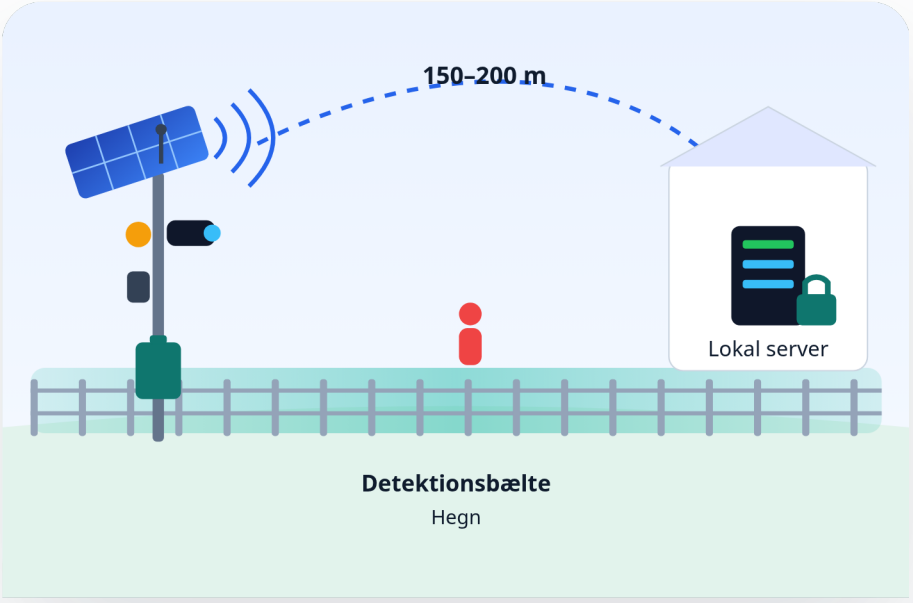
SIKKERHED PÅ EJENDOMMENS FÆLLESAREAL

CLARYEL Perimetro

Projekt for et autonomt intelligent sikringssystem til fællesarealet

Ét autonomt intelligent kamerapunkt langs hegnet. Alle data bliver udelukkende hos os, på ejendommen, i krypteret form: ingen skyer, ingen tredjepartstjenester, alt kun lokalt.

- Kun lokalt
- Krypteret
- Ingen sky
- Øjeblikkelig låsning ved enhver alarm



GRUNDPRINCIP

Alt bliver hos os — på ejendommen

Alle billeder, hændelsesklip og logfiler gemmes udelukkende på den lokale server i bygningen, på ejendommen.

Al information gemmes og overføres i krypteret form.

Ved enhver alarm kan al information låses øjeblikkeligt: adgangen til arkivet lukkes, og hændelsesklippene beskyttes mod ændring og sletning.

Ingen skyer og ingen tredjepartstjenester: behandling med kunstig intelligens og lagring foregår kun lokalt.

- Lokal server i bygningen
- Kryptering
- Øjeblikkelig låsning
- Ingen sky
- Ingen tredjepartstjenester



ALTERNATIV TIL KAMERAET

Detektion via Wi-Fi-signaler: ingen billeder, ingen identifikation

- Intet kamera
- Ingen billeder
- Ingen identifikation
- Kun lokalt

Som alternativ til kameraet kan der installeres to Wi-Fi-enheder langs hegnet, én i hver ende af den overvågede strækning.

Ud fra rådata fra Wi-Fi-signalet mellem de to enheder (dets variationer, kendt som CSI — Channel State Information) udleder systemet konturerne af personer, der bevæger sig i bæltet, uden noget billede og uden at identificere, hvem de er.

Teknikken undersøges allerede inde i boliger: forskningen »DensePose From WiFi« fra Carnegie Mellon University genskaber for eksempel silhuetterne af personer i et rum alene ud fra Wi-Fi-signaler. Vi foreslår at anvende den udendørs, langs hegnet.

Systemet registrerer kun tilstedeværelse, bevægelsesretning og en anonym silhuet. Behandlingen foregår krypteret på den lokale server, som i resten af projektet, og udløser de samme advarsler: lys, talemeddelelse og meddelelser til beboerne.

