CCPOA visitor and incident coordination

Veyra proposal for discussion
24 November 2026

The proposed decision

Support the design of a governed pilot with willing buildings and existing technology providers. Confirm the lawful sharing model and required approvals before live incident sharing.

The problem

A disruptive rental group can return using a different lead booker. Individual guest verification and reviewed incident history could give participating buildings continuity across bookings.

How the service would work

Before arrival: the owner authorises the stay and submits the intended guests, with a responsible contact and backup.

At the building: security checks each guest against the authorised stay and issues access for the approved period.

During the stay: guards record complaints, observations, interventions and the guests' response.

After review: authorised reviewers record findings and determine which limited alerts may lawfully inform later checks.

Five capabilities for the pilot

Guest and day-visitor registration; individual access passes; owner escalation; guided incident handling; and unit-level reporting.

Participation by existing providers

A proposed free, open-source CCPOA component would offer controlled APIs. Providers could submit permitted updates and incident reports, with limited verification responses. Personal records would remain protected.

Fair records and a workable pilot

Cooperation is part of the history

If security requests lower volume and confirms that guests comply, record “resolved after intervention”. If disturbance continues or recurs, document the further interventions and escalate. Keep allegations, observations and findings distinct.

Individual accountability

A guest list identifies people relevant to a stay. It does not prove that everyone caused an incident. A returning guest’s relevant record may prompt authorised review under agreed policy. A flag should not automatically refuse entry.

Privacy and governance

Use the minimum necessary data, restricted permissions, audit records, retention limits and a correction process. A new visitor has no established history. Numerical scoring remains a policy option for later assessment.

POPIA assessment must precede implementation. Sharing information about objectionable or criminal conduct for third parties may require Information Regulator prior authorisation. Broad registration consent alone does not settle these obligations. [1, 2]

What CCPOA would need to agree

Nominate a governance lead and willing pilot buildings. Agree legal roles, incident-review authority, provider participation and operating costs. Test with synthetic records, then assess registration quality, response times, case outcomes and guard workload during an authorised live pilot.

Future options

Disclosed noise-level alerts and emergency visitor accounting could follow. These require separate scope and privacy review. The free core would still need funding arrangements for hosting, support, integrations and other operating costs.

References

[1] Protection of Personal Information Act 4 of 2013, particularly sections 11 and 57–58.
[2] Information Regulator prior-authorisation guidance.
Sources checked 23 November 2026. Proposed service, subject to agreed governance and legal assessment.