ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

The Data Privacy Laws in India: A Legal Analysis of Digital Personal Data Protection Act- 2023

Dr. Deepali Rani Sahoo,

Associate Professor in Law, School of Legal Studies, Central University of Tamil Nadu, Tiruvarur, India

DOI: https://doi.org/10.51583/IJLTEMAS.2026.150700040

Received: 07 May 2026; Accepted: 12 May 2026; Published: 07 August 2026

ABSTRACT

The Digital Personal Data Protection Act, 2023 establishes India's first comprehensive framework for safeguarding digital personal data. By 2027, 900 million Indians are expected to utilize the Internet, making the Data Protection Act essential. The Digital Personal Data Protection (DPDP) Act, 2023 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 mechanism. 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 efforts on cross border data transfers. The Act also establishes the Data Protection Board of India (DPBI) as regulatory body for monitoring compliance and resolving disputes. This paper the absence of an independent Data Protection Board with sufficient autonomy is critically evaluated. The DPDP Act and the laws that followed it provide a hopeful framework for a future in which technology supports humankind rather than subjugates it. The Government must uphold commitment to keeping the internet safe place citizens as the role of the internet in sustainable economic growth expands daily.

Keywords: Digital Personal Data Protection Act, Significant Data Fiduciary, digital economy, Legislative framework.

INTRODUCTION

The Digital Personal Data Protection Act, 2023 is an important piece of Legislation. The previous personal Data Protection Bills of 2019 & 2022 being ascribed to numerous amendments, laced with several issues relating to data localization, the Central Government had withdrawn transparency, compliance intensive etc. The said Bill came into being after the Supreme Court, in Justice K.S. Puttaswamy vs. Union of India. As a part of the Fundamental Right" 'Right to Life' enshrined under Article 21 of the Indian Constitution and has suggested the Central Government to put in place an Act/ regime for protection of personal Data. Previously the Indian Supreme Court in the Kharak Singh case denied it.

Due to judicial interpretation that the fundamentals rights in the Indian Constitution do not encompass right to privacy. The main problem with the nine judges bench ruling in the above- said case is that after proclaiming privacy as a Fundamental Right, it has not defined privacy. It is now left to all adjudicators to give multiple interpretations in order to understand the term. The regulation intended to safeguard citizen privacy and, more critically, consumer data. The Digital Personal Data Protection (DPDP) Bill, which has been under consideration for years, was approved by the Moonsoon Session of Parliament and is now an Act after Hon'ble President Droupadi Murmu's signature. In the seventy-seventh year of independence, India's experimentation with data privacy laws has finally ended with the passing of the Digital Personal Data Protection Bill, of August 11th, 2023 (3). The Journey of this legislation from a Bill to an Act was an arduous one. India lacked a stand-alone data protection law although the information Technology (IT) Act of 2000 governed the use of personal data, It has been noted that this framework is insufficient to guarantee the protection of personal data. The voyage of the legislation in the vast sea of possibilities started with a committee of Experts on Data Protection, headed by Justice B.N. Srikrishna, which was established by the national government in 2017 to look in to the matters

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

pertaining to data protection in the nation. In July 2018, the committee turned in this report and the Personal Data Protection Bill, 2019 was presented in Lok Sabha in December 2019 based on the Committee's recommendation. A joint Parliamentary Committee was given the Bill for review, and it delivered its report in December 2021. But the Bill was withdrawn from parliament in August 2022 due to the remorse of Stakeholders and data hoarders. With an increasing population, India is the biggest market for business companies like "Meta' and 'Google', and a comprehensive data protection law in India will be unfavorable for them. 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. The major focus of the DPDP Rules is to protect the rights of the citizens. Data Principals are granted stronger rights, including the right to request correction or deletion of their data and to appoint digital nominees. Correspondingly, Data Fiduciaries are required to follow stricter data management practices such as defining retention timelines, enforcing encryption and access controls, and promptly reporting any data breaches. The most pressing compliance challenge arises for significant Data Fiduciaries, who must now conduct mandatory Data Protection Impact Assessments and annual audits. Therefore, organizations need to act quickly to review their current data practices and align them with these evolving regulatory standards.

Objectives of the study:

In this research paper the following discussion will be made.

- Analyze the key features of the Digital Personal Data protection (DPDP) Act, 2023.
- Compare DPDP Act with is contemporary General Data Protection Regulation.
- Discuss the adequacy of the DPDP Act concerning data protection required to India.

Research Methodology:

The researcher used both primary and secondary sources to gather the information needed this article. The researcher employed a questionnaire and Technical working in–person interviews to ask fundamental questions about the General Data Protection Act and Digital Personal Protection Act. The second resource consists of Law books, journals, case records, newspapers, websites on the internet.

