Evolving Jurisprudence on Data Protection in India

By: M K SIL

25-April-2025

The Digital Personal Data Protection Act

Introduction: The Digital Personal Data Protection Act, 2023, enacted on August 11, 2023, provides a framework for processing digital personal data that recognizes both the rights of individual to protect their personal data and the need to process such personal data for lawful purpose.

Aim: This is the first comprehensive legislation in India aimed of safeguarding Personal Data in the increasing digitized world; the Act aim to ensure “privacy rights” while enabling technological and economic growth.

The implementation of the Act would take full effect once the “Rule & Regulations” are formally passed by the parliament.

Key Features – Scope and Applicability

- **Data Fiduciaries:**
  The Act applies to any entity, whether a company, government body, or NGO that processes digital personal data within India, including foreign firms offer goods/services to Indian users.

- **Data Principals:**
  Primarily Indian citizens, whose personal data is collected and processed under the Act.

- **Exemptions:**
  - **Government Agencies** are exempt for purposes related to **national security, law enforcement**, and delivery of **public services**.
  - **Small Businesses** with minimal data processing obligations to reduce compliance burden.

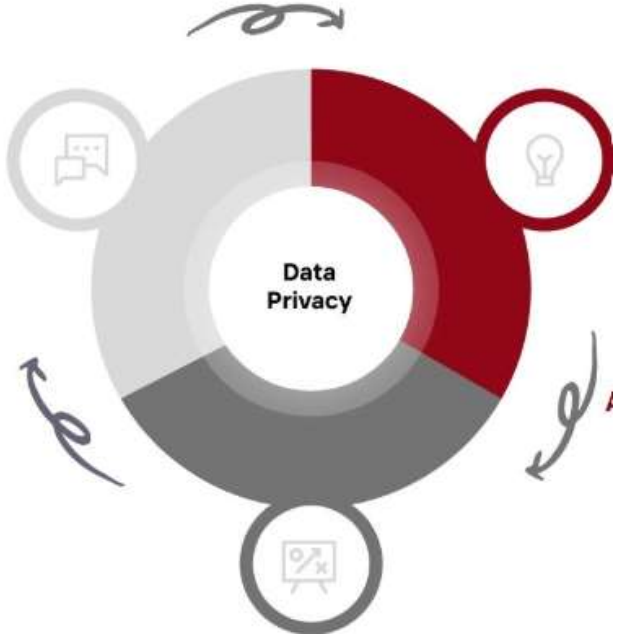
7 Key Legal Principles in the DPDP Act, 2023

Lawful and Transparent
Personal data must be collected and used in a fair, lawful, and transparent manner, with individuals aware of how their data is being used.

Purpose Limitation
Data should only be used for the specific, legitimate purpose it was collected for - no hidden or unrelated use.

Data Minimization
Only collect the minimum amount of personal data necessary to fulfill the intended purpose—nothing excessive

Accountability
Entities handling data (called Data Fiduciaries) are responsible for complying with the law and must be able to demonstrate that compliance



Data Accuracy
Ensure personal data is accurate, complete, and up to date. Inaccurate data should be corrected or deleted promptly.

Security Safeguards
Protect personal data with appropriate technical and organizational measures to prevent breaches or misuse.

Storage Limitation
Keep data only for as long as necessary to achieve the purpose it was collected for, then securely delete it.

Core Legal Principles under the Digital Personal Data Protection Act, 2023 (India)

- **Consent based data processing**
    - Data Collection must be based on clear informed and explicit consent
    - Individual have the right to withdraw consent any time.
    - Companies must make the “Process of consent withdrawal “ simple and accessible.

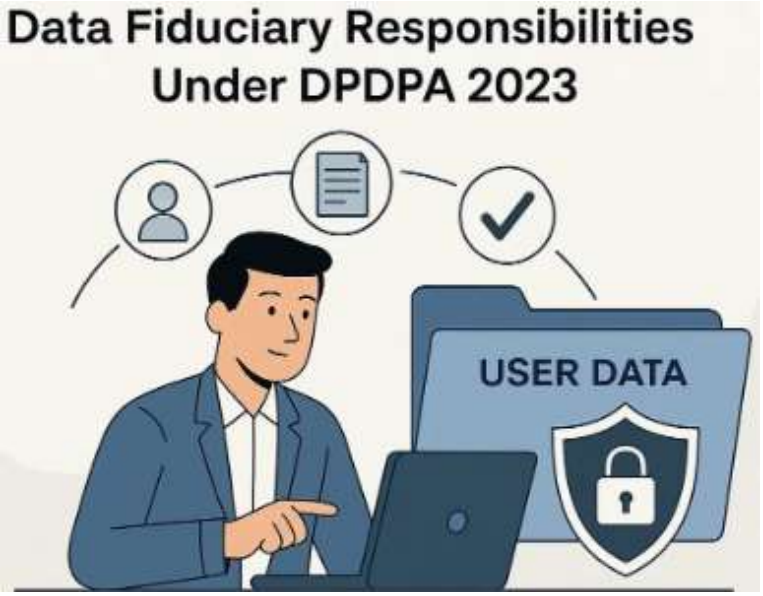
- **Processing Without Consent (Legitimate Use)** : Certain situations allow data processing without consent, including:
    - National Security & Public interest activities
    - Govt mandated services viz. Health Care, Taxation, Subsidies etc.
    - Disaster management and law enforcement investigations

Rights of Data Principles (Individuals)

- **Right to Access:** Individuals have the right to know how their personal data is being processed and for what purposes.
- **Right to Correction and Erasure:** Individuals can request correction, completion, or deletion of their inaccurate, outdated, personal data.
- **Right to Grievance Redressal:** Complaints can be filed with the Data Fiduciary (the company or entity processing the data). Or to the **Data Protection Board (DPB)**.
- **Right to Nominate:** Individuals can nominate another person to exercise their data rights in the event of death or incapacity.
- **Right to Withdraw Consent:** Withdraw consent and opt out of data processing at anytime.