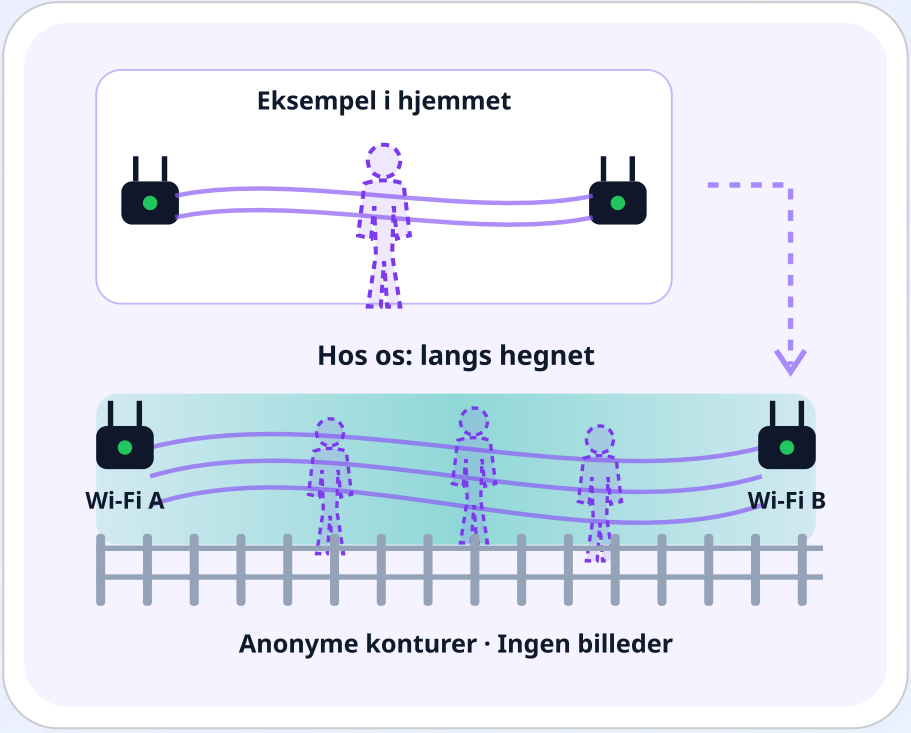
Juridiske aspekter — skal kontrolleres med databeskyttelsesrådgiveren (DPO) eller en rådgiver

Wi-Fi-detektion optager ikke billeder eller video: det er derfor ikke et kameraovervågningssystem, og de særlige regler om kameraovervågning (for eksempel det informationsskilt, som Garante angiver for kameraer) gælder ikke som sådan.

GDPR finder dog fortsat anvendelse, hvis oplysningerne kan vedrøre en identificeret eller identificerbar person (artikel 4, nr. 1, i GDPR). Derfor er systemet udformet til kun at behandle anonym tilstedeværelse og konturer, uden identifikation, kun lokalt og i krypteret form.

Denne vurdering skal bekræftes med DPO'en eller en rådgiver før installationen og udgør ikke en juridisk garanti.

Eksempel i en bolig: »DensePose From WiFi«, Carnegie Mellon University (arXiv) ↗



Projektets formål

Det foreslås at installere ét autonomt punkt til intelligent kameraovervågning langs hegnet om ejendommens fællesareal.

Systemet skal registrere mulig uautoriseret indtrængen, advare den indtrængende og hurtigt informere beboerne.

Projektets grundprincipper:

01

Minimalt indgreb i privatlivet.

02

Overvågning af kun et smalt bælte langs hegnet.

03

Fuldt lokal billedbehandling med kunstig intelligens.

04

Ingen obligatoriske skytjenester.

05

Kryptering af overført og lagret information.

06

Automatiske advarsler og meddelelser til beboerne.

07

Mulighed for hurtigt at kontakte politiet.