1. Objectives of Digital Personal Data Protection Act, 2023

As the preamble of the Digital Personal Data Protection Act states that:

"An Act to provide for the processing of digital personal data in a manner that recognises both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes and for matters connected therewith or incidental thereto".

There are two main terms used in the said Act which are "data" and "digital personal data", which are protected under this Act. The Digital Personal Data Protection Act, 2023 seeks to address a range of issues related to data processing, privacy, and individual rights. It is part of India's effort to establish a comprehensive framework for data protection in the digital era.It offers a promising blueprint for the future where technology serves humanity. Now this Act is India's most comprehensive statute in the field of privacy, bringing in a much-needed framework for assuring individuals visibility and control over their online personal data.

The DPDP Act borrows significantly from the European General Data Protection Regulation (GDPR), with some foundational deviations.

Applicability and Scope:

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

- The Act applies to the processing of digital personal data within India, whether collected online or digitized from offline sources.
- It extends its jurisdiction to processing data outside India if it is intended for offering goods or services within India.

Consent and Lawful Processing:

- Personal data can only be processed for lawful purposes, and the consent of the individual is required.
- Exemptions from consent include specified legitimate uses, such as voluntary data sharing by individuals and processing by the State for licenses, permits, benefits, and services.

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.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

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 cyber attacks. 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

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

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.

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.

2. Right to restriction of processing: Limiting how their data is processed.
3. Right to data portability: Receiving data in a machine-readable format and transferring it to another service provider.
4. **Digital Personal Data –** Section 2(n) of the Act defines digital personal data (DPD) as "personal data in digital form." A natural person i.e., a data principal who can be recognized or located using such data is said to be the subject of any organized representation of information, facts, thoughts, views, or instructions in digital form. It will contain personal data that was gathered digitally or non-digital sets that were later converted to digital format. Pseudonymized data will be considered personal data and covered by the DPDP Act since it can be paired with identifiers to reveal the identity of the Data Principal. Furthermore, although it may be an important factor in determining the categorization of Data Fiduciaries and the imposition of fines, the DPDP Act's applicability is independent of whether personal data sensitive, such as health, financial, biometric, etc. Since the SPDI Rules currently only apply to the processing of sensitive personal data, many businesses that do not deal with sensitive data nonetheless handle personal data as needed to meet actual business requirements. Any entity that processes any personal data after the DPDP Act is implemented will need to comprehend it and abide by its requirements.
5. **Processing –** Processing includes the complete data processing lifespan, from data collection to deletion, and includes wholly or partly "automated" activities done on personal data. Any digital data processing that may operate automatically in response to commands or otherwise is considered automated. So, only non-automated procedures are excluded, and semi-automated processing will be covered.
6. **Territorial nexus –** The Digital Personal Data Protection Act must be followed whenever a person whether natural or legal, processes personal data inside of India, regardless of whether they are physically present or have an Indian incorporation and regardless of whether the personal data belongs to the Data Principal inside or outside of India. For instance, the DPDP Act will be applicable to the processing of

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

personal data of Data Principals based in Russia but inside of India by a Russian enterprise. The DPDP Act only applies when processing takes place outside of India and is done so in order to provide data principals with goods or services within Indian Territory. Processing carried out only for the aim of profiling people is not considered to be an extraterritorial application.

7. **Exemptions –** According to the DPDP Act, processing of personal data (PD) for the following reasons is exempted –

(i) For domestic or personal use; and

(ii) If personal data becomes publicly available as a result of the Data Principal's voluntary actions, such as comments made on social media or as a result of disclosures made in accordance with applicable law;

(iii) Furthermore, for the sake of specific protective grounds like sovereignty, maintaining public order, etc., the Central Government has the authority to inform authorities from the state government that would be excluded from the DPDP Act. Also, for a period of five years from the DPDP Act's start date, the central government may exclude various categories of Data Fiduciaries from any of its provisions.

