Background & Need for the DPDP Act 2023

Digital Growth

India has 900 million+ internet users. Digital transactions, e-governance and social media generate massive personal data daily.

Legal Vacuum

Prior to DPDP Act 2023, no comprehensive legislation specifically governed personal data protection in India.

Global Alignment

GDPR (EU), PDPA (Singapore) set global benchmarks. India needed a comparable framework for cross-border data trust.

Key Milestones

2017 – Puttaswamy judgment: Right to Privacy declared fundamental

2018 – B.N. Srikrishna Committee Report

2019 – Personal Data Protection Bill introduced in Lok Sabha

2021 – JPC Report submitted

2022 – Bill withdrawn, redrafted

2023 – DPDP Act passed on August 11, 2023

Received Presidential assent on August 11, 2023

Structure of the Act & Key Definitions

Act Structure

- 9 Chapters
- 44 Sections
- Preamble
- Ch. I – Preliminary
- Ch. II – Data Obligations
- Ch. III – Rights & Duties
- Ch. IV – Data Fiduciaries
- Ch. V – DPBI
- Ch. VI – Appeals
- Ch. VII – Offences
- Ch. VIII – Exemptions
- Ch. IX – Miscellaneous

Personal Data
Any data about an identifiable individual (Data Principal)

Data Principal
Individual to whom personal data relates (minors: guardian)

Data Fiduciary
Entity that determines purpose & means of data processing

Data Processor
Entity processing data on behalf of the Data Fiduciary

Consent Manager
Registered body managing consent on behalf of Data Principal

Significant Data Fiduciary (SDF)
Data Fiduciary notified by Central Govt based on risk criteria

Applicability & Territorial Scope

Section 3 – Applicability of the DPDP Act 2023

✅ APPLIES TO

- Processing of digital personal data within India
- Processing outside India if related to offering of goods/services to individuals in India
- Both automated and digitised data processing
- Government and private entities alike (unless exempted)
- Foreign companies targeting Indian data principals

❌ DOES NOT APPLY TO

- Non-digital (offline) personal data not digitised
- Personal data processed for personal/domestic purposes
- Anonymised data (not re-identifiable)
- Data notified as exempt by Central Government
- Research, archiving and statistical purposes (with safeguards)

Consent & Lawful Bases for Processing (Sections 6–7)

Section 6 – Consent Requirements

1. **Free:** Must be freely given without coercion
2. **Specific:** Specific to the stated purpose
3. **Informed:** Clear notice in plain language, available in all 22 Scheduled Languages
4. **Unconditional:** Not bundled with other services without choice
5. **Unambiguous:** Explicit affirmative action required; silence not consent
6. **Withdrawable:** Withdrawal must be as easy as giving consent

Section 7 – Legitimate Use (Without Consent)

- State purposes – subsidies, benefits, services, licences under law
- Legal obligations under Indian law
- Medical emergencies threatening life
- Epidemics, public health emergencies
- Disasters and public order maintenance
- Employment purposes (reasonable expectations)
- Prevention of offences or legal proceedings

Obligations of Data Fiduciaries (Sections 8–11)

§8 – General Obligations
Must ensure accuracy & completeness of data; implement appropriate security safeguards; notify DPBI and affected principals of data breaches; delete data when purpose is served

§8 – Notice Requirements
Plain language notice before/at time of collecting consent; must include what data is collected, purpose of processing, how to exercise rights, and how to file complaints

§9 – Children's Data
Verifiable parental consent required before processing data of minors (under 18). No tracking, behavioural monitoring, or targeted advertising directed at children.

§10 – Significant Data Fiduciary
SDFs must appoint Data Protection Officer (DPO), conduct Data Protection Impact Assessments (DPIAs), audit algorithms for bias and risk, and appoint independent data auditor.

§11 – Data Retention

Data must not be retained beyond the period necessary for the stated purpose. Must have clear deletion/anonymisation policy.

Cross-Cutting

All obligations apply regardless of whether processing is by the DF directly or through a Data Processor. DF remains accountable at all times.

Rights of Data Principals (Sections 12–16)

Every individual (Data Principal) has the following statutory rights:

§12 – Right to Access

Right to obtain summary of personal data being processed, identities of Data Fiduciaries and Processors, and grievance redressal information.

§13 – Right to Correction & Erasure

Right to correct inaccurate/misleading data, complete incomplete data, and request erasure of data no longer needed.

§14 – Right to Grievance Redressal

Right to file complaints with the Data Fiduciary first; if unresolved, escalate to Data Protection Board.

§15 – Right to Nominate

Right to nominate another individual to exercise rights in case of death or incapacity of the Data Principal.

