[recovered from the vector store — section1.html p.1]

Section 1 DPDPA

Short Title and Commencement.

1) This Act may be called the Digital Personal Data Protection Act, 2023.

(2) It shall come into force on such date as the Central Government may, by notification in the Official Gazette, appoint and different dates may be appointed for different provisions of this Act and any reference in any such provision to the commencement of this Act shall be construed as a reference to the coming into force of that provision.

Section 2 DPDPA →

DPDPA
Table of contents

Report error

Your message
×

Please keep in mind that this form is only for feedback and suggestions for improvement. Unfortunately, questions will not be answered.

Do not fill this field

0 of 1000 max characters

Submit

Comprehensive Legal Interpretation of Section 1 of the Digital Personal Data Protection Act, 2023

"Every great law begins with a name, a territory, and a date." - Legal Tradition

Section 1 - Short Title, Extent and Commencement

Statutory Text

Section 1(1). This Act may be called the Digital Personal Data Protection Act, 2023.
Section 1(2). It extends to the whole of India and applies to—

the processing of digital personal data within the territory of India where the personal data is collected—

in digital form; or

in non-digital form and digitised subsequently;

the 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.

Section 1(3). It shall come into force on such date as the Central Government may, by notification in the Official Gazette, appoint, and different dates may be appointed for different provisions of this Act, and any reference in any such provision to the commencement of this Act shall be construed as a reference to the coming into force of that provision.

Related Notification:

Commencement Notification: To be issued by Ministry of Elect

[recovered from the vector store — section1.html p.2]

ronics & IT (MeitY)

Table of Contents

1. Executive Summary: The Foundation Stone
Section 1 is the foundation of the DPDPA - it answers three fundamental questions:

□□ The Three Foundational Questions

Question 1: What is this law called?

Answer (Section 1(1)): "Digital Personal Data Protection Act, 2023"

Why it matters: Name defines scope - it's about DIGITAL data, PERSONAL data, PROTECTION

Question 2: Where does this law apply?

Answer (Section 1(2)):

□ Entire India (all states and union territories)

□ PLUS extraterritorial application (foreign companies serving Indian users)

Why it matters: Google in USA, Facebook in Ireland, TikTok in Singapore ALL subject to DPDPA if they serve Indian users

Question 3: When does this law come into effect?

Answer (Section 1(3)): When Central Government notifies in Official Gazette

Status: Passed by Parliament August 2023, Rules notified January 2025, Act expected to be enforced in phases starting 2025

Why it matters: Organizations need time to prepare; government can phase in different provisions

Key Insight: Section 1 establishes DPDPA as one of the world's most ambitious data protection laws in terms of territorial reach - it claims jurisdiction over ANY processing of Indian personal data ANYWHERE in the world.
2. Section 1(1): Short Title & Naming Convention

Statutory Language: "This Act may be called the Digital Personal Data Protection Act, 2023."

2.1 Deconstructing the Name

□ What's in a Name? Everything.

1. "Digital" - Scope Limitation

Includes:

Data collected directly in digital form (online forms, apps, websites)

D

[recovered from the vector store — section1.html p.3]

ata collected in non-digital form then digitized (paper forms scanned, physical documents converted to PDF)

Purely paper-based records never digitized

Oral communications never recorded digitally

Physical observations never documented digitally

Doctor writes prescription on paper → Scanned and stored in hospital's electronic medical records system → ☐ DPDPA applies

Doctor writes prescription on paper → Filed in physical cabinet, never digitized → ☐ DPDPA doesn't apply (other laws like Indian Medical Council Act may apply)

Practical Reason: Digital data is easily copied, transmitted, analyzed at scale - poses unique privacy risks

Policy Reason: Applying to paper records would be administratively unworkable for small businesses

Future-Proofing: As India digitizes, more data naturally falls under DPDPA

Definition (Section 2(t)): Data about an individual who is identifiable by or in relation to such data

Online identifiers (IP addresses, cookies, device IDs)

Behavioral data (browsing history, purchase patterns)

Statistical data where individuals can't be identified

The law PROTECTS personal data - it's a rights-based law, not a data-use enablement law

[recovered from the vector store — section1.html p.4]

t (Personal Data Protection Bill, 2018)

2019: Revised draft (Personal Data Protection Bill, 2019)

2021: Joint Parliamentary Committee Report

2022: Bill withdrawn, fresh draft started

2023: Digital Personal Data Protection Bill introduced → Passed → DPDPA, 2023

2.2 Significance of "Short Title"

Legal Tradition: Every Act has a "short title" for convenient reference

Full vs Short Title:

Long Title: "An Act to provide for the processing of digital personal data in a manner that recognises both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes and for matters connected therewith or incidental thereto."