02

Begrænsning af kameraovervågningen og beskyttelse af privatlivet

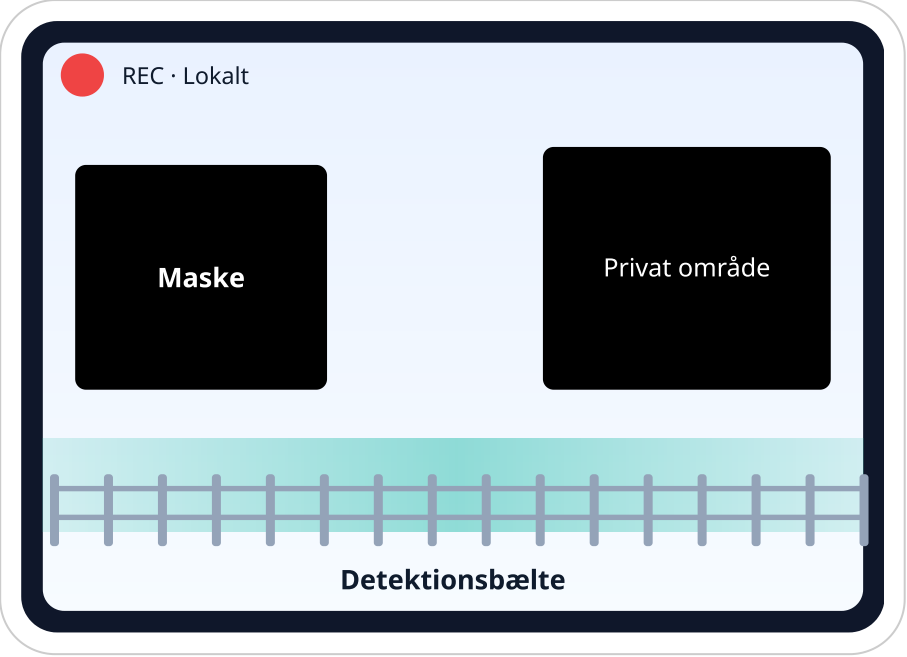
Kameraet rettes udelukkende mod en forudbestemt del af fællesarealet direkte langs hegnet.

Alle dele af billedet, der kan vise tilstødende private grunde, vinduer, altaner og andre områder uden for den overvågede zone, dækkes helt med uigennemsigtige sorte masker.

Maskeringen sker direkte i kameraet, før videostrømmen overføres eller optages.

Desuden defineres et smalt detektionsbælte i softwaren. Den kunstige intelligens analyserer ikke objekter uden for dette område.

Systemet omfatter ikke ansigtsgenkendelse, identifikation af bestemte personer, overvågning af køretøjer eller observation af beboernes hverdag.



03

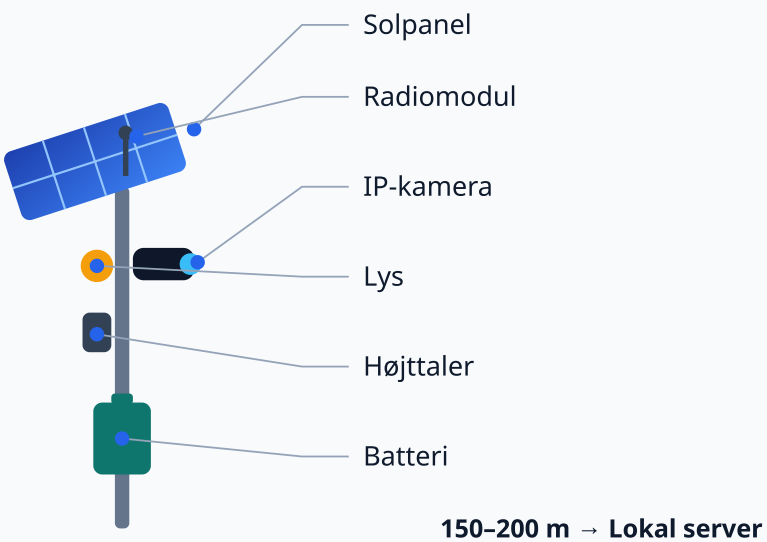
Autonomt udstyr

Det fjerne punkt udstyres med et IP-kamera, et solpanel, et batteri, et modul til trådløs kommunikation, et advarselslys og en lille højttaler.

Den forventede afstand til den lokale server er 150–200 meter.

Billedet overføres via en sikker trådløs forbindelse til en server inde i bygningen.

Systemet vil ikke være afhængigt af eksternt internet. Internetadgang er kun nødvendig for at sende meddelelser uden for det lokale netværk og til eventuel kontakt med politiet.



