International Journal of Law
www.lawjournals.org
ISSN: 2455-2194
Received: 09-02-2025, Accepted: 10-03-2025, Published: 25-03-2025
Volume 11, Issue 3, 2025, Page No. 127-131

The digital personal data protection Act, 2023: A legal analysis in light of global data protection standards

Prabhash Dalei
Assistant Professor, Department of Law, Utkal University, Bhubaneswar, Odisha, India

Abstract
The Digital Personal Data Protection (DPDP) Act, 2023 represents a landmark development in India's legislative approach to data privacy, aiming to regulate the processing of personal data while balancing individual rights and business interests. This research paper critically examines the Act's key provisions, including its definitions of personal data, obligations of data fiduciaries, rights of data principals, and enforcement mechanisms. A comparative analysis with international data protection regimes, particularly the European General Data Protection Regulation (GDPR), is undertaken to assess the Act's compatibility with global best practices. The study also explores the Act's impact on privacy rights as recognized under Article 21 of the Indian Constitution, its implications for government surveillance, and its potential effects on cross-border data transfers. Key concerns such as the lack of a distinct category for sensitive personal data, the broad exemptions granted to the government, and the absence of an independent Data Protection Board with sufficient autonomy are critically evaluated. Furthermore, the research identifies gaps in the Act's enforcement mechanisms and proposes reforms to enhance its effectiveness in ensuring robust data protection while fostering digital innovation and economic growth. By addressing these concerns, this paper contributes to the ongoing discourse on data protection law in India and provides recommendations for a more balanced and rights-centric regulatory framework.

Keywords: Data protection personal data, digital economy, legislative framework.

Introduction

In the digital age, personal data has emerged as a critical asset, driving economic, technological, and governance innovations. However, with this digital transformation comes the challenge of safeguarding individuals' privacy and ensuring responsible data usage. The growing concerns over data breaches, surveillance, and the misuse of personal information have necessitated strong legal frameworks to regulate data protection.

India's journey towards a comprehensive data protection law gained momentum following the landmark judgment in K.S. Puttaswamy vs. Union of India (2017), wherein the Supreme Court recognized the right to privacy as a fundamental right under Article 21 of the Indian Constitution. This ruling underscored the urgent need for a dedicated legal framework to regulate the collection, processing, and storage of personal data in India. Consequently, the government initiated efforts to draft a data protection law, starting with the Justice B.N. Srikrishna Committee Report (2018), which laid the groundwork for subsequent legislative developments.

The first draft, the Personal Data Protection Bill, 2019, proposed a comprehensive data protection regime but faced criticism for its exemptions granted to the government and potential dilution of privacy rights. After multiple revisions and consultations, the bill was withdrawn and replaced with a fresh framework, culminating in the enactment of the Digital Personal Data Protection (DPDP) Act, 2023.

The DPDP Act, 2023, aims to strike a balance between individual privacy rights and the growing needs of a digital economy. It introduces a structured regulatory mechanism for data fiduciaries (entities that process personal data) and grants specific rights to data principals (individuals whose data is collected). The Act also establishes the Data Protection Board of India (DPBI) as a regulatory body for monitoring compliance and resolving disputes.

Despite its progressive elements, the DPDP Act has sparked debates on various fronts, including the extent of governmental exemptions, cross-border data transfer policies, and the adequacy of safeguards for data principals. This paper seeks to examine the DPDP Act's key provisions, compare it with global data protection standards like the GDPR, and highlight areas that require further refinement to ensure stronger data privacy protections in India.

Key Principles of the DPDP Act, 2023

The Digital Personal Data Protection (DPDP) Act, 2023, is based on seven key principles that ensure lawful and responsible data processing, balancing individual privacy with business and government interests. The first principle, Consent, Lawfulness, and Transparency, mandates that personal data be collected lawfully with explicit and informed consent. Data fiduciaries must clearly communicate the purpose of data collection and processing, ensuring fairness and transparency. Purpose Limitation restricts the use of personal data strictly to its original purpose, preventing unauthorized secondary use without fresh consent. Similarly, Data Minimization ensures that only necessary data is collected, reducing privacy risks associated with excessive data hoarding. The Data Accuracy principle requires data fiduciaries to maintain correct and updated personal data, allowing individuals to request corrections. This is particularly important for sectors like finance and healthcare, where accuracy is critical. Storage Limitation mandates that personal data be erased once it is no longer needed, reducing the risk of breaches and unauthorized access. Reasonable Security Safeguards obligate data fiduciaries to implement encryption, access

