Resident Welfare Associations & Housing Society Ecosystem

DPDPA 2023 Implementation Handbook

Digital Personal Data Protection Act, 2023 • India

For RWAs, apartment management committees, society management apps, visitor management systems, security agencies, facility management firms, and property portals like NoBroker acting as society management platforms.

1. Overview & Applicability

Resident Welfare Associations (RWAs) and Apartment Owners' Associations (AOAs) collect significant personal data of residents — identity documents, vehicle details, family composition, employee/domestic staff details, visitor logs, and payment records. With the rise of society management platforms (MyGate, NoBroker for Housing, ApnaComplex, ADDA), this data is now digitised and shared with third-party apps, security agencies, facility management firms, and payment gateways. The DPDPA applies to all these entities — the RWA as a Data Fiduciary and third-party apps and vendors as Data Processors.

2. Key Definitions Under DPDPA

These definitions govern how the Act applies to your sector:

Resident Data	Name, flat number, ownership/tenancy status, Aadhaar/PAN (for KYC), vehicle registration, phone, email — personal data of every resident.
Domestic Worker Data	Name, Aadhaar, photo, address, and biometric scan of maids, cooks, drivers — personal data requiring resident and worker consent.
Visitor Log Data	Name, phone, vehicle number, photo, purpose of visit, time of entry/exit — personal data collected at the gate.
Society Management App	Platforms like MyGate, NoBroker Housing, ApnaComplex, ADDA — Data Processors acting on behalf of the RWA.
CCTV / Surveillance Data	Video footage from common area cameras — personal data of residents and visitors captured continuously.
Payment Data	Maintenance fees, parking charges, sinking fund — collected digitally via UPI, payment gateways.
Security Agency	Third-party security guards managing entry/exit and collecting visitor and resident data — Data Processors.
Facility Management Firm	Housekeeping, plumbing, elevator companies — receive resident contact data for service scheduling.
Third-Party Vendor / NoBroker	Platforms that manage listings, rentals, maintenance requests, and visitor management — Data Processors with significant data access.

3. Core Compliance Obligations

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

1 Resident Onboarding Consent

At the time of a resident moving in, the RWA must obtain written/digital consent covering: purpose of data collection, who the data will be shared with (security agency, society app, facility firm), retention period, and resident rights. Do not simply collect documents without disclosing use.

2 Domestic Worker & Domestic Help Data

Collecting Aadhaar, photo, and biometric of domestic workers (maids, cooks, drivers) requires the worker's own consent — not

	just the employing resident's permission. Provide a simple consent form in local language. Biometric enrolment requires explicit opt-in.
3	**Visitor Management System** The visitor management system (physical register or app like MyGate) collects personal data of every visitor. Display a prominent notice at the main gate: what data is collected, why, how long it is retained. Do not share visitor data with third parties.
4	**CCTV & Surveillance** Prominently display CCTV notices at all camera locations. Restrict access to footage to security personnel and the Management Committee only. Implement a retention limit — typically 30–60 days. Residents and visitors cannot be tracked beyond the premises.
5	**Society Management App DPA** Execute a formal Data Processing Agreement with your society management platform (MyGate, ApnaComplex, ADDA, NoBroker for Housing). The DPA must specify: data categories processed, purpose, sub-processor restrictions, security standards, and deletion on termination of the contract.
6	**Payment Gateway & Maintenance Fee** Digital maintenance payment data (amount, account details, UPI ID) is financial personal data. Execute a DPA with your payment gateway. Do not store raw payment credentials in the society app or RWA systems.
7	**Security Agency Data Governance** Security agencies at your gate collect and process resident and visitor data. Execute a DPA with the agency. They must collect only the minimum data required, not retain it beyond the shift/day, and not share it with their parent company for any other purpose.
8	**Facility Management Vendors** Plumbers, electricians, housekeeping firms receive residents' flat number and phone number for service scheduling. This data must be used only for the specific service call and deleted thereafter. Execute DPAs.
9	**NoBroker & Property Listing Portals** When RWA partners with NoBroker or similar platforms for rental listings, move-in verification, or visitor management, the platform receives extensive resident data. A robust DPA is mandatory. Residents must be informed that their data is shared with the platform.
10	**Resident Rights** Every resident has the right to: access their personal data held by the RWA, correct errors, request deletion of data of former residents, and raise grievances. Implement a simple process — a written request to the Management Committee or the designated Grievance Officer.

