

CCTV Under the DPDPA 2023: A Complete Compliance Guide

How India's Digital Personal Data Protection Act Regulates Every Camera You Operate

India has over 15 million CCTV cameras deployed across homes, offices, malls, hospitals, banks, and public spaces. Until recently, their operation was largely unregulated. The Digital Personal Data Protection Act 2023 (DPDPA) changed that. Every camera that can identify a person is now a compliance obligation - with penalties of up to ₹250 crore for violations.

Home CCTV

Household exemption under Section 3(c)(i), its limits, and what makes it legally defensible.

Business CCTV

Lawful basis under Section 7(a), signage requirements, and when consent is mandatory.

Employee Monitoring

Section 7(i) framework - what is permitted, what is prohibited, and proportionality requirements.

FRT, Retention & GDPR

Facial recognition obligations, dual-track retention model, and DPDPA vs. GDPR comparison.

This deck is a legal analysis of the DPDPA 2023 and its Rules as applicable to CCTV deployments in India. It does not constitute legal advice.

Prepared by: Shubhank Suman, Privacy, AI & IP Counsel

Foundational Definitions: What the DPDPA Means for CCTV

Before examining specific scenarios, three foundational concepts determine whether and how the DPDPA applies to any CCTV system. If all three are satisfied, the Act applies in full - and the entity operating the cameras bears primary legal responsibility.

01

What Is 'Personal Data'? - Section 2(t)

The DPDPA defines personal data as any data about an identifiable individual. CCTV footage that captures faces, gait, vehicle registration plates, or movement patterns is personal data. If your camera can identify a person - directly or indirectly - the Act applies. This is not limited to high-resolution cameras. Even low-resolution footage that, combined with other data, can identify an individual falls within the definition.

02

What Is 'Processing'? - Section 2(x)

Processing is defined broadly to include every operation performed on personal data: recording, storing, retrieving, using, sharing, transmitting, aligning, combining, restricting, erasing, or destroying. There is no stage of a CCTV system's operation that falls outside this definition. The moment a camera records footage, processing has begun. The moment footage is deleted, processing ends. Every step in between is regulated.

03

Who Is the 'Data Fiduciary'? - Section 2(i)

A Data Fiduciary is any person who, alone or jointly with others, determines the purpose and means of processing personal data. If your organisation decides where cameras are placed, how long footage is retained, who can access it, and for what purpose - you are the Data Fiduciary. This is the entity that bears primary legal and financial responsibility under the DPDPA, including liability for penalties of up to ₹250 crore.

- ❏ The DPDPA applies to digital personal data processed within India, and to processing outside India if it involves offering goods or services to individuals in India. There is no minimum threshold - even a single camera in a small shop triggers the Act if it records identifiable individuals.

Home CCTV: The Household Exemption and Its Limits

Section 3(c)(i) of the DPDPA exempts personal data processed for a "personal or domestic purpose." Many assume home CCTV is automatically outside privacy law. That assumption is legally incorrect. The household exemption is narrow, conditional, and easily lost. It applies only when surveillance stays strictly inward-looking, proportionate, and confined to the resident's private sphere.

The Lawful Basis Question

Domestic CCTV is exempt under Section 3(c)(i), so a private household does not ordinarily need a separate lawful basis - provided the system stays personal and inward-facing. The exemption ends the moment a camera captures third-party data: neighbours, visitors beyond the household, or public areas. At that point, the processing is no longer covered by the household carve-out, and a lawful basis under Section 4 or Section 7 would be required.

Data Minimisation - Section 6(3)

Even within the household exemption, Section 6 requires collecting only what is necessary for the stated purpose of home security. This means: avoid extra camera angles that capture beyond the private space; disable audio recording (which captures private conversations and is disproportionate to security needs); and avoid blanket 24x7 recording of spaces that do not require continuous monitoring. Motion-triggered recording is the defensible default.

The Purpose Test

The exemption survives only if the purpose remains genuinely personal and domestic. If footage is shared with third parties, monetised, or accessed by outsiders beyond household security needs, the purpose changes - and the exemption is lost, even if the camera is physically located at home. The same applies if footage is repurposed for any commercial or non-domestic use.