Short Title: "Digital Personal Data Protection Act, 2023" (or "DPDPA 2023")

Usage: Courts, lawyers, businesses refer to the law as "DPDPA 2023" or simply "the Act"

3. Section 1(2): Territorial & Extraterritorial Reach
Section 1(2) is REVOLUTIONARY - it gives DPDPA global reach.

3.1 Territorial Application (Section 1(2)(a))

Statutory Language: "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"

⁉️ Territorial Application Explained

Rule: If processing happens IN INDIA, DPDPA applies

"Territory of India" means:

All 28 States

All 8 Union Territories

Territorial waters (12 nautical miles from coast)

Continental shelf and Exclusive Economic Zone

Airspace above

Two Collection Scenarios:

Scenario 1(i): Collected Digitally

Example: User fills online form on website, submits via app, provides data through chatbot

Location of Server Irrelevant: Even if data goes to US servers, if collection happened in India → DPDPA applies

Scenario 1(ii): Collected Non-Digitally, Then Digitized

Example:

Patient fills paper form at clinic → Receptionist enters into computer

Employee submits handwritten leave application → Manager scans and emails to HR

Customer signs phy

[recovered from the vector store — section1.html p.5]

sical contract → Company digitizes for records

Indian user visits US website, enters data → Data collected in India (from Indian user on Indian soil) → □ DPDPA applies

US company processes that data in US servers → Still □ DPDPA applies (because collected in India)

3.2 Extraterritorial Application (Section 1(2)(b))

Statutory Language: "the 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"

This is the GDPR-inspired "long-arm" provision.

□ Extraterritorial Reach - India's Global Jurisdiction

Rule: Foreign companies processing Indian data OUTSIDE India are subject to DPDPA IF they offer goods/services to Indians

Data is of Data Principals (individuals) IN India

Processing connected to offering goods/services

Goods/services offered TO Indians in India

Broad connection - doesn't require processing to be "for the purpose of" offering, just "in connection with"

Streaming service has Indian content, accepts INR

Social media platform available in India, has Indian users

Cloud service marketed to Indian businesses
Website accessible from India but not specifically targeting Indians (e.g., no INR pricing, no Indian payment methods, no Indian shipping)

Generic global platform used by Indians but not marketed to them

Service explicitly excludes Indian residents in Terms of Service

B2B service only, no individual consumers

Location: Headquarters in USA, servers worldwide

[recovered from the vector store — section1.html p.6]

Services: Search, Gmail, YouTube, Maps, all targeted to Indians

Result: DPDPA applies (Section 1(2)(b))

Location: Headquarters in USA, CDN globally

Services: Streaming specifically offered to Indians (INR pricing, Indian content, payment via Indian cards/UPI)

Result: DPDPA applies (Section 1(2)(b))

Location: Owned by ByteDance (China), operated from Singapore for most regions

Services: App was hugely popular in India before ban

Result: If operational, DPDPA would apply (Section 1(2)(b))

Personal blog accessible globally, no specific Indian targeting

Some Indian readers, but not marketed to them

Result: Arguably not "offering services to Indians" - DPDPA may not apply

"This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

(a) the offering of goods or services... to such data subjects in the Union; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union."

DPDPA Section 1(2)(b) is almost identical to GDPR 3(2)(a)
Key Difference: GDPR also covers "monitoring of behaviour" - DPDPA doesn't explicitly include this

Aspect | GDPR Art 3(2) | DPDPA Sec 1(2)(b)
Offering goods/services | Covered explicitly | Covered explicitly
Monitoring behaviour | Covered explicitly (Art 3(2)(b)) | ? Arguably covered under "in connection with" but not explicit
Threshold | "data subjects who are in the Union" | "Data Principals within the territory of India"

 Extraterritoriality Enforcement Challenges

Indian Data Protection Board can issue orders to foreign companies, but enforcing those ord

[recovered from the vector store — section1.html p.7]

ers abroad is difficult

Example:

Board fines US company ₹100 crores

Company ignores

Board cannot seize US-based assets

Would need cooperation of US courts (comity principles)

Solution: Board can:

Block company's services in India (coordinate with telecom/ISPs)

Prohibit payment processors from processing Indian transactions

Issue public notice of non-compliance (reputational damage)

Coordinate with foreign regulators (EU, US) for joint action

Challenge 2: Service of Notice

How to serve legal notice to foreign company with no Indian presence?

