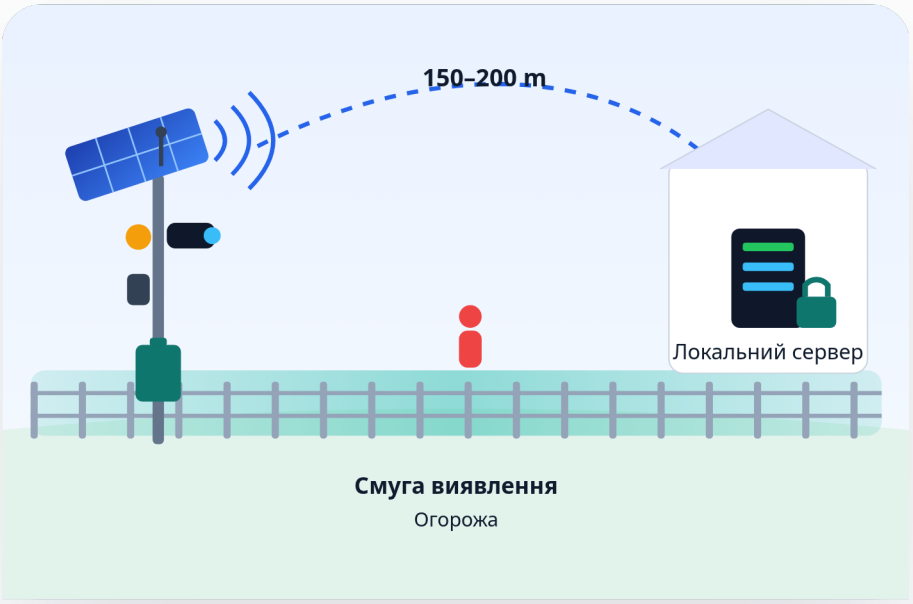
БЕЗПЕКА СПІЛЬНОЇ ТЕРИТОРІЇ КОНДОМІНІУМУ

CLARYEL Perimetro

Проєкт автономної інтелектуальної системи охорони спільної території

Одна автономна точка інтелектуального відеоспостереження вздовж огорожі. Усі дані зберігаються лише в нас, на території кондомініуму, у зашифрованому вигляді: жодних хмар, жодних сторонніх сервісів, усе тільки локально.

- Тільки локально
- Зашифровано
- Без хмари
- Миттєве блокування за будь-якої тривоги



КЛЮЧОВИЙ ПРИНЦИП

Усе залишається в нас — на території кондомініуму

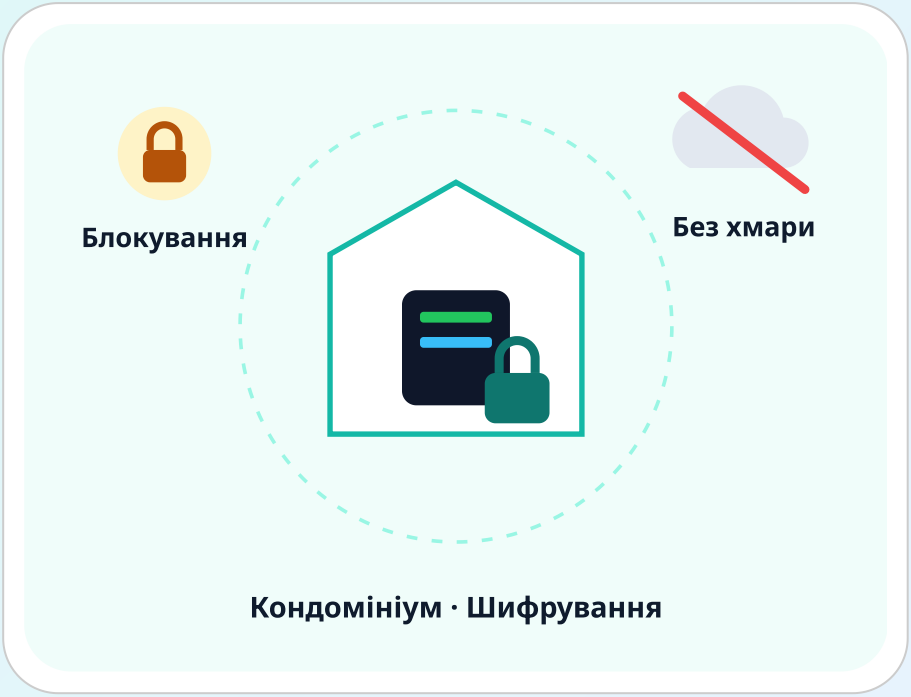
Усі зображення, фрагменти подій і журнали зберігаються лише на локальному сервері в будинку, на території кондомініуму.

