

2.Digital Personal Data Protection Rules, 2025

The Government of India Has Notified the Digital Personal Data Protection (Dpdp) Rules, 2025, Marking the Full Operationalisation of The Digital Personal Data Protection (Dpdp) Act, 2023

Key Highlights of The Dpdp Rules (2025)

Phased Implementation Approach

The Government Has Adopted An 18-Month Staggered Compliance Timeline, Enabling Organisations—Particularly Start-up's, Msmes, And Smaller Entities—To Gradually Upgrade Their Data Systems and Governance Frameworks. This Phased Rollout Prevents Compliance Shocks and Ensures Smoother Adoption of Consent Frameworks, Breach-Response Mechanisms, And Accountability Standards.

Consent Managers as Indian Entities

Consent Managers (A New Class of Intermediaries Who Help Citizens Track, Grant, Withdraw, Or Review Consent) Must Be Incorporated in India, Ensuring -

- 1.Clear Jurisdiction Under Indian Law.
- 2.Higher Accountability for User Grievance Resolution.
- 3.Greater Trust Due to Localisation of Data-Governance Intermediaries.

They Are Expected to Operate Through Standardised Apies, Similar to Account Aggregators in The Financial Sector.

Personal Data Breach Notification Protocols

Data Fiduciaries Must Promptly Inform Affected Individuals and The Dpb About -

1. Nature Of the Breach (E.G., Data Theft, Unauthorized Access).
2. Possible Consequences (Identity Theft, Financial Loss, Privacy Harms).
3. Remedial Or Mitigation Actions Taken.

This Ensures Timely User Awareness, Which Is Essential for Preventing Secondary Harms Such as Phishing or Fraud.

• Special Safeguards for Children & Persons with Disabilities

Verifiable Parental Consent Is Mandatory Before Processing Personal Data of Children (<18 Years).

Exemptions For Sectors Like Education, Healthcare, And Emergency Response Reduce Friction Where Data Processing Is Essential.

Additional Obligations Include –

1. No Behavioural Tracking of Children.
2. No Targeted Advertising to Minors.
3. Higher Standards for Accessibility for Persons with Disabilities.

Digital-First Data Protection Board (Dpb)

The Dpb Will Function as A Paperless Adjudicatory Authority With –

1. Online Submission of Complaints.
2. Digital Dashboards for Tracking Cases.
3. Virtual Hearings and Automated Scheduling.

A Dedicated Web Portal and Mobile App Will Increase Transparency and Reduce Procedural Delays.

Enhanced Transparency & Accountability

Data Fiduciaries Must Provide Clear, Prominent Contact Details of Their Grievance Redressal Officer or Data Protection Officer. Privacy Notices Must Be Simple, Multilingual, And Accessible, Ensuring Meaningful Understanding of Data Practices.

Timeline Of India's Data Protection Reforms

2011–2012 – Initial Expert Committee

The First Expert Group Studied Digital Privacy Norms and Submitted a Baseline Report.

2017–2018 – Foundation for Modern Data Protection Law

Justice Ks Puttaswamy (2017) Judgment Declared Privacy as A Fundamental Right, Creating Constitutional Necessity for A Data Protection Law. The **Justice Bn Srikrishna Committee** Drafted the First Major Privacy Framework.

2018–2021 – Evolving Drafts & Parliamentary Review

Multiple Versions of The Personal Data Protection (Pdp) Bill Were Introduced. The Joint Parliamentary Committee (Jpc) Submitted A Detailed Report in December 2021.

2022 – Withdrawal and Fresh Consultations

The Pdp Bill Was Withdrawn Due to Industry Concerns, Global Tech Implications, And Need for A Simpler, More Modern, And Agile Law.

2023 – Dpdp Act Formalised

The Digital Personal Data Protection Bill, 2023 Was Introduced, Passed by Parliament, And Enacted.

It Shifted from A Gdpr-Like Model to A Rights-Based, Consent-Centric, Flexible Governance Framework.

2025 – Draft & Final Rules

January 2025 – Draft Rules Released for Public Comments.

November 2025 – Final Dpdp Rules Notified by The Government.

Key Provisions of The Dpdp Act, 2023

Consent-Based Data Processing

Processing Requires Free, Specific, Informed, Unconditional Consent.

Notices Must Clearly Explain What Data Is Collected, why, For How Long, And Who It Will Be Shared With. **Data Minimization**

Data Fiduciaries Must Collect Only Essential Data and Avoid Excessive Profiling.

Purpose Limitation Ensures Data Is Used Strictly for The Stated Objective.

Right To Erasure

Individuals Can Request Deletion of Personal Data

1. After Withdrawal of Consent.
2. After The Purpose of Data Use Is Completed.
3. After Prolonged Inactivity.

This Strengthens User Control Over Digital Footprints.

Data Retention Limits

Companies Must Delete Data After Three Years of User Inactivity. Users Must Be Given 48-Hour Notice Before Deletion. Ensures Accountability and Prevents Indefinite Storage.

Cross-Border Data Transfer

Data Can Be Transferred to Government-Notified “Trusted” Countries. The Criteria Will Consider Reciprocity, Adequacy, And Data Security Standards.

Penalties & Enforcement

The Act Imposes Graded Financial Penalties, Up To

1. ₹250 Crore for Data Breaches.
2. High Fines for Failure to Secure Data or Notify Breaches.
3. Penalties For Violating Children’s Data Rules.

Dpb Can Order Remedial Actions, Warnings, Or Stricter Compliance Audits.

Controversies And Concerns

Government Exemptions & Surveillance Powers

The Act Grants Exemptions to Government Agencies for Reasons Of

1. National Security,
2. Public Order,
3. Public Interest,
4. Prevention/Detection of Crime.

Critics Argue This Can Lead to Broad Surveillance Powers and Weaken Individual Rights.

Impact On RTI & Transparency

Amendments To the RTI Act Restrict Access to Personal Information of Public Officials, Even When Such Information Is Crucial for Public Accountability. Civil Society Groups Warn of Reduced Transparency in Governance.

High Compliance Burden on Businesses

Companies Must Implement

1. Data Audits,
2. Grievance Redressal Systems,
3. Consent Dashboards,
4. Data Breach Response Protocols.

This Increases Operational Costs, Especially for start-up's, Ott Platforms, And Entertainment Apps.

Impact On Child-Focused Platforms

Platforms Targeting Children Must Ensure -Parental Verification, No Behavioural Profiling, Stricter Age-Gating Systems. This Raises Compliance Expenditure and Impacts Business Models Reliant on Personalized Ads.

Uncertainty On Cross-Border Data Transfer

"Trusted Country" Criteria Are Undefined, Creating Uncertainty For

1. Global Tech Firms,
2. Cloud Service Providers,
3. Multinational Corporations.

Potential Risk of Data Localization Through Ambiguity, Even If Not Explicitly Mandated.

Source - <https://Indianexpress.Com/Article/Business/Centre-Notifies-Data-Protection-Rules-Paving-Way-For-Indias-First-Privacy-Law-10365324/>