DHARANA
International Journal of Business

https://doi.org/10.18311/DBIJB/2025/50101

Personal Data Protection in Business: Legal and Operational Challenges

M.G. Kodandaram

Introduction

In the digital age, businesses must prioritise personal data protection to comply with the Digital Personal Data Protection (DPDP) Act, 2023, while mitigating risks related to security breaches, legal compliance, and operational disruptions. Neglecting data protection can lead to severe penalties, reputational damage, and erosion of consumer trust.

Personal data security is a pressing concern as businesses face cyber threats. Implementing strong security measures -encryption, multi-factor authentication, and real-time monitoring - is essential to prevent unauthorized access. Additionally, optimising data collection and secure storage reduces liability and cyber risks. Adopting data minimisation and robust storage protocols helps prevent unnecessary exposure.

Legal compliance is another challenge, as the DPDP Act mandates explicit consent, lawful processing, and transparent privacy policies. Non-compliance can result in regulatory scrutiny and huge financial penalties. Businesses must also ensure clear, multilingual policies and proactive compliance strategies.

Beyond regulations, consumer trust hinges on ethical data handling. Transparent policies and empowering users with control over their data develop credibility. Moreover, operational resilience requires investment in cybersecurity, incident response plans, and recovery strategies. By prioritising compliance, risk mitigation, and consumer trust, businesses can steer across the complexities of personal data protection while maintaining efficiency.

In today's digital era, protecting personal data has become a major legal and operational challenge for businesses, governments, social utilities and societies. Personal information is a basic asset in the modern economy, driving targeted advertising, customised services, and data-driven decision-making in all business environments. However, mishandling of personal data can lead to serious repercussions, such as privacy breaches and cybercrimes, ultimately causing harm to innocent individuals. Stolen personal information is frequently abused for phishing attacks, fraud, and corporate espionage. The rising frequency of personal data breaches exposes millions to identity theft, financial fraud, and reputational harm.

Weak and Inadequate data management practices often lead to unauthorised access, data theft, and exploitation of sensitive personal information. Once leaked, sensitive data can end up on the dark web, fuelling illicit activities and reinforcing the need for strict data protection

M.G. Kodandaram
IRS, Assistant Director of Customs and Central Excise (Retd.), Advocate and Consultant;
mgkodandarm@gmail.com

measures. As digital economies grow, the demand for robust security infrastructure, comprehensive legal frameworks, and regulatory oversight intensifies. To mitigate personal data security concerns, nations worldwide are implementing exclusive laws that govern personal data collection, storage, and usage. Regulations like the General Data Protection Regulation (GDPR) in Europe establish standardised approaches to data privacy, ensuring accountability among individuals and businesses.

Indian Law for Personal Data Protection

A major milestone in India's data protection terrain is the Digital Personal Data Protection Act, 2023 (hereinafter 'DPDP Act' or 'the Act' for brevity), which received presidential approval on August 11, 2023[1]. This legislation aims to create a structured regulatory framework for handling digital personal data, safeguarding individual rights while enabling responsible data use by businesses. It enforces explicit consent for data collection, promotes data minimisation, and holds data fiduciaries accountable for protecting sensitive information. Non-compliance can result in substantial penalties, ensuring adherence to data protection standards.

As a further step to implement the DPDP Act, the Ministry of electronics has notified draft DPDP Rules 2025 on January 3, 2025[2], inviting public feedback before finalisation. These rules are expected to refine compliance mechanisms, addressing aspects such as data localisation, grievance redressal, and mandatory reporting of data breaches. As global economies become increasingly data-driven, the DPDP Act establishes a foundation for responsible data governance and cybersecurity measures. Businesses must prioritise investments in secure data storage, advanced cybersecurity solutions, and employee training programs to minimise risks. Without effective data protection policies, Business organisations not only face financial and legal repercussions but also risk losing consumer trust, which is essential for long-term success in the present cyber society.