Уся інформація зберігається та передається в зашифрованому вигляді.

За будь-якої тривоги всю інформацію можна миттєво заблокувати: доступ до архіву закривається, а фрагменти події захищаються від зміни та видалення.

Жодних хмар і жодних сторонніх сервісів: обробка штучним інтелектом і зберігання відбуваються тільки локально.

- Локальний сервер у будинку
- Шифрування
- Миттєве блокування
- Без хмари
- Без сторонніх сервісів



АЛЬТЕРНАТИВА ВІДЕОКАМЕРІ

Виявлення за сигналами Wi-Fi: без зображень, без ідентифікації

- Без камери
- Без зображень
- Без ідентифікації
- Тільки локально

Як альтернативу відеокамері вздовж огорожі можна встановити два Wi-Fi-пристрої — по одному на кожному кінці контрольованої ділянки.

За сирими даними сигналу Wi-Fi між двома пристроями (його змінами, відомими як CSI — Channel State Information) система визначає контури людей, що рухаються в смузі, без будь-якого зображення та без ідентифікації особи.

Цю технологію вже досліджують усередині житлових приміщень: наприклад, дослідження «DensePose From WiFi» Університету Карнегі — Меллона відновлює силуети людей у кімнаті лише за сигналами Wi-Fi. Ми пропонуємо застосувати її назовні, вздовж огорожі.

Система визначає лише присутність, напрямок руху та анонімний силует. Обробка відбувається на локальному сервері в зашифрованому вигляді, як і в усьому проєкті, і вмикає ті самі попередження: світло, голосове повідомлення та сповіщення мешканцям.

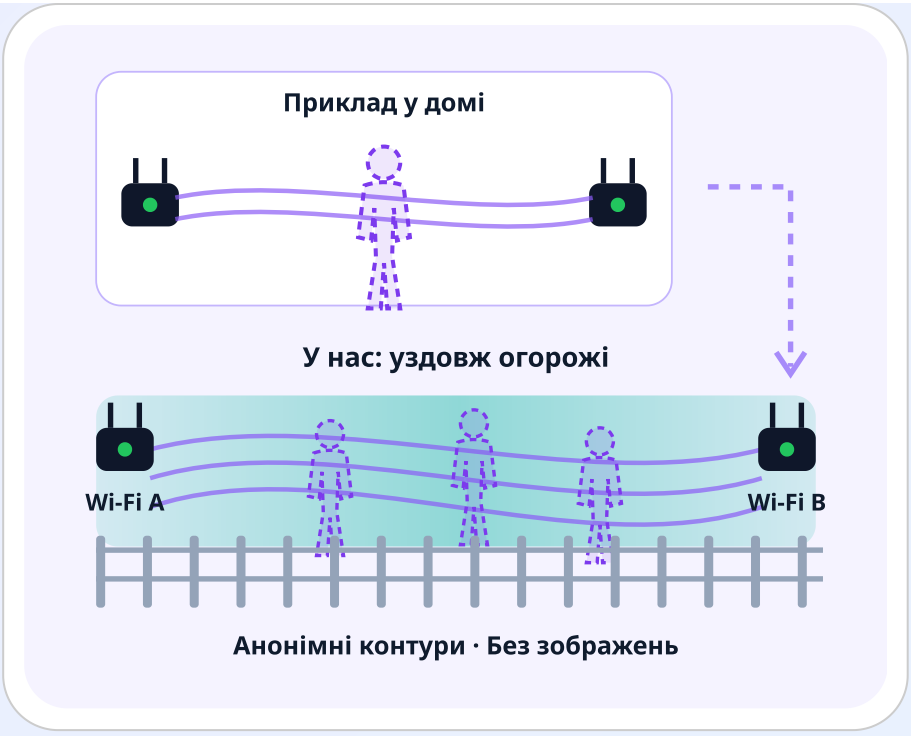
Правовий аспект — потребує перевірки з DPO або консультантом