7. **Processing of personal data only for a 'lawful reason' –** Only legitimate uses of personal data may be carried out with the consent of the data subject. In some circumstances, consent may be assumed. There are many exclusions from the Bill that pertain to the State's handling of personal data. The State is defined as the following under Article 12 of the Constitution:

(i) the central government;

(ii) the state government;

(iii) the local bodies; and

(iv) the authorities and businesses

established by the government. In 2017, the Supreme Court ruled that any violation of the right to privacy must be proportional to the justification for the intrusion. Data collection, processing, and retention may go beyond what is required as a result of the exceptions. This might not be reasonable and go against people's basic right to privacy. The Act gives the central government the authority to exclude processing by government agencies from any regulations where doing so will benefit goals like maintaining public order and state security. Except for data security, no rights of data principals and no duties of data fiduciaries will apply in some circumstances, such as when processing data to prevent, investigate, and prosecute crimes. After the intended purpose of processing has been satisfied, the Bill does not mandate that government entities erase personal data. Using the aforementioned exceptions, a government agency may gather information on persons to build a 360-degree profile for monitoring on the grounds of national security. For this, it could make use of information stored by various government agencies. The question of whether these exemptions will pass the proportionality test is brought up by this. In *PUCL vs. Union of India*[10], the Supreme Court required a number of protections for communication interceptions, including (i) demonstrating need, (ii) purpose limitation, and (iii) storage limitation. These are comparable to the duties that data fiduciaries under the Bill, whose applicability has been prohibited. The Srikrishna Committee in the year 2018 had suggested that responsibilities other than fair and reasonable processing and security precautions should not apply in cases of processing for reasons like national security and the prevention and prosecution of crimes. It noted that a different statute would carry out responsibilities like purpose definition and storage restriction, if relevant; there is no such legal system in India. Similar exclusions are provided for national security and defense under the 2018 data privacy law that was passed in the United Kingdom. The Secretary of State (i.e., the Home Minister) issues a warrant for such action, which needs previous approval by a Judicial Commissioner. It is necessary to prove the need and proportionality of such activities. Data retention is limited after the warrant's expiration date. Also included in this statute is legislative oversight. The Investigatory Powers Act, of 2016, however, regulates operations such as bulk processing of personal information for intelligence and law enforcement purposes by government entities.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

8. Penalty for violation – The Schedule of the DPDP Act, provides for a penalty ranging from ten thousand rupees to five hundred Crore Rupees in case of breach by data fiduciaries and non-compliant companies which is also advantageous since it holds companies responsible for leaks. Businesses would be forced to strengthen their systems and implement the appropriate data protection measures by harsh criminal penalties. In the past several years, we have seen a rash of data breaches; from bra sizes to medical and financial details, cyber leaks are only getting worse. After the US, India is the country that is most frequently the target of cyberattacks. Digital corporations will be required to manage residents' data under "absolute legal responsibility," according to the Indian government, providing them a right to protect their data from exploitation.

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.

Comparative analysis of the General Data Protection Regulation (GDPR) and Digital Personal Data Protection (DPDP) Act-

The Indian Government has long recognized the need to implement a thorough and dedicated data protection framework that is on par with international norms due to the constantly conflicting need to respect individual privacy and allow data processing by corporate enterprises. One of the most important regulations that establish the precedent for and clarifies the necessity of preserving people's privacy in a globalised society is the General Data Protection Regulation (GDPR). It is the strictest privacy and security regulation in the world. Although it was created and approved by the European Union (EU), it imposes requirements on any organizations that target or gather information about individuals residing in the European Union. The rule becomes effective on May 25, 2018. The GDPR imposes severe fines—up to tens of millions of euros—on those who break its privacy and security criteria. In a time when more individuals are entrusting their data with cloud services and breaches are occurring on a daily basis, Europe is signaling with the GDPR its tough position on data privacy and security.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

The connection between Indian privacy law and its certain parallels to the GDPR is only reasonable. The similarities between the two laws are discussed below.

(i) Although the GDPR specifically excludes anonymized data from its application, the DPDP argues that it would not apply to data that is anonymized in such a way that it cannot be used to identify a specific person.

(ii) Data processing without consent is authorized under certain conditions. The DPDP outlines a number of "legitimate purposes" for the processing of personal data by data fiduciaries (data controllers) for a number of unique use cases. Such "legitimate uses" (for which the data subject's consent is not necessary) include processing for employment-related purposes, responding to medical emergencies, carrying out any required legal obligations, or the State offering the data subject any service or benefit, among other things. Similar to this, the GDPR imposes some requirements on the data controller while giving the data controller the option to treat personal data without consent in certain circumstances.

(iii) One of the fundamental tenets under which a data fiduciary or data controller may treat personal data is the consent of the data principal. The fundamental requirements for permission under the DPDP and the GDPR, namely that it be free, specific, and informed, are broadly the same. Furthermore, in order to treat personal data, GDPR and DPDP both demand a legal basis. Another requirement shared by the GDPR and DPDP is that the data fiduciary must show that consent was acquired in accordance with the relevant laws. By mandating that the permission request be presented in a number of languages, at the data principal's choice, DPDP places extra requirements on accessibility.