§16 – Duties of Data Principal

Must not impersonate others, suppress material info, file false complaints, or furnish false particulars.

Data Protection Board of India (Sections 17–29)

Constitution

Set up by Central Govt; Chairperson + Members as notified; digital-first body

Proceedings

All hearings virtual; no civil court jurisdiction; bound by principles of natural justice

Powers

Inquiry into breaches; issue directions; impose financial penalties

Appeals

Appeals to Appellate Tribunal within 60 days; further appeal to High Court

Penalties & Enforcement (Section 33 & Schedule)

Schedule – Financial Penalties (All amounts in Indian Rupees)	
Breach of children's data obligations (§9)	₹200 Crore
Failure to implement adequate security safeguards	₹250 Crore
Failure to notify Board of data breach	₹200 Crore
Non-compliance by Significant Data Fiduciary	₹150 Crore
Failure to respond to Data Principal grievance	₹10,000
Other violations of the Act or Rules	₹50 Crore
Repeated / continuing violations	Up to ₹500 Crore cumulative

Exemptions under the DPDP Act 2023 (Section 17)

The Central Government may, by notification, exempt:

National Security & Defence

Processing by State instrumentalities for national security, sovereignty, or public order. Intelligence agencies notified under Schedule lists.

Prevention & Investigation

Law enforcement agencies for prevention, detection, investigation, and prosecution of offences.

Research & Statistics

Processing for academic research, archiving, or statistical purposes with appropriate safeguards.

Startups & SMEs

Central Government may exempt certain categories of Data Fiduciaries (incl. startups) from certain obligations to encourage innovation.

Courts & Parliament

Proceedings before courts, tribunals, Parliament, and state legislatures are outside the Act's scope.

Diplomatic/Consular Functions

Foreign states, diplomatic missions, and international organisations in India.

DPDP Rules 2025 – Overview & Status

Draft DPDP Rules released for public consultation – January 2025

Rule 3 – Notice
Consent notices must be in plain language, available in all 22 Scheduled Languages, specify purpose, categories of data, retention period, and rights available.

Rule 4 – Consent Manager

Registration, obligations, technical standards, and accountability mechanisms for Consent Managers.

Rule 5 – Children's Data

Verifiable parental/guardian consent mechanisms; age verification standards; prohibited processing activities.

Rule 6 – SDF Obligations

Criteria for classification; DPO role and qualifications; DPIA methodology; algorithmic auditing standards.

Rule 7 – Data Breach

Notification timelines (72 hours to DPBI); format of breach reports; communication to affected principals.

Rule 8 – Localisation

Cross-border data transfer rules; list of approved countries; restricted transfers for sensitive categories.

Rules on Notice, Consent & Consent Managers

Notice Requirements (Draft Rule 3)

- Itemised list of personal data being collected
- Specific purpose for each category of data
- Name and contact details of Data Fiduciary
- Manner of exercising rights (access, correction, erasure)
- Procedure and means for withdrawal of consent
- How to contact the Data Protection Board for complaints

Language Access: Notices must be available in ALL 22 Scheduled Languages listed in the 8th Schedule of the Constitution of India a landmark multilingual inclusion mandate.

Consent Manager (Rule 4)

- Registered with Data Protection Board
- Acts on behalf of Data Principal
- Interoperable & accessible platform
- Maintains audit trail of consents
- Must not charge Data Principals
- Accountable for accuracy of consent records
- Minimum net worth requirements applicable

Protection of Children's Personal Data (Section 9 & Rules)

⚠️ **Highest Penalty: ₹200 Crore – Children's Data is a Priority Protection Area**

✅ Allowed (With Consent)

- Processing with verifiable parental/guardian consent
- Health and emergency services (limited exceptions)
- Educational/welfare activities with parental consent
- Activities not involving tracking or profiling

❌ Strictly Prohibited

- Behavioural monitoring or tracking of children
- Targeted advertising directed at children
- Data processing likely to harm children's wellbeing
- Processing without age verification mechanisms
- Profiling based on a child's online behaviour

Significant Data Fiduciaries (SDF) – Section 10

Classification Criteria

- Volume of personal data processed
- Sensitivity of personal data
- Risk to rights of Data Principals
- Potential impact on national security
- Risk to electoral democracy
- Security of the State
- Public order implications
- Sovereignty & integrity of India

Additional SDF Obligations

Data Protection Officer

Must be appointed; must be a key managerial person or equivalent; liable to DPBI

Independent Data Auditor

Periodic audits of compliance with the Act and Rules

Data Protection Impact Assessment

DPIA mandatory before processing high-risk activities

Algorithmic Accountability

Review and audit of AI/ML algorithms for bias, fairness, and risk to Data Principals