Виявлення за Wi-Fi не знімає зображень і відео, тому це не система відеоспостереження, і спеціальні правила щодо відеоспостереження (наприклад, інформаційна табличка, передбачена Garante для камер) як такі не застосовуються.

Проте GDPR залишається застосовним, якщо дані можуть стосуватися ідентифікованої або такої, що може бути ідентифікована, особи (ст. 4 п. 1 GDPR). Тому систему спроєктовано так, щоб обробляти лише анонімну присутність і контури, без ідентифікації, тільки локально та в зашифрованому вигляді.

Цю оцінку необхідно підтвердити з DPO або консультантом до встановлення; вона не є юридичною гарантією.

Приклад у житловому приміщенні: «DensePose From WiFi», Університет Карнегі — Меллона (arXiv) ↗



01

Мета проєкту

Пропонується встановити одну автономну точку інтелектуального відеоспостереження вздовж огорожі спільної території кондомініуму.

Система призначена для виявлення можливого несанкціонованого проникнення, попередження порушників і оперативного інформування мешканців.

Основні принципи проєкту:

01

Мінімальне втручання в приватне життя.

02

Контроль лише вузької смуги вздовж огорожі.

03

Повністю локальна обробка зображення штучним інтелектом.

04

Відсутність обов'язкових хмарних сервісів.

05

Шифрування інформації, що передається та зберігається.

06

Автоматичні попередження та сповіщення мешканцям.

07

Можливість оперативного звернення до правоохоронних органів.

02

Обмеження відеоспостереження та захист приватності

Камеру буде спрямовано виключно на заздалегідь визначену ділянку спільної території безпосередньо вздовж огорожі.

Усі частини зображення, на яких можуть бути видні сусідні приватні ділянки, вікна, балкони та інші простори за межами контрольованої зони, буде повністю закрито непрозорими чорними масками.

Маскування виконується безпосередньо в камері, до передавання чи запису відеопотоку.

Крім того, програмно задається вузька смуга виявлення. Штучний інтелект не аналізуватиме об'єкти поза цією зоною.

Система не передбачає розпізнавання облич, ідентифікації конкретних людей, відстеження транспортних засобів чи спостереження за повсякденним життям мешканців.



