

Installation of cameras in the workplace

Many employers today use video surveillance systems to ensure the safety of people or property on their premises, for example, or to protect access to buildings.

These systems often result in the collection of information that can be used to **identify a specific or identifiable individual**, even though this is sometimes not the intended purpose, thus raising particular problems in terms of the protection of personal data.



For what purposes can an employer set up a video surveillance system?

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 enable access control;
- to allow for the gathering of evidence in the event of an offence

In addition to these imperatives, there may be purposes specific to the activity of the employer concerned, such as, for example, assessing the equipment and workforce on the site when the employer is a public works company.

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 implementation of a video surveillance system can be justified by:

- compliance with a **legal obligation** to which the controller or its representative is subject;
- a reason of **public interest** pursued by a legal person governed by public law or by a legal person governed by private law entrusted with a mission of general interest or a public service concession;
- the fulfilment of a **legitimate interest** pursued by the controller or a third party, **provided that this does not adversely affect the interests or fundamental rights and freedoms of the data subject.**

The last justification is the one most often used by data controllers, who often consider the installation of cameras to be necessary to protect themselves against the risks of theft and assault.

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



The installation of a video surveillance system may in some cases be justified by the consent of individuals. However, this justification is assessed very strictly by the APDP, particularly in the context of an employment contract establishing a relationship of subordination between employer and employee.



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

It is up to the employer to demonstrate that the rights and freedoms of the data subjects will be protected.

Consequently, the APDP asks the employer to ensure that the video surveillance system implemented:

- does not make it possible to **monitor the work or working hours** of staff;
- does not lead to **permanent and inappropriate monitoring** of the data subjects.

This is why it considers that cameras can film:

- the entrances and exits of buildings/offices, taking care, however, to film only the area strictly necessary so as not to film any neighboring buildings;
- the emergency exits;
- the **main** traffic areas;
- the places where goods are stored;
- the production machinery, provided that employees are not filmed;
- the technical premises;
- archives;
- areas that may be considered sensitive (e.g. server rooms);
- Indoor, outdoor and/or underground parking lots, provided that the neighboring buildings are not filmed;
- delivery or loading areas, delivery and unloading docks, provided that neighboring buildings are not filmed.

However, the APDP considers that the installation of video surveillance systems is **strictly prohibited** :

- in the garage workshop, the production workshop, the workshop, the assembly/dismantling workshop;
- In the changing rooms, showers, toilets;
- In the staff offices or workstations;
- In the waiting rooms;
- at the reception desk;
- in the private areas made available to employees for relaxation or lunch breaks (rest rooms, kitchens, sofas, smoking areas, etc.);
- in the trade union premises and those of the Staff Delegates and their access when these lead only to these premises;
- towards the accesses, windows, courtyard(s) and/or terraces of neighboring buildings.



In addition, it points out that cameras must not film employees at their workstations, except in specific, duly justified circumstances. For example, a camera may film an employee handling money, provided that it is positioned in such a way as to film the cash register rather than the cashier.



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 and silhouette 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.

The APDP will therefore **pay particular attention to the justification** provided by the employer.

For example: a camera may be authorized in an « *interrogation room* » in the event of theft and/or offences when its purpose is to protect both the persons being interrogated and the shop staff.



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**.



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**.

This could be the in-house manager of a shop, who may have access to delayed viewing of the images in the event of an offence; reception staff, who may have access to the images for ongoing viewing; or the service provider, who may have access to the processing as part of the maintenance of the system.

With regard to the latter, the APDP points out that its access rights must be limited to what is **strictly necessary for the performance of its service provision contract**. In addition, the service provider is subject to the same security and confidentiality obligations as those imposed on the data controller.



When the Human Resources Department has access to the images, the APDP points out that such access for consultation purposes may only be carried out in the context of a disciplinary procedure in line with the purposes of the processing, i.e. in the event of an attack on the safety of property or individuals.

The APDP also considers that the communication of data to the Police Department (Direction de la Sûreté Publique) may be justified for the purposes of a **judicial investigation**.

In this respect, it points out that in the event of transmission, the aforementioned department may only have access to the 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 surveillance system must be brought to the attention of the data subjects.

In this respect, article 84 of the Law specifies that the public must be 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 premises concerned**.

In places **not open to the public**, this same article provides that 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 providing 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 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**.

Video surveillance systems installed in **areas not open to the public** are immediately **brought immediately to the attention the APDP**.



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?