controls, and other measures to protect data from cyber threats. Finally, Accountability ensures compliance by requiring organizations to maintain records, adhere to data protection norms, and be answerable for breaches. The Data Protection Board of India (DPBI) oversees enforcement, investigates violations, and imposes penalties.

Together, these principles create a robust framework that protects individual privacy while supporting digital innovation and economic growth. The Act aligns with global standards like the GDPR, ensuring India's data protection framework is comprehensive and effective.

Key Provisions of the DPDP Act, 2023

The Digital Personal Data Protection (DPDP) Act, 2023, establishes a comprehensive framework for the regulation of personal data processing in India. The Act sets out specific provisions regarding its applicability, the rights and duties of individuals (data principals), obligations of entities processing data (data fiduciaries), the role of the regulatory authority, special provisions for children, cross-border data transfers, and exemptions granted under the law. These provisions collectively aim to safeguard individual privacy while facilitating the responsible use of personal data in the digital economy.

Applicability

The DPDP Act applies to the processing of personal data in a broad range of circumstances, ensuring that individuals' privacy is protected across different domains. The law covers all digital personal data collected within India, meaning any data that is either initially collected in digital form or later digitized falls under its jurisdiction. Additionally, it extends to offline personal data that is later digitized, ensuring that the legal framework remains relevant in an increasingly digitalized society. Moreover, the Act has extra-territorial applicability, meaning that even if data is processed outside India, it still falls within the scope of the law if it is related to the offering of goods or services to individuals in India. This provision is crucial in regulating multinational companies that collect and process Indian citizens' data from offshore locations, aligning the law with global best practices such as the General Data Protection Regulation (GDPR) of the European Union.

Rights and Duties of Data Principals

The DPDP Act grants several rights to data principals, who are individuals whose personal data is being collected or processed. These rights are designed to empower individuals and provide them with control over their data. One of the most fundamental rights is the right to seek information regarding how their data is being processed. Data principals can request details about the nature, purpose, and extent of data processing, ensuring transparency and accountability.

Furthermore, individuals have the right to request correction and erasure of their data**.** If any personal data is found to be inaccurate or outdated, data principals can demand its rectification. Similarly, if the data is no longer required for its original purpose, individuals can request its deletion to prevent unnecessary retention. The Act also introduces the right to nominate a representative in case of death or incapacity. This provision allows individuals to appoint someone to exercise their data rights on their behalf, ensuring continuity in protecting their privacy even in unforeseen circumstances.

Another crucial right granted under the Act is the right to file grievances regarding data breaches**.** If a data principal believes that their data has been mishandled, misused, or exposed in a security breach, they can file a complaint with the data fiduciary. If the issue remains unresolved, they can escalate the grievance to the Data Protection Board of India (DPBI)**,** which serves as the regulatory authority overseeing compliance with the Act.

Obligations of Data Fiduciaries

Entities that collect, store, or process personal data, referred to as data fiduciaries, are subject to a set of stringent obligations to ensure responsible data handling. One of their primary responsibilities is to maintain the accuracy and security of personal data. This requires data fiduciaries to adopt appropriate technological and organizational measures to ensure that the data they store is up to date, protected from unauthorized access, and secured against cyber threats.

Data fiduciaries are also required to inform the Data Protection Board of India (DPBI) in case of a data breach. This notification obligation ensures that affected individuals can take necessary precautions to mitigate potential harm arising from data leaks or cyberattacks. Additionally, fiduciaries must erase personal data once its purpose is fulfilled. This aligns with the principle of storage limitation, ensuring that personal data is not retained indefinitely without justification.