03

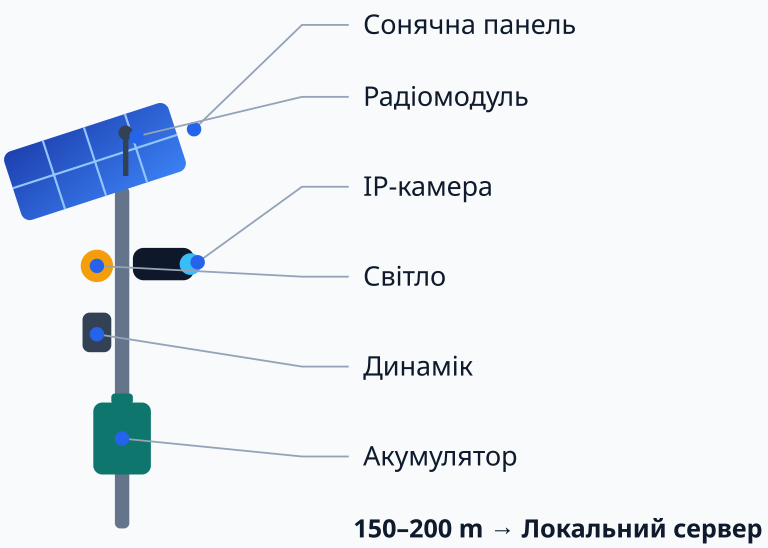
Автономне обладнання

Віддалений вузол буде оснащено IP-камерою, сонячною панеллю, акумулятором, модулем бездротового зв'язку, попереджувальним світлом і невеликим динаміком.

Орієнтовна відстань до локального сервера — 150–200 метрів.

Зображення передаватиметься захищеним бездротовим каналом на сервер, розташований у будинку.

Система не залежатиме від зовнішнього інтернету. Доступ до інтернету потрібен лише для надсилання сповіщень поза локальною мережею та для можливого звернення до правоохоронних органів.



04

Локальний штучний інтелект

На локальному сервері працюватиме спеціалізований алгоритм комп'ютерного зору.

Попередньо планується аналіз зображення з частотою два кадри на секунду з можливістю підвищення частоти за потреби.

Система відрізнятиме людей від руху дерев, кущів, тварин, дощу та інших природних змін у зображенні.

Попередження спрацьовуватимуть лише тоді, коли в заданій зоні підтверджено присутність людини.

Крім того, можна аналізувати напрямок руху, перетин віртуальної межі та час перебування в контрольованій смузі.



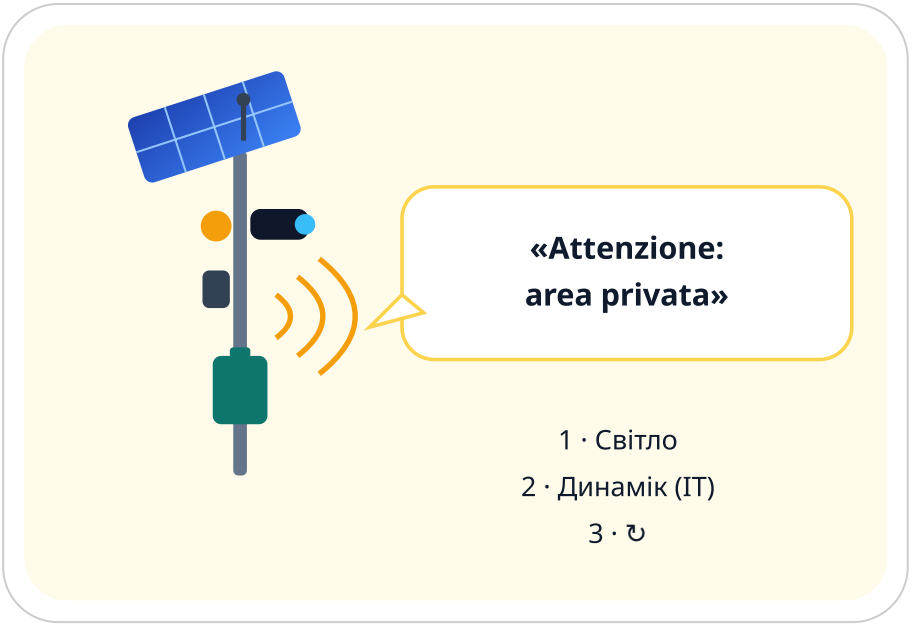
05

Автоматичне попередження на місці

Коли людина з'являється в захищеній зоні, система зможе:

1. Увімкнути попереджувальне світло.
2. Відтворити голосове повідомлення італійською мовою про те, що людина перебуває на приватній території.
3. За потреби повторити попередження в установлених межах.

Гучність, години роботи та умови спрацьовування буде налаштовано так, щоб мінімізувати незручності для мешканців.



06

Сповіщення всіх мешканців

Усі зацікавлені мешканці зможуть отримувати сповіщення на мобільний телефон без надсилання фотографій чи відеозображень.