Judicial Guidance: How Courts Have Applied the Exemption

Agnes Michale v. Cheranelloor Grama Panchayath (Kerala HC, 2023)

A home security camera captured a neighbour's property. The Court held that continuous monitoring beyond one's own premises violates the right to privacy. The domestic exemption cannot shield intrusive surveillance that extends beyond the resident's private sphere. The judgment establishes that camera angle and field of view are legally material - not just the location of the camera.

Shuvendra Mullick v. Indranil Mullick (Calcutta HC + Supreme Court, 2025)

Cameras installed in shared residential hallways without the consent of affected occupants were ordered removed. The Supreme Court's affirmation makes clear that recording shared residential space - even within a residential building - requires the clear consent of all affected occupants. The domestic exemption does not extend to common areas, regardless of the camera owner's residential status.

The practical rule: home CCTV remains within the household exemption only if it is strictly inward-looking, captures no third-party data, is used solely for personal security, and is not shared or repurposed. Any deviation from these conditions brings the system within the DPDPA's full regulatory scope.

Home CCTV: Compliance in Practice

Before installing or continuing to operate CCTV at home, residents must examine not only whether the purpose is domestic, but also whether the system adheres to purpose limitation and data minimisation under Section 6(3). The following table sets out the compliance requirements across five key dimensions.

Compliance Aspect	What the Law Requires	Allowed ✓	Not Allowed X
Camera Type (Audio vs. Video)	Collect only what is strictly necessary for home security. Audio recording is disproportionate to intrusion detection and captures private conversations.	Video-only motion-triggered camera at the front door or entrance.	Recording visitors' or neighbours' conversations; cameras with always-on microphones.
Camera Angle & Direction	Cameras must face inward and capture only the resident's exclusive private space. Wide-angle and pan/tilt features increase third-party capture risk.	A camera facing the flat entrance or inside the living room.	A camera pointed at a neighbour's door, shared corridor, or public street.
Coverage Area (Private vs. Shared Spaces)	The household exemption applies only where others' privacy is not affected. Shared spaces are not part of the resident's private sphere.	Inside the living room, private driveway, or exclusive garden.	Shared hallways, staircases, lifts, parking areas, or society roads.
Privacy Masking	Where outside areas are unavoidably visible, device-level masking must permanently block those areas during recording - not as a post-processing step.	A neighbour's door or window permanently blacked out at the device level before recording begins.	Leaving masking to manual review after footage is recorded; relying on software blur applied retrospectively.
Recording Mode	Motion-based recording avoids excessive data collection and is the defensible default under data minimisation principles.	Motion-triggered recording that activates only when someone enters the private monitored area.	Continuous 24×7 recording of empty corridors, public paths, or spaces that do not require constant monitoring.
Footage Sharing & Access	Footage must remain within the household for domestic security purposes. Sharing with third parties changes the purpose and loses the exemption.	Sharing with police in response to a specific incident or legal requirement.	Sharing with neighbours, posting on social media, or providing access to third-party apps without legal basis.
Retention Period	Footage must be deleted once the security purpose is no longer served. There is no fixed period, but prolonged retention without purpose is indefensible.	Automatic deletion after 15-30 days for routine footage with no incident.	Indefinite retention of all footage "just in case"; no deletion policy in place.

☐ If your home CCTV system fails any of the above tests, the household exemption may not apply. You may be processing personal data of third parties without a lawful basis - which constitutes a violation of the DPDPA, regardless of the domestic setting.

Business CCTV: Lawful Basis and Compliance Requirements

The household exemption does not apply to CCTV in corporate offices, commercial establishments, retail stores, hospitals, banks, hotels, warehouses, or apartment common areas. In these contexts, CCTV footage is regulated digital personal data processing, and the entity controlling its use is the Data Fiduciary under the DPDPA. Businesses need a valid lawful basis - and the choice of that basis determines the entire compliance architecture.

The Consent Challenge - Section 5

Section 5 requires consent to be free, specific, informed, unconditional, and unambiguous. In a store, lobby, corridor, branch, or entrance, obtaining that standard of consent from every visitor, customer, patient attendant, contractor, or delivery person is operationally unrealistic. CCTV is often used precisely because access is open and movement is constant. Section 7(a) addresses this challenge - but only within defined limits.

The Practical Legal Basis - Section 7(a)

Commercial CCTV typically relies on Section 7(a), which allows processing where the Data Principal has voluntarily provided personal data for a specified purpose and has not indicated non-consent. In practice, this voluntary provision is established when a person receives clear prior notice and still chooses to enter the monitored premises. This is not vague implied consent. It works only if the notice is genuine, prominent, and specific enough to inform the person before entry. Signage must appear at every entry point before the monitored area begins.