(iv) Given the criteria used to determine whether a data fiduciary qualifies as a large data fiduciary under the DPDP (such as the amount and sensitivity of the data handled), additional duties like the appointment of data protection officers appear to be compliant with GDPR. Even if the DPDP and GDPR have many parallels, the DPDP is distinctive in its own position. The distinctiveness of the two regulations has been discussed below in a tabular form.

The table of comparison

Sl. No.	Basis of Comparison	GDPR	DPDP
(i)	No division of classes of data	The GDPR divides personal data into a number of distinct components. These types of personal data must adhere to specific regulations, which also include their intended uses.	However, compliance with the DPDP is not based on the kind of personal data; all types of personal data are subject to the same requirements.
(ii)	Notice for taking consent	The notification obligations under GDPR are applicable whenever data is obtained from the data subject and are not just tied to consent.	Only in cases where permission is the justification for data processing does the DPDP require notification to be given (and not for legitimate uses).
(iii)	Composition of such notice	The breadth of the information that must be disclosed to a data subject under the GDPR is significantly broader and does not appear to be limited to situations when the data subject's consent is necessary.	The DPDP specifies the components a disclosure must include in order for a data principal to give their permission. These components include details on the type of personal data being collected, the reason it is gathered, how consent may be withdrawn, information about grievance redressal, and details about how a complaint may be filed to an enforcement body.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

(iv)	Monitoring of data related to children	The GDPR does not specifically forbid behavioral tracking or child-targeted advertising.	DPDP requires verified parental permission or its unequivocal and comprehensive restriction on processing data that is likely to have a negative impact on a child's well-being.
(v)	Grievance Redressal	The GDPR does not mandate that a data subject seek remedies from the controller before filing a complaint with the relevant Supervisory Authority or in court.	DPDP mandates an aggrieved person to apply before the Data Protection Board of India.
(vi)	Transmission of data to other territories	Under the GDPR, the permissibility of the transfer of personal data ranges from restricted authorization to transfer under specific conditions to unfettered transferability to a country or an international organization authorized by an adequacy judgement.	The DPDP gives the Central Government the ability to limit a data fiduciary is transfer of personal information to specified nations or territories outside of India. Personal data can therefore be transferred freely, with the exception of nations that are on the Central Government's forthcoming negative list.
(vii)	Consent Managers	No such concept is present in the GDPR.	This is a novel idea in the DPDP. An individual who has registered with the Data Protection Board is known as a "consent manager". This person is responsible for the data principal and serves as a single point of contact for the data principal so they may manage their consent through easily accessible platforms. The regulations will specify the duties and other technical, operational, financial, and other requirements that apply to consent managers.

Analysis on the point of consistency with other Law:

As per Section 38(1) of the DPDP Act, all the provisions of this Act shall be in addition to any other existing law for the time being in force. On bare interpretation of the above said section, it is clear that the provisions of this section are only in addition to other transparency laws enacted in India. But on the other hand, Section 38(2) of this Act state that " In the event of any conflict between a provision of this act and a provision of any other law for the time this Act in force, the provision of this Act shall prevail to the extent of such conflict" [(4)]. The text of this section give overriding effect to the provisions of the Digital Personal Data Protection Act, 2023 on all the transparency laws in case of conflict, on the interpretation of this section it is clear that in case of conflict with any other provision of other law, the overriding effect of this section is only limited to the extent of such conflict. It means as and when the question arises to disclose the digital personal data of an individual held by any government functionaries under the RTI Act[15], the provision of Section 38(2) of the DPDP Act shall be invoked. The Indian Supreme Court ruled that Right to Information will be treated as a Fundamental Right under Article 19. The Supreme Court held that in Indian democracy, people are the masters and they have the right to know about the working of the Government[16]. Thus, the government enacted the Right to Information Act in 2005 which provides machinery for exercising this fundamental right [(5)].

Section 17(2) (a) of DPDP Act empowers the central government to exempt instrumentalities of the state by way of notification.

CONCLUSION & SUGGESTIONS

The Digital Personal Data Protection Act, 2023, represents a critical and long-overdue step in safeguarding the fundamental right to privacy in India. In time with the problem statement, the above analysis confirms that the operational and financial demands of the DPDP Act, particularly the costs of retrofitting technology,