Role of the Data Protection Board of India (DPBI)

The Data Protection Board of India (DPBI) plays a central role in enforcing the provisions of the DPDP Act and ensuring compliance among data fiduciaries. The DPBI is entrusted with responsibilities such as monitoring data protection practices, adjudicating disputes, and penalizing entities that violate data protection norms. It has the authority to investigate complaints, impose fines, and issue directions to erring organizations.

An essential feature of the DPBI's mandate is its quasi-judicial authority, which allows it to hear disputes between individuals and organizations regarding data protection violations. In cases where data principals or fiduciaries are dissatisfied with the DPBI's rulings, they can appeal to the Telecom Disputes Settlement and Appellate Tribunal (TDSAT). This appeal mechanism ensures an additional layer of oversight and accountability in data protection enforcement.

Special Provisions for Children

Recognizing the heightened need for protecting minors' personal data, the DPDP Act includes special provisions to safeguard the privacy of children. The Act categorically prohibits data fiduciaries from engaging in tracking, behavioural monitoring, or targeted advertising for minors under the age of 18**.** This is a significant departure from global data protection frameworks like the GDPR, which allows member states to set the age of digital consent between 13 and 16.

By setting the age of consent at 18, the DPDP Act takes a stricter approach to protecting children's privacy. However, this provision also raises concerns about potential compliance burdens for businesses that offer digital services to young users. The ban on behavioural monitoring and

targeted advertising aims to protect children from online exploitation, but it also limits their access to age-appropriate digital content and services tailored to their needs.

Cross-Border Data Transfer

One of the most debated provisions of the DPDP Act is its approach to cross-border data transfer. The Act permits the transfer of personal data outside India, except to countries that are specifically blacklisted by the government. This represents a more flexible approach compared to previous drafts of data protection laws, which proposed stringent data localization requirements.

By allowing cross-border data flows with restricted exceptions, the DPDP Act seeks to balance national security interests with the operational needs of global businesses. However, critics argue that the Act does not provide adequate safeguards to ensure that data transferred abroad is subject to the same level of protection as in India. Unlike the GDPR, which mandates binding corporate rules or adequacy decisions for international transfers, the DPDP Act relies on government-issued notifications, leaving uncertainty about the criteria for restricting or permitting data transfers.

Exemptions

The DPDP Act includes several exemptions for specific categories of data processing, which has sparked considerable debate regarding its impact on privacy rights. The Act grants exemptions to government agencies for purposes such as national security, law enforcement, and public interest. This means that government entities can bypass certain data protection requirements when processing personal data for surveillance, investigation, or administrative functions.

Additionally, exemptions are provided for research, archiving, and judicial functions, allowing data to be used for academic studies, historical preservation, and legal proceedings without being subject to strict data protection norms. While these exemptions may be necessary for operational efficiency, they also raise concerns about potential misuse, particularly regarding government surveillance and lack of accountability in cases where personal data is processed without individual consent.

Comparison of the Digital Personal Data Protection (DPDP) Act, 2023, with the General Data Protection Regulation (GDPR)

The Digital Personal Data Protection (DPDP) Act, 2023, and the General Data Protection Regulation (GDPR) of the European Union are both designed to regulate the processing of personal data, ensure privacy protection, and establish accountability for data processors and fiduciaries. However, these two legal frameworks differ significantly in their scope, definitions, rights of individuals, obligations of entities processing data, breach notification requirements, cross-border data transfer mechanisms, and compliance measures. The following is a detailed comparison of the key differences and similarities between the DPDP Act and the GDPR.

Scope and Applicability

The GDPR applies to all forms of personal data processing, whether carried out wholly or partly by automated means, or as part of a structured filing system, irrespective of whether the data is digital or physical. This broad coverage ensures that even traditional paper records, if organized systematically, fall under the GDPR's jurisdiction. On the other hand, the DPDP Act applies only to digital personal data, covering both data collected in digital form and non-digital data that is subsequently digitized. This means that purely physical records that are never converted into digital form remain outside the scope of the DPDP Act.

Furthermore, the GDPR has a broader extraterritorial reach, applying to any organization that processes the personal data of EU citizens regardless of where the processing occurs. The DPDP Act, while also extending to data processing outside India, applies only if the data processing is related to goods and services offered in India. This difference means that GDPR's enforcement is more extensive on a global scale compared to the DPDP Act.