What Compliant Signage Must State

For Section 7(a) to function as a lawful basis, signage must do real legal work. It must state: that CCTV is in operation on the premises. The notice must be specific, legible, and positioned before the monitored area begins.

Deployment Type	Applicable Lawful Basis	Key Compliance Requirement
Retail store / mall	Section 7(a) - notice + voluntary entry	Prominent signage at all entry points before monitored area; purpose-specific notice
Corporate office (visitors)	Section 7(a) - notice + voluntary entry	Signage at reception and all entry points; visitor register noting CCTV notice
Hospital / clinic	Section 7(a) - notice + voluntary entry	Signage at entrance; avoid cameras in clinical consultation areas
Bank / financial institution	Section 7(a) - notice + voluntary entry	Signage at entrance; cameras in cash areas; no cameras in private consultation booths
Hotel / hospitality	Section 7(a) - notice + voluntary entry	Signage at entrance and lobby; no cameras in rooms, bathrooms, or changing areas
Apartment common areas	Section 7(a) or consent of residents	Resident association resolution; notice to all residents; no cameras in private areas
Facial recognition at entry	Explicit consent - Section 5	Written, purpose-specific consent before biometric processing; Section 7(a) is insufficient

FRT & Advanced Analytics: When Section 7(a) Is Not Enough

Facial Recognition Technology (FRT) and AI-based surveillance go beyond ordinary security CCTV. They process biometric and behavioural data - making the Data Fiduciary's obligations significantly heavier. Section 7(a) (notice + voluntary entry) is not a valid lawful basis for FRT or AI analytics. Explicit, purpose-specific consent under Section 5 is required before deployment.

Why FRT Is Categorically Different

FRT processes biometric data - unique physical identifiers that cannot be changed if compromised. Unlike ordinary CCTV footage that captures presence and movement, FRT identifies, tracks, and profiles individuals by matching their facial geometry against a database. This is categorically more intrusive than recording. The general surveillance framework does not cover it. Illustration: A mall deploys FRT at its entrance. Every shopper's face is scanned and matched against a database - not just recorded - to analyse shopping behaviour and flag known individuals. This is biometric processing, not security surveillance.

Why Section 7(a) Fails for FRT

Section 7(a) works where a person voluntarily enters a notified space. But FRT operates silently - the individual may not know they are being identified, not merely recorded. Notice alone cannot substitute for consent when the processing involves biometric identification, profiling, or behavioural inference. Illustration: A hotel puts up a sign saying "Premises under CCTV surveillance." A guest walks in. Section 7(a) is satisfied for the video recording. But if the hotel's cameras are also running FRT to flag blacklisted guests, the guest never consented to biometric identification - the sign does not cover it. The processing is unlawful.

What the Data Fiduciary Must Do

Before deploying FRT or AI analytics, the Data Fiduciary must: (1) obtain free, specific, informed, and unambiguous consent under Section 5 - a privacy notice or signage is insufficient; (2) specify the exact purpose of biometric processing (e.g., access control, not general surveillance); (3) document the necessity and proportionality of FRT over less intrusive alternatives; (4) implement a mechanism for individuals to withdraw consent; and (5) ensure biometric data is not retained beyond the specific purpose for which consent was given.

Use Case	Lawful Basis Required	Why Section 7(a) Is Insufficient
FRT for visitor identification	Explicit consent - Section 5	Visitors have not consented to biometric identification; entry-based notice does not cover biometric matching
AI-based crowd behaviour analysis	Explicit consent - Section 5	Behavioural profiling goes beyond security; individuals cannot anticipate this use from a CCTV notice
Customer footfall analytics (non-identifying)	Section 7(a) may suffice if truly anonymised	If footage is anonymised before analysis and no individual can be identified, the DPDPA may not apply - but anonymisation must be genuine and irreversible
Emotion recognition / sentiment analysis	Explicit consent - Section 5	Processes sensitive inferences about mental state; no legitimate basis without specific, informed consent
Licence plate recognition (LPR)	Section 7(a) with specific notice	LPR identifies vehicles linked to individuals; notice must specifically mention LPR, not just "CCTV"

Employee Monitoring Through CCTV: Section 7(i) Framework

When CCTV is used to monitor employees, the compliance framework is different from public-facing surveillance. The DPDPA provides a narrow lawful basis under Section 7(i), allowing processing without direct consent where necessary to safeguard the employer from loss, liability, or specified threats. This is not a general licence for workplace surveillance. It must stay tied to legitimate employment objectives and satisfy purpose limitation and proportionality. For each camera, the employer must show a specific, identifiable risk - not just convenience or custom. The burden of justification lies with the employer.

