[recovered from the vector store — dpdpa-faq.html p.1]

Your comprehensive guide to understanding India's Digital Personal Data Protection Act 2023 and DPDP Rules 2025

 Preparing for a Data Protection Interview?

Check out our comprehensive 150+ DPDPA Interview Questions with expert model answers!

 DPDPA Basics 15
 Consent & Notice 12
 Data Principal Rights 10
 Data Fiduciary 12
 Significant Data Fiduciary 8
 Children's Data 8
 Penalties 10
 Data Breach 8
 Cross-Border Transfer 6
 Data Protection Board 8
 Exemptions 10
 Practical Scenarios 18

1
What is the Digital Personal Data Protection Act (DPDPA), 2023?
+

The Digital Personal Data Protection Act, 2023 is India's comprehensive data protection legislation that governs the processing of digital personal data. It establishes a legal framework for data collection, storage, and processing while empowering individuals with rights over their personal data.

Applies to digital personal data processed within India

Has extra-territorial application for processing related to offering goods/services to Indian individuals

Establishes the Data Protection Board of India for enforcement

Prescribes penalties up to ₹250 crore for non-compliance
 Key Date: Passed by Parliament on August 11, 2023, with Presidential assent on the same day.

2
When did the DPDP Rules 2025 come into effect?
+

The DPDP Rules 2025 were officially notified on January 3, 2025, providing detailed implementation guidelines for the DPDPA 2023.

Consent Manager registration and obligations

[recovered from the vector store — dpdpa-faq.html p.2]

3
What is "Personal Data" under DPDPA?
+

Under Section 2(t), "Personal Data" means any data about an individual who is identifiable by or in relation to such data.

Biometric data (fingerprints, facial recognition)

Financial data (bank accounts, transactions)

Online identifiers (IP address, device ID)

 Note: Unlike GDPR, DPDPA does not have a separate category for "sensitive personal data" - all personal data is treated similarly.

A Data Fiduciary (Section 2(i)) is any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data.

In simple terms: If your organization decides WHY and HOW personal data is collected and used, you are a Data Fiduciary.

 Example: An e-commerce company collecting customer data for order fulfillment is a Data Fiduciary. The cloud provider hosting that data is a Data Processor.

A Data Principal (Section 2(j)) is the individual to whom the personal data relates. Simply put: If it's YOUR data, YOU are the Data Principal.

For children (under 18): Parent/lawful guardian acts as Data Principal

For persons with disabilities with lawful guardian: The guardian acts as Data Principal
A Data Processor (Section 2(k)) is any person who processes personal data on behalf of a Data Fiduciary.

Follows instructions from Data Fiduciary

Does not determine purpose or means of processing

Has contractual liability, not direct DPDPA liability

 Examples: Cloud service providers, payroll processing companies, CRM service providers, data analytics vendors.

[recovered from the vector store — dpdpa-faq.html p.3]

cessing" of personal data mean?
+

Under Section 2(x), "Processing" means any automated operation on digital personal data, including:

Collection and recording

Organisation and structuring

Storage and adaptation

Retrieval and use

Sharing and disclosure

Restriction and erasure

⚠ Important: Even viewing personal data on a screen constitutes "processing" - the definition is extremely broad. ⚠

Consent & Notice Requirements

12 FAQs

⚠

8
What are the requirements for valid consent under DPDPA?
+

Under Section 4, valid consent must be:

Free: Given voluntarily without coercion

Specific: Related to a particular purpose

Informed: Data Principal understands what they're consenting to

Unconditional: Cannot be bundled with unrelated services

Unambiguous: Clear affirmative action required

⚠ Invalid: Pre-ticked checkboxes, buried consent in T&C, forced bundling with unrelated services.
9
What must be included in a Notice to Data Principal?
+

Under Section 6 and Rule 3, Notice must include:

Personal data being collected

Purpose of processing

How to exercise Data Principal rights

How to make complaints to Data Protection Board

Language Requirements: Must be in English AND any of the 22 Scheduled languages as chosen by Data Principal. 10
Can consent be withdrawn? How?
+