Наприклад:

> **«Увага! На контрольованій ділянці огорожі виявлено людину. Система ввімкнула попередження.»**

Для отримання звичайних сповіщень мешканцям не знадобиться доступ до камери чи архіву.

Підписка на сповіщення буде добровільною. Кожен учасник зможе відмовитися від отримання повідомлень.

Адміністратор системи керуватиме лише списком одержувачів і налаштуваннями сповіщень.

Повідомлення надсилатимуться з дотриманням вимог щодо захисту контактних даних учасників.



07

Реагування на підтверджене проникнення

Передбачено додатковий режим підвищеної тривоги.

Він може вмикатися, якщо система виявляє послідовність ознак можливого проникнення, наприклад:

- Людина перетнула встановлену межу огорожі.
- Вона продовжує рух у бік внутрішньої території.
- Вона перебуває в зоні, де люди зазвичай не проходять.
- Подію підтверджено аналізом кількох кадрів.

У такому разі система зможе автоматично зберегти відеофрагмент і надіслати мешканцям термінове сповіщення.

Можливість звернення до поліції

Технічна архітектура дає змогу підготувати автоматичне повідомлення для правоохоронних органів.

У разі підтвердженого проникнення система зможе підготувати:

- Голосове повідомлення італійською мовою з адресою, характером події та часом виявлення.
- Кілька зображень або короткий відеофрагмент.
- Інформацію про місце події.
- Контактні дані уповноваженого представника кондомініуму.

Для екстрених випадків передбачено швидкий дзвінок до поліції через уповноважену особу.

Надалі інформацію та зображення можна буде передавати електронною поштою, захищеним електронним каналом або іншим офіційно погодженим засобом зв'язку.

Повністю автоматичне звернення безпосередньо до поліції можливе лише за наявності відповідного офіційно погодженого порядку взаємодії. До його погодження дзвінок і передавання зображень здійснюватимуться після підтвердження уповноваженою особою.

Це необхідно, щоб уникнути необґрунтованих звернень через технічні помилки чи хибні тривоги.



08

Зберігання даних і керування доступом

Усе зберігається тільки локально, на території кондомініуму, у зашифрованому вигляді. За будь-якої тривоги інформацію можна миттєво заблокувати. Жодних хмар і жодних сторонніх сервісів.

Відеопотік оброблятиметься на локальному сервері без використання зовнішніх сервісів штучного інтелекту.

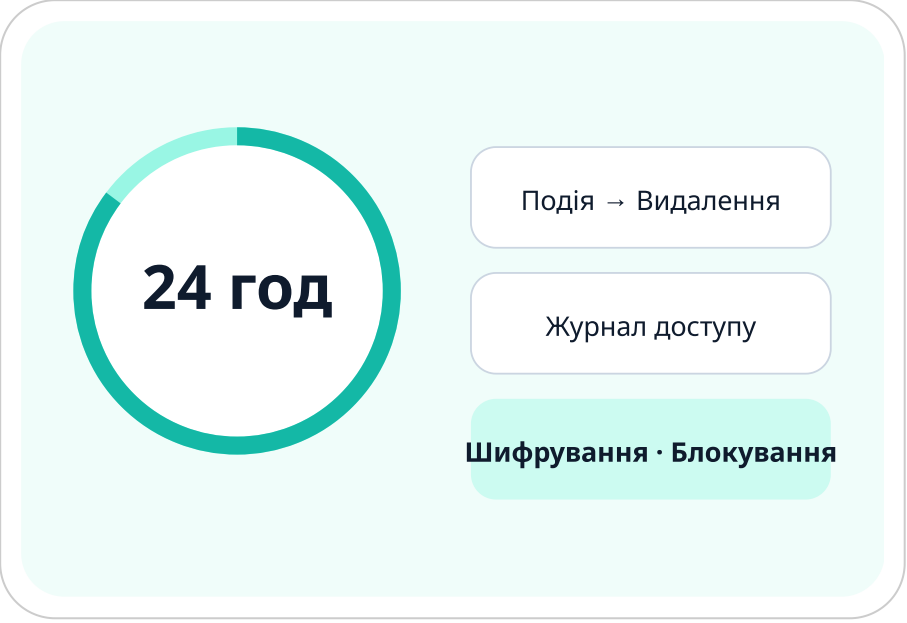
Безперервний запис усього відеопотоку не планується. За потреби зберігатимуться короткі фрагменти, що стосуються виявлених подій.