Aspect	What the Law Allows	What the Law Prohibits
Underlying Purpose	CCTV may protect the employer from loss, liability, or security threats under Section 7(i).	CCTV cannot be used to monitor behaviour, productivity, or discipline employees.
Permissible Locations	Server rooms, data centres, cash handling areas, vaults, warehouses, entry/exit gates, and high-security restricted access zones.	Employee desks and workstations, restrooms, changing rooms, prayer rooms, and break rooms.
Use of Footage	Investigating theft, sabotage, unauthorised access, or specific security incidents.	Productivity tracking, measuring time away from desk, routine behavioural surveillance, or performance reviews.
Transparency & Notice	Employees must be informed about CCTV, its purpose, and camera locations through employment contracts, HR policies, or workplace notices.	Covert surveillance without any notice or disclosure, except for a documented, time-limited investigation into a specific threat.
Covert Cameras	Permitted only for a documented, time-limited investigation into a specific, identified threat - approved at senior level and reviewed regularly.	Permanent covert cameras; covert cameras deployed for general monitoring without a specific documented threat.
Retention of Employee Footage	Footage tied to a security incident may be kept for the duration of the investigation and related legal proceedings.	Indefinite retention of routine footage; reuse of footage for performance reviews or disciplinary proceedings unrelated to the original security purpose.
Access Rights	Employees monitored under Section 7(i) do not have a right under Section 11 to request access to footage of themselves - Section 11 applies only where consent was the lawful basis.	Employers cannot use this limitation to deny employees access to footage in the context of disciplinary proceedings where natural justice requires disclosure.
FRT on Employees	Requires explicit consent under Section 5 in addition to Section 7(i) - biometric processing cannot be justified by employment necessity alone.	Deploying FRT on employees without specific, informed, and freely given consent; consent is not freely given if refusal affects employment.

❏ Section 7(i) is not an unrestricted authorisation. Its use must remain closely connected to legitimate employment-related security objectives. An employer who deploys CCTV at workstations to monitor productivity - even with a notice - is processing personal data without a valid lawful basis under the DPDPA.

Designing Defensible CCTV Processing: Minimisation, Proportionality & Retention

The DPDP Act does not give CCTV-specific rules, but CCTV is still governed by lawful basis, purpose limitation, and data minimisation under Sections 5 and 6. A defensible setup should capture only what is necessary for security and keep it only as long as required.

- 1

Capture Only What Is Necessary - Section 6 (Data Minimisation)

Each camera must be justified by a specific security need and limited to the smallest workable field of view. The design should exclude or mask unnecessary areas.

 - Document the specific threat
 - Explain why CCTV is necessary
 - Set the minimum field of view
 - Exclude or mask nearby property, public paths, and sensitive areas
- 2

High-Intrusion Features Require Stronger Justification

Higher-risk features need a documented, specific justification before use. Covert cameras, FRT, audio recording, and PTZ controls should all be tightly limited.

 - Covert cameras: time-limited, senior-approved, threat-specific
 - FRT: explicit consent under Section 5
 - Audio recording: last resort only
 - PTZ cameras: technically restrict beyond the stated area
- 3

Keep Footage Only for a Defensible Period - Section 8(7)

Delete footage once the purpose ends unless law requires retention. Routine footage, incident footage, and access logs should each follow a separate retention rule.

 - Routine footage: delete after 90 days
 - Incident footage: preserve for the investigation and any proceedings
 - Access logs: retain for 1 year
 - Separate logs from footage

Compliance Measure	Practical Implementation
Camera placement documentation	Keep a camera register with location, purpose, and justification, reviewed annually.
Privacy masking	Apply device-level masking before deployment, not after recording.
Audio recording	Disable audio unless a documented legal or operational need exists.
Automated deletion	Set systems to automatically delete footage after the retention period.
Incident flagging protocol	Use a documented process to flag and preserve incident footage before deletion.
Access log retention	Keep access logs separately for 1 year.
Privacy notice	Issue a CCTV notice covering purpose, retention, lawful basis, identity, and rights.
Annual review	Review placement, retention, and access controls annually or when the purpose changes.

