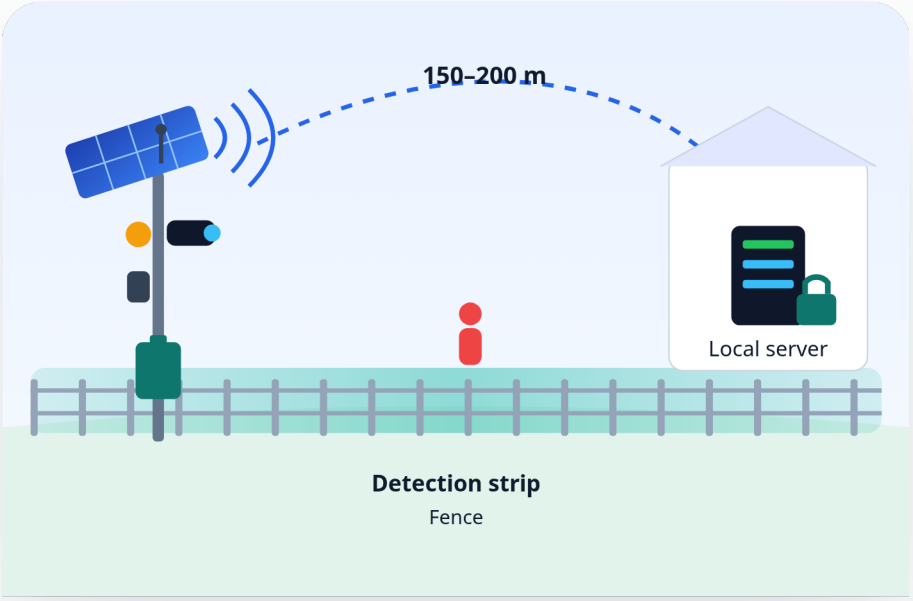
SECURITY OF THE CONDOMINIUM'S COMMON AREA

CLARYEL Perimetro

Project for an autonomous intelligent security system for the common area

A single autonomous intelligent video surveillance point along the fence. All data stays only with us, on the condominium premises, in encrypted form: no clouds, no third-party services, everything local only.

- Local only
- Encrypted
- No cloud
- Instant lock on any alarm



CORE PRINCIPLE

Everything stays with us — on the condominium premises

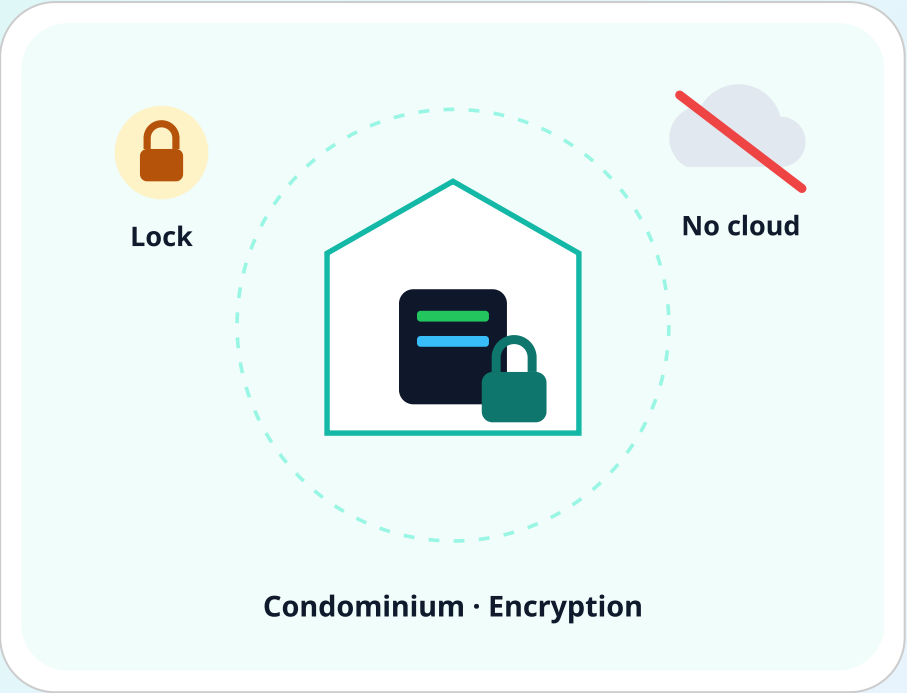
All images, event clips and logs are stored only on the local server inside the building, on the condominium premises.