04

Lokal kunstig intelligens

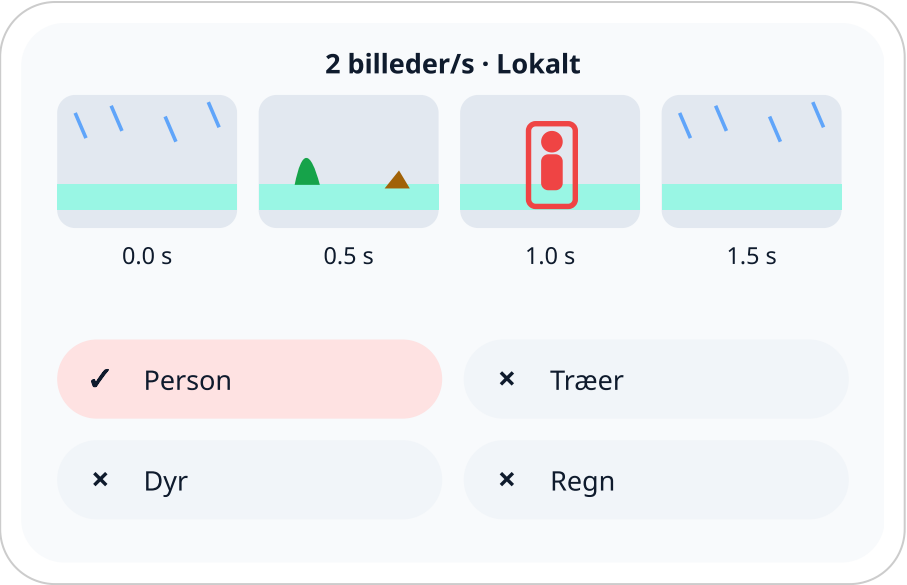
En specialiseret algoritme til computersyn kører på den lokale server.

Den foreløbige plan er at analysere billedet med to billeder i sekundet, med mulighed for at øge frekvensen efter behov.

Systemet skelner mennesker fra bevægelser af træer, buske, dyr, regn og andre naturlige ændringer i billedet.

Advarsler udløses kun, når en person er bekræftet i den definerede zone.

Desuden kan bevægelsesretning, passage af en virtuel grænse og opholdstid i det overvågede bælte analyseres.



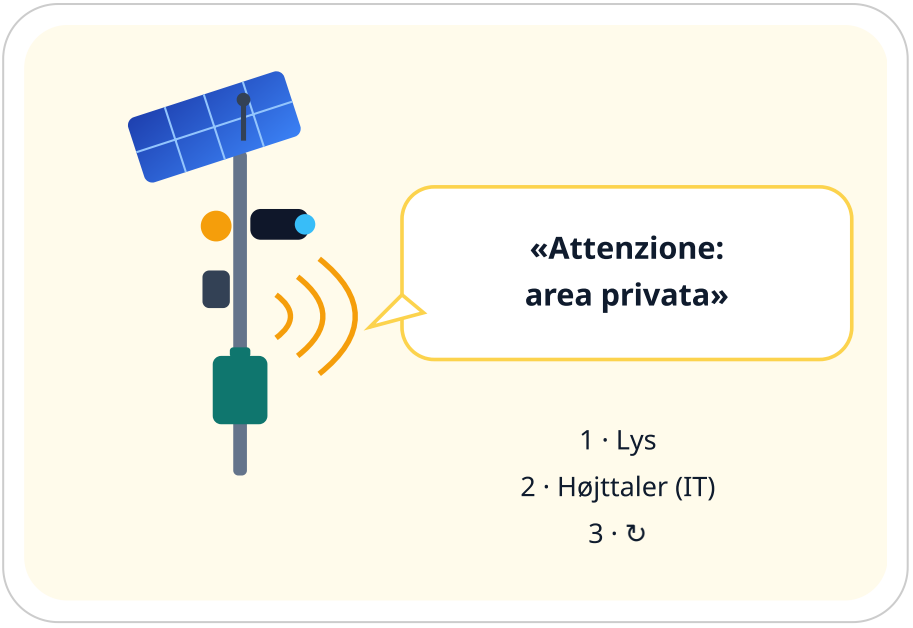
05

Automatisk advarsel på stedet

Når en person viser sig i den beskyttede zone, kan systemet:

1. Tænde et advarselslys.
2. Afspille en talemeddelelse på italiensk om, at personen befinder sig på privat område.
3. Om nødvendigt gentage advarslen inden for de fastsatte grænser.