Age of Consent for Minors

The GDPR establishes 16 years as the default age at which individuals can provide valid consent for data processing. However, it allows EU member states to lower this age to 13 based on national regulations. This flexibility enables countries within the EU to determine an appropriate threshold for their local contexts.

In contrast, the DPDP Act mandates that all individuals under 18 years of age must obtain parental or guardian consent before their data can be processed. This stricter approach aligns with India's broader child protection laws but raises concerns about feasibility, as it may restrict teenagers from independently accessing digital services that require personal data.

Personal Data Breach Notification

The GDPR requires data controllers to notify the relevant supervisory authority within 72 hours of becoming aware of a personal data breach. Additionally, if the breach poses a high risk to the rights and freedoms of individuals, organizations must also inform the affected data subjects without undue delay. This strict requirement ensures transparency and allows individuals to take necessary protective measures.

On the other hand, the DPDP Act does not specify a fixed timeframe within which a data fiduciary must notify the Data Protection Board of India (DPBI) about a data breach. The absence of a mandatory deadline could lead to delays in reporting breaches, potentially increasing risks for affected individuals.

Rights of Individuals (Data Principals vs. Data Subjects)

Both laws provide individuals with rights over their personal data, but there are key differences in their scope. Under the GDPR, individuals (referred to as data subjects) have rights such as:

- Right to access: Requesting copies of their personal data.
- Right to rectification: Correcting inaccurate or incomplete data.
- Right to erasure (Right to be Forgotten): Requesting deletion of data under certain conditions.
- Right to restriction of processing: Limiting how their data is processed.
- Right to data portability: Receiving data in a machine-readable format and transferring it to another service provider.

The DPDP Act grants similar rights to data principals (individuals whose data is processed), including the right to information, correction, erasure, and grievance redressal. However, unlike the GDPR, the DPDP Act does not explicitly provide the right to data portability, meaning individuals cannot demand a copy of their data in a transferable format for use with another service provider.

One unique provision in the DPDP Act is the right to nominate a representative who can exercise data rights on behalf of an individual in case of death or incapacity. This right is absent in the GDPR. Additionally, while the GDPR requires organizations to respond to data subject requests within 30 days, the DPDP Act does not specify any mandatory response timeframe, potentially leading to delays in fulfilling data access or correction requests.

Cross-Border Data Transfers

The GDPR establishes strict mechanisms for transferring personal data to third countries, ensuring that data exported outside the EU receives an adequate level of protection. These mechanisms include:

- **Adequacy decisions:** The European Commission determines whether a country ensures an equivalent level of data protection.
- **Standard contractual clauses (SCCs):** Legal agreements between organizations to protect transferred data.
- **Binding corporate rules (BCRs):** Internal policies for multinational organizations governing data transfers.

In contrast, the DPDP Act does not outline a structured mechanism for cross-border data transfers. Instead, it permits personal data transfer except to countries that the Indian government explicitly blacklists. This means that rather than requiring companies to implement stringent safeguards, the government will decide which countries are restricted, potentially making cross-border data transfers more uncertain and subject to political considerations.

Data Protection Officers (DPOs) and Compliance Requirements

Under the GDPR, both data controllers and data processors are required to appoint a Data Protection Officer (DPO) in specific circumstances, such as when processing large-scale sensitive data or monitoring individuals systematically. The DPO acts as a point of contact for regulators and ensures compliance with data protection laws.

The DPDP Act, however, mandates the appointment of a DPO only for significant data fiduciaries (organizations handling large-scale or sensitive data, as designated by the government). Regular data fiduciaries are not required to appoint a DPO, potentially limiting the effectiveness of compliance oversight in many organizations.

Record-Keeping and Processing Activity Logs

The GDPR mandates that both data controllers and data processors maintain records of data processing activities to ensure transparency and accountability. These records help regulators assess compliance and investigate data protection violations.

Conversely, the DPDP Act does not impose a similar obligation on data fiduciaries to maintain records of processing activities. This lack of a record-keeping requirement may reduce administrative burdens for businesses but also limits transparency in data management practices.