Як попередня пропозиція, звичайні записи автоматично видалятимуться через 24 години. Довше зберігання конкретної події допускається за обґрунтованої потреби, наприклад для передавання матеріалів правоохоронним органам.

Доступ до зображень надається лише спеціально призначеним особам.

Звичайні мешканці отримують письмові сповіщення, але не мають доступу до камери.

Усі звернення до архіву фіксуються в системному журналі.



09

Необхідні погодження

Для реалізації пропонується такий порядок:

Перший етап — обговорення з мешканцями.

Публікація технічного опису проєкту та збір зауважень.

Другий етап — погодження з адміністрацією.

Адміністратор кондомініуму отримує опис системи, план розміщення камери, схему обмеження контрольованої зони та правила обробки даних.

Третій етап — рішення загальних зборів.

Встановлення обладнання на спільній території виноситься на голосування відповідно до статей 1122-ter і 1136 Цивільного кодексу Італії.

Четвертий етап — розроблення правил експлуатації.

Кондомініум визначається контролером даних. За потреби призначається технічний оператор системи з обмеженими повноваженнями.

Затверджуються правила доступу, строки зберігання, порядок сповіщення мешканців і використання відеозаписів.

Встановлюються обов'язкові інформаційні таблички про відеоспостереження.

П'ятий етап — експериментальна експлуатація.

Після отримання необхідних дозволів встановлюється одна експериментальна точка. Перевіряються надійність виявлення, хибні тривоги, якість зв'язку, живлення та сповіщення.

Надсилання повідомлень безпосередньо правоохоронним органам розглядається окремо з відповідними службами.

10

Висновок

Запропонована система є автономною інтелектуальною охоронною установкою, призначеною виключно для контролю обмеженої ділянки спільної території.

Її завдання — не стежити за мешканцями, а вчасно виявити можливе проникнення через огорожу, попередити порушника та поінформувати мешканців.

Локальна обробка штучним інтелектом, обмежене поле зору, фізичне маскування приватних зон і відсутність вільного доступу до відеозаписів мають забезпечити високий рівень захисту приватності.

Надалі систему може бути доповнено засобами оперативної взаємодії з правоохоронними органами.

Проєкт передбачається реалізовувати поетапно, починаючи з однієї експериментальної точки, і лише після необхідних погоджень.



Локально · Маска · Шифрування

+

Пропозиції щодо вдосконалення

Нижче наведено пропозиції CLARYEL для обговорення з мешканцями та адміністрацією. Вони не є частиною затвердженого проєкту й не є юридичним висновком: кожну пропозицію варто перевірити з адміністратором і, за потреби, з фахівцем із захисту даних.

ПРОПОЗИЦІЯ ДЛЯ ОБГОВОРЕННЯ · 1

Оцінка впливу на захист даних

До встановлення провести й задокументувати оцінку впливу (DPIA, ст. 35 GDPR) або письмово пояснити, чому в цьому випадку вона не потрібна.

ПРОПОЗИЦІЯ ДЛЯ ОБГОВОРЕННЯ · 2

Інформування мешканців і перехожих

Встановити інформаційну табличку за зразком Garante Privacy для відеоспостереження та підготувати повне повідомлення за ст. 13 GDPR з урахуванням рекомендацій Garante та EDPB щодо відеоспостереження.