Lydstyrke, driftstider og aktiveringsbetingelser indstilles, så generne for beboerne minimeres.



06

Meddelelser til alle beboere

Alle interesserede beboere kan modtage meddelelser på mobilen, uden at der sendes fotos eller videobilleder.

For eksempel:

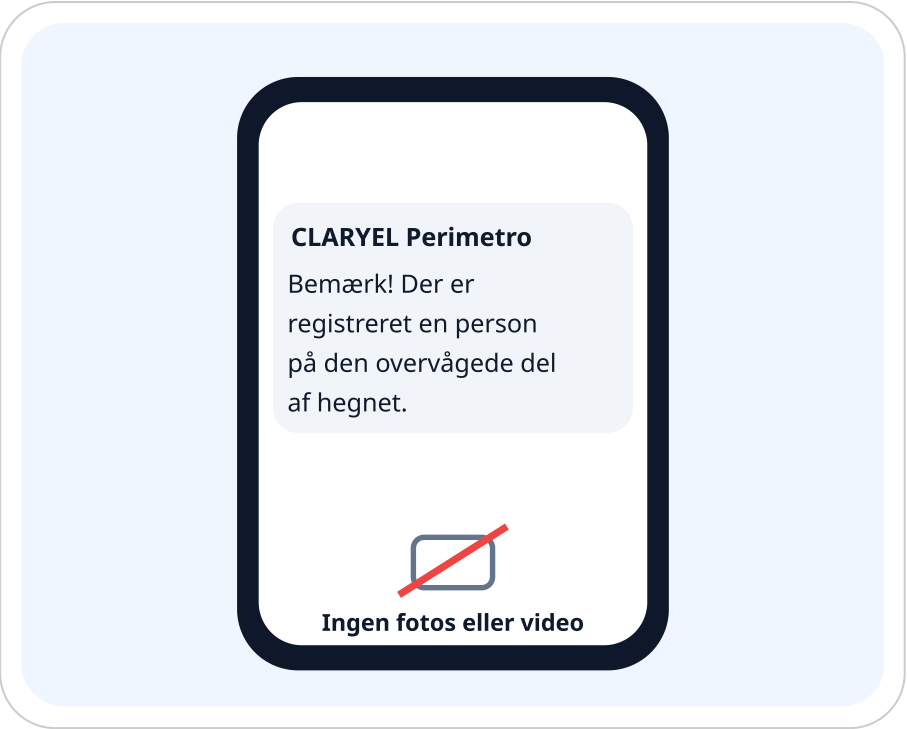
> **»Bemærk! Der er registreret en person på den overvågede del af hegnet. Systemet har aktiveret en advarsel.«**

Beboerne behøver ikke adgang til kameraet eller arkivet for at modtage almindelige meddelelser.

Tilmelding til meddelelser er frivillig. Enhver deltager kan fravælge at modtage beskeder.

Systemadministratoren håndterer kun modtagerlisten og indstillingerne for meddelelser.

Beskeder sendes i overensstemmelse med kravene til beskyttelse af deltagernes kontaktoplysninger.



07

Reaktion på bekræftet indtrængen

Der planlægges en ekstra tilstand med skærpet alarm.

Den kan aktiveres, hvis systemet registrerer en række tegn på mulig indtrængen, for eksempel:

- En person har krydset den definerede grænse ved hegnet.
- Personen fortsætter mod det indre område.
- Personen befinder sig i en zone, hvor folk normalt ikke færdes.
- Hændelsen bekræftes ved analyse af flere billeder.

I så fald kan systemet automatisk gemme et videoklip og sende en hastemeddelelse til beboerne.

Mulighed for at kontakte politiet

Den tekniske arkitektur gør det muligt at forberede en automatisk meddelelse til politiet.