All information is stored and transmitted in encrypted form.

On any alarm, all information can be locked instantly: access to the archive is closed and the event clips are protected from modification and deletion.

No clouds and no third-party services: artificial intelligence processing and storage take place locally only.

- Local server in the building
- Encryption
- Instant lock
- No cloud
- No third-party services



ALTERNATIVE TO THE CAMERA

Detection using Wi-Fi signals: no images, no identification

- No camera
- No images
- No identification
- Local only

As an alternative to the camera, two Wi-Fi devices can be installed along the fence, one at each end of the monitored section.

From the raw Wi-Fi signal data between the two devices (its variations, known as CSI — Channel State Information) the system derives the contours of people moving in the strip, without any image and without identifying who they are.

The technique is already being studied inside homes: for example, the research “DensePose From WiFi” by Carnegie Mellon University reconstructs the silhouettes of people in a room using Wi-Fi signals only. We propose applying it outdoors, along the fence.

The system detects only presence, direction of movement and an anonymous silhouette. Processing takes place on the local server, encrypted, like the rest of the project, and triggers the same warnings: light, voice message and notifications to residents.

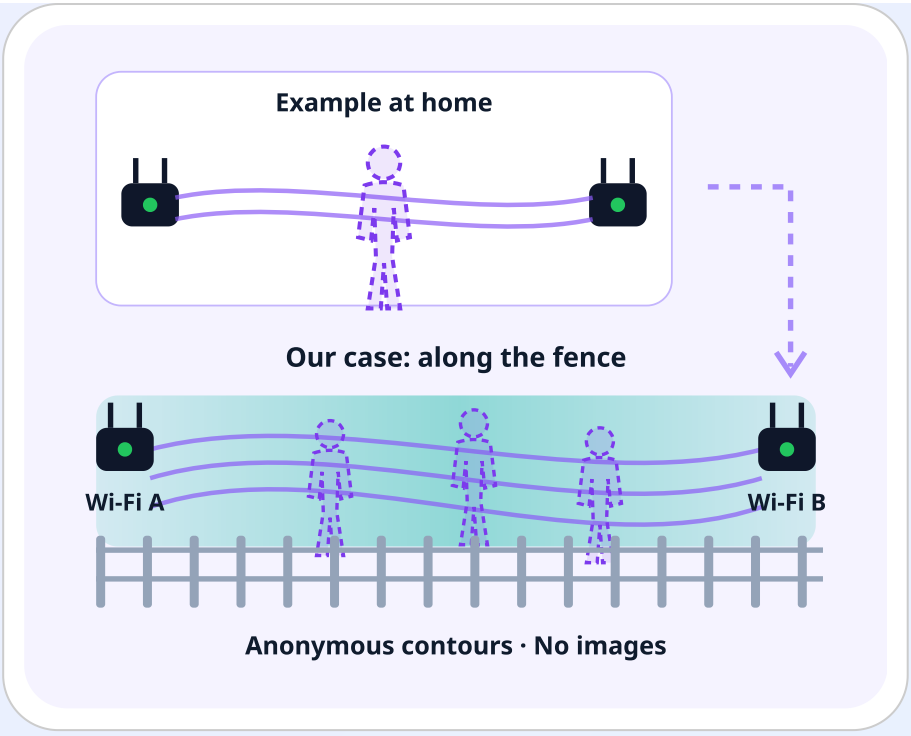
Legal aspects — to be checked with the DPO or a consultant

Wi-Fi detection does not capture images or video: it is therefore not a video surveillance system, and the specific video surveillance rules (for example the information sign indicated by the Garante for cameras) do not apply as such.

The GDPR nevertheless still applies if the data can relate to an identified or identifiable person (Art. 4(1) GDPR). For this reason the system is designed to process only anonymous presence and contours, without identification, locally only and in encrypted form.

This assessment must be confirmed with the DPO or a consultant before installation and does not constitute a legal guarantee.

Example in a home setting: “DensePose From WiFi”, Carnegie Mellon University (arXiv) ↗



01

Purpose of the project

We propose installing a single autonomous intelligent video surveillance point along the fence of the condominium's common area.