Yes! Under Section 4(6)-(7):

Data Principal may withdraw consent at any time

Withdrawal must be as easy as giving consent

Data Fiduciary must provide clear withdrawal mechanism

Upon withdrawal, processing must stop and data erased (unless legally required to retain)

 Good Practice: One-click unsubscribe, easily accessible settings, clear instructions, no penalties for withdrawal. 11
What are "Legitimate Uses" where consent is NOT required?
+

Section 5 provides Legitimate Uses without explicit consent:

Voluntary provision: Data Principal provides for specified purpose

State functions:

[recovered from the vector store — dpdpa-faq.html p.4]

Subsidies, benefits, services, certificates, licenses

Legal obligations: Compliance with judgments or laws

Medical emergencies: Threat to life/health

Employment: Recruitment, verification, performance (with safeguards)

Public interest: Mergers, acquisitions, restructuring

A Consent Manager (Section 14) is a registered entity that enables Data Principals to:

Give consent to multiple Data Fiduciaries through one platform

Manage, modify, or withdraw consent easily

Track and maintain records of all consents

Requirements (Rule 4): Must be registered with Data Protection Board, interoperable, no conflict of interest, maintain technical safeguards.

 Unique to India: Similar to Account Aggregators in financial services - no direct GDPR equivalent.

13
What rights do Data Principals have under DPDPA?
+

Right to Access: Know what data is being processed

Right to Correction: Correct inaccurate data

Right to Erasure: Request deletion of data

Right to Grievance Redressal: Complain to Data Fiduciary

Right to Nominate: Designate someone to act on their behalf (Section 12)

 Note: Unlike GDPR, DPDPA does NOT include right to data portability.
14
How long does a Data Fiduciary have to respond to a data access request?
+

Under Rule 14, Data Fiduciaries must respond within 7 days of receiving a valid request.

Categories of data shared with third parties

15
What are the duties of Data Principals?
+

Provide authentic information when exercising rights

Not impersonate another person while providing data

 Penalty: Up to ₹10,000 for false complaints or frivolous applications.

[recovered from the vector store — dpdpa-faq.html p.5]

16
What are the penalties for non-compliance under DPDPA?
+

₹250 Crore: Failure to take reasonable security safeguards leading to data breach

₹200 Crore: Failure to notify Board and Data Principal of breach

₹150 Crore: Non-compliance with children's data provisions

₹50 Crore: Other violations (per instance)

₹10,000: False complaints by Data Principals

 Key Point: These are maximum caps - actual penalty depends on nature, gravity, and circumstances of breach.

17
What factors are considered when imposing penalties?
+

18
Is there criminal liability under DPDPA?
+

No. Unlike earlier drafts (2019), DPDPA 2023 does NOT prescribe criminal penalties.

Possible blocking of services in extreme cases

 Note: This was a significant change from earlier drafts which included imprisonment provisions.

19
What is a Significant Data Fiduciary (SDF)?
+

A Significant Data Fiduciary is a Data Fiduciary notified by the Central Government based on:

Volume and sensitivity of personal data processed

Potential impact on sovereignty, public order, security

20
What additional obligations apply to SDFs?
+

Under Section 10 and Rule 13, SDFs must:
Appoint a DPO: Based in India, point of contact for Board

Appoint Independent Data Auditor: Evaluate compliance

Conduct DPIA: Before high-risk processing

Periodic Audits: Regular compliance reviews

[recovered from the vector store — dpdpa-faq.html p.6]

Publish DPO contact: Business contact information

21
What is a Data Protection Impact Assessment (DPIA)?
+

A DPIA is an assessment conducted before processing activities that may pose significant risk. It should assess:

 Tip: Document DPIAs thoroughly - they're evidence of compliance and due diligence.

Under Section 2(f), a "Child" means an individual who has not completed eighteen years of age.

 GDPR Comparison: GDPR defines child as under 16 (with flexibility down to 13). India's uniform 18-year threshold is more conservative.