4. Implementation Checklist

Use this checklist to track your DPDPA compliance readiness:

- ☐ Obtain written resident onboarding consent — covering all data uses, processors, and retention periods.
- ☐ Display a DPDPA-compliant notice at the main gate: data collected from visitors and purpose.
- ☐ Display CCTV notices at ALL camera locations — mention retention period and access restriction.
- ☐ Execute a Data Processing Agreement with your society management app (MyGate, ApnaComplex, ADDA, NoBroker, etc.).
- ☐ Execute a DPA with your security agency — specify data minimisation and no third-party sharing.
- ☐ Execute DPAs with payment gateways and maintenance collection apps.
- ☐ Obtain domestic worker's own consent for Aadhaar/biometric collection — use local-language consent forms.
- ☐ Implement CCTV footage retention limit — maximum 30–60 days, then delete automatically.
- ☐ Build a resident data rights mechanism — written request to Management Committee; respond within 30 days.
- ☐ Appoint a Grievance Officer from the Management Committee — display name and contact on society notice board.
- ☐ Publish a society privacy policy on the society app and notice board — plain language, regional language if needed.
- ☐ Train security guards on data minimisation — collect only name, phone, purpose, and vehicle number for visitors.
- ☐ Review NoBroker / property portal partnership — ensure residents are informed and a DPA is in place.
- ☐ Implement access controls on the society management app — not all committee members need access to all data.
- ☐ Conduct an annual review of all third-party vendors accessing resident data.

Rs. 250 Crore	Data breach due to inadequate security (e.g., society app hacked, CCTV footage leaked)
Rs. 200 Crore	Breach involving children's data (e.g., school bus tracking, children's activity logs)
Rs. 50 Crore	Denial of resident rights, failure to appoint Grievance Officer, or non-compliance with notice obligations

6. Implementation Roadmap

Follow this phased approach to achieve full DPDPA compliance:

1	**Week 1–2: Data Audit** List all personal data held by the RWA — resident files, visitor logs, domestic worker records, CCTV footage, payment records.
2	**Week 3–4: Notices & Consent** Design gate notice, CCTV notice, and resident onboarding consent form. Translate into local languages.
3	**Month 2: Vendor DPAs** Contact society management app, security agency, payment gateway, and facility vendors — execute DPAs.
4	**Month 2–3: Domestic Worker Consent** Roll out local-language consent forms for all domestic workers registered with the society.
5	**Month 3: Resident Rights** Establish a simple written process for residents to exercise data rights. Designate and communicate the Grievance Officer.
6	**Month 3+: Ongoing** Quarterly Management Committee review of data practices. Annual vendor DPA renewal. Monthly CCTV deletion check.

🏘️ The RWA collects data of residents, domestic workers, AND visitors — three distinct categories of Data Principals, each requiring separate notice and consent. Do not treat them as a single category.

Special Focus: NoBroker, MyGate & Society Management Platforms

Society management platforms like NoBroker for Housing, MyGate, ApnaComplex, and ADDA act as Data Processors on behalf of the RWA. However, these platforms also have their own business interests — they may use aggregated resident and visitor data for their own analytics, marketing, or service development. As an RWA, you must:

- Read the platform's privacy policy carefully — understand what data they collect, use, and share.
- Negotiate a DPA that explicitly prohibits the platform from using resident data for their own commercial purposes.
- Ensure the platform deletes all resident data if you switch providers or terminate the contract.
- Inform residents that a third-party platform processes their data — include this in your onboarding consent form.
- Verify the platform's security certifications — ISO 27001 or equivalent. Request their breach notification policy.
- Ensure residents can exercise their data rights directly with you — not just through the platform.

📋 NoBroker's rental listing service and society management service are different products. If your RWA uses NoBroker for society management, a separate DPA specific to that service is required — not just acceptance of NoBroker's general terms of service.

Disclaimer: *This handbook is for awareness and informational purposes only. It does not constitute legal advice. Please consult a qualified data protection lawyer for specific compliance guidance. | DPDPA 2023 · India*