The system is designed to detect possible unauthorised intrusion, warn intruders and promptly alert residents.

Core principles of the project:

01

Minimal intrusion into private life.

02

Monitoring of only a narrow strip along the fence.

03

Fully local image processing by artificial intelligence.

04

No mandatory cloud services.

05

Encryption of transmitted and stored information.

06

Automatic warnings and notifications to residents.

07

The option to contact law enforcement promptly.

02

Limiting video surveillance and protecting privacy

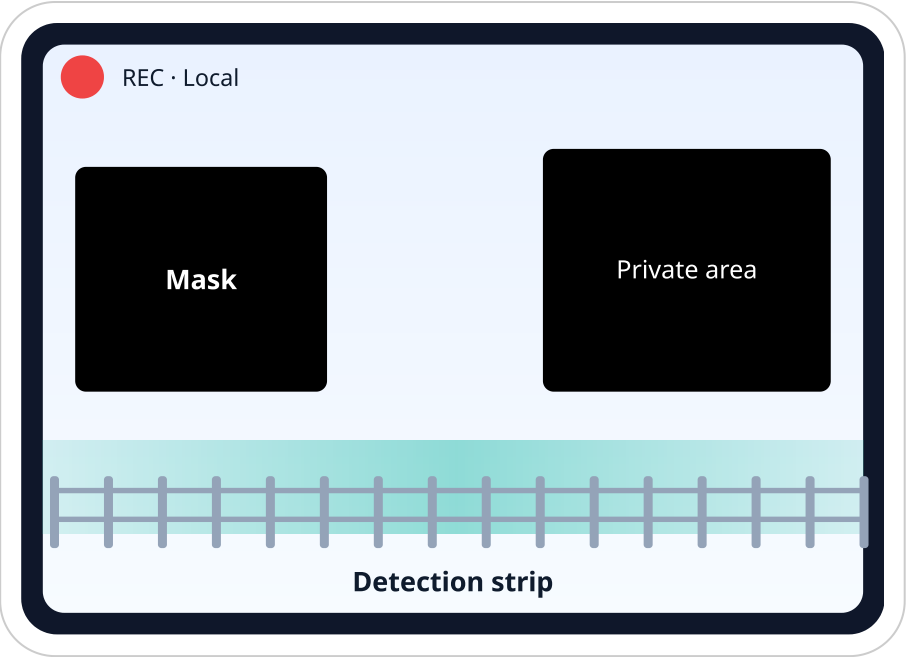
The camera will be pointed exclusively at a predefined section of the common area directly along the fence.

Any parts of the image that might show neighbouring private plots, windows, balconies and other spaces outside the monitored zone will be completely covered by opaque black masks.

Masking is performed directly in the camera, before the video stream is transmitted or recorded.

In addition, a narrow detection strip is defined in software. The artificial intelligence will not analyse objects outside this area.

The system does not include face recognition, identification of specific people, vehicle monitoring or observation of residents' daily lives.



03

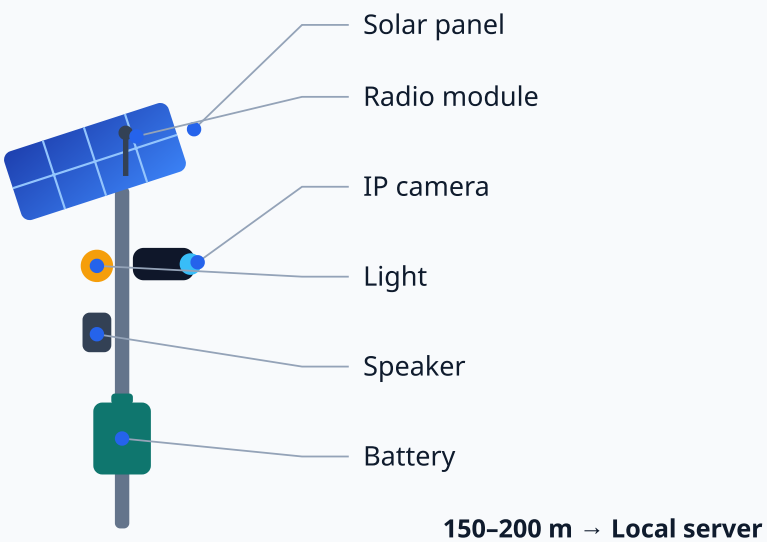
Autonomous equipment

The remote node will be equipped with an IP camera, a solar panel, a battery, a wireless communication module, a warning light and a small speaker.

