

MARCH 2025, VOL. 008

MONTHLY NEWSLETTER



**AI AND PRIVACY: SAFEGUARDING
PERSONAL DATA IN THE AGE OF
ARTIFICIAL INTELLIGENCE**

INTRODUCTION

AI is now integrated into nearly every app and service we use, from personal assistants to healthcare and financial tools. Currents research report 2023 reveals that **49%** of tech industry founders, executives, and employees are leveraging AI and ML tools to drive business innovation—a clear indication of AI's growing role in shaping modern business strategies. AI based applications brings significant benefits, but also a range of data privacy concerns. These risks require attention and proactive solutions to safeguard personal and organizational data.

The **Digital Personal Data Protection (DPDP) Act, 2023** reflects India's effort to address the growing concerns of data privacy in the digital era. Built on the foundation of the 2017 Puttaswamy judgment, which affirmed **privacy as a fundamental right**, the Act aims to protect individuals' privacy while fostering an environment of innovation.

"In the age of AI, innovation and privacy risks walk hand in hand—a dynamic that the DPDP Act seeks to balance through clarity, protection, and proactive regulation."

LET'S EXPLORE >>>>>

Cisco's research 2022 found that **60% of consumers** have lost trust in organizations due to their use of AI, highlighting the need for robust data governance and ethical AI practices. These statistics reveal a growing concern among consumers about how AI impacts their privacy.

The relationship between AI and the DPDP Act revolves around how AI technologies handle personal data while ensuring compliance with privacy and data protection regulations.

THE INTERSECTION OF AI AND DATA PRIVACY



3. Subject to the provisions of this Act, it shall—

(a) apply to the processing of digital personal data within the territory of India where the personal data is collected—

(i) in digital form; or

(ii) in non-digital form and digitised subsequently;

(b) also apply to processing of digital personal data outside the territory of India, if such processing is in connection with any activity related to offering of goods or services to Data Principals within the territory of India;

Application of Act.

While the DPDP Act does not explicitly mention Artificial Intelligence, its **overarching purpose** is to protect individual privacy. By regulating lawful data processing practices, the Act sets the foundation for responsible AI data usage.

The DPDP Act applies to AI applications whenever personal data is involved in the development, deployment, or operation of systems. If you handle personal data in any form—whether by collecting, storing, analyzing, or sharing it—either within India or across borders, for the purpose of providing goods or services to individuals in India, and you control the data processing decisions, you are required to comply with the DPDP Act.

“The true power of AI lies not just in data, but in the responsibility to protect it—DPDP Act makes that possible.”



AI-POWERED APPLICATIONS RELY ON VAST AMOUNTS OF PERSONAL DATA TO IMPROVE EFFICIENCY, PERSONALIZE EXPERIENCES, AND OPTIMIZE DECISION-MAKING. THE BELOW TABLE INDICATES THE TYPES OF DATA COLLECTED:

CATEGORY	EXAMPLES
PERSONAL IDENTIFIERS	NAME, EMAIL, ADDRESS
BIOMETRIC DATA	FINGERPRINT, FACE SCAN
BEHAVIORAL DATA	BROWSING HISTORY, PURCHASES
HEALTH DATA	HEART RATE, MEDICAL HISTORY
FINANCIAL DATA	BANK DETAILS, CREDIT SCORE



»»»» AI'S HUNGER FOR PERSONAL DATA

AI-DRIVEN APPLICATIONS COLLECT PERSONAL DATA THROUGH MULTIPLE MEANS, OFTEN TO IMPROVE SERVICES, PERSONALIZE EXPERIENCES, OR ENHANCE SECURITY.

SOME COMMON METHODS INCLUDE:



Direct User Input



Device and Sensor Data



Online Tracking and Cookies



Biometric & Facial Recognition Systems



Social Media



Public Sources



Transactional Data

TRANSPARENT AI MODEL: ADAPTING TO THE DPDP ACT

Notice.

5. (1) Every request made to a Data Principal under section 6 for consent shall be accompanied or preceded by a notice given by the Data Fiduciary to the Data Principal, informing her,—

(i) the personal data and the purpose for which the same is proposed to be processed;

(ii) the manner in which she may exercise her rights under sub-section (4) of section 6 and section 13; and

(iii) the manner in which the Data Principal may make a complaint to the Board, in such manner and as may be prescribed.



Data Collection, Notice and Consent

AI providers must provide a **clear and transparent notice** to individuals before collecting their personal data, outlining the purpose, categories of data, retention period, and the rights of the data subject.

Specifically, **Section 7** mandates that data controllers inform individuals about the processing activities, including the legal basis for processing, and if any changes occur in the data usage, an updated notice must be provided.

AI systems often require large datasets to improve accuracy.

The **Section 7 of DPDP Act** emphasizes obtaining explicit consent from data subjects (individuals whose data is being processed).

AI developers must ensure they have consent for the data they collect and use, particularly for sensitive personal data.