Way Forward for Strengthening India's Data Protection Framework

As India refines its digital privacy framework, key reforms are needed to enhance the effectiveness, accountability, and transparency of the Digital Personal Data Protection (DPDP) Act, 2023. One major concern is the lack of a structured mechanism for cross-border data transfers. While the Act permits transfers except to blacklisted nations, it does not specify minimum safeguards. To ensure adequate protection, the government should implement mechanisms like adequacy decisions, standard contractual clauses (SCCs), and binding corporate rules (BCRs), similar to the GDPR, ensuring uniform data protection across jurisdictions.

Expanding individual rights is also crucial. The Act should include the right to data portability, allowing individuals to transfer their data between service providers, and the right to be forgotten, enabling removal of outdated or irrelevant data. Additionally, broad government exemptions raise concerns about privacy erosion. While national security is a valid concern, exemptions must be clearly defined and subject to judicial oversight. Establishing independent review mechanisms would ensure transparency and proportionality. The Act should also mandate time-bound data deletion, as the current lack of retention limits may lead to indefinite storage, increasing risks of misuse. Automatic erasure protocols would help mitigate these concerns.

The independence of the Data Protection Board of India (DPBI) must be strengthened to prevent government influence. It should have financial autonomy, a multi-stakeholder governance structure, and independent appointments with parliamentary oversight. Transparency in government data collection should also be mandated, requiring public authorities to disclose the types of data collected, its purpose, and retention periods. Strengthening these areas will ensure India's data protection framework upholds individual privacy while fostering digital innovation and aligning with global best practices.

Conclusion

The Digital Personal Data Protection (DPDP) Act, 2023, marks a significant step toward establishing a structured data protection framework in India. While it shares foundational similarities with the European Union's General Data Protection Regulation (GDPR), key differences exist in scope, individual rights, cross-border data transfer mechanisms, and enforcement. The DPDP Act focuses solely on digital data, lacks a well-defined data portability right, and grants broad exemptions to government agencies, which raises concerns about accountability and privacy protection.

To strengthen India's data governance framework, several reforms are necessary. Establishing clear mechanisms for cross-border data transfers, such as adequacy decisions and standard contractual clauses, will enhance international data security. Expanding individual rights, particularly by incorporating data portability and the right to be forgotten, will empower users with greater control over their personal data. Furthermore, ensuring judicial oversight for government exemptions and strengthening the independence of the Data Protection Board of India (DPBI) will enhance transparency and accountability.

The Act should also introduce time-bound data deletion mechanisms to prevent indefinite data retention and mitigate security risks. Additionally, mandating transparency in government data collection practices will foster public trust and align India's data protection framework with global best practices.

By implementing these reforms, India can move toward a more robust, rights-based, and internationally compatible data protection regime that balances privacy, security, and innovation in the digital economy.

References

1. Maurya H, Prasad S. Data Protection Laws and a Comparative Analysis of GDPR and PDPB. AIP Conference Proceedings,2022:2519(1):030077.
2. Gupta N, George A. Digital Personal Data Protection Act, 2023: Charting the Future of India's Data Regulation. Data Governance and the Digital Economy in Asia, 2024.
3. Naithani P. Regulating Artificial Intelligence under Data Protection Law: Challenges and Solutions for India. Indian Journal of Law & Justice,2023:14(1):436-458.
4. Singh A, Anusha. The Digital Personal Data Protection Act, 2023: An Ambitious Government Step Towards Ensuring Its Wide Reach. SAGE Journals, 2024. Available at: https://journals.sagepub.com/doi/full/10.1177/00195561241271533 (last visited Mar 5, 2025).
5. Sundara K, Narendran N. The Digital Personal Data Protection Act, 2023: Analysing India's Dynamic Approach to Data Protection. Computer Law Review International,2023:24(2):129-145.
6. Kuner C. The Path to Recognition of Data Protection in India: The Role of the GDPR and International Standards. National Law School of India Review,2021:33(1):69-90.
7. Rodrigues GAP, *et al*. Understanding Data Breach from a Global Perspective: Incident Visualization and Data Protection Law Review. Data,2024:9(1):27-45.