26th November 2025

Understanding Digital Personal Data Protection Rules, 2025

Background

- The Digital Personal Data Protection Rules, 2025 are issued under the DPDP Act, 2023. The Act follows the SARAL approach, means Simple, Accessible, Rational and Actionable.
- **Objectives:** Strengthen personal data governance, ensure transparency, and enforce accountability. The law rests on seven core principles which include consent and transparency, purpose limitation, data minimization, accuracy, storage limitation, security safeguards and accountability
- **Applicable to:** All Data Fiduciaries (companies collecting or processing personal data).
- **Implementation:** Staggered rollout (some rules immediate, others within 12–18 months).

Key Definitions

- Personal Data – Any data related to an individual (name, contact, financial, etc.)
- Data Principal – Individual whose personal data is being processed.
- Data Fiduciary – Company determining purpose & means of data processing.
- Data Processor – Entity processing data on behalf of a Data Fiduciary.
- Consent Manager – Registered company that manages user consents on a certified platform.
- Verifiable Consent – Traceable, authentic, specific, and informed consent.

Mandatory Notice Requirement

Each Data Fiduciary must provide a **clear, independent and simple** notice containing:

- ❑ What personal data is collected (itemized).
- ❑ Purpose of processing & services enabled.
- ❑ Website/app links for privacy rights.
- ❑ Methods to opt-out or raise concerns.

Security Obligations

Data Fiduciaries must adopt:

- ❑ Encryption, masking, tokenisation.
- ❑ Strict access controls.
- ❑ Logs & monitoring for unauthorised access.
- ❑ Backup & continuity systems.
- ❑ Contracts with Data Processors to ensure compliance.
- ❑ Mandatory retention of logs for **1 year**.

Data Breach Reporting

❑ **To Data Principal:**

- Describe breach & timeline
- Likely Consequences
- Proactive Steps to take
- Contact of responsible officer

❑ **To Data Protection Board:**

- Immediate intimation
- Full details within 72 hours
- Root cause, corrective steps, and mitigation plan

Data Retention & Erasure

- ❑ **Personal data must be erased once the purpose is fulfilled**
- ❑ For certain sectors (social media, e-commerce, gaming): mandatory erasure after **3 years** of user inactivity.
- ❑ Data & logs must be stored for **min. 1 year** even after deletion request.

Rights of Data Principals

- **Companies must enable:-**

- Right to access personal data
- Right to correction of personal information
- Right to Grievance Redressal
- Right to nominate another person
- Rights visibly listed on website/app
- Grievance response within 90 days

Children's Data Requirements

- ❑ Mandatory **parental verifiable consent**.
- ❑ Use identity proofs, tokens, or digital locker data for age verification.
- ❑ Exemptions only for healthcare, education & safety-related institutions.
- ❑ Strict ban on tracking/targeted ads for harmful content.

Grievance Redressal

- ❑ Appoint a Data Protection Officer (DPO) or responsible contact
- ❑ Provide contact details on Website/App
- ❑ Resolve complaints within 90 days; document all grievance redressed

Data Transfers & Third Parties

- ❑ If transferring data outside India, comply with government conditions and restrictions
- ❑ Ensure third parties also follow DPDP compliance

FIN VAL
RESEARCH & CONSULTANCY

Who Is Impacted & How They Can Deal With It

❑ **Financial Services**
- Implement automated consent and opt-out platforms
- Regular staff training on privacy & compliance
- Quick data breach notification systems

❑ **E – Commerce & Retail**
- Update privacy notices, simplify data request portals

❑ **Tech / IT Services**
- Adopt robust cyber-security frameworks
- Regular audits of international data transfers

❑ **Healthcare**
- Encrypt health records, restrict access
- Separate data processing for minors

Who Is Impacted & How They Can Deal With It

❑ **Educational Institutes**

- Create simple, clear consent forms for students (with parental/guardian approval for minors).
- Restrict data access—only authorized staff should handle private information.
- Use secure, encrypted systems for student records and personal files.
- Train teachers/administration regularly on data privacy and DPDP compliance.
- Enable easy ways for students and parents to update, access, or request deletion of their data.

Who Is Impacted & How They Can Deal With It

❑ **Large Corporate (Significant Data Fiduciaries)**

- Set up advanced security protocols: strong encryption, access controls, monitoring.
- Implement comprehensive consent management systems - track, update, and withdraw consents easily.
- Prepare a speedy breach-response plan with clear notification processes.
- Ensure partners/vendors meet high data protection standards, especially for international data transfers.
- Provide regular staff training—make privacy culture part of business.

About US

Founded in 2011, we are a boutique consulting firm focused on providing world class financial consulting, valuations and corporate finance services.
Managed and advised by Registered Valuers with more than 70 years of cumulative experience and more than 200 valuation assignments.

Investment Banking Solutions

- Preparing IMs and Financial model
- Financial Due diligence
- M&A Transaction and Deal structuring
- End to end solutions for fund raising
- Stressed Asset Consulting

Valuation Service

- Valuation of Startups
- Valuation of Intangible Assets, ESOPS.
- Valuation of Purchase Price Allocation
- Fair value valuations as per IND AS Companies Act
- Valuations for regulatory requirements for SEBI, RBI, Income Tax
- Valuation of Securities for M&A and Fund raising

Virtual CFO Solutions / Management Consulting

- Project Finance Consulting
- Financial Planning & Analysis
- Budgeting & Variance Analysis
- Business restructuring
- Strategy Consulting
- FEMA/RBI Compliance & Advisory

THANK YOU

VALUATION@FINVALRESEARCH.IN
+91 98 112 13275
WWW.FINVALRESEARCH.IN