strong data protection principles: The bill should establish clear and comprehensive data protection principles, such as data minimization, data accuracy, data security, and data retention. These principles should be binding on all data controllers and processors and should be enforceable by a regulatory body.
- Right to be informed: The bill should give individuals the right to be informed about how their personal data is being collected, used, and shared. This should include clear and concise explanations of the data controller's purpose for collecting the data, the types of data being collected, and the rights of the data subject.

- **Right to access:** The bill should give individuals the right to access their personal data and to receive a copy of it. This should include the right to request that any inaccuracies are corrected or that data be erased.
- **Right to object:** The bill should give individuals the right to object to the processing of their personal data for certain purposes, such as direct marketing.
- **Right to data portability:** The bill should give individuals the right to receive their personal data in a structured, commonly used, and machine-readable format, and to transmit it to another data controller.
- **Right to be forgotten:** The bill should give individuals the right to have their personal data erased in certain circumstances.
- **Data security:** The bill should require data controllers and processors to implement appropriate technical and organizational measures to protect personal data from unauthorized access, use, alteration, or destruction.
- **Data breach notification:** The bill should require data controllers and processors to notify individuals and the relevant regulatory authority in the event of a data breach.
- **Regulatory oversight:** The bill should establish an independent regulatory body with the power to enforce the data protection provisions and to impose penalties on data controllers and processors that violate the law.

BRILLOPEDIA

Overall, a comprehensive digital personal data protection bill should provide individuals with control over their personal data and should hold data controllers and processors accountable for complying with the data protection principles. If a bill is able to do this, then it can be considered a strong bill that can protect personal data effectively.

Focused Areas Of The Bill

The Digital Personal Data Protection Bill, 2022 is not yet an official bill, but it is expected to give importance to the following areas:

- **Collection, storage, and use of personal data:** The bill is expected to lay down rules for how organizations can collect, store, and use personal data, with a focus on obtaining informed consent from individuals.
- **Data security:** The bill is expected to require organizations to implement measures to protect personal data from unauthorized access, use, disclosure, alteration, or destruction.
- **Data accuracy:** The bill is expected to require organizations to take steps to ensure that personal data is accurate and up-to-date.
- **Data retention and destruction:** Data retention and destruction: The bill sets out rules for the retention and destruction of personal data, including the time period for which data can be retained and the procedures for destruction.
- **Data portability:** The bill is expected to give individuals the right to obtain a copy of their personal data in a commonly used format and to have it transmitted to another organization.
- **Right to be Forgotten:** The bill is expected to give individuals the right to request that their personal data be deleted by the organization.
- **Data breaches:** The bill is expected to require organizations to notify individuals and authorities in the event of a data breach.
- **Appointing Data Protection Officer (DPO):** The bill is expected to make it mandatory for organizations to appoint DPO.

- **Penalties:** The bill lays out penalties for non-compliance, including fines and penalties for companies and organizations that fail to adhere to the bill's provisions.

These are some of the main areas that are expected to be covered in the Digital Personal Data Protection Bill, 2022. However, it is important to note that this bill is not yet officially released and the actual content of the bill may differ from what is currently expected.

Problems That Might Be Faced While Implementing the Bill

In general, data protection laws and regulations can have loopholes that may be exploited by malicious actors. These can include weak enforcement mechanisms, ambiguities in the language of the law, or exceptions that allow certain types of data collection or sharing to occur without consent. It is important for individuals and organizations to stay informed about data protection laws and regulations and advocate for stronger protections to close any loopholes that may exist.

Requirements for Successful Implementation of The Bill

The success of the implementation of the Digital Personal Data Protection Bill, 2022 can be achieved through several key steps:

- **Clear and consistent communication:** The government and relevant authorities should communicate clearly and consistently about the bill's provisions, requirements, and penalties for non-compliance.
- **Education and training:** Both organizations and individuals should be educated and trained on the bill's provisions, as well as best practices for protecting personal data.
- **Strong enforcement:** The government and relevant authorities should have strong enforcement mechanisms in place to ensure compliance with the bill and to hold organizations and individuals accountable for any breaches or violations.

- **Regular reviews and updates:** The bill should be regularly reviewed and updated to ensure that it remains relevant and effective in protecting personal data.
- **Collaboration with stakeholders:** The government should collaborate with industry groups, privacy advocates, and data protection authorities to ensure that the bill effectively protects personal data.
- **Adequate resources:** Adequate resources should be provided to the relevant authorities to implement and enforce the bill effectively.
- **Public participation:** The government should encourage public participation in the process of implementing the bill, by providing opportunities for feedback and input from citizens.
- **Strong oversight:** The bill should establish an independent oversight body responsible for enforcing the legislation and ensuring compliance.
- **Public education and awareness:** The government should conduct a public education campaign to raise awareness about the bill and the rights of individuals with regard to their personal data.
- **Cooperation between government and private sector:** The government should work closely with private sector organizations to ensure that they are aware of their obligations under the bill and are able to comply with it.

- Regular review and updates: The legislation should be reviewed and updated regularly to keep up with the evolving digital landscape and changing technologies.

Context of Right To Be Forgotten in The Bill

The "right to be forgotten" is a concept that gives individuals the ability to request that their personal data be deleted from a company's records. In the context of a digital personal data protection bill, it would likely give individuals the right to request that their personal information be removed from a company's databases and any other places where it is stored.

It is important to note that the right to be forgotten is not absolute and may be subject to certain limitations or exceptions. For example, in some cases, the company may not be able to delete certain information due to legal or regulatory requirements.

In terms of how the data would actually be deleted, it would depend on the specific language of the bill and the technological capabilities of the company in question. The company would likely be required to take reasonable steps to delete the data in question, which may include physically destroying records, overwriting data, or using other data-erasure techniques.

One potential method for erasing data would be for companies to have a process in place for receiving and reviewing requests for data deletion, and then physically removing the data from their servers and backups. Another method could involve the use of software tools that can search for and delete specific data points across a company's systems.

The right to be forgotten gives individuals the ability to request that their personal data be deleted from a company's systems. However, it is not a guarantee that all copies of the data will be completely erased from all systems, as it may have been shared with third parties or backup systems.

Conclusion

In conclusion, the Digital Personal Data Protection Bill of 2022 represents a significant step toward ensuring the privacy and protection of individual digital data. The bill recognizes the growing importance of personal data in the digital age and the need for legislation to secure it. The provisions of the bill, including the requirement for organizations to obtain consent for data collection, the establishment of a data protection authority, and the penalties for violations, provide robust safeguards for individuals' digital privacy.

However, the implementation of the bill will require careful consideration and monitoring to ensure that it is effective in practice. The bill will also have to adapt to the evolving landscape of technology and privacy concerns and be updated as necessary to remain relevant.

Overall, the Digital Personal Data Protection Bill of 2022 is a positive development that lays the foundation for a secure and privacy-respecting digital environment. It is up to organizations and individuals to work together to ensure that the protections provided by the bill are upheld and that personal digital data remains secure.

However, it is important to note that the overall effectiveness of data protection legislation depends on a variety of factors, including the specific provisions of the law and its implementation and enforcement.



BRILLOPEDIA