Solution (Rule 2): DPDP Rules require foreign Data Fiduciaries to:

Appoint "Consent Manager" or representative in India

Provide Indian address for service of notice

Maintain grievance redressal mechanism accessible to Indians

Challenge 3: Discovery & Evidence

Investigating foreign company's data practices when servers abroad

Solution: Board's powers (Section 32):

Require information and documents

Conduct inspections (if Indian presence)

Rely on international cooperation (MLATs - Mutual Legal Assistance Treaties)
4. Section 1(3): Commencement & Phased Implementation

Statutory Language: "It shall come into force on such date as the Central Government may, by notification in the Official Gazette, appoint, and different dates may be appointed for different provisions of this Act"

4.1 What is "Commencement"?

Commencement = When law becomes enforceable

 From Bill to Enforceable Law

Stage 1: Bill Introduced in Parliament

Digital Personal Data Protection Bill, 2023 - August 3, 2023

Stage 2: Parliamentary Debate & Voting

Lok Sabha passes - August 7, 2023

Rajya Sabha passes - August 9, 2023

Stage 3: Presidential Assent

President signs - August 11, 2023

NOW IT'S AN "ACT" but NOT YET ENFORCEABLE

Stage 4: Rules Drafted

Ministry of Electronics & IT drafts subordinate rules

Rules published for public consultation - 2024

Final Rules notified - January 3, 2025

Stage 5: Commencement Notification

Central Go

[recovered from the vector store — section1.html p.8]

vernment notifies date(s) in Official Gazette

Status: Awaited (as of January 2025)

Stage 6: Enforcement Begins

Data Protection Board constituted, penalties enforceable, rights exercisable

Expected: Phased rollout 2025-2026

4.2 Why the Gap Between Enactment & Commencement?

Reason 1: Rules Must Be Finalized

DPDPA delegates many details to Rules (consent manager standards, breach notification procedures, penalties calculation, etc.). Can't enforce Act without Rules.
Reason 2: Institutional Setup

Data Protection Board must be constituted (members appointed, office established)

Complaint mechanisms set up

IT systems for filing grievances

Training of Board members and staff

Reason 3: Industry Preparation Time

Organizations need time to:

Understand obligations

Update systems and processes

Train employees

Hire Data Protection Officers

Establish consent mechanisms

Typical Gap: 6 months to 2 years (GDPR had 2-year preparation period)

4.3 Phased Implementation

Key Phrase: "different dates may be appointed for different provisions"

This allows PHASED rollout - bringing different sections into force at different times

 Likely Phased Implementation Schedule (Hypothetical)

PHASE 1 (Day 1 - Immediate)

Effective Date: January 2026 (hypothetical)

Provisions:

Section 3 (Application)

Sections 18-32 (Board establishment, powers, composition)

Rationale: Institutional framework must exist before rights/obligations enforced

PHASE 2 (6 months later - July 2026)

Provisions:

Sections 4-8 (Obligations of Data Fiduciaries - notice, consent, purpose, security)
Section 16 (Cross-border transfers)

Rationale: Core obligations first, gives organizations 6 months to comply

PHASE 3 (12 months later - January 2027)

Provisions:

Section 9 (Children's data - stricter requirements)

Section 10 (Significant Data Fiduciary obligations - DPIA, audit, DPO)

Rationale: More complex obligations need more prep

[recovered from the vector store — section1.html p.9]

aration time

PHASE 4 (18 months later - July 2027)

Provisions:

Sections 11-15 (Rights of Data Principals - access, correction, erasure, grievance, nomination, duties)

Section 33 (Penalties)

Rationale: Rights become enforceable once organizations have systems in place; penalties begin after grace period

Note: Actual schedule will be determined by Central Government

4.4 Retrospective vs Prospective Application

General Rule: Laws apply PROSPECTIVELY (from commencement forward), not RETROSPECTIVELY (to past actions)

DPDPA Application:

Scenario | DPDPA Applies? | Reasoning
Data collected BEFORE commencement, processed AFTER | ✅ YES | Processing after commencement is covered
Data collected AND processed BEFORE commencement | ❌ NO (retrospectively) | But ongoing processing after commencement = covered prospectively
Breach occurred BEFORE commencement, discovered AFTER | ⚠️ COMPLEX | Breach itself not penalized, but failure to notify after commencement may be
Consent obtained BEFORE commencement (invalid by DPDPA standards) | ❌ Must obtain fresh valid consent after commencement | Ongoing processing requires valid consent
5. Philosophical Foundations: Sovereignty & Jurisdiction

5.1 Territorial Sovereignty (Hugo Grotius)

Hugo Grotius (1583-1645), "On the Law of War and Peace": States have absolute sovereignty within their territorial boundaries.