ПРОПОЗИЦІЯ ДЛЯ ОБГОВОРЕННЯ · 3

Письмова політика зберігання

Закріпити в правилах: 24 години за замовчуванням, перелік допустимих винятків, хто ухвалює рішення про продовження і як видаляється продовжений запис.

ПРОПОЗИЦІЯ ДЛЯ ОБГОВОРЕННЯ · 4

Тихі години та обмеження динаміка

Уночі лише світло або знижена гучність, максимальна кількість повторів на одну подію та пауза між попередженнями.

ПРОПОЗИЦІЯ ДЛЯ ОБГОВОРЕННЯ · 5

Контроль втручання та несправностей

Окремі сповіщення адміністратору, якщо камеру закрили чи зрушили, змінилося зображення, вузол вийшов з мережі або розряджається акумулятор.

ПРОПОЗИЦІЯ ДЛЯ ОБГОВОРЕННЯ · 6

Контроль «пульсу» вузла

Вузол регулярно надсилає серверу сигнал про роботу; якщо сигнал пропав, адміністратор отримує повідомлення.

ПРОПОЗИЦІЯ ДЛЯ ОБГОВОРЕННЯ · 7

Захист каналу та сховища

Шифрування радіоканалу (наприклад, WPA3 і тунель WireGuard), зашифроване зберігання фрагментів, журнал доступу, оновлення прошивки камери та зміна заводських паролів.

ПРОПОЗИЦІЯ ДЛЯ ОБГОВОРЕННЯ · 8

Доступ удвох

Перегляд і вивантаження фрагментів лише в присутності двох призначених осіб із записом у журналі.

ПРОПОЗИЦІЯ ДЛЯ ОБГОВОРЕННЯ · 9

Перевірка масок перед запуском

Показати мешканцям кадр із накладеними масками й долучити його до протоколу зборів до запуску системи; повторювати після кожного переналаштування камери.

ПРОПОЗИЦІЯ ДЛЯ ОБГОВОРЕННЯ · 10

Показники експериментального етапу

Фіксувати хибні тривоги та пропуски, заздалегідь погодити критерії «продовжуємо / не продовжуємо» і представити звіт зборам.

ПРОПОЗИЦІЯ ДЛЯ ОБГОВОРЕННЯ · 11

Канали сповіщень

Сповіщення формуються на локальному сервері й містять лише письмове повідомлення без зображень; спосіб доставки обирають збори, віддаючи перевагу варіантам без сторонніх хмарних сервісів; кожен може відписатися будь-коли.

ПРОПОЗИЦІЯ ДЛЯ ОБГОВОРЕННЯ · 12

Мінімізація даних

Без розпізнавання облич, без зчитування номерних знаків, без запису звуку; зберігати лише те, що потрібно для конкретної події.

ПРОПОЗИЦІЯ ДЛЯ ОБГОВОРЕННЯ · 13

Зимова автономність

Перевірити запас енергії сонячної панелі та акумулятора в короткі похмурі дні й заздалегідь визначити поведінку вузла при низькому заряді.

ПРОПОЗИЦІЯ ДЛЯ ОБГОВОРЕННЯ · 14

Розміщення табличок

Таблички розміщуються перед входом до зони зйомки й добре видні вдень і вночі.

ПРОПОЗИЦІЯ ДЛЯ ОБГОВОРЕННЯ · 15

Періодичний перегляд

Регулярно, наприклад раз на рік, представляти зборам звіт про роботу системи, налаштування зони та строки зберігання.

ПРОПОЗИЦІЯ ДЛЯ ОБГОВОРЕННЯ · 16

Шаблон звернення до поліції

Заздалегідь підготовлена форма: дата й час, ділянка, опис, фрагменти, контакт уповноваженого представника, хто й коли підтвердив подію.

?

Поширені запитання

Чи зніматиме камера вікна, балкони та приватні ділянки?

Ні. Ці частини зображення закриваються непрозорими чорними масками безпосередньо в камері, до передавання та запису. Штучний інтелект аналізує лише вузьку смугу вздовж огорожі.