The expected distance to the local server is 150–200 metres.

The image will be transmitted over a secure wireless link to a server located inside the building.

The system will not depend on the external internet. Internet access will only be needed to send notifications outside the local network and for possible contact with law enforcement.



04

Local artificial intelligence

A specialised computer vision algorithm will run on the local server.

The preliminary plan is to analyse the image at two frames per second, with the option to increase the rate if necessary.

The system will distinguish people from the movement of trees, shrubs, animals, rain and other natural changes in the image.

Warnings will only be triggered when a person is confirmed in the defined zone.

In addition, the direction of movement, the crossing of a virtual boundary and the time spent in the monitored strip can be analysed.



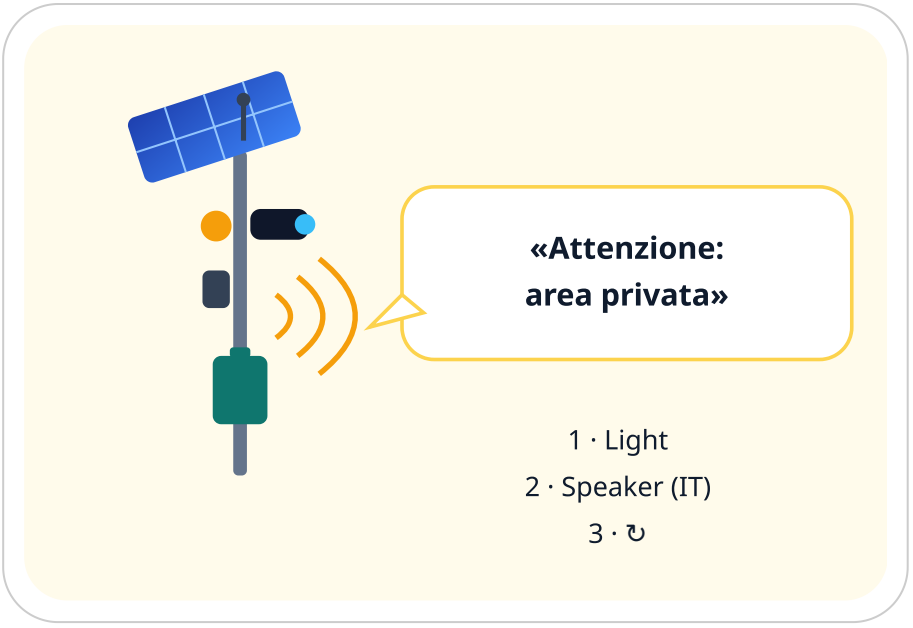
05

Automatic on-site warning

When a person appears in the protected zone, the system will be able to:

1. Switch on a warning light.
2. Play a voice message in Italian stating that the person is on private property.
3. If necessary, repeat the warning within the set limits.

Volume, operating hours and activation conditions will be configured to minimise any disturbance to residents.



06

Notifications to all residents

All interested residents will be able to receive notifications on their mobile phones without any photos or video images being sent.

For example:

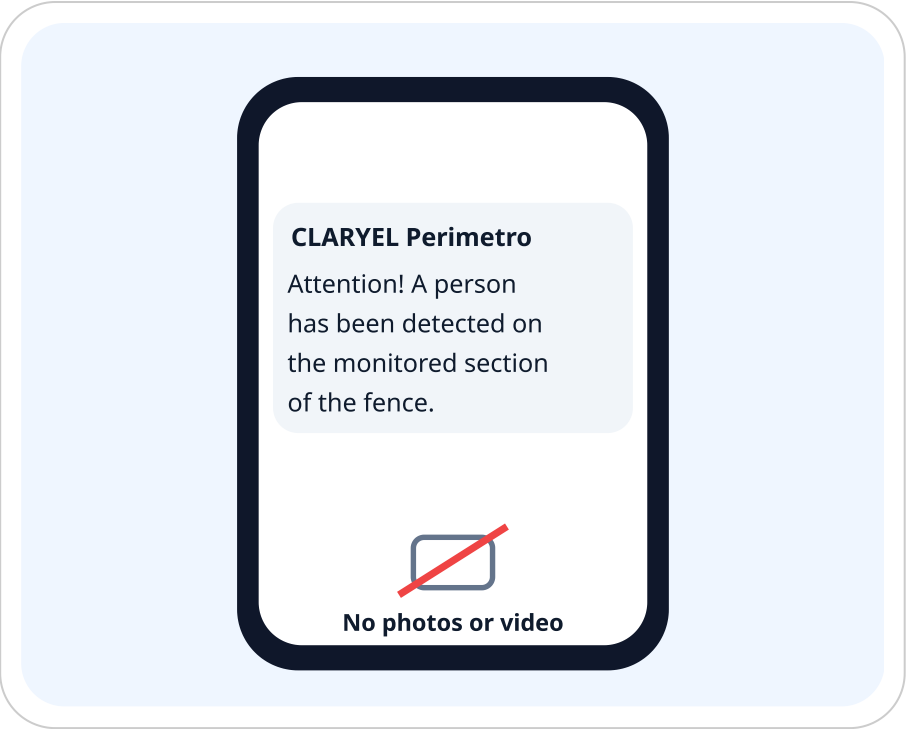
> **“Attention! A person has been detected on the monitored section of the fence. The system has activated a warning.”**

Residents will not need access to the camera or the archive to receive regular notifications.

Subscribing to notifications will be voluntary. Every participant will be able to opt out of receiving messages.

The system administrator will only manage the list of recipients and the notification settings.

Messages will be sent in compliance with the requirements for protecting participants' contact data.



07

Response to a confirmed intrusion

An additional high-alert mode is planned.

It can be activated if the system detects a sequence of signs of a possible intrusion, for example:

- A person has crossed the defined fence boundary.
- They continue moving towards the inner area.
- They are in a zone where people would not normally pass.
- The event is confirmed by analysing several frames.

In this case the system will be able to automatically save a video clip and send an urgent notification to residents.

Option to contact the police

The technical architecture allows for preparing an automatic message to law enforcement.

In the event of a confirmed intrusion, the system will be able to prepare:

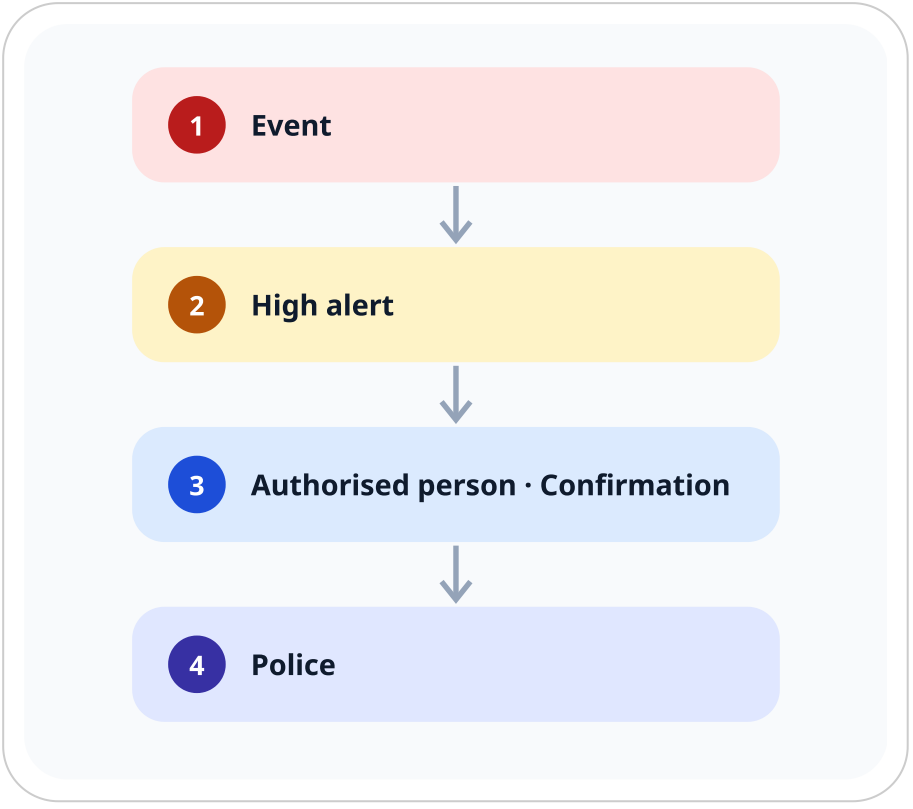
- A voice message in Italian with the address, the nature of the event and the time of detection.
- Several images or a short video clip.
- Information about the location of the incident.
- Contact details of the condominium's authorised representative.

