

The ten commandments of video surveillance

You operate a restaurant, a shop, you run a company or a public service, you are co-owner and you want to use a video surveillance device.

There are some things that you must know!

Preliminary

Under Article 83 of Law No. 1.565 of December 3, 2024, a video surveillance system is "*any operation consisting of the capture, transmission, recording, and exploitation of images taken in any place, whether public, open to the public, or private, by a natural or legal person under private law or a legal person under public law acting outside the exercise of its prerogatives as a public authority*".

1 – A formality you shall carry out

While Law No. 1.565 of December 3, 2024 no longer subjects video surveillance devices to the prior authorization of the APDP, It nevertheless requires that certain formalities be carried out by the data controllers.

Thus, under Article 85 of Law No. 1.565 of December 3, 2024, "*Video surveillance systems installed in **places open to the public** or filming the surroundings of public roads, areas open to the public or to public traffic, are subject to the **prior authorization of the Minister of State***".

Systems installed in places **not open to public** are brought immediately to the attention of the APDP.

In some cases, the data controller must also carry out an impact assessment, particularly when the surveillance is carried out on a large scale (shopping centre, etc.).

What do we mean by places open to the public and places not open to the public?

According to the explanatory memorandum, "*places open to the public*" should be understood to mean establishments such as a restaurant, a shopping mall, or an administration counter.

"*Places not open to the public*" are, for example, a private place (home, garage, etc.) or business premises such as offices or warehouses.

In the case of homes or any other place used for personal or domestic purposes, the declaration to the APDP must be carried out **only if people outside the family or friends' circle intervene in the home**, e.g. housekeepers, home helpers.

2 – A legitimate reason you shall find

In accordance with Article 4 of Law No. 1.565 of December 3, 2024, any data controller must ensure that personal data are "*processed in a lawful manner*".

To this end, Article 5 of the Law provides that to be lawful, the processing must meet at least 1 of the 6 requirements laid down by the Law.

In most case, the implementation of a video surveillance system will be justified by a **legitimate interest** pursued by the data controller.

Example: to protect one's shop and the valuables it contained against the risk of theft and to protect the staff against the risk of assault.

The video surveillance system may also be justified by a **legal obligation** to which the controller is subject or **for the purpose of public interests** pursued by private holding concessions of public utility or entrusted with a mission of general interest.

Example: the obligation in the specifications to install cameras to monitor sensitive installations.



The **consent of the data subject** may also be invoked, but this justification will be assessed very strictly by the APDP, particularly in view of the relationship of subordination arising from an employment contract concluded between the employer and his/her employee, and will need to be substantiated and explained.

3 – Your neighbors you shall not spy

Considering the intrusive nature of video surveillance systems, these must only be used for the following functions:

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

All other functionality shall be scrutinized very carefully by the Authority.



The APDP prohibits that video surveillance systems be used to **monitor the work or working hours** of staff and/or leading to **permanent and inappropriate monitoring** of the data subjects.

Thus, the Authority requests that no cameras be installed:

- in changing rooms, toilets, shower baths, changing rooms;
- in offices as well as private areas where employees can relax or take a lunch break,
- in waiting rooms or meeting rooms;
- in pathways or corridors used to access flats;
- in the direction of customers' tables in restaurants.

4 – You shall not listen to other people's conversations

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*".

Therefore, 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.

On the other hand, with regards to the collection of voice (audio) when operating a video surveillance system, the APDP frequently considers that such a collection is clearly excessive in view of the functionalities of the processing. Indeed, the collection of audio (voice), for example to ensure the safety of property and individuals, may lead to inappropriate surveillance of the data subjects. The Authority will therefore pay particular attention to the justification provided by the data controller.

5 – The data subjects, you shall inform

In accordance with Article 10 of the Law No. 1.165 of December 3, 2024, all video surveillance systems must be brought to the attention of the data subjects.

In this regard, Article 84 of the Law specifies that the public is informed of the presence of a video surveillance system in **places open to the public** by the data controller in a **visible and permanent** manner by means of a **notice board placed outside the related premises**.

In places **not open to public**, the same article provides that the data subject must be informed by the data controller in a **visible and permanent** manner by means of a **notice board placed inside the places concerned or by relevant 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.



6 – A right of access, you shall provide

The right of access is the right of any data subject to obtain from an entity having implemented a video surveillance system the confirmation that the information relating to the said data subject has been collected and the communication of this information in a written, non coded form consistent with the content of the recordings.

The entity is free to choose the methods by which the persons concerned can contact it to exercise their right of access (by post, by e-mail, by telephone, on site, etc.).

When a copy of the camera recording is provided, the rights of third parties must be preserved (blurring, etc.).

7 – Internal access, you shall restrict

Recorded images **should not be freely accessible** to all employees or customers.

The data controller must therefore ensure that only authorized persons have access to the images, **strictly for the purposes of fulfilling** their missions.

Furthermore, for each category of authorized persons who have access to the information (management, sales staff, IT provider...), the entity must determine precisely the rights that each of these categories has (viewing images as they happen, deferred consultation, deletion of images, maintenance, all rights, etc.).

The APDP pays particular attention to the categories of people who have access to information.

It also requires that a journal access log be implemented.

8 – Security measures, you shall take

In accordance with Article 31 of Law No. 1.565 of December 3, 2024, data controllers must take **appropriate technical and organizational measures** to ensure a **level of security adapted to the risks** to the rights and freedoms of individuals.

These risks include:

- Data destruction;
- Loss of data;
- Data alteration;
- Unauthorized data disclosure;
- Unauthorized access to personal data.

These risks may occur **accidentally** or **unlawfully**.

In addition, the various video surveillance architectures must be based on servers, peripherals, connection equipment (switches, routers, firewalls) that must be protected by a login and a regularly renewed password that is deemed to be strong, and all unused ports must be deactivated.

9 – Communications and remote access, you shall protect

The images from cameras are likely to be communicated to the Police Department and Monegasque Courts for the purposes of a judicial investigation or to insurers for the purposes of a compensation claim enquiry.

It is therefore important that any copy or extraction of the information collected during the processing is encrypted on the supporting medium (CD, USB key, and so on).

Moreover, remote accesses, where provided for, must be protected. The APDP requests that equipment allowing such access be imperatively protected by a **strong password** as well as by SSL-type protocols (https, VPN, etc.).

In addition, the APDP asks that they be configured to lock automatically after a short period of inactivity.

Finally, with regard to “smart phones”, tablets, and laptops in particular, the APDP asks that access to the application to view the images shall also be via a **strong password**.

10 – The retention period, you shall limit

In accordance with Article 4 of Law No. 1.565 of December 3, 2024, the personal data subject to the processing may only be kept in a form that allows the data subjects to be identified for a period not exceeding that necessary for the achievement of the purposes for which they are processed;

Article 84 of the Law also provides that images from video surveillance systems must not exceed **30 days**.

As a general rule, keeping the images for just a few days is enough to carry out the necessary checks in the event of an incident and to enable any possible criminal proceedings to be initiated.