DPDPA vs. GDPR: Key Differences for CCTV Processing

GDPR compliance does not automatically satisfy the DPDPA for CCTV operations in India. The two regimes use different legal structures, so India-specific compliance must be built separately.

Key Parameter	EU GDPR Position	India DPDPA Position
Lawful Basis for Ordinary CCTV	Article 6(1)(f) allows legitimate interests if the controller shows necessity and balances them against individual rights. Ordinary security CCTV can rely on this test.	There is no open-ended legitimate interests ground. Ordinary commercial CCTV must rely on Section 7(a) or explicit consent under Section 4.
Employee Surveillance	Employee monitoring is assessed under legitimate interests and proportionality standards. Labour law may further limit continuous surveillance.	Section 7(i) allows processing to protect the employer from loss, liability, or security threats. It does not extend to productivity monitoring or behavioural surveillance.
Facial Recognition Technology	FRT usually involves biometric data under Article 9. It generally requires explicit consent or another Article 9(2) ground.	FRT requires explicit consent under Section 5. Section 7(a) is not sufficient.
Individual Access Rights	Article 15 allows individuals to request access to their personal data, subject to third-party rights. In CCTV, this can include footage in which they appear.	Section 11 gives Data Principals a right to a summary of their personal data and processing activities, not an automatic copy of footage. Employees monitored under Section 7(i) cannot use Section 11 for access to footage of themselves.
Retention & Logs	Article 5(1)(e) requires retention only for as long as necessary. There is no fixed CCTV retention period.	Section 8(7) requires deletion once the purpose is served. Routine CCTV footage is defensibly retained for 90 days.

📌 GDPR compliance is not a substitute for DPDPA compliance because the two regimes differ in legal structure, rights, and enforcement.

Key Takeaways: CCTV Compliance Under the DPDPA 2023

The DPDPA 2023 has transformed CCTV from an unregulated security tool into a regulated personal data processing activity. The following five principles summarise the compliance framework and the actions every Data Fiduciary must take.

01	02	03
Identify Your Role as Data Fiduciary If your organisation controls why cameras are placed, how long footage is retained, and who can access it - you are a Data Fiduciary under Section 2(i). This comes with primary legal and financial responsibility for all footage processed under your control. There is no minimum size threshold: a single camera in a small shop triggers the Act if it records identifiable individuals.	Apply the Correct Lawful Basis for Each Deployment Home CCTV: household exemption under Section 3(c)(i) - strictly inward-looking only; any capture of third-party data loses the exemption. Business CCTV (public-facing): Section 7(a) with prominent, specific signage at all entry points before the monitored area. Employee CCTV: Section 7(i) - limited to security and loss prevention; not productivity monitoring. FRT and AI analytics: explicit consent under Section 5 - Section 7(a) is insufficient. There is no one-size-fits-all lawful basis.	Minimise, Restrict, and Document Capture only what is necessary for the stated security purpose. Restrict camera angles, disable audio, avoid covert cameras unless specifically justified and time-limited. Apply device-level privacy masking where third-party areas are unavoidably visible. Maintain a camera register documenting each camera's location, purpose, field of view, and justification. Review annually.
04	05	
Adopt the Dual-Track Retention Model Routine footage: delete automatically after 90 days. Incident footage: flag and preserve immediately upon identification of a security incident; retain for the duration of investigation and legal proceedings under Section 17(1)(a). Access logs: retain for 1 year regardless of whether footage has been deleted. Rule 8(3)'s one-year obligation applies only to Seventh Schedule purposes - it is not a blanket mandate for routine CCTV.	Do Not Rely on GDPR Compliance Alone GDPR and the DPDPA use fundamentally different legal structures. GDPR's "legitimate interests" ground has no equivalent in the DPDPA. India-specific compliance must be separately structured around the DPDP Act's own statutory bases, rights framework, and retention architecture. A business that is GDPR-compliant for its European operations must build a separate, India-specific CCTV compliance framework for its Indian deployments.	

 Penalties under the DPDPA for failure to implement reasonable security safeguards can reach ₹250 crore per instance. Non-compliance with the Data Protection Board's directions can attract an additional ₹150 crore. The cost of compliance is a fraction of the cost of a single enforcement action.