Businesses also must ensure compliance with the Information Technology Act, 2000 (IT Act), which provides the basic legal framework for secure and reliable electronic, digital, and online transactions while aiming to reduce cyber-crimes in India and protect digital data, including personal information. This legislation outlines the responsibilities of businesses that manage digital data, ensuring they implement necessary safeguards to prevent unauthorised access, data breaches, and misuse of personal information.

In addition to the IT Act, the DPDP Act[3] has been introduced as a standalone law to regulate the processing of personal data in a diligent manner with an objective to protect the privacy rights of the citizens. The DPDP Act mandates strict compliance from Data Fiduciaries that includes all business and non-business entities dealing with digital personal information of individuals. Under this law, businesses are

[1]https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf (visited on 26.02.2025)

[2]https://innovateindia.mygov.in/dpdp-rules-2025/ (visited on 26.02.2025)

[3]A Detailed Analysis of DPDP Act,2023 -refer https://fdppi.in/library/2024/DPDP%20Act%20part%201%20overview%20FDPPI_MGK.pdf (visited on 26.02.2025)

required to implement robust personal data protection mechanisms, obtain explicit user consent for data collection, ensure secure storage and processing, and uphold individuals' rights concerning their personal data.

Furthermore, the DPDP Act imposes stringent obligations on organisations to safeguard sensitive data and report breaches promptly to an authority namely 'the Data Protection Board of India', which is going to be formed on implementation of this act. Non-compliance can result in severe penalties on the fiduciaries, reinforcing the need for businesses to adopt strong data governance policies, cybersecurity measures, and transparent data-handling practices. By aligning with both the IT Act and the DPDP Act, businesses can ensure regulatory compliance, enhance consumer trust, and mitigate risks associated with data breaches and cyber threats.

This article provides an overview of India's Personal Data Protection law and the mandatory compliance requirements for business fiduciaries. It also examines the operational challenges of managing personal data and outlines essential steps for businesses to achieve compliance with the DPDP Act while steering the evolving regulatory landscape.

Personal Data Defined

The Act includes several key definitions that clarify its scope and application. The term "data" refers to representations of information, including facts, concepts, opinions, or instructions, conveyed in a manner suitable for human understanding, transmission, interpretation, or automated processing[4]. "Personal data" is defined as any information related to an identifiable individual, while "digital personal data" specifically refers to such information in digital form[5]. Notably, non-personal data - data without person identifiers - is not covered under this law.

The DPDP Act governs the management of digital personal data within India's jurisdiction. It applies to personal data that is collected in digital form or converted into digital format after being initially gathered in a non-digital medium. Additionally, the Act extends its applicability to the processing of digital personal data outside India if such processing pertains to goods or services offered to individuals within India[6]. The provisions of this law will come into effect on dates notified by the Central Government, with different provisions potentially being implemented at separate times.

Rights of Data Principal

The Act identifies the "Data Principal[7]" as the individual to whom personal data pertains. Also referred to as 'data subjects' in other data protection laws, the 'data Principal' is the person whose personal information is processed by a data Fiduciary. If the Principal is a child (anyone under the age of eighteen), their parents or legal guardians assume responsibility, and for individuals with disabilities, their lawful guardian acts on their behalf.

[4]Sec 2(h) of DPDP Act, 2023
[5]Sec 2(t) and Sec 2(n) ibid
[6]Sec 3 ibid
[7]Sec 2(j) ibid

However, the Act excludes certain scenarios from its scope, such as personal data managed by individuals for domestic or personal use and data that has been intentionally made public by the principal or disclosed under applicable Indian laws.

The DPDP Act grants several rights to data principals, empowering individuals to have better control over their personal data. One of the key rights is the Right to Access, which allows data principals to obtain a summary of their personal data being processed. They can also seek details of all data fiduciaries and processors who have access to their data, ensuring awareness of how their information is being utilised. Further, they hold the Right to Correction, enabling them to request rectifications, updates, or completions of any inaccurate or incomplete personal data held by data fiduciaries. Further strengthening their autonomy, data principals have the Right to Erasure, permitting them to request the deletion of their personal data when it is no longer necessary for legal or business purposes. However, if the retention of data is essential for specific obligations, the data fiduciary may continue to hold it.