Minor and Guardian Consent

For AI applications, this means:

- ◆ Strict Age Verification – Ensuring systems can accurately identify users under 18.
- ◆ Guardian Consent Mechanisms – Implementing verifiable consent processes for parents/legal guardians.
- ◆ Privacy by Design – Minimizing data collection and ensuring child-friendly AI interactions.

The requirements are covered under **Section 9**



Building Responsible AI Model

AI models must ensure **data accuracy, completeness, and consistency** in decision-making processes.

🤖 AI Models That Influence Decisions
AI models must be designed to:

- ◆ Process personal data in a lawful manner.
- ◆ Avoid discriminatory outcomes by ensuring fair and unbiased processing.
- ◆ Uphold privacy-first principles to maintain user trust.

🚫 AI Models with Prohibited Uses

- ◆ No processing that harms a child's well-being.
- ◆ No behavioral tracking or targeted advertising for minors, except under government exemptions.

“Start your DPDP compliance journey with us today”

PRIVACY CHALLENGES OF AI IN THE CONTEXT OF THE DPDP ACT



Bias and Discrimination

AI systems can inadvertently introduce bias into decision-making processes, potentially resulting in unfair or discriminatory outcomes for individuals.

Businesses must ensure that AI systems are designed to be fair, transparent, and accountable, in line with the DPDP Act's provisions on data fairness and non-discrimination.



Data Security and Breaches

AI systems may become targets for cyber-attacks due to the large volumes of personal data they process.

Organizations must implement robust data security measures to safeguard against unauthorized access.



Lack of Transparency

Many AI algorithms operate as "black boxes," making it difficult to understand how personal data is being used to arrive at a decision.

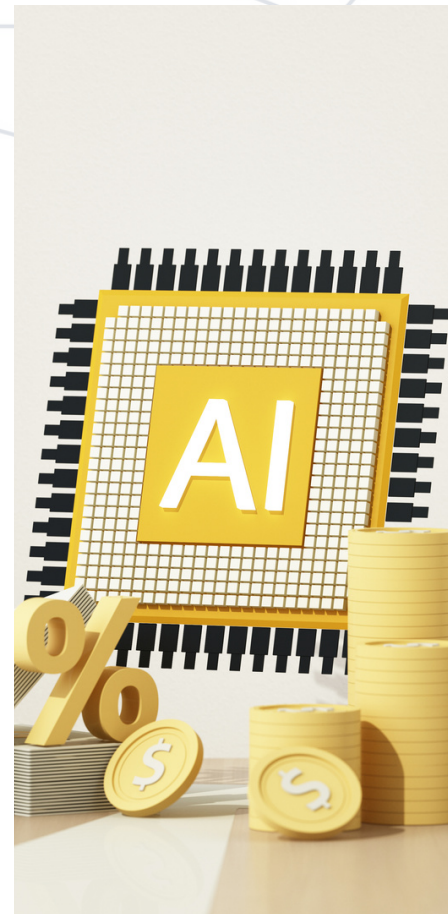
The DPDP Act mandates that organizations provide clear information about the processing of personal data, including the purpose, methods, and implications of AI-driven decisions.



Data Protection Impact Assessments

AI-driven systems must undergo DPIAs to evaluate the risks to privacy and data protection.

Businesses should assess potential risks, including the misuse of personal data, and put in place mitigation measures to comply with the DPDP Act.



A Few Notes To Remember

- Educate employees, especially those involved in AI development and data processing, on the importance of data privacy and ethical AI practices.
- Use anonymization or pseudonymization techniques where possible to minimize the risks of data exposure and ensure compliance.
- Regularly audit AI systems for compliance with data protection principles such as data minimization, transparency, and fairness.
- Remember non-compliance may lead fines up to 250 crore rupees.



FUTURE OUTLOOK

The intersection of AI and privacy under the DPDP Act will continue to evolve as AI technologies advance and the regulatory landscape adapts.

As AI systems become more sophisticated, businesses will need to remain vigilant in ensuring compliance with data protection laws while fostering innovation.

Keeping a proactive approach to data privacy will not only help organizations avoid legal pitfalls but will also build trust with customers, enhancing brand reputation and loyalty.

The DPDP Act provides a critical framework for balancing technological advancement with the fundamental right to privacy.

The future of AI is bright, and with the right safeguards in place, we can ensure it benefits all stakeholders without compromising on what matters most: trust, security, and respect for individual rights.

IF YOU WOULD LIKE TO LEARN MORE ABOUT HOW TO ENSURE YOUR AI SYSTEMS COMPLY WITH THE DPDP ACT OR NEED ASSISTANCE IN CONDUCTING STAFF TRAININGS, REACH OUT TO OUR TEAM OF EXPERTS TODAY!

Thank you for reading!

<u>ALPHA MD PVT. LTD.</u>	info@alphamd.com
www.alphamd.com	19, Unique Industrial Estate, Prabhadevi, Mumbai - 25.

"Start your DPDP compliance journey with us today"