Government & Public Sector

DPDPA 2023 Implementation Handbook

Digital Personal Data Protection Act, 2023 • India

For central and state government departments, PSUs, regulatory bodies, and public authorities.

1. Overview & Applicability

Government bodies and public sector entities are subject to the DPDPA when processing citizens' personal data. However, the Act provides targeted exemptions for state instrumentalities in the interest of national security, public order, and sovereignty — subject to procedural safeguards. Despite exemptions, the spirit of the Act requires government departments to process citizen data fairly, transparently, and with appropriate security. Citizens' rights to access and correct data held by government agencies must be honoured.

2. Key Definitions Under DPDPA

These definitions govern how the Act applies to your sector:

State	Includes the Central Government, state governments, Parliament, legislatures, and authorities exercising government functions.
Citizen Data	Aadhaar, PAN, ration card, driving licence, tax records, social welfare beneficiary data — all personal data.
Exemptions	National security, sovereignty, public order, and prevention of cognisable offences — data processing for these purposes is exempt from certain provisions.
Instrumentality of State	PSUs, public universities, government hospitals — subject to DPDPA unless specifically exempted.
Purpose Limitation	Data collected for one welfare scheme (e.g., MGNREGA) cannot be used for another (e.g., Ayushman Bharat) without a lawful basis.
Legitimate Use	Government may process data for several prescribed purposes without consent — but must still issue a notice.

3. Core Compliance Obligations

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

1	**Data Inventory & Classification** Maintain a comprehensive inventory of all citizen data held. Classify by sensitivity — Aadhaar, health, financial, social welfare.
2	**Privacy Notice to Citizens** Even where consent is not required, issue a notice to citizens explaining what data is collected, for what purpose, and how to exercise rights.
3	**Access & Correction Rights** Citizens have the right to access their data held by government departments and to request correction of errors. Implement a mechanism for this — RTI portals can be a starting point.
4	**Security of Citizen Data** Implement encryption, access controls, and audit trails for all citizen data systems. Government databases are high-value targets for cyberattacks.
5	**Data Sharing Between Ministries** Sharing citizen data across ministries requires a lawful basis. Document each inter-ministry data flow and its legal authority.
6	**PSU Obligations**

	Government-owned companies operating commercially (banks, oil companies, airlines) have full DPDPA obligations with limited exemptions.
7	**Exemptions Documentation** When invoking security/sovereignty exemptions, document the necessity, proportionality, and procedural compliance for each instance.

4. Implementation Checklist

Use this checklist to track your DPDPA compliance readiness:

- ☐ Conduct a citizen data inventory across all departments — identify what data is held, where, and for how long.
- ☐ Publish simplified privacy notices on government portals, Jan Seva Kendras, and scheme enrollment forms.
- ☐ Implement a citizen data rights mechanism — access and correction requests through DigiLocker or dedicated portals.
- ☐ Encrypt all citizen databases — Aadhaar, PAN, health, and welfare data must be protected at rest and in transit.
- ☐ Implement access controls and audit logs for all government data systems..
- ☐ Review inter-ministry data sharing arrangements — document the legal basis for each.
- ☐ Appoint a Grievance Officer or designate an existing officer as the data rights contact.
- ☐ Audit all outsourced government IT systems — third-party vendors handling citizen data require DPAs.
- ☐ Train IAS/IPS officers and departmental IT staff on DPDPA obligations.
- ☐ Review exemption reliance — document when and why security/sovereignty exemptions are invoked.

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 1–2: Data Mapping** Inventory all citizen data systems across the ministry/department.
2	**Month 3: Legal Review** Map DPDPA obligations against existing government data laws and identify applicable exemptions.
3	**Month 4: Notice Design** Design citizen-friendly privacy notices for all government portals and scheme forms.
4	**Month 5: Rights Mechanism** Build or adapt existing portals (DigiLocker, UMANG) to support citizen data access and correction requests.
5	**Month 6: Security Uplift** Conduct a security audit of all citizen data systems and implement recommended controls.
6	**Month 6+: Training** Train all departmental staff involved in citizen data processing.

🏛 Government exemptions under DPDPA are subject to procedural conditions. They are not a blanket waiver of all privacy obligations. Citizens still have rights that must be respected.