Ved en bekræftet indtrængen kan systemet forberede:

- En talemeddelelse på italiensk med adresse, hændelsens art og tidspunktet for registreringen.
- Nogle billeder eller et kort videoklip.
- Oplysninger om hændelsens placering.
- Kontaktoplysninger på ejendommens bemyndigede repræsentant.

I nødsituationer planlægges et hurtigt opkald til politiet via en bemyndiget person.

I fremtiden kan information og billeder overføres via e-mail, en sikker elektronisk kanal eller et andet officielt aftalt kommunikationsmiddel.

Fuldt automatisk anmeldelse direkte til politiet er kun mulig, hvis der foreligger en passende officielt aftalt samarbejdsprocedure. Indtil den er aftalt, sker opkaldet og overførslen af billeder efter bekræftelse fra en bemyndiget person.

Det er nødvendigt for at undgå ubegrundede anmeldelser som følge af tekniske fejl eller falske alarmer.



Datalagring og adgangsstyring

Alt bliver kun lokalt, på ejendommen, i krypteret form. Ved enhver alarm kan informationen låses øjeblikkeligt. Ingen skyer og ingen tredjepartstjenester.

Videostrømmen behandles på den lokale server uden brug af eksterne tjenester til kunstig intelligens.

Kontinuerlig optagelse af hele videostrømmen er ikke planlagt. Efter behov gemmes korte klip vedrørende registrerede hændelser.

Som et foreløbigt forslag slettes almindelige optagelser automatisk efter 24 timer. Længere opbevaring af en bestemt hændelse er tilladt ved et begrundet behov, for eksempel for at udlevere materiale til politiet.

Adgang til billeder gives kun til særligt udpegede personer.

Almindelige beboere modtager skriftlige meddelelser, men ingen adgang til kameraet.

Al adgang til arkivet registreres i systemloggen.



09

Nødvendige godkendelser

Følgende fremgangsmåde foreslås for gennemførelsen:

Første fase — drøftelse med beboerne.

Offentliggørelse af projektets tekniske beskrivelse og indsamling af bemærkninger.

Anden fase — aftale med administrationen.

Ejendommens administrator modtager systembeskrivelsen, planen for kameraets placering, skemaet, der afgrænser den overvågede zone, og reglerne for databehandling.

Tredje fase — generalforsamlingens beslutning.

Installationen af udstyr på fællesarealet sættes til afstemning i henhold til artikel 1122-ter og 1136 i den italienske civillov.

Fjerde fase — udarbejdelse af driftsreglerne.

Ejendommen udpeges som dataansvarlig. Om nødvendigt udpeges en teknisk operatør af systemet med begrænsede beføjelser.

Regler for adgang, opbevaringsperioder, proceduren for meddelelser til beboerne og brugen af videooptagelser godkendes.

De obligatoriske informationsskilte om kameraovervågning opsættes.

Femte fase — forsøgsdrift.

Når de nødvendige tilladelser er opnået, installeres ét enkelt forsøgspunkt. Detektionens pålidelighed, falske alarmer, forbindelsens kvalitet, strømforsyning og meddelelser kontrolleres.

Afsendelse af meddelelser direkte til politiet behandles særskilt med de relevante myndigheder.

Konklusion

Det foreslåede system er en autonom intelligent sikringsinstallation, der udelukkende er beregnet til overvågning af en begrænset del af fællesarealet.

Dets opgave er ikke at overvåge beboerne, men i tide at registrere en mulig indtrængen gennem hegnet, advare den indtrængende og informere beboerne.

Lokal behandling med kunstig intelligens, et begrænset synsfelt, fysisk maskering af private områder og fravær af fri adgang til videooptagelser skal sikre et højt niveau af beskyttelse af privatlivet.

I fremtiden kan systemet suppleres med midler til hurtigt samarbejde med politiet.

Projektet skal gennemføres gradvist, begyndende med ét enkelt forsøgspunkt, og kun efter de nødvendige godkendelser.



+

Forbedringsforslag

Nedenfor følger CLARYEL's forslag til drøftelse med beboerne og administrationen. De er ikke en del af det godkendte projekt og er ikke en juridisk udtalelse: hvert forslag bør kontrolleres med administratoren og om nødvendigt med en specialist i databeskyttelse.

