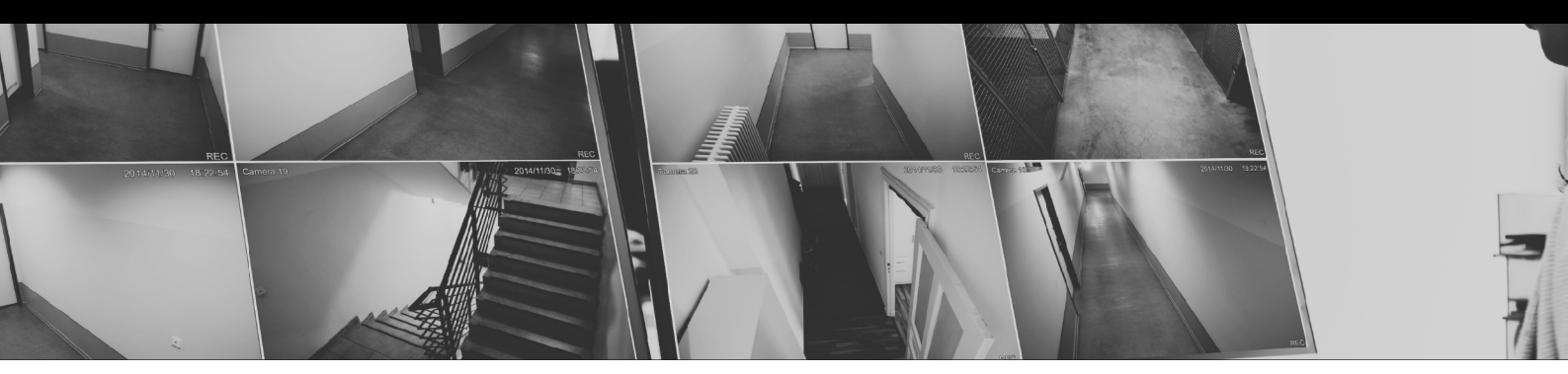


REGULATORY

CCTV Footage: What the Information Regulator's Draft Code Means for Surveillance Governance

26 March 2026 *8 min read*

by Ahmore Burger-Smidt, Director and Head of Regulatory

> *We are rapidly entering the age of no privacy, where everyone is open to surveillance at all times; where there are no secrets from government.*
>
> *"Osborn v. United States, 385 U.S. 323", U.S. Supreme Court case, December 12, 1966*

For most organisations, CCTV is invisible infrastructure, bolted to a wall, quietly recording, and only thought about when something goes wrong. But that comfortable obscurity is ending. Under South Africa's privacy regime, CCTV footage is personal information whenever an individual (or, in certain contexts, a juristic person) is identifiable. That single legal fact transforms video from a facilities line item into a regulated data asset, carrying with it governance obligations, lifecycle controls, and enforceable rights that many organisations have yet to reckon with.

The Information Regulator's ("**Regulator**") draft code of conduct on the processing of personal information at gated access communities is the clearest signal yet that the Regulator is moving beyond high-level principles and into operational expectations for high-risk environments. CCTV is named explicitly as a key risk area, and the implications reach well beyond residential estates.

What the draft code does, and why it matters for CCTV

The draft code is a sector-specific instrument designed to align data processing practices in gated-access environments with POPIA. It targets the full ecosystem: owners and managers of premises, homeowners' associations and bodies corporate, security operators, and the technology suppliers that underpin modern access control.

For those of us who advise on CCTV governance, the draft code's significance lies in the structural reality it addresses. Gated-access CCTV deployments are multi-party by design. An estate management company, a contracted guarding firm, a remote monitoring service, and a cloud or video platform provider may all touch the same footage on any given day. The draft code's emphasis on governance, accountability, and the formal differentiation between Responsible Parties and Operators forces organisations to formalise roles and relationships that, in practice, have often been left to assumption and goodwill.

That informality is precisely where risk accumulates.

Six areas where the draft code reshapes CCTV practice

Processing Basis: The End of "Implied Consent" as a Default

The draft code identifies several high-risk and non-compliant patterns, including reliance on consent as a processing basis without prior assessment of legitimate interest, and the absence of a personal information impact assessment ("**PIIA**"). CCTV processing is listed alongside biometrics as a prominent risk category. The direction of travel is unmistakable: CCTV governance must be designed to stand on its own without leaning on consent as a primary legal crutch. In practical terms, organisations should document the security purpose and necessity of each CCTV deployment, record the lawful justification within their POPIA framework (and ensure consistency across signage, privacy notices, contracts, and internal policy), and treat a PIIA as a baseline control rather than an aspirational exercise.

Purpose Limitation: Guarding Against Function Creep

The draft code's core principles include strict purpose limitation, use CCTV footage for access control and security, and nothing more. In my experience, the fastest route to legal exposure is function creep, and it is far more common than most organisations appreciate. Footage originally captured for perimeter security is repurposed for employee performance management. Clips are shared on internal messaging groups under the banner of vigilance. Recordings end up in marketing materials or social media posts. Audio recording and advanced analytics are enabled because the hardware supports them, not because a risk assessment demands them. A defensible CCTV programme draws a hard line: repurposing is not an operational convenience. Every use beyond the stated purpose requires separate justification.