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

implementing granular consent mechanisms and remediating high-value legacy data impose a disproportionate strain on resource constrained. The DPDP Act focuses solely on digital data, lacks a well defined data portability right, and grant board 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 mechanism for cross-border data transfers, such as adequacy decisions and standard contractual clauses, will enhance international data security. Expanding individual rights, particularly by in corporating data portability and the right to be forgotten, will empower users with greater control over their personal data. Further, more ensuring judicial oversight for government exemptions and strengthening the independence of the Data Protection Board of India (DPBI) will enhance transparency and accountability. Section 17 (3) of the Act provides a clear legal pathway to prevent excessive regulatory burden, while mechanisms like the Micro Fiduciary and privacy instruments to reduce friction and enable innovation. As far as the substance of the matter is concerned, the Indian legislator can be criticized for making timed choices with regard to the issues at stake in such a regulation- in particular, with regard to the rights of individuals and the principle of transparency, which are essentially confined to processing based on the consent of individuals similarly, the choice of two legal bases in all is too limited. Finally, it is regrettable that the supervisory authority created by the law is unable to create soft-law, which condemns to a certain inertia.

As per suggestions- (1) No government agency should be exempted from disclosure of information to avoid misuse of personal data and promote transparency. (2) Complaint filing should be made easy in DPDP Act, 2023 as online filing of complaints is the only mode available in the Act. Both online as well as offline modes of filing complaints should be available. It is needless to mention here that we will have to wait for the supplements to the law to be enacted by the Indian government to get a clearer picture of the new data protection system and whether the weaknesses mentioned can be overcome. The DPDP Act is proposed to come into force in a phased manner, i.e. as and when the central Government notifies the provisions of the DPDP Act, from time to time. Also its weaknesses. To data, in fact, the law remains imprecise, due to the many subjects that have been deferred to later additions, leaving an impression of unfinished business. As far as the substance of the matter is concerned, the Indian legislator can be criticized for making timid choices with regard to the issues at stake in such a regulation- in particular, with regard to the rights of individuals and the principle of transparency, which are essentially confined to processing based on the consent of individuals. Similarly, the choice of two legal bases in all is too limited. Finally, it is regrettable that the supervisory authority created by the law is unable to create soft-law, which condemns the system to a certain inertia. However, the most pressing criticism of the DPDP is undoubtedly the numerous derogations provided for in the law, which give rise to heterogeneous, mixed regulations and relative legal uncertainty. The very broad exemptions granted to public authorities give rise to fears of uncontrolled state surveillance. We'll have to wait for the supplements to the law to be enacted by the Indian government, to get a clearer picture of the new data protection system and whether the weaknesses mentioned can be overcome.

REFERENCES

1. Singh Anu, Mishra Megha, " The Nascence Data Privacy Laws in India: An analysis of Digital Personal Data Protection Act, 2023", A landmark on the Indian Constitution Journal, 2024. Vol-2, Issue-1, PP-145-150.
2. Singh A, Anusha, "The Digital Personal Data Protection Act.2023: An ambitious Government step towards Ensuring Its Wide Reach". Sage Journals, 2024, Avilablehttp://Journals.sagepub.com/doi/full/10.1177/00195561241271533(Last visited on September 4th, 2025)
3. Kashyap Pranav, Gupota Gaurav, "Decoding India's DPDP Act and its Impact on Business."Available-http://bridgecounsels.com/decodingindias-dpdp-act-its-impact-on-business/.
4. (Last visited on September 21st , 2025)
5. Dalei Prabhash, "The Digital Personal Data Protection Act, 2023: A legal analysis in light of Global Data Protection Standards", Journal-International Journal of Law, Volume-II, Issue-3, 2025, PP-127-131, ISSN-2455-2194.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

6. Nigam Aishwarya, " Startups and the Digital Personal Data Protection Act, 2023 and the Draft Rules 2025: Compliance and Challenges", Journal- International Journals of Law Management & Humanities, Volume-8, Issue-5, PP-1476-1486, DOI: http://doij.org/10.10000/ULMH.1110890, ISSN-2582-5369. (Last visited on 29th Sept. 2025)
7. Tewari Aakanksha, "DPDPA's Global Reach: Cross Boarder Data, AI Impact, and International Alignment, TRUSTARC. Available -http://trustarc.com/resource/dpdpas-global-reach-cross-boarder-data-ai/.
8. (Last visited on 04.10.2025)
9. Article 19(1)(a) of the Constitution of India.
10. Article 21 of the Constitution of India.
11. Article 32 and 226 of the Constitution of India.

12. WEB SOURCES

13. http://blog.ipleaders.in/supreme-courts-Judgements-right-information/.
14. http://datareportal.com/reports/digital-2024.india/.
15. http://indiankanoon.org/doc/778875/.
16. http://rti.gov.in/rtiact.asp/.
17. http://www.meity.gov.in/writereaddata/files/Digital%20personal%20Data%20protection%20Act%202023-pdf.
18. (Last visited May, 20th, 2025)