Application to Section 1(2)(a): India has unquestioned right to regulate data processing within its territory

5.2 The Effects Doctrine (International Law)

Effects Doctrine: State can regulate foreign conduct if it has substantial effects within the state's territory

Origin: US antitrust law (Alcoa case, 1945) - foreign cartels affecting US markets subject to US law

Application to Section 1(2)(b):

Foreign company processing Indian data has EFFECTS in India

Privacy violations harm Indians in India

Therefore, India can regulate that foreign processing

Legitimacy: Widely accepted in international law (EU's GDPR uses

[recovered from the vector store — section1.html p.10]

same principle)

5.3 Data Sovereignty Debates

Two Competing Visions:

 Global Data Governance Models

Model 1: Data Localization (China, Russia)

Principle: All data about citizens must be stored within national borders

Rationale: National security, government access, economic protectionism

Criticism: Balkanizes internet, increases costs, enables authoritarian surveillance

Model 2: Free Flow of Data (USA, Big Tech)

Principle: Data should flow freely across borders for efficiency

Rationale: Economic efficiency, innovation, global platforms

Criticism: Enables surveillance capitalism, weakens national laws

Model 3: Regulated Cross-Border Flows (EU, India via DPDPA)

Principle: Data can cross borders IF destination provides adequate protection

Rationale: Balances privacy rights with economic realities

Implementation: GDPR Chapter V, DPDPA Section 16

DPDPA's Position: Model 3 - Pragmatic middle ground
6. Constitutional Framework: Legislative Competence

6.1 Article 245 - Extent of Laws

Article 245(1): "Parliament may make laws for the whole or any part of the territory of India"

Article 245(2): "No law made by Parliament shall be deemed to be invalid on the ground that it would have extra-territorial operation"

Application:

Section 1(2)(a): Parliament's power to legislate for "whole of India" - clearly covered by Art 245(1)

Section 1(2)(b): Extraterritorial application - permitted by Art 245(2)

6.2 Entry 13, List I (Union List) - Seventh Schedule

Entry 13: "Participation in international conferences, associations and other bodies and implementing of decisions made thereat"

Argument: DPDPA implements international data protection standards (similar to GDPR, APEC Privacy Framework)

6.3 Residuary Powers (Article 248 + Entry 97, List I)

Article 248: Parliament has exclusive power to make laws on matters not in State or Concurrent Lists

Entry 97, List I: "Any other matter not enumerated in List II or List III..."

Data Protection: Not explicitly in Sta

[recovered from the vector store — section1.html p.11]

te or Concurrent Lists → Residuary power of Parliament

6.4 Right to Privacy (Article 21)

K.S. Puttaswamy v. Union of India (2017): Right to privacy is fundamental right under Article 21

DPDPA as Implementation: Parliament enacting DPDPA to PROTECT constitutional right to privacy

Quote from Puttaswamy:

"The right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution."
7. Comparative Analysis: GDPR, CCPA, Other Jurisdictions

Aspect | India (DPDPA) | EU (GDPR) | California (CCPA) | China (PIPL)
Territorial Scope | Whole of India | All 27 EU member states | California only (one state) | Whole of China
Extraterritorial Reach | Yes (1(2)(b)) | Yes (Art 3(2)) | Limited (must do business in CA) | Yes (similar to GDPR)
Trigger for Foreign Cos | Offering goods/services to Indians | Offering goods/services to EU citizens OR monitoring behaviour | Doing business in CA + meeting thresholds | Offering goods/services to Chinese
Data Localization | Not required (Section 16 allows cross-border with safeguards) | Not required (Chapter V allows transfers with safeguards) | Not required | Required for "critical information infrastructure"
Commencement | Phased (notified by Govt) | May 25, 2018 (2 years after adoption) | Jan 1, 2020 (CCPA) Jan 1, 2023 (CPRA) | Nov 1, 2021