Obligations of Data Fiduciaries (Businesses and Organizations)

- **Obtain Explicit Consent:** Personal data must be collected and processed only with clear, informed, and specific consent from the Data Principal, unless exempt under legitimate use provisions.
- **Ensure Data Minimization:** Collect only the minimum data necessary for the specified purpose of processing.
- **Maintain Accuracy and Security:** Organizations must ensure data is accurate, secure and protected from breaches.
- **Report Data Breaches Promptly** : In case of a breach, companies must immediately notify the authorities and affected individuals.
- **Maintain Transparency:** Organizations must publish clear, accessible privacy policies detailing how personal data is collected, processed, stored, and shared.
- **Ensure Accountability and Compliance:** Appoint a **Data Protection Officer (DPO)** responsible for compliance and act as a point of contact for grievance redressal.



Cross-Border Data Transfers

- The act allows “Cross-border transfer” of Personal data to countries approved by Union Government

- Sensitive Data Considerations: Sensitive data (e.g., health, biometrics, etc.) subject to localization requirement.

Challenges of Cross-Border Transfers

Special Protections for Children

- **Parental Consent**: Processing personal data of individuals under 18 requires *verifiable consent* from a parent or legal guardian.
- **No Harm Principle**: Data processing must not cause *detrimental effects* to the well-being of children.
- **Prohibition on Targeting**: *Tracking, profiling, behavioral monitoring,* and *targeted advertising* directed at children are *strictly prohibited*.
- **Safe Digital Experience**: Entities must promote a *secure and age-appropriate online environment* for minors.

Enforcement & Penalties

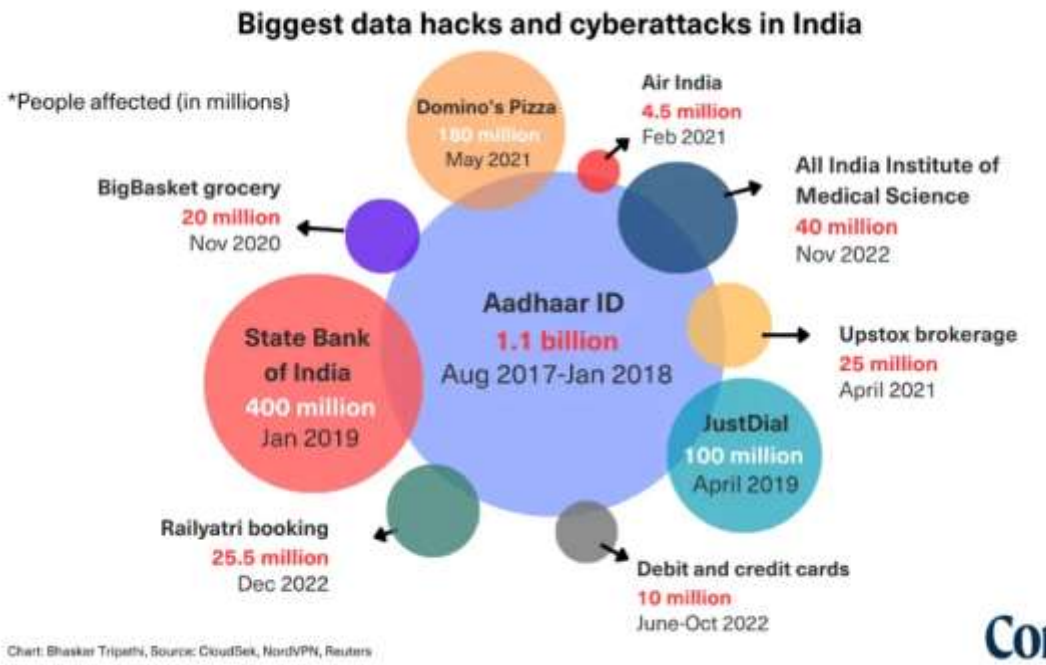
- Data Protection Board of India (DPB) is responsible for:
  - Investigating complaints and enforcing compliance.
  - Issuing penalties for violations as the adjudicating body.
  - Ensuring data protection laws are upheld.

- Fines & Penalties:
  - Up to ₹250 crore per violation for data breaches and non-compliance.
  - Additional penalties for repeat offenses and failure to protect sensitive data.
- Appeals:
  - Appeals against the decisions of DPBI will lie with the Telecom Dispute Settlement and appellate tribunal (TDSAT).

Impact on Data Privacy & Business in India

- Positive Impact:
  - Empowers individuals with control over their personal data.
  - Enhances trust and transparency in digital transactions.
  - Encourages businesses to implement better security and data governance.
  - Facilitates innovation by enabling businesses to handle data responsibly.

- Challenges:
  - Compliance Costs: Companies, especially startups and MSMEs, need to invest in security measures.
  - Government Exemptions: Raises concerns about surveillance and privacy risks.
  - Enforcement & Awareness: Businesses and individuals must be educated on compliance requirements.



People affected (in millions) by data breaches

Conclusion

- “DPDPA 2023” is a landmark step in India’s “data privacy and protection framework”.
- Strikes a “balance between individual rights, business growth, and national security”.
- The Act’s success depends on "effective implementation, awareness, and regulatory enforcement”.
- Businesses must adopt *privacy-first policies* to ensure smooth compliance.