Хто може переглядати відео?

Лише спеціально призначені особи. Мешканці отримують письмові сповіщення без фото й відео та не мають доступу до камери чи архіву. Кожне звернення до архіву фіксується в журналі.

Де і скільки зберігаються дані?

Лише на локальному сервері на території кондомініуму, у зашифрованому вигляді, без хмар і сторонніх сервісів. Безперервного запису немає: короткі фрагменти подій, як попередня пропозиція, автоматично видаляються через 24 години; довше зберігання — лише за обґрунтованої потреби.

Чи можна відмовитися від сповіщень?

Так. Підписка добровільна, і ви можете будь-коли припинити отримувати повідомлення.

А як щодо хибних тривог?

Система відрізняє людей від дерев, кущів, тварин і дощу, а попередження спрацьовують лише після підтвердження присутності людини. До поліції звертаються лише після підтвердження уповноваженою особою. Хибні тривоги перевіряються на експериментальному етапі.

Чи розпізнаватиме система обличчя або номерні знаки?

Ні. Проєкт не передбачає розпізнавання облич, ідентифікації конкретних людей чи відстеження транспортних засобів.

Скільки це коштуватиме?

Вартість ще не визначено. Її буде обговорено окремо, після погодження технічних рішень із мешканцями та адміністрацією.

§

Нормативні посилання

Офіційні джерела, корисні для обговорення. Посилання мають інформаційний характер і не замінюють професійної консультації.

Регламент (ЄС) 2016/679 (GDPR) — офіційна версія ↗ — https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32016R0679
Зокрема ст. 13 (інформування) і ст. 35 (оцінка впливу).

Кодекс Італії про захист персональних даних — законодавчий декрет 196/2003 ↗ — https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2003-06-30;196
Normattiva, чинна редакція.

Цивільний кодекс Італії, ст. 1122-ter — системи відеоспостереження на спільних частинах ↗ — https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:regio.decreto:1942-03-16;262~art1122ter
Normattiva.

Цивільний кодекс Італії, ст. 1136 — скликання зборів і чинність рішень ↗ — https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:regio.decreto:1942-03-16;262~art1136
Normattiva.

Garante Privacy — Відеоспостереження ↗ — https://www.garanteprivacy.it/temi/videosorveglianza
Тематична сторінка італійського органу із захисту даних.

Garante Privacy — FAQ, посібник і зразок таблички щодо відеоспостереження ↗ — https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9496574
Роз'яснення щодо спрощеного інформування (табличка) і строків зберігання.

EDPB — Настанови 3/2019 щодо обробки персональних даних за допомогою відеопристроїв ↗ — https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_it
Європейська рада із захисту даних.

Місцевий контекст

Кондомініум розташований у муніципалітеті Fino Mornasco (провінція Комо). Перелічені нижче органи — можливі сторони для координації: проєкт не передбачає жодних уже укладених із ними домовленостей.

У будь-якій надзвичайній ситуації завжди діє єдиний європейський номер екстреної допомоги 112.

Муніципалітет Fino Mornasco ↗ — https://www.comune.finomornasco.co.it/
Муніципальна адміністрація та місцева поліція (Polizia Locale): координація щодо місцевих правил і табличок.

Arma dei Carabinieri ↗ — https://www.carabinieri.it/
Територіально компетентна станція: можливий погоджений порядок звернень.

✉

Ваша пропозиція або зауваження

Перший етап проєкту — обговорення з мешканцями. Розкажіть, що можна покращити і що викликає запитання чи сумніви.

Або зв'яжіться з нами напряму

CLARYEL Perimetro — Це проєкт для обговорення з мешканцями та адміністрацією кондомініуму. Реалізація можлива лише після необхідних погоджень.

Матеріали мають інформаційний характер і не є юридичною консультацією.

CLARYEL SRLS · Fino Mornasco (CO) · ПДВ 04258140138 · Сайт CLARYEL: claryel.com