Data Breach Notification & Security Obligations

Breach Occurs

0 hrs

Unauthorised access, disclosure, alteration, or loss of personal data

Internal Detection

T+0

Data Fiduciary's internal security team identifies breach scope

DPBI Notification

T+72 hrs

Board notified within prescribed time (Rules specify 72 hrs)

Principal Communication

T+72 hrs+

Affected Data Principals notified in prescribed format

Remediation

Ongoing

Technical and organisational measures to contain breach

DPBI Review

Post-Breach

Board may initiate inquiry; penalties if safeguards were inadequate

Cross-Border Data Transfer Rules

Section 16 – Transfer of Personal Data Outside India

Whitelist Approach
Central Government will notify a list of countries/territories to which data may be transferred. Transfer to non-notified countries is restricted.

Central Government Powers
May restrict transfer to any country or territory for reasons of sovereignty, security, or diplomatic considerations.

No Blanket Prohibition
Unlike earlier draft Bills, DPDP Act 2023 does not mandate data localisation by default. Transfer is allowed subject to whitelist.

Sensitive Categories
Draft Rules indicate stricter transfer restrictions for sensitive personal data categories (financial, health, biometric) — country-specific restrictions likely.

Contractual Safeguards
Data Fiduciaries transferring to third countries must ensure equivalent data protection through contracts or other legally binding instruments.

Pending Notification
As of 2024, the final whitelist of approved countries has not yet been notified — a critical pending rule for global businesses.

Government Sector – Special Provisions & AI Implications

Government as Data Fiduciary – Obligations, Privileges & AI Deployment

Broader Legal Basis

State can process data without consent for benefits, subsidies, licences, and legal obligations (§7). Enables e-governance AI systems.

SDF Classification Risk

Key government platforms (DigiLocker, UMANG, Aadhaar ecosystem) may be classified as SDFs requiring DPIAs and DPOs.

Sweeping Exemptions (§17)

Intelligence agencies, defence, border management, and national security AI largely exempt from most Act provisions.

AI & Algorithmic Accountability

SDFs including public sector entities must audit algorithms — directly applies to welfare AI, predictive policing, and credit scoring.

Citizen Rights Still Apply

Rights to access, correction, and grievance redressal remain intact against government bodies (unless specifically exempted).

IndiaAI + DPDP Synergy

IndiaAI Mission provides infrastructure; DPDP Act provides guardrails. Combined, they form India's emerging responsible AI governance framework.

Comparison: Pre-DPDP vs DPDP Act 2023

Aspect	Pre-DPDP (IT Act 2000 + Rules)	DPDP Act 2023
Dedicated Law	No comprehensive data law	Yes – standalone legislation
Consent	Not explicitly required for all data	Explicit, informed, withdrawable consent
Regulatory Authority	None (IT Ministry oversight)	Data Protection Board of India
Children's Data	No specific provisions	Verifiable parental consent + prohibitions
Cross-Border Transfer	No restrictions	Whitelist of approved countries
Penalties	IT Act §43A max ₹5 crore	Up to ₹250–500 crore per violation
Individual Rights	Minimal	5 explicit statutory rights
Data Localisation	None	Selective (per notified categories)

Implementation Roadmap & Compliance Checklist

Aug 2023
DPDP Act Enacted

Jan 2025
Draft Rules Released

2025
Rules Finalisation

2025–26
DPBI Constituted

2026
Full Enforcement

Compliance Checklist for Organisations

- ✓ Map all personal data flows and classify data categories
- ✓ Review and update consent mechanisms and notice formats
- ✓ Translate notices into applicable Scheduled Languages
- ✓ Establish children's age verification mechanisms
- ✓ Appoint DPO if classified or likely to be SDF
- ✓ Implement data breach detection and 72-hour notification protocol
- ✓ Update vendor contracts with Data Processor obligations
- ✓ Conduct Data Protection Impact Assessment for high-risk activities

Summary & Way Forward

Key Takeaways

- India's first comprehensive data protection law — landmark legislation
- Centralised enforcement via Data Protection Board of India
- Strong consent rights with 22-language multilingual mandate
- Significant Data Fiduciaries face heightened AI accountability
- Broad exemptions for national security and government functions
- Rules still being finalised — dynamic compliance landscape
- Digital India Act expected to further regulate AI explicitly

Way Forward

- Final DPDP Rules notification (2025)
- Establishment of DPBI and Appellate Tribunal
- Notification of approved countries for data transfer
- AI-specific regulation via Digital India Act
- Sector-specific guidelines (RBI, SEBI, IRDAI)
- Corporate compliance programmes and audits
- Awareness campaigns for Data Principals
- Technical standards for security safeguards