

Workplace surveillance

PROFESSIONAL MESSAGING: CAN I ACCESS THE WORK EMAILS OF MY EMPLOYEES?

No, except under certain conditions.

For the APDP, the **respect of the privacy of private correspondence** is an intangible principle. Thus, the employer cannot access the contents of the private messages of their employees sent or received from the work messaging system, without the said employee being present and **expressly** agreeing to it.

However, for messages to be considered personal, employees should identify them as such, for example:

- by specifying in the subject line of the message keywords like « **private** », « **[PRV]** », or even « **personal** »;
- by including in the subject line of the message a mention that clearly suggests that the said message is private, such as « **vacation in Japan** »;
- by storing messages in a folder named « **personal** » or « **private** ».

Furthermore **only a judge's authorization** can allow the employer to lawfully access the private messages of its employees when the latter have not authorized the employer to read their private messages, even if the employer has legitimate grounds to suspect acts of unfair competition or any other infringement of its interests or of the law. This may take the form of a court order instructing a bailiff to access or even record the private messages in question.

To learn more:

- Factsheet [Focus on professional messaging at work](#)

PROFESSIONAL MESSAGING: IF AN EMPLOYEE IS TEMPORARILY ABSENT, CAN I GRANT ACCESS TO THEIR PROFESSIONAL EMAIL TO A SUBSTITUTE?

Yes. To ensure the **continuity of the company's business** during the absence of an employee (holidays, illness...), the APDP considers that the employer may have access to the professional messages of the said employee using one of the following methods:

- setting up an automatic out-of-office reply to the sender with the names of people to contact in case of emergency;
- designating a substitute who has personalized access rights to their colleague's messaging system;
- forwarding all incoming messages to a substitute.

In the last two cases, the employee must be **informed of the identity of their substitute**, and this substitute must not read messages **identified as private or personal**.

To learn more:

- Factsheet [Focus on professional messaging at work](#)

ACCESS TO THE PREMISES: CAN I INSTALL A MAGNETIC BADGE ACCESS CONTROL SYSTEM FOR MY PREMISES?

Yes, provided that the implementation of such a system has no other purposes than:

- to control access to the entrances and exits of the company;
- to control access to certain premises specifically identified as subject to circulation restrictions, justified by the safety of the property and the people working there (such as the computer room);
- to manage employee schedules and attendance times;
- to control visitor access;
- to allow, if necessary, the collection of evidence in case of a violation.

The employees must be informed of the aforementioned usage and the data collected.

Furthermore, in accordance with Article 4 of Law No. 1.565 of December 3, 2024, personal data subject to processing may only be retained in a form that allows identification of the individuals concerned for a **duration not exceeding what is necessary for the purposes for which they are processed**.

Also, for example, time-related information or time stamps and those concerning accesses should not be kept for more than **3 months, unless they are used for monitoring the attendance** of employees in the company or organization, in which case the period is extended to **5 years**, in accordance with the limitation period for payroll and wage processing specified in Article 2092 bis of the Civil Code.

To learn more:

- Factsheet [Non-biometric access to business premises, with or without control of hours](#)

RECORDING TELEPHONE CONVERSATIONS: CAN I RECORD MY EMPLOYEES' TELEPHONE CONVERSATIONS IN THE WORKPLACE?

No, unless for a specific purpose or in case of a legal obligation.

For example, it is possible to have test phone calls made by mystery clients to a customer service department, but recording **should not be systematic** and employees **should not be penalized** based on a recording.

On the other hand, it is required for banking institutions **to record client orders for evidentiary purposes**.

In all cases, employees must be informed of the implementation of any conversation recording device.

They must also be able to use an **unrecorded telephone**, either personal or provided by the employer, or have **the option of disconnecting the recording** for their own personal calls.

To learn more:

- Factsheet [Listening to and recording telephone calls at work](#)

GEOLOCATION: CAN I INSTALL A GEOLOCATION SYSTEM IN MY EMPLOYEES' COMPANY VEHICLES?

Yes under certain conditions. The APDP considers that, given the intrusive nature of vehicle geolocation devices and the information that may be associated with them, the implementation of such devices is only acceptable within the following functionalities:

- the safety or security of the employee themselves or of the goods or vehicles in their care (delivery vehicle drivers, lone workers, cash and valuables transport, etc.)
- a better allocation of resources for services to be carried out in dispersed locations (emergency interventions, breakdown fleets, etc.);
- the monitoring and invoicing of a transport service for people or goods or a service directly related to the use of the vehicle (school transportation, cleaning of the roadside, etc.);
- the monitoring of working hours, when this monitoring cannot be carried out by other means.

On the other hand, the use of a geolocation system is not justified when the employees have freedom in organizing their travels (medical representatives, sales representatives, etc.)

If the use of the vehicle for private purposes is allowed, the geolocation function **must be deactivated outside working hours**.

Finally, employees must be **aware of the system** and the data collected.

To learn more:

- Factsheet [Geolocation of vehicles provided to employees](#)

CAMERAS IN THE WORKPLACE: CAN I INSTALL CAMERAS IN MY ESTABLISHMENT?

Yes, but only for the following security purposes:

- to ensure the safety of people;
- to ensure the security of property;
- to enable access control;
- to allow for the gathering of evidence in case of an offense.

In addition to these requirements, there may be other functions specific to the employer's business, such as assessing equipment and personnel on a construction site if the employer is a public works company.

However, it is up to the employer to demonstrate that the rights and freedoms of the data subjects will be protected by **not allowing the monitoring of the work or working hours of staff**, and by **not conducting permanent and inappropriate monitoring of the data subjects**.

The APDP therefore 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 believes that the installation of video surveillance systems is strictly prohibited in:

- the workshops (production, assembly/disassembly...) where employees work, unless there is a specific justification;
- the changing rooms, restrooms, shower rooms, toilets;
- the offices as well as all private areas made available to employees for relaxation or lunch breaks;
- the trade union premises and their access when they only lead to those premises.

Furthermore, cameras should not film employees at their workstations, except in specific circumstances that are duly justified. For example, a camera may film an employee handling money, but it must be oriented in such a way as to focus more on the cash register than on the cashier.

To learn more:

- Factsheet [**Installation of cameras in the workplace**](#)
- Factsheet [**Location of CCTV cameras: what is allowed and what is prohibited**](#)

CAMERAS IN THE WORKPLACE: DO I HAVE TO INFORM MY EMPLOYEES AND VISITORS ABOUT THE PRESENCE OF CAMERAS IN MY ESTABLISHMENT?

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 a minimum:

- 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.

To learn more:

- Factsheet