Real Estate & Housing

DPDPA 2023 Implementation Handbook

Digital Personal Data Protection Act, 2023 • India

For developers, property portals, housing finance companies, co-working spaces, and property management firms.

1. Overview & Applicability

Real estate businesses collect extensive personal data — KYC documents, income proofs, bank statements, property documents, and family details — during the sales, registration, and loan process. Property portals hold profiles of millions of buyers and sellers. Co-working spaces collect access data and billing information. Housing finance companies process credit and financial data. DPDPA requires all these entities to implement proper consent, limit data sharing with brokers, and protect documents shared during transactions.

2. Key Definitions Under DPDPA

These definitions govern how the Act applies to your sector:

KYC Documents	Aadhaar, PAN, passport, driving licence — submitted during property purchase or loan application.
Financial Data	Bank statements, salary slips, IT returns, CIBIL scores — submitted for home loan eligibility.
Property Documents	Sale deed, encumbrance certificate, title documents — personal and legal data.
Third-Party Broker	Property agents, channel partners who receive buyer/seller data for facilitating transactions — require DPAs.
Purpose Limitation	Data collected for property purchase cannot be used for marketing future projects without consent.
Access Log Data	Entry/exit logs from apartment complexes, co-working spaces — personal data when linked to individuals.

3. Core Compliance Obligations

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

1. **Buyer/Seller Consent**
   Obtain explicit consent before collecting KYC documents, financial statements, and property details. Clearly state the purpose — property purchase, loan processing — and do not use data for marketing without separate consent.
2. **Broker Data Sharing**
   Property data shared with channel partners and brokers must be governed by a DPA. Brokers cannot retain buyer data beyond the transaction. Implement data sharing protocols.
3. **Property Portal Governance**
   Portals must obtain consent before displaying user profiles to agents. Allow buyers and sellers to download, correct, and delete their listings and profiles.
4. **Home Loan Data**
   Income and credit data collected for loan eligibility must not be shared with insurers, marketing teams, or third parties without consent.
5. **Access Control Systems**
   Biometric or RFID access logs in apartments or co-working spaces constitute personal data. Obtain resident/member consent and limit retention.

6	**Construction Site Workers** If you collect biometric data of construction workers, obtain consent and provide alternative attendance methods.
7	**RERA Compliance Alignment** Ensure DPDPA obligations are aligned with RERA buyer data protection requirements.

4. Implementation Checklist

Use this checklist to track your DPDPA compliance readiness:

- ☐ Audit all buyer/seller data collected during inquiry, site visits, booking, and registration stages.
- ☐ Implement consent forms at each data collection touchpoint — inquiry form, site visit registration, booking agreement.
- ☐ Execute DPAs with all brokers, channel partners, legal firms, and financial partners receiving buyer data.
- ☐ Build a buyer rights portal on your website — access, correction, and data deletion for registered users.
- ☐ Publish a privacy notice on your website and include data processing information in sale agreements.
- ☐ Restrict access to KYC documents and financial statements — only authorised sales and legal staff.
- ☐ Implement a data retention and destruction schedule for transaction documents — align with RERA timelines.
- ☐ Review access control systems in your properties — obtain resident consent for biometric/RFID logging.
- ☐ Train sales teams and relationship managers on data handling and consent obligations.
- ☐ Appoint a Grievance Officer and publish contact details on your website and in your offices.

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: Transaction Data Map** Map all personal data collected across the property sales lifecycle — inquiry to registration.
2	**Month 2: Consent Design** Design consent collection points at inquiry, booking, and registration stages.
3	**Month 3: Broker & Vendor DPAs** Execute DPAs with all brokers, lawyers, banks, and property portal partners.
4	**Month 4: Digital Rights** Build buyer portal for data access and correction; appoint Grievance Officer.
5	**Month 5: Security & Training** Implement document security protocols; train sales and legal teams.
6	**Month 6+: Review** Annual audit of broker data handling and retention compliance.

🤝 Brokers and channel partners are your data processors. They receive buyer information on your behalf. You remain responsible for how they handle that data — DPAs and clear data handling instructions are mandatory.