FORSLAG TIL DRØFTELSE · 1

Konsekvensanalyse vedrørende databeskyttelse

Før installationen gennemføres og dokumenteres en konsekvensanalyse (DPIA, artikel 35 i GDPR), eller det forklares skriftligt, hvorfor den ikke er påkrævet i dette tilfælde.

FORSLAG TIL DRØFTELSE · 2

Information til beboere og forbipasserende

Opsætning af informationsskiltet efter Garante Privacys model for kameraovervågning og udarbejdelse af den fulde oplysning efter artikel 13 i GDPR under hensyntagen til vejledningen fra Garante og EDPB om kameraovervågning.

FORSLAG TIL DRØFTELSE · 3

Skriftlig opbevaringspolitik

Fastsætte i reglerne: 24 timer som standard, listen over tilladte undtagelser, hvem der beslutter en forlængelse, og hvordan en forlænget optagelse slettes.

FORSLAG TIL DRØFTELSE · 4

Stille timer og højttalergrænser

Om natten kun lys eller nedsat lydstyrke, et maksimalt antal gentagelser pr. hændelse og en pause mellem advarslerne.

FORSLAG TIL DRØFTELSE · 5

Overvågning af sabotage og fejl

Særskilte meddelelser til administratoren, hvis kameraet tildækkes eller flyttes, billedet ændrer sig, punktet går offline, eller batteriet er ved at være fladt.

FORSLAG TIL DRØFTELSE · 6

Overvågning af punktets »hjerteslag«

Punktet sender jævnligt et signal til serveren om, at det fungerer; udebliver signalet, modtager administratoren en besked.

FORSLAG TIL DRØFTELSE · 7

Beskyttelse af forbindelse og lagring

Kryptering af radioforbindelsen (for eksempel WPA3 og en WireGuard-tunnel), krypteret lagring af klip, adgangslog, opdatering af kameraets firmware og ændring af fabriksadgangskoderne.

FORSLAG TIL DRØFTELSE · 8

Adgang med to personer

Visning og eksport af klip kun i nærværelse af to udpegede personer, med registrering i loggen.

FORSLAG TIL DRØFTELSE · 9

Kontrol af masker før idriftsættelse

Vise beboerne et billede med maskerne anvendt og vedlægge det generalforsamlingens referat før idriftsættelse; gentages efter enhver justering af kameraet.

FORSLAG TIL DRØFTELSE · 10

Målinger for forsøgsfasen

Registrere falske alarmer og oversete registreringer, aftale kriterier for »fortsæt / fortsæt ikke« på forhånd og fremlægge en rapport for generalforsamlingen.

FORSLAG TIL DRØFTELSE · 11

Kanaler til meddelelser

Meddelelserne dannes på den lokale server og indeholder kun en skriftlig besked uden billeder; generalforsamlingen vælger leveringsmåden og foretrækker løsninger uden skytjenester fra tredjepart; alle kan framelde sig når som helst.

FORSLAG TIL DRØFTELSE · 12

Dataminimering

Ingen ansigtsgenkendelse, ingen aflæsning af nummerplader, ingen lydoptagelse; der gemmes kun det, der er nødvendigt for den konkrete hændelse.

FORSLAG TIL DRØFTELSE · 13

Vinterautonomi

Kontrollere energireserven i solpanel og batteri på korte, overskyede dage og fastlægge på forhånd, hvordan punktet opfører sig ved lavt batteri.

FORSLAG TIL DRØFTELSE · 14

Placering af skilte

Skiltene placeres før indgangen til den filmede zone og er tydeligt synlige både dag og nat.

FORSLAG TIL DRØFTELSE · 15

Regelmæssig gennemgang

Regelmæssigt, for eksempel én gang om året, fremlægge en rapport for generalforsamlingen om systemets drift, zoneindstillingerne og opbevaringsperioderne.

FORSLAG TIL DRØFTELSE · 16

Rapportskabelon til politiet

En formular forberedt på forhånd: dato og klokkeslæt, strækning, beskrivelse, klip, kontakt til den bemyndigede repræsentant, hvem der bekræftede hændelsen og hvornår.

?

Ofte stillede spørgsmål

Vil kameraet filme vinduer, altaner og private grunde?