In scenarios where individuals may be unable to exercise their rights due to death, mental incapacity, or physical infirmity, the Right to Nominate allows them to designate someone to act on their behalf. Additionally, the Right to Revoke Consent ensures that individuals can withdraw their consent for data processing at any time. These rights collectively empower data principals, reinforcing their autonomy over personal information while ensuring that data fiduciaries remain accountable and transparent in their practices.

To ensure that individuals can seek recourse in case of disputes or grievances, the Act also provides the Right to Grievance Redressal. Data fiduciaries are mandated to establish accessible mechanisms for resolving complaints, and if grievances remain unresolved, data principals can escalate their concerns to the Data Protection Board.

Data Fiduciary and Significant Data Fiduciary

A 'Data Fiduciary[8]' is any individual, organisation, or entity that determines the purpose and means of processing personal data, either independently or in collaboration with others, known as processors. This definition mandates that all entities - whether commercial, governmental, or otherwise - must collect personal data from individuals (Principals) in a legally regulated manner. Any personal data obtained must be stored and processed strictly for the designated purposes outlined by law. A fundamental and indispensable requirement in this process is obtaining the individual's informed and fair consent before collecting personal data. Fiduciaries are authorised to collect, store, and process personal data only if their activities comply with the Act. Processing must serve a lawful purpose or fall under legitimate uses as defined by the Act.

A Significant Data Fiduciary[9] (SDF) is a notified subcategory of Data Fiduciaries that handle high volumes of personal data or process sensitive data that poses greater risks to individual rights

[8]Sec 2(i) ibid
[9]Sec 2(z) ibid

and freedoms. Such notified SDFs are required to appoint a Data Protection Officer (DPO), who acts as the central point of contact for regulatory authorities and data principals. The appointed officer must serve as a representative of the Fiduciary, operate within India, and report to the governing body. Responsibilities of SDOs include conducting regular Data Protection Impact Assessments, mitigating risks to data rights, and implementing measures in accordance with the Act.

Obligations of Data Fiduciaries

Under the Act, data fiduciaries are entrusted with the responsibility of handling personal data in a manner that upholds privacy, security, and accountability. Their duties are designed to ensure that data processing is conducted ethically, legally, and with the utmost regard for the rights of data principals.

One of the fundamental principles under the DPDP Act is data minimisation, which mandates that data fiduciaries collect only the necessary personal data required for a specific purpose. Once the data is no longer needed or if the data principal withdraws consent, fiduciaries must ensure its deletion, including erasing it from processors' systems. Purpose limitation is another crucial duty, ensuring that personal data is only used for the purpose for which consent was obtained. However, certain exceptions allow data fiduciaries to process personal data without explicit consent, such as when data is voluntarily provided without objection, for legal compliance, governmental functions, maintaining public order, handling medical emergencies, and safeguarding national security. These provisions allow flexibility while maintaining strict compliance with personal data protection norms.

Transparency in data processing is upheld through privacy notices, which must be clear, accessible, and available in English as well as all languages listed in the Eighth Schedule of the Indian Constitution. These notices must provide details about the categories of data collected, the specific purpose of collection, the process of exercising consumer rights, the revocation of consent, and the mechanism for filing complaints with the Data Protection Board. Businesses must also ensure that their contact information is easily accessible for data principals to seek clarifications regarding data processing. The DPDP Act stipulates that data fiduciaries cannot process personal data without obtaining prior consent unless for legitimate use or exempted under the Act. When processing the personal data of children (individuals under 18 years) or persons with disabilities, verifiable consent from parents or legal guardians must be obtained.

Data fiduciaries also have a duty to ensure accuracy and completeness of personal data, particularly when the data is likely to be used for decision-making that affects data principals or when sharing data with another fiduciary. This prevents misinformation and ensures that data principals are not adversely impacted by erroneous data handling.