23
What special protections exist for children's data?
+

Verifiable parental consent: Must obtain before processing

No behavioral monitoring: Tracking children is prohibited

No targeted advertising: Cannot target ads at children

No harmful processing: Processing likely to cause detrimental effect on child's well-being is prohibited

 Penalty: Up to ₹150 Crore for non-compliance with children's data provisions.

24
Are there exemptions for children's data processing?
+

Yes, Rule 12 provides exemptions from verifiable consent for:

25
What are the data breach notification requirements?
+

Timeline: Within 72 hours of becoming aware of breach

[recovered from the vector store — dpdpa-faq.html p.7]

26
What security safeguards are required?
+

Under Section 8(4) and Rule 6, Data Fiduciaries must implement reasonable security safeguards:

Encryption of data at rest and in transit

27
Can personal data be transferred outside India?
+

Yes, with conditions. Under Section 16 and Rule 15:

Default: Transfer permitted to all countries

Negative list: Government may notify restricted countries

Restricted countries: Transfer prohibited unless specific approval

 GDPR Comparison: DPDPA takes permissive approach with blacklist; GDPR takes restrictive approach with whitelist (adequacy decisions).

28
What is data localization under DPDPA?
+

DPDPA does NOT mandate blanket data localization. However:

Government may notify countries where transfer is restricted

Sectoral regulations (RBI, SEBI) may require localization for specific data types

Critical personal data localization may be prescribed separately

29
What is the Data Protection Board of India (DPBI)?
+

The DPBI is the regulatory body established under Section 18 to enforce DPDPA.

Digital by design - functions as "digital office"

Appeals lie to Telecom Disputes Settlement and Appellate Tribunal (TDSAT)

[recovered from the vector store — dpdpa-faq.html p.8]

31
What exemptions are available under DPDPA?
+

Under Section 17, exemptions include processing for:

National security: Sovereignty, integrity, security of India

Legal proceedings: Enforcement of legal rights/claims

Research/archiving: Statistical, research purposes (with safeguards)

Startups: Notified startups may get relaxations

32
Is personal data for personal use exempt?
+

Yes! Under Section 3, DPDPA does NOT apply to:

Personal data processed by individuals for personal or domestic purposes

Personal data made publicly available by Data Principal

 Example: Your personal phone contacts or family photos are not covered by DPDPA.

33
How should companies update their privacy policies for DPDPA?
+

Privacy policies should be updated to include:

Clear statement of data collected and purposes

Complaint mechanism to Data Protection Board

34
What records should organizations maintain for DPDPA compliance?
+

Consent records: When, how, what consent was obtained

Data inventory: What personal data is processed and why

Data Principal requests: Access, correction, erasure requests

Breach records: Incidents and response actions

Vendor contracts: Data processing agreements
Training records: Employee awareness programs

Audit reports: Internal and external compliance reviews

 Retention: SDFs must maintain records for 7 years per Rule 13.

35
How does DPDPA apply to employee data?
+

Under Section 5(b) and Rule 22, employee data processing is a Legitimate Use for:

[recovered from the vector store — dpdpa-faq.html p.9]

and onboarding

Attendance verification

Performance assessment

Salary processing

Termination procedures

HR Best Practices:

Update employment contracts with data provisions

Provide employee privacy notices

Train HR staff on data handling

Secure personnel files

Define retention periods

36
What is the relationship between DPDPA and IT Act 2000?
+

DPDPA supplements IT Act. Key interactions:

Section 43A (IT Act): Compensation provisions amended

Section 72A (IT Act): Breach of confidentiality provisions continue

IT Rules 2011 (SPDI): Effectively superseded by DPDPA

Section 69A (Blocking): Continues independently

 Key Point: Section 38 establishes DPDPA supplements and doesn't derogate from other laws unless explicitly stated.

 Want More In-Depth Content?

Explore our comprehensive resources: Certificate Course, Templates, Case Laws, and more!

Explore Course →

↑

Link copied to clipboard!