Nej. Disse dele af billedet dækkes med uigennemsigtige sorte masker direkte i kameraet, før overførsel og optagelse. Den kunstige intelligens analyserer kun et smalt bælte langs hegnet.

Hvem kan se videoen?

Kun særligt udpegede personer. Beboerne modtager skriftlige meddelelser uden fotos eller video og har ingen adgang til kameraet eller arkivet. Enhver adgang til arkivet logges.

Hvor gemmes data, og hvor længe?

Kun på den lokale server på ejendommen, i krypteret form, uden sky eller tredjepartstjenester. Der er ingen kontinuerlig optagelse: korte hændelsesklip slettes, som et foreløbigt forslag, automatisk efter 24 timer; længere opbevaring kun ved et begrundet behov.

Kan jeg fravælge meddelelser?

Ja. Tilmeldingen er frivillig, og du kan til enhver tid stoppe med at modtage beskeder.

Hvad med falske alarmer?

Systemet skelner mennesker fra træer, buske, dyr og regn, og advarsler udløses kun, når en person er bekræftet. Politiet kontaktes kun efter bekræftelse fra en bemyndiget person. Falske alarmer kontrolleres i forsøgsfasen.

Vil systemet genkende ansigter eller nummerplader?

Nej. Projektet omfatter ikke ansigtsgenkendelse, identifikation af bestemte personer eller overvågning af køretøjer.

Hvad kommer det til at koste?

Omkostningerne er endnu ikke fastlagt. De drøftes særskilt, når de tekniske løsninger er aftalt med beboerne og administrationen.

§

Juridiske henvisninger

Officielle kilder, der er nyttige for drøftelsen. Linkene er kun til orientering og erstatter ikke professionel rådgivning.

Forordning (EU) 2016/679 (GDPR) — officiel udgave ↗ — https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32016R0679
Især artikel 13 (oplysning) og artikel 35 (konsekvensanalyse).

Italiensk lov om beskyttelse af personoplysninger — lovdekret 196/2003 ↗ — https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2003-06-30;196
Normattiva, gældende udgave.

Italiensk civillov, artikel 1122-ter — kameraovervågning af fællesarealer ↗ — https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:regio.decreto:1942-03-16;262~art1122ter
Normattiva.

Italiensk civillov, artikel 1136 — generalforsamlingens beslutningsdygtighed og beslutningers gyldighed ↗ — https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:regio.decreto:1942-03-16;262~art1136
Normattiva.

Garante Privacy — Kameraovervågning ↗ — https://www.garanteprivacy.it/temi/videosorveglianza

Temaside fra den italienske databeskyttelsesmyndighed.

Garante Privacy — Ofte stillede spørgsmål, vejledning og skiltmodel for kameraovervågning ↗ — https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9496574

Vejledning om forenklet oplysning (skilt) og opbevaringsperioder.

EDPB — Retningslinjer 3/2019 om behandling af personoplysninger via videoudstyr ↗ — https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_it

Det Europæiske Databeskyttelsesråd.

Lokale forhold

Ejendommen ligger i kommunen Fino Mornasco (provinsen Como). De nedenfor nævnte organer er mulige parter for koordinering: projektet forudsætter ingen allerede indgåede aftaler med dem.

I enhver nødsituation gælder altid det europæiske alarmnummer 112.

Kommunen Fino Mornasco ↗ — https://www.comune.finomornasco.co.it/

Kommunal administration og lokalpoliti (Polizia Locale): koordinering om lokale regler og skilte.

Arma dei Carabinieri ↗ — https://www.carabinieri.it/

Den lokalt kompetente station: en mulig aftalt procedure for anmeldelser.

✉

Dit forslag eller din kommentar

Projektets første fase er drøftelse med beboerne. Fortæl os, hvad der kan forbedres, og hvad der giver anledning til spørgsmål eller tvivl.

Eller kontakt os direkte

CLARYEL Perimetro — Dette er et projekt til drøftelse med beboerne og ejendommens administration. Det kan kun gennemføres efter de nødvendige godkendelser.

Indholdet er kun til orientering og udgør ikke juridisk rådgivning.

CLARYEL SRLS · Fino Mornasco (CO) · Momsnr. 04258140138 · CLARYEL's websted: claryel.com