To safeguard personal data, robust security measures must be implemented at both technical and organisational levels. These include encryption, obfuscation, masking, access controls, and regular monitoring of access logs to detect unauthorised activity. Other security measures involve ensuring data backup to maintain continuity in case of

data loss. Data fiduciaries must also include provisions in contracts with data processors to maintain compliance with the DPDP Act. Other obligations of fiduciary under the Act include complying with government restrictions on cross-border data transfers, maintaining contractual relationships with data processors to enforce compliance, and ensuring timely delivery of consumer requests.

Establishing effective grievance redressal mechanisms is another critical duty. Data fiduciaries must provide clear procedures for data principals to exercise their rights and appoint a dedicated employee / DPO to handle grievances. Consumer requests must be addressed within a reasonable timeframe.

Companies operating in India or catering to Indian consumers must reassess their data policies and operations to remain compliant with the DPDP Act. In the regime of DPDP Act, all organisations may have to undergo significant transformations in processes, technology, and corporate policies to align with the Act, which may involve huge cost to the organisation. Beyond avoiding substantial penalties[10], which may go up to 250 crores, adherence to the Act enhances customer trust, strengthens market credibility, and ensures long-term business sustainability.

Formation of Board

In pursuance of the Act, the central government will establish the Data Protection Board (DPB) of India. The main functions of the Board include: (i) monitoring compliance and imposing penalties, (ii) directing data fiduciaries to take necessary measures in the event of a data breach, and (iii) hearing grievances made by affected persons. In case of data breaches, fiduciaries have an obligation to promptly report incidents to the DPB as well as to affected individuals i.e. Principals. Timely reporting ensures that necessary remedial actions can be taken to abate potential harm.

Compliance Requirements under DPDP Act

The DPDP Act lays down strict compliance requirements for fiduciary organisations, with the aim of safeguarding citizens' privacy while enabling a responsible data economy. Some of the essential compliance requirements are as follows:

1. **Consent-Based Data Processing:** One of the core principles of the DPDP Act, is the requirement for explicit, informed consent from individuals before their personal data is collected or processed. Gone are the days of vague or hidden consent mechanisms; businesses must now adopt clear and transparent methods to acquire consent from users. The Act mandates that principals must be fully aware of what their data is being used for, who will access it, and how long it will be retained. Organisations must offer an opt-in mechanism where individuals voluntarily agree to the processing of their data. Furthermore, principals must have the option to withdraw their consent at any time, ensuring that they maintain control over their personal information. This compliance requirement is important as it empowers individuals to make informed

[10]Sec 33(1) read with schedule ibid

decisions about their data, reducing the risks of unauthorised data usage.

2. **Data Minimisation Principle:** Another essential compliance requirement under the Act is the principle of data minimisation. Businesses must ensure that they collect only the personal data that is necessary for the specific purpose they intend to fulfil. This is a direct response to the growing concerns about over-collection and misuse of personal information. Once the data is no longer needed, it must be securely deleted or anonymised under intimation to the principal. This ensures that organisations do not hold onto unnecessary or outdated information, thereby reducing the risk of data breaches or misuse.

3. **User Rights and Grievance Redressal:** Users must be provided with an easy and accessible means to view the data an organisation holds about them, correct inaccuracies, and request the deletion of unnecessary or obsolete data. In addition to these rights, businesses must establish a robust grievance redressal mechanism. This means that users who feel their data rights have been violated can lodge complaints, and organisations are obligated to address these grievances in a timely and effective manner. This system ensures that individuals have avenues for recourse if they believe their data privacy is being compromised.

4. **Data Breach Reporting:** Organisations must be proactive in identifying and addressing data breaches under the DPDP Act. If a breach occurs, businesses are required to report it to the Data Protection Board of India without undue delay. The Act stipulates that organisations must notify affected individuals about the breach if it is likely to result in significant harm. By mandating prompt reporting, the DPDP Act aims to overcome the damage caused by data breaches and ensure that appropriate corrective actions are taken swiftly. Failure to comply with these breach notification obligations can result in hefty fines and reputational damage.