For emergencies, a quick call to the police through an authorised person is planned.

In future, information and images could be transmitted by email, a secure electronic channel or another officially agreed means of communication.

Fully automatic reporting directly to the police is only possible if a suitable officially agreed cooperation procedure is in place. Until it is agreed, the call and the transmission of images will take place after confirmation by an authorised person.

This is necessary to avoid unjustified reports caused by technical errors or false alarms.



Data storage and access management

Everything stays local only, on the condominium premises, in encrypted form. On any alarm, the information can be locked instantly. No clouds and no third-party services.

The video stream will be processed on the local server without using external artificial intelligence services.

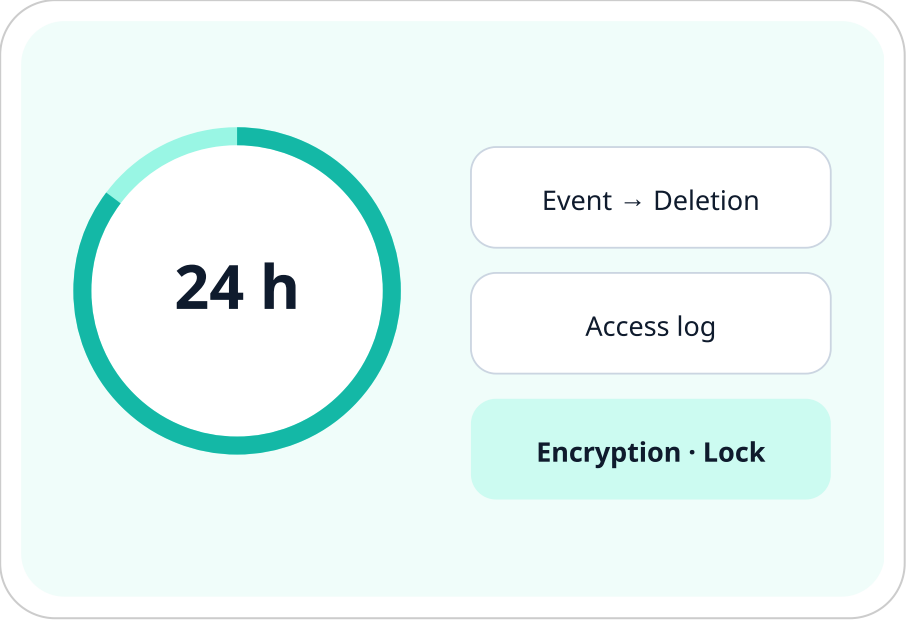
Continuous recording of the entire video stream is not planned. Where necessary, short clips relating to detected events will be saved.

As a preliminary proposal, regular recordings will be deleted automatically after 24 hours. Longer storage of a specific event is allowed where there is a justified need, for example to hand material over to law enforcement.

Access to images is granted only to specially designated persons.

Regular residents receive written notifications, but no access to the camera.

All access to the archive is recorded in the system log.



09

Required approvals

The following procedure is proposed for implementation:

Stage one — discussion with residents.

Publication of the project's technical description and collection of feedback.

Stage two — agreement with the administration.

The condominium administrator receives the system description, the camera location plan, the diagram limiting the monitored zone and the data processing rules.

Stage three — decision of the general meeting.

The installation of equipment in the common area is put to a vote in accordance with articles 1122-ter and 1136 of the Italian Civil Code.

Stage four — drawing up the operating rules.

The condominium is designated as the data controller. If necessary, a technical operator of the system with limited powers is appointed.

Rules on access, retention periods, the procedure for notifying residents and the use of video recordings are approved.

The mandatory information signs on video surveillance are installed.

Stage five — experimental operation.

After the necessary permissions are obtained, a single experimental point is installed. Detection reliability, false alarms, link quality, power supply and notifications are checked.

Sending messages directly to law enforcement is considered separately with the relevant services.