Data Minimisation: Design Before You Record

The draft code's principle of lawfulness and minimality is direct: collect only what is necessary. For CCTV, minimisation does not begin at the storage layer; it begins at the lens. Thoughtful design controls include positioning and masking cameras to avoid filming neighbouring properties or public spaces unnecessarily, limiting coverage of sensitive areas such as private dwellings, medical rooms, restrooms, and prayer spaces, calibrating zoom and resolution to the stated purpose rather than maximising capability by default, and treating advanced features like facial recognition or behavioural analytics as discrete risk decisions, not standard settings to be left on.

Retention and Deletion: No More Ambiguity

Retention and deletion are foregrounded in the draft code as core governance obligations. Every organisation operating CCTV should be able to answer four questions consistently and auditably. How long is footage kept by default? Who may extend retention, and under what documented trigger, an incident, a claim, or an investigation? How is deletion executed and evidenced? And what happens when footage is exported and its retention moves outside the primary system? If the answers to these questions vary depending on whom you ask within the organisation, the retention framework is not yet fit for purpose.

Security Safeguards: Assume CCTV Is High-Value, High-Risk Data

Under the draft code's treatment of security (aligned with Condition 7 of POPIA), the Regulator highlights technical and organisational measures to prevent loss, unlawful access, damage, or unauthorised destruction, including restricted access to CCTV footage, encryption, password protection, and secure systems, as specific expectations. In reality, CCTV security failures are rarely sophisticated. They are shared passwords across guards and supervisors, unlogged exports to USB devices, system installers retaining remote access long after a project is complete, network video recorders left exposed to the internet, and uncontrolled circulation of clips once they have been exported. A mature compliance posture treats CCTV as what it is, high-value, high-risk data, and implements controls accordingly: role-based access, strong authentication, comprehensive audit logs, export controls, vendor hardening requirements, and secure disposal protocols.

Data Subject Rights: A Real Operational Workload

The draft code explicitly reinforces the full spectrum of data subject rights, including the rights to be informed, to access, to correction, to deletion, to object, to withdraw consent, to restrict processing, and to lodge complaints. For CCTV operators, these rights create a genuine operational challenge. A subject access request for footage requires balancing the privacy rights of other individuals visible in the recording, the integrity of any ongoing security or disciplinary investigation, and the organisation's own POPIA obligations. In practice, this means designing workflows around viewing rather than copying, investing in redaction and blurring capability, and establishing clear internal decision rights for the release of footage.

A Practical Compliance Playbook

For organisations that want to move from reactive risk to structured governance, the following framework offers a pragmatic starting point.

Treat CCTV as a full data lifecycle, not a camera network. Map the end-to-end flow of footage: capture (camera placement and fields of view), transmission (network architecture and remote access), storage (on-premises or cloud, including backups), access (who watches live feeds versus who reviews recordings), export and sharing (to law enforcement, insurers, residents, HR, or other parties), and retention and disposal. Until the lifecycle is mapped, it cannot be governed.

Clarify who is the Responsible Party and lock down operator controls. The draft code foregrounds governance roles – the Responsible Party, the Information Officer, and operators acting on a need-to-know basis. For CCTV, this means aligning contracts and operating procedures so that the Responsible Party can demonstrate it controls the purpose and manner of processing, that operators process only on documented instructions, and that access to footage is restricted, logged, and revocable.

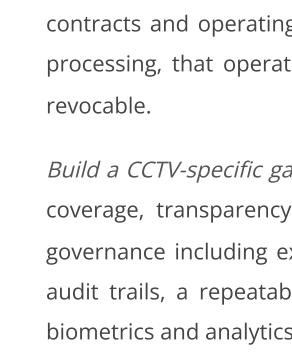
Build a CCTV-specific gap analysis. Consider what a regulator or a complainant would probe: necessity and proportionality of coverage, transparency through signage and notices, alignment between retention settings and retention policy, access governance including export and sharing approvals, security hardening across authentication, patching, vendor access, and audit trails, a repeatable process for handling rights requests, and a documented position on high-risk features such as biometrics and analytics.

Anticipate the leak moment. Most reputational and regulatory harm materialises after an incident, when someone exports a clip and circulates it without adequate controls. Design for this inevitability by watermarking exported footage, restricting export permissions and requiring case numbers or formal authorisations, mandating secure sharing channels rather than ad hoc messaging, using short-lived links where feasible, and establishing a defined escalation path for urgent requests so that urgency does not become a standing excuse for bypassing controls.

Looking ahead

The Regulator's strategic planning frames the gated-access code as a priority response to public concern about overprocessing at gated communities, set against a backdrop of escalating security compromises. This is not an isolated initiative. What we should expect to see is increasing complaints-driven scrutiny of CCTV practices in estates, business parks, and controlled-access premises, particularly where footage is shared widely, retention periods are long, or transparency is weak. The compliance baseline is shifting from policy on paper to demonstrable system configuration and operational discipline – access controls, retention automation, and auditable exports. There will be heightened attention on CCTV combined with biometrics and analytics, which the draft code already positions as risk-heavy processing categories.

The strategic opportunity for organisations is to treat CCTV compliance not as a constraint on security operations, but as a means of making security more trustworthy, more defensible, and far less fragile under regulatory or public scrutiny. The organisations that invest in structured CCTV governance now will find themselves better positioned, not only to satisfy the Regulator, but to maintain the trust of the communities and stakeholders they serve.



Ahmore Burger-Smidt

Head of Regulatory

View Profile