Legal & Professional Services

DPDPA 2023 Implementation Handbook

Digital Personal Data Protection Act, 2023 • India

For law firms, accounting firms, audit companies, management consultants, and cybersecurity professionals.

1. Overview & Applicability

Legal and professional service firms are custodians of some of the most confidential personal and organisational data — client legal strategies, financial records, tax filings, and sensitive business information. Under DPDPA, lawyers, accountants, and consultants are Data Fiduciaries when they collect and process personal data of their clients and counterparties. Attorney-client privilege and professional confidentiality obligations coexist with, and in some respects overlap with, DPDPA duties.

2. Key Definitions Under DPDPA

These definitions govern how the Act applies to your sector:

Client Data	Identity documents, financial statements, legal case details, tax records, business plans — personal and confidential data.
Professional Privilege	Attorney-client privilege and professional confidentiality protect certain communications — coexists with DPDPA.
Counterparty Data	Personal data of opposing parties, witnesses, and third parties in legal or advisory matters.
Data Processor	E-discovery platforms, document management systems, cloud storage providers — require DPAs.
Purpose Limitation	Client data collected for one matter cannot be used for business development, seminars, or marketing without consent.
Retention	Legal and audit files must be retained per professional standards — but DPDPA requires deletion of surplus personal data after the matter concludes.

3. Core Compliance Obligations

Every entity in this sector that processes personal data must comply with the following obligations:

1. **Client Engagement Consent**
   Include DPDPA-compliant data processing disclosure in client engagement letters. Clearly state what data is collected, for what purpose, and who it may be shared with (courts, regulators, co-counsel).
2. **Document Security**
   Encrypt all client documents stored digitally. Implement access controls — only matter team members access client files. Audit logs for document access.
3. **Third-Party Platform Governance**
   E-discovery tools, document review platforms, and virtual data rooms must comply with DPDPA. Execute DPAs with all technology providers.
4. **Employee Background Checks**
   Conducting background checks on new hires requires candidate consent. Use only DPDPA-compliant verification agencies.
5. **Client Data at Matter Conclusion**
   Define a clear data return and destruction policy. Return original documents to clients. Securely destroy copies after the statutory retention period.
6. **Counterparty Data Handling**

	Personal data of opposing parties obtained during litigation must be used only for the legal matter and not retained beyond necessity.
7	**Data Breach** A breach of client data must be reported to DPBI. Also review professional indemnity insurance implications.

4. Implementation Checklist

Use this checklist to track your DPDPA compliance readiness:

- ☐ Update client engagement letters to include DPDPA-compliant data processing disclosures.
- ☐ Implement encrypted document management systems with role-based access for client files.
- ☐ Execute DPAs with all technology providers — e-discovery, DMS, cloud storage, virtual data rooms.
- ☐ Define client data retention and destruction schedules — aligned with professional standards and DPDPA.
- ☐ Build a client rights process — allow clients to access, correct, and request deletion of their data.
- ☐ Appoint a Grievance Officer (may be a senior partner) and communicate to clients.
- ☐ Train all lawyers, accountants, and associates on DPDPA obligations and client data handling.
- ☐ Review cross-border client data sharing — multinational matters may involve international transfers.
- ☐ Implement clean desk and clear screen policies for client documents.
- ☐ Conduct an annual audit of all data processors (technology vendors) used in client work.

5. Applicable Penalties

The Data Protection Board of India (DPBI) may impose the following penalties for non-compliance:

Rs. 250 Crore	Failure to implement reasonable security safeguards resulting in a personal data breach
Rs. 200 Crore	Breach of obligations related to processing children's personal data
Rs. 150 Crore	Failure to fulfill obligations as a Significant Data Fiduciary (SDF)
Rs. 50 Crore	Failure to comply with Data Principal rights or other provisions of the Act

6. Implementation Roadmap

Follow this phased approach to achieve full DPDPA compliance:

1	**Month 1: Data & Matter Audit** Inventory all client data stores — physical files, digital documents, email archives.
2	**Month 2: Engagement Letter Update** Revise all client engagement templates to include DPDPA disclosures.
3	**Month 3: Technology DPAs** Execute DPAs with DMS, e-discovery, cloud, and collaboration tool providers.
4	**Month 4: Retention Policy** Implement matter data retention and destruction schedules.
5	**Month 5: Training** Train all fee-earners and staff on client data handling obligations.
6	**Month 6+: Ongoing** Annual client data audit and technology vendor review.

⚖️ Professional confidentiality is not a substitute for DPDPA compliance. Both obligations run in parallel. DPDPA adds a layer of individual rights (access, correction, erasure) to client data that professional privilege does not address.