

Video surveillance in apartment buildings

More and more apartment buildings are equipping themselves with video surveillance systems to ensure the **safety** of their residents.

However, if used indiscriminately, such systems can lead to **abusive surveillance of the lifestyle or behavior** of the data subjects, thereby infringing their privacy.



For what purposes can a video surveillance system be installed in an apartment building?

Personal data may be collected for **several purposes**, provided that these purposes are:

- **determined**;
- **explicit**;
- **legitimate**; and
- **not further processed** in a manner incompatible with these purposes

By virtue of this principle of **purpose limitation**, the APDP considers that, given the intrusive nature of video surveillance systems, the implementation of such devices is permissible only in the context of the following security requirements:

- to ensure the safety of people;
- to ensure the security of property;
- to allow for the gathering of evidence in the event of an offence

What justification is needed to install a video surveillance system?

To be lawful, automated processing of personal data must meet at least one of the requirements set out in Article 5 of Law no. 1.565 of December 3, 2024.



The APDP thus considers that the installation of a video surveillance system **can only be justified by a legitimate interest** pursued by the data controller or by a third party, **provided that the interest or the fundamental rights and freedoms of the data subject are not disregarded.**

The installation of cameras must be decided by the owner of the building or must be voted on by the co-owners in a general assembly meeting.

Data controllers very often highlight the need to protect themselves against the risks of theft and assault.

The APDP is, however, very vigilant in ensuring that the rights and freedoms of the data subjects are respected, in particular by ensuring that the installation of the cameras does not infringe on their private sphere.



Sometimes, data controllers set up cameras to combat the risk of vandalism or damage. In this respect, the APDP recalls that images from cameras may only be used in case of an **event constituting an offence.**



What safeguards should be put in place to respect the privacy of the data subjects?

The data subjects concerned by a video surveillance system installed in an apartment building are of course the **residents and their visitors**, but also the **staff working there** as well as **any service provider** who may intervene in the said building.

Given the intrinsically intrusive nature of video surveillance systems, the APDP recall that these:

- must not lead to **permanent and inappropriate** surveillance of residents or their visitors;
- must not allow the **work or working hours** of staff or service providers to be monitored.

This is how the APDP considers that cameras can film:

- the entrances and exits of the building, being careful, however, to film only the surface area that is strictly necessary;
- the common areas (entrance hall, car park, bicycle or stroller room, lift doors).

On the other hand, the APDP considers that the installation of video surveillance systems is **strictly prohibited**:

- in the pathways or corridors used to access flats;
- when pointing towards the entrance doors to the flats;
- inside elevators;
- at the level of the private terraces;
- at the level of a swimming pool or a gym;
- in offices or employees' workstations;
- when pointing towards entrances, windows, courtyards and/or terraces of a neighboring building.



What information may be collected?

In accordance with the provisions of Article 4 of Law no. 1.565 of December 3, 2024, the collected personal data must be "*adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed*".

The APDP considers that the following information may be collected and processed:

- identity: image, face, silhouette and voice of people;
- electronic identification data: connection logs of the persons authorized to access the images;
- time information and timestamp: camera location and identification, date and time the image was captured.

The APDP considers that the **collection of voice** in the case of video surveillance processing appears to be manifestly excessive in the light of the objectives pursued by this processing.



Indeed, the collection of voice in order to ensure the safety of property and people can lead to **inappropriate** surveillance with regards to the data subjects.



How long can data from a video surveillance system be kept?

In accordance with Article 84 of Law no. 1.565 of December 3, 2024, the retention of images from video surveillance systems must not exceed **30 days**.



How to inform data subjects?

In accordance with Article 10 of Law no. 1.565 of December 3, 2024, any video surveillance system must be brought to the attention of the data subjects.

To this extent, Article 84 of the Law provides that in places **not open to the public**, the data subject shall be informed by the data controller in a **visible and permanent** manner by means of a **notice board placed inside the premises concerned or by appropriate information to the data subjects**.



The **notice board** referred to in Article 84 must include at least:

- the purposes of the processing;
- the identity of the data controller;
- the information relating to the exercise of the rights of the data subject;
- the retention period;
- if appointed, the contact details of the Data Protection Officer;
- a link to more complete information.



Video surveillance devices installed in places not open to the public **shall be brought to the attention of the APDP**. This is the case for residential buildings.



Who can access the data from the video surveillance system?

Access to video surveillance data must be limited to **only those persons** who, in the context of their function(s), can **legitimately have access to the data with regards to the objectives of the system**.

For apartment buildings, the APDP considers that images should not be accessible to all residents and believes that, as a general rule, only the following are authorized:

- the property manager;
- the building manager;
- the guardian(s)/concierge(s).

The latter are often the only ones allowed to view the images as they appear; the other categories of people generally only have access to the images on a deferred basis in the event of problems.



Display screens must be located **out of sight of people who are not authorized to access the images**. In addition, when the screen is located in the concierge's lodge or apartment, the screens must be **put on standby** on a regular basis and activated by a password **deemed to be strong**.

The APDP considers that the technical service provider may also have access to the device as part of its maintenance missions. In this respect, access rights must be limited to what is **strictly necessary for the execution of his or her contract**. In addition, the said provider is subject to the same security and confidentiality obligations as those imposed on the data controller.

Finally, the communication of images to the Police Department (Direction de la Sûreté Publique) may be justified for the purposes of a **judicial investigation**.

The APDP recalls however that in the event of transmission, the said Department may only have access to information within the strict framework of its legally conferred missions.



What security measures should be put in place?

The APDP considers that the data controller must take **all necessary precautions to protect the security of the data** being processed and to prevent unauthorized access, in particular by implementing control and identification measures.

In general, the APDP considers that any data controller should ask themselves the following questions before installing cameras:

- Is the server located in a closed room, accessible only to those authorized to access it?
- Are there remote monitors or PCs? Where are they located and what is their purpose? Are they (monitors) out of the public eye? How are PCs secured (e.g. secured session, anti-virus, etc.)?
- Are there connection logs (traceability) of the personnel authorized to access the images and processing?
- Is the server protected by a login and password specific to each person authorized to access it?

- Is there remote access (PCs, tablets, smartphones, etc.)? If so, are these connections protected by a user-specific login and password? Is the connection secure (HTTPS, VPN, others...)?
- How many cameras are deployed?
- Are the cameras mobile? Do they have a zoom function? Is the sound recording feature enabled?
- For data extraction:
 - who is in charge of the extraction (e.g. the service provider) and what is the procedure?
 - on which medium is the extraction done (USB key, CD, etc.)?
 - Is the medium encrypted? Is the information encrypted?