5. **Accountability and Governance:** Under the DPDP Act, organisations are required to implement strong accountability and governance structures to ensure ongoing compliance with data protection principles. This includes the appointment of a nodal persons and in case of SDFs a DPO responsible for overseeing data protection measures within the organisation. The DPO ensures that the company's practices align with the DPDP Act's requirements, conducts regular audits, and liaises with the Data Protection Board of India when necessary. Further, organisations must establish internal compliance frameworks, including policies and procedures for data processing, training programs for staff, and mechanisms for monitoring compliance. This internal governance framework with due diligence as a policy, serves as a safeguard to ensure that the organisation maintains high standards of data protection across all operations.

6. **Children's Data Protection:** Recognising the vulnerability of minors in the digital age, the Act includes specific provisions for the protection of children's data. Companies must implement stricter safeguards when processing the personal data of minors, which includes obtaining explicit parental consent before collecting or processing such data. Organisations must also be transparent

about their practices regarding children's data and provide mechanisms for parents or guardians to access, correct, and delete their child's data if necessary.

Overcoming Operational Challenges in Handling Personal Data

Responsible management of personal data is not only a legal obligation under the DPDP Act but also a critical business necessity. To address operational challenges in data protection in an effective manner, businesses must focus on the following basic requirements.

1. **Strengthening Data Security:** Businesses are prime targets for cyberattacks such as hacking, ransomware, and phishing. Security breaches expose sensitive customer information, leading to financial losses, reputational damage, and erosion of consumer confidence. To counter these threats, organisations should implement encryption, multi-factor authentication, firewalls, and continuous monitoring to prevent unauthorised access.

2. **Optimising Data Collection and Storage:** Excessive data collection increases liability without corresponding benefits. Implementing data minimisation strategies ensures only essential information is gathered, reducing exposure to risks. Secure storage, reinforced by proper classification and encryption, is crucial to protecting data from cyber threats.

3. **Updating Privacy Policies:** Privacy policies must comply with current legal frameworks and be easily understandable. Regular reviews and updates should clearly define data collection practices, usage, and individuals' rights. Ensuring accessibility in multiple languages, as required by the DPDP Act, promotes inclusivity and compliance.

4. **Addressing Legal Consequences:** Non-compliance with the DPDP Act can lead to heavy penalties, regulatory scrutiny, and legal disputes. Businesses must obtain explicit user consent, process data lawfully, and implement protective measures. Regular audits, policy updates, and employee training are essential to maintaining compliance.

5. **Preserving Consumer Trust:** Mishandling personal data weakens consumer relationships, diminishing loyalty and market competitiveness. Data breaches and unethical practices cause long-term reputational harm. Transparent policies, clear communication of security measures, and enhanced user control over personal data help promote trust.

6. **Mitigating Operational Disruptions:** Data breaches and regulatory failures can cause system downtime, compliance enforcement actions, and workflow inefficiencies. Organisations may be subjected to mandatory audits or additional safeguards, straining resources. Investing in cybersecurity, incident response plans, and recovery mechanisms strengthens operational resilience.

7. **Preventing Data Misuse and Identity Theft:** Unauthorised access to personal data enables identity theft, financial fraud, and phishing scams. Criminals exploit stolen information for malicious purposes, exposing businesses to legal and financial liabilities. Strong access

controls, data minimisation, and secure authentication are essential in mitigating these risks.

8. **Conducting Data Protection Impact Assessments (DPIAs):** Evaluating the risks associated with data processing - especially when adopting new technologies or handling sensitive information - helps identify vulnerabilities and implement safeguards. DPIAs play a crucial role in preventing breaches and ensuring compliance.

9. **Enhancing Employee Awareness and Preventing Insider Threats:** Human error is a leading cause of data breaches, whether through phishing scams, weak passwords, or improper data handling. Additionally, insider threats pose significant risks. Comprehensive training programs, strict access controls, and multi-factor authentication help mitigate these challenges, reinforcing security and compliance.

10. **Managing Third-Party Vendors:** Organisations frequently rely on third parties for data processing, making compliance across the data supply chain essential. Strong contractual agreements and periodic audits ensure adherence to regulatory standards, minimising external risks.

11. **Seeking Legal and Compliance Expertise:** Navigating complex data protection laws requires expert legal guidance. Staying informed on regulatory changes and proactively implementing compliance measures reduces risks and legal repercussions.

12. **Balancing Security and Business Efficiency:** While robust data protection is necessary, excessive restrictions can hinder operations. A risk-based approach prioritising sensitive data protection while ensuring seamless processes is key. Embedding privacy-by-design principles enables compliance without compromising efficiency.

By implementing these strategies, and by continuously improving the personal data protection measures, businesses can effectively address data protection challenges, ensuring regulatory compliance while maintaining consumer trust and operational agility.

Essential Steps to Achieve DPDP Act Compliance

As organisations handle vast amounts of personal data from consumers (principals), vendors, and employees, they must navigate a complex landscape of legal obligations and operational challenges to ensure effective data protection. Compliance with the DPDP Act requires a structured and proactive approach. Below is a comprehensive guide outlining the essential steps organisations must take to achieve compliance:

1. **Obtain Valid Consent:** Ensure that explicit and informed consent is obtained from data principals before processing their personal data.

2. **Provide Transparent Privacy Notices:** Accompany consent requests with clear privacy notices in English and all languages listed in the Eighth Schedule of the Indian Constitution, ensuring accessibility for diverse stakeholders.

3. **Limit Data Collection:** Collect only the data necessary for the specified purpose, minimising excess data accumulation.

4. **Implement Robust Security Measures:** Enforce stringent security protocols, including encryption, access controls, and incident response mechanisms to prevent data breaches.

5. **Secure Special Category Data:** Obtain verifiable consent for processing the data of children and individuals with disabilities, adhering to heightened protection standards.

6. **Ensure Timely Data Deletion:** Establish mechanisms for data deletion once the processing purpose is fulfilled, consent is revoked, or upon request by the data principal.

7. **Facilitate Data Principal Rights:** Develop efficient processes to respond promptly to requests for data access, correction, portability, or erasure.

8. **Protect Children's Data:** Prohibit behavioural monitoring, targeted advertising, and tracking of children to comply with child data protection laws.

9. **Maintain Data Accuracy:** Implement validation procedures to ensure data accuracy and consistency, preventing errors that could negatively impact data principals.

10. **Conduct Audits and Risk Assessments:** If classified as a SDF, conduct periodic audits and DPIAs to mitigate potential risks.

11. **Comply with Cross-Border Data Transfer Regulations:** Ensure adherence to government regulations concerning data transfers to restricted countries.

12. **Establish Strong Data Processor Agreements:** Enter into legally binding contracts with data processors to enforce compliance and accountability.

13. **Implement Data Breach Notification Protocols:** Report all data breaches to the Data Protection Board (DPB) and notify affected individuals, regardless of severity or volume.

14. **Appoint a Data Protection Officer (DPO):** Designate a responsible officer to oversee compliance efforts, handle grievances, and liaise with regulatory authorities. Document data processing activities, consent records, and risk assessments to demonstrate compliance during audits or regulatory inquiries.

15. **Train Employees on Data Protection:** Conduct regular training sessions to ensure employees understand data protection principles and their responsibilities under the DPDP Act.

16. **Integrate Privacy-by-Design Principles:** Embed data protection considerations into business processes, products, and services from the outset.

As India strengthens its data protection framework, businesses must proactively develop comprehensive compliance strategies. While adherence to the DPDP Act presents operational challenges, organisations that prioritise data security, regulatory alignment, and consumer trust can mitigate risks and gain a competitive edge.

By promoting a culture of responsible data management, businesses not only meet legal obligations but also enhance their reputation and ensure sustainable growth in an increasingly data-driven economy. Implementing robust security measures, ensuring alignment with global data protection standards, and integrating privacy-conscious practices into operations will enable businesses to safeguard personal data while maintaining operational efficiency and public trust in a connected world.