Summary

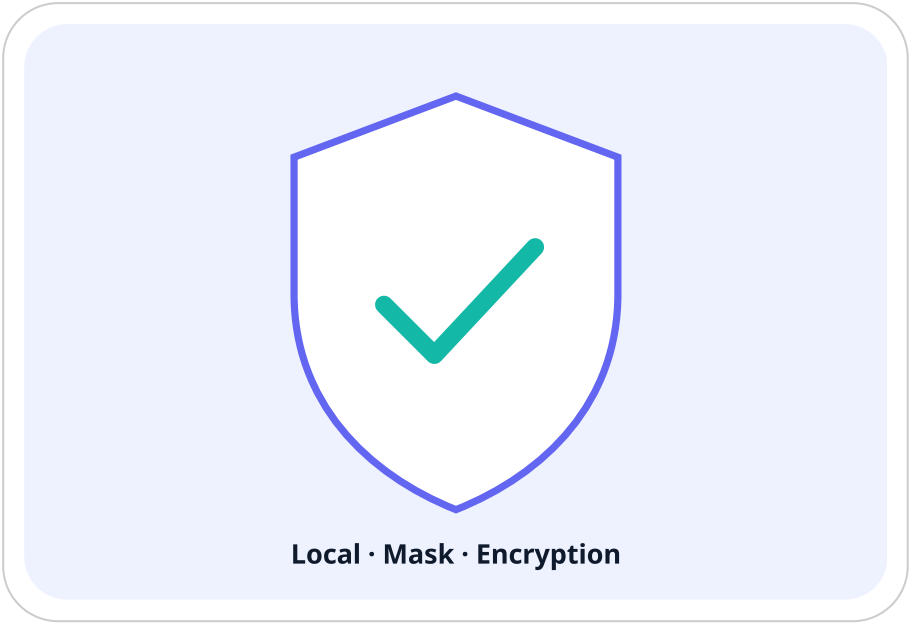
The proposed system is an autonomous intelligent security installation intended exclusively for monitoring a limited section of the common area.

Its task is not to watch residents, but to detect a possible intrusion through the fence in good time, warn the intruder and inform the residents.

Local artificial intelligence processing, a limited field of view, physical masking of private areas and the absence of free access to video recordings should ensure a high level of privacy protection.

In future, the system may be supplemented with means for prompt cooperation with law enforcement.

The project is intended to be implemented gradually, starting with a single experimental point, and only after the necessary approvals.



+

Improvement proposals

Below are CLARYEL's proposals for discussion with the residents and the administration. They are not part of the approved project and are not a legal opinion: each proposal should be checked with the administrator and, where necessary, with a data protection specialist.

PROPOSAL FOR DISCUSSION · 1

Data protection impact assessment

Before installation, carry out and document an impact assessment (DPIA, Art. 35 GDPR), or explain in writing why it is not required in this case.

PROPOSAL FOR DISCUSSION · 2

Information for residents and passers-by

Put up the information sign following the Garante Privacy model for video surveillance and prepare the full notice under Art. 13 GDPR, taking into account the guidance of the Garante and the EDPB on video surveillance.

PROPOSAL FOR DISCUSSION · 3

Written retention policy

Set out in the rules: 24 hours by default, the list of permitted exceptions, who decides on an extension and how an extended recording is deleted.

PROPOSAL FOR DISCUSSION · 4

Quiet hours and speaker limits

At night, light only or reduced volume, a maximum number of repeats per event and a pause between warnings.

PROPOSAL FOR DISCUSSION · 5

Tamper and fault monitoring

Separate alerts to the administrator if the camera is covered or moved, the view changes, the node goes offline or the battery is running low.

PROPOSAL FOR DISCUSSION · 6

Node “heartbeat” monitoring

The node regularly sends the server a signal that it is working; if the signal is missed, the administrator receives a message.

PROPOSAL FOR DISCUSSION · 7

Protecting the link and the storage

Encryption of the radio link (for example WPA3 and a WireGuard tunnel), encrypted clip storage, an access log, camera firmware updates and changing the factory passwords.

PROPOSAL FOR DISCUSSION · 8

Two-person access

Viewing and exporting clips only with two designated persons present, recorded in the log.

PROPOSAL FOR DISCUSSION · 9

Mask check before go-live

Show residents a frame with the masks applied and attach it to the meeting minutes before the system goes live; repeat after any camera readjustment.

