

Video surveillance of private homes

Many private individuals are increasingly using video surveillance systems in order to protect themselves, for example, by **detering** burglaries in the absence of the owner or tenant.

While the use of such a system is not problematic in itself, the use of it in the presence of **domestic employees** or **non-casual service providers such as home helpers** requires certain special precautions.

Indeed, these systems allow the collection of personal data within the meaning of Article 2 of Law No. 1.565 of December 3, 2024, namely the image of individuals.

Used indiscriminately, however, 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 a private home?

Personal data can be collected for **several purposes** providing 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, considering the intrusive nature of these video surveillance systems, the installation of such systems is permissible only in the context of the following security requirements:

- to ensure the safety of people;
- to ensure the security of property;
- to enable access control;
- 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.**



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 a private home, 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 home.

The installation of cameras must therefore be carried out in such a way as to film **only the private spaces concerned**, taking particular care to ensure that the neighborhood (through windows, bay windows, etc.) is not exposed to said video surveillance.

Furthermore, given the **intrinsically intrusive** nature of video surveillance devices for domestic employees, the APDP recalls 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.

Cameras must not film employees all the time.

Remote access allowing images to be viewed **in real time**, from a computer, tablet, smartphone or any other device **while a domestic employee is present in the home** infringes the rights and freedoms of the said employee.

The APDP also considers that the installation of a video surveillance devices is **strictly prohibited** on premises made available to employees, such as:

- the changing rooms;
- the toilets;
- the bathrooms;
- the offices;
- the bedrooms;
- any private area made available to employees for relaxation or lunch breaks.



What information may be collected?

In accordance with the provisions of Article 4 of Law No. 1.565 of 3 December 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.

About voice or, more generally, sound



The APDP considers such a collect to be particularly **sensitive, as any person visiting the home is subject to it (relatives, friends, etc.)**. It therefore prohibits its use in the presence of third parties.



How long can data from a video-protection 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**.



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**.

In addition, the communication of images to the Police Department 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.



How to inform data subjects?

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

This information must be provided in an appropriate manner and communicated by any means the data controller deems appropriate.

Thus, in the case of employees, this can be done, for example, by means of a mention in the employment contract, an amendment or an information note.

With regard to occasional or non-occasional service providers (delivery persons, plumbers, home nurses, etc.), the APDP considers that, at the very least, information should be provided verbally to the latter when entering residential premises subject to video surveillance.

Finally, the APDP considers that prior information of the data subjects may also be done by means of a **notice board** which must include at least, in accordance with Article 84 of Law No. 1.565 of December 3, 2024:

- a pictogram representing a camera;
- the exercise of the rights of the data subject;
- the data retention period;
- a link to more complete information.



Video surveillance devices installed in private homes must be **brought to the attention of the APDP, as soon as people outside the family or friendship circle intervene in the said homes** (e.g. domestic staff, home helpers).



What security measures should be put in place?

The APDP considers that the data controller must take **all necessary precautions to safeguard the security of the data** subject to processing and to prevent, in particular by putting in place control and identification measures, unauthorized employees from gaining access to the data.

In this respect, the APDP asks in particular that the people assigned to operate the system receive **strict instructions** with due regard to confidentiality.

The APDP admits that, in special circumstances relating to the **need to prevent or punish attacks on persons or property**, data may be extracted and/or copied in order to be kept on a separate medium with a view to communicating images and identification elements to the judicial or police authorities legally authorized to receive such a delegation.

However, the APDP requests that this medium and the information stored on it be protected, until it is destroyed or the information erased, by security devices and procedures which, on the one hand, **encrypt the medium** to ensure secure access to the information for authorized persons only and, on the other hand, **guarantee the authenticity, reliability and legibility of the data**, taking into account the state of the art.