8. Practical Implications for Organizations

8.1 Who is Covered?

 Organizations Subject to DPDPA

1. Indian Companies

ALL Indian companies processing digital personal data → Covered
2. Foreign Companies with Indian Operations

Google India, Amazon India, Microsoft India → Covered (obviously)

3. Foreign Companies Serving Indians (No Indian Entity)

Netflix (no Indian subsidiary but serves Indians) → Covered via Section 1(2)(b)

4. Indian Branches of Foreign Companies

HSBC India, Citibank India → Covered

5. Individual Professionals (if processing digital data)

Doctors with ele

[recovered from the vector store — section1.html p.12]

ctronic medical records, CAs with client data in computers, lawyers with client files digitized → Covered

6. Startups & Small Businesses

Size irrelevant - even 1-person startup processing digital personal data → Covered

7. NGOs & Non-Profits

If processing donor data, beneficiary data digitally → Covered
Government & Public Authorities

Subject to DPDPA (with some exemptions under Section 17)

8.2 Action Items Before Commencement

 Pre-Commencement Compliance Checklist

PHASE 1: Assessment (Now - 3 months before commencement)

 Conduct data inventory (what personal data do we process?)

 Map data flows (collection → storage → processing → deletion)

 Identify legal basis for processing (consent vs Section 7 grounds)

 Assess if we're Significant Data Fiduciary (Section 10 criteria)

 Review existing privacy policies

 Gap analysis: Current practices vs DPDPA requirements

PHASE 2: Technical Implementation (3 months before commencement)

 Implement consent management system

 Update notice mechanisms (Section 5 compliance)

 Enhance security measures (Section 8 compliance)

 Build data subject rights portal (access, correction, erasure - Sections 11-12)

 Implement breach detection and notification systems (Section 8(6))

 Update data retention and deletion policies

PHASE 3: Governance (2 months before commencement)

 Appoint Data Protection Officer (if SDF) (Section 10)

 Establish grievance redressal mechanism (Section 13)

 Update vendor contracts (Data Processing Agreements)

 Train employees on DPDPA obligations

 Create compliance documentation (policies, procedures, records)

PHASE 4: Legal (1 month before commencement)

 Update Terms of Service

 Update Privacy Policy (link to Section 5 notice requirements)

 Review and update all consent forms

 Establish record-keeping systems for compliance demonstration

 Prepare for potential Board inquiries/audits

PHASE 5: Post-Commencement (Ongoing)

 Monitor compliance continuously

[recovered from the vector store — section1.html p.13]

Conduct Data Protection Impact Assessments (if SDF)

 Annual Data Protection Audits (if SDF)

 Stay updated on Board guidance and rules

 Review and improve processes based on experience

Section 1 is the gateway to India's data protection regime.

"A journey of a thousand miles begins with a single step." - Lao Tzu

The DPDPA's journey begins with Section 1 - defining its name, its reach, and its timeline.

Key Takeaways:

Name Matters: "Digital Personal Data Protection Act, 2023" - every word defines scope

Pan-India Application: Covers entire territory of India (all states, UTs)

Extraterritorial Reach: Foreign companies serving Indians subject to DPDPA (game-changer)

Not Yet Fully Enforced: Awaiting commencement notification (likely phased 2025-2026)

Preparation Time: Gap between enactment and enforcement allows organizations to comply

Global Standard: DPDPA joins GDPR, CCPA, PIPL as major data protection law with global reach

Constitutional Basis: Parliament has clear power (Article 245, residuary powers)

Enforcement Challenge: Extraterritorial enforcement difficult but not impossible (blocking, cooperation)
Section 1 establishes DPDPA as a comprehensive, globally-reaching, rights-based data protection framework - the foundation upon which all subsequent sections build.

Comprehensive Legal Interpretation Complete

Section 1 DPDPA 2023 - Short Title, Extent and Commencement

 Three foundational questions answered

 Name deconstruction (Digital + Personal + Data + Protection)

 Territorial application (Section 1(2)(a))

 Extraterritorial reach (Section 1(2)(b))

 Commencement & phased implementation (Section 1(3))

 GDPR comparison (Art 3 parallel)

 Enforcement challenges & solutions

 Constitutional framework (Article 245, Entry 13, Article 248)

 Philosophical foundations (Grotius, Effects Doctrine)

 Pre-commencement compliance checklist

 Practical examples (Google, Netflix, TikTok, startups)