PROPOSAL FOR DISCUSSION · 10

Metrics for the experimental phase

Track false alarms and missed detections, agree “continue / do not continue” criteria in advance and present a report to the meeting.

PROPOSAL FOR DISCUSSION · 11

Notification channels

Notifications are generated on the local server and contain only a written message, without images; the meeting chooses the delivery method, preferring options without third-party cloud services; anyone can unsubscribe at any time.

PROPOSAL FOR DISCUSSION · 12

Data minimisation

No face recognition, no number plate reading, no audio recording; keep only what is needed for the specific event.

PROPOSAL FOR DISCUSSION · 13

Winter autonomy

Check the power reserve of the solar panel and battery on short, overcast days and define in advance how the node behaves when the battery is low.

PROPOSAL FOR DISCUSSION · 14

Placement of signs

Signs are placed before the entrance to the filmed zone and are clearly visible both day and night.

PROPOSAL FOR DISCUSSION · 15

Periodic review

Regularly, for example once a year, present the meeting with a report on the system's operation, the zone settings and the retention periods.

PROPOSAL FOR DISCUSSION · 16

Report template for the police

A form prepared in advance: date and time, section, description, clips, contact of the authorised representative, who confirmed the event and when.

?

Frequently asked questions

Will the camera film windows, balconies and private plots?

No. These parts of the image are covered by opaque black masks directly in the camera, before transmission and recording. The artificial intelligence only analyses a narrow strip along the fence.

Who can watch the video?

Only specially designated persons. Residents receive written notifications without photos or video and have no access to the camera or the archive. Every access to the archive is logged.

Where is the data stored and for how long?

Only on the local server on the condominium premises, in encrypted form, with no cloud or third-party services. There is no continuous recording: short event clips are, as a preliminary proposal, deleted automatically after 24 hours; longer storage only where there is a justified need.

Can I opt out of notifications?

Yes. Subscription is voluntary and you can stop receiving messages at any time.

What about false alarms?

The system distinguishes people from trees, shrubs, animals and rain, and warnings are only triggered when a person is confirmed. The police are contacted only after confirmation by an authorised person. False alarms are checked during the experimental phase.

Will the system recognise faces or number plates?

No. The project does not include face recognition, identification of specific people or vehicle monitoring.

How much will it cost?

The cost has not yet been defined. It will be discussed separately, after the technical solutions have been agreed with the residents and the administration.

§

Legal references

Official sources useful for the discussion. The links are for information only and do not replace professional advice.

Regulation (EU) 2016/679 (GDPR) — official version ↗ — https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32016R0679
In particular Art. 13 (information) and Art. 35 (impact assessment).

Italian Personal Data Protection Code — Legislative Decree 196/2003 ↗ — https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2003-06-30;196
Normattiva, current version.

Italian Civil Code, Art. 1122-ter — video surveillance systems on common parts ↗ — https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:regio.decreto:1942-03-16;262~art1122ter
Normattiva.

Italian Civil Code, Art. 1136 — constitution of the meeting and validity of resolutions ↗ — https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:regio.decreto:1942-03-16;262~art1136
Normattiva.

Garante Privacy — Video surveillance ↗ — https://www.garanteprivacy.it/temi/videosorveglianza
Topic page of the Italian Data Protection Authority.

Garante Privacy — Video surveillance FAQ, guide and sign template ↗ — https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9496574
Guidance on the simplified notice (sign) and on retention periods.

EDPB — Guidelines 3/2019 on processing of personal data through video devices ↗ — https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_it
European Data Protection Board.

Local setting

The condominium is located in the Municipality of Fino Mornasco (province of Como). The bodies listed below are possible counterparts for coordination: the project does not involve any agreement already made with them.

In any emergency, the European emergency number 112 always applies.

Municipality of Fino Mornasco ↗ — https://www.comune.finomornasco.co.it/
Municipal administration and Local Police (Polizia Locale): coordination on local rules and signs.

Arma dei Carabinieri ↗ — https://www.carabinieri.it/
The locally competent station: a possible agreed procedure for reports.

✉

Your proposal or comment

The first stage of the project is discussion with the residents. Tell us what could be improved and what raises questions or doubts.

Or contact us directly

CLARYEL Perimetro — This is a project for discussion with the residents and the administration of the condominium. It can only be implemented after the necessary approvals.

The content is for information only and does not constitute legal advice.