BLOGS

Decoding the DPDP Act, 2023: A Guide to India’s New Data Privacy Regime

Khushi Malviya · 18 Aug 2025

Introduction

In today’s world, data is the new oil. Every online transaction, social media post, and app usage generates a trail of personal information. For years, India operated without a dedicated, overarching law to govern this digital gold rush, relying on the limited provisions of the IT Act, 2000. That has now changed with the enactment of the **Digital Personal Data Protection (DPDP) Act, 2023**.

This landmark law establishes a comprehensive framework for how companies can collect, store, and use the personal data of Indian citizens. Understanding the DPDP Act is not just about learning a new law; it’s about grasping the fundamental principles that will govern the digital economy for decades to come. Let’s break down the core concepts you need to know.

The Key Players: Fiduciaries, Principals, and Processors

The DPDP Act revolves around three central actors. Understanding their roles is the first step to decoding the law.

1. Data Principal: This is you. A Data Principal is the individual to whom the personal data relates. If a company collects your name, email, or phone number, you are the Data Principal. The Act is designed to empower you with rights over your data.
2. Data Fiduciary: This is the entity that decides the “purpose and means” of processing personal data. Think of companies like Google, Amazon, your bank, or your telecom operator. They collect your data for specific reasons (the “purpose”) and decide how it will be used (the “means”). The term “fiduciary” is intentionally used to imply a relationship of trust; these entities have a duty to handle your data responsibly.
3. Data Processor: This is any entity that processes personal data on behalf of a Data Fiduciary. For example, a small company might hire a larger cloud service provider to store its customer

data. In this case, the small company is the Data Fiduciary (as it decides the purpose), and the cloud provider is the Data Processor (as it processes the data on instructions).

The Concept of Consent under DPDP Act

The entire edifice of the DPDP Act is built on the foundation of consent. A Data Fiduciary can only process your personal data for a lawful purpose after obtaining your free, specific, informed, and unambiguous consent.

Let's understand these terms:

- Free: Consent must be given without any coercion or force.
- Specific: You must be told the exact purpose for which your data is being collected. Vague or blanket requests for consent are not valid.
- Informed: You must be provided with clear information about the data being collected and the purpose of processing.
- Unambiguous: Your consent must be given through a clear, affirmative action. Pre-ticked boxes or implied consent are generally not acceptable.

Crucially, **Section 6** of the Act mandates that every request for consent must be accompanied by a notice that clearly explains the personal data to be collected and the specific purpose. The Act also gives the Data Principal the right to withdraw their consent at any time with the same ease with which it was given.

The Concept of Deemed Consent

While direct consent is the norm, the DPDP Act introduces a significant and debated concept known as "Deemed Consent" under Section 7. This allows a Data Fiduciary to process personal data without explicit consent in certain specific situations where it can be reasonably assumed.

Some key grounds for deemed consent include:

- When a Data Principal voluntarily provides her data for a specific purpose (e.g., giving your address to an e-commerce site for delivery).
- For the performance of any function under Indian law or by the State (e.g., providing data for a subsidy).

- For compliance with any court order or judgment.
- For responding to a medical emergency or for public health purposes.
- For employment-related purposes.

This concept provides practical exemptions, but it also requires careful interpretation to ensure it isn't misused to bypass the need for explicit consent.

Rights of a Data Principal

The DPDP Act equips every Data Principal with a set of powerful rights to control their personal data. These are laid out in **Chapter III** of the Act.

- Right to Access Information (Section 12): You have the right to get confirmation from a Data Fiduciary about whether they are processing your data, a summary of that data, and the names of all other entities with whom your data has been shared.
- Right to Correction and Erasure (Section 13): You can request the correction of inaccurate or misleading data and the erasure of personal data that is no longer needed for the purpose for which it was collected.
- Right of Grievance Redressal (Section 14): You have the right to a readily available means of grievance redressal provided by the Data Fiduciary. If you are not satisfied, you can escalate the complaint to the Data Protection Board.
- Right to Nominate (Section 15): In the event of your death or incapacity, you can nominate another individual to exercise your rights on your behalf.

Obligations of Data Fiduciaries

The Act places significant obligations on Data Fiduciaries to ensure they handle data lawfully.

The DPDP Act also places a special emphasis on protecting children's data. Organizations must obtain verifiable parental consent before processing any personal information of children, and they are expressly prohibited from using such data for tracking, targeted advertising, or other practices that may exploit minors. This child-centric provision reflects growing global concerns about the effects of digital technologies on younger users and attempts to provide a safer online environment.

- Purpose Limitation: Data must be collected only for a specified, legitimate purpose.

- Data Minimisation: Only the personal data that is necessary for the specified purpose should be collected.
- Accuracy: Fiduciaries must take reasonable steps to ensure that personal data is accurate and up-to-date.
- Storage Limitation: Data cannot be stored indefinitely. It must be erased once the purpose for which it was collected is fulfilled.
- Reasonable Security Safeguards: Fiduciaries must implement appropriate technical and organizational measures to prevent data breaches.
- Breach Notification: In the event of a personal data breach, the Fiduciary must notify both the Data Protection Board of India and the affected Data Principals.

While individual rights and organizational responsibilities form the backbone of the DPDP Act, the law also includes important exemptions. Data processing for purposes such as national security, prevention of crime, or research and statistical analysis may be exempted from some provisions of the Act.

Similarly, to ease the compliance burden on startups and smaller enterprises, the government has the discretion to relax certain requirements. These exemptions, however, have sparked debate about whether they undermine the privacy rights the Act seeks to protect, highlighting the challenge of balancing citizen rights with broader state and economic interests.

The Data Protection Board of India (DPBI)

The DPDP Act establishes a new regulatory body, the **Data Protection Board of India (DPBI)**. This board will be the primary authority for adjudicating disputes, investigating data breaches, and imposing penalties for non-compliance. Its functions are digital by design, meaning proceedings will largely be conducted online.

The Board has significant powers to impose monetary penalties, which can be substantial. For instance, a failure to take reasonable security safeguards to prevent a data breach can result in a penalty of up to **₹250 crore**. A failure to notify the Board and affected users about a breach can attract a penalty of up to **₹200 crore**.

Conclusion

The DPDP Act, 2023, marks a paradigm shift in India’s legal landscape. It moves the country from a sparse data protection framework to a detailed, rights-based regime. For you, the future lawyer, this Act opens up new frontiers in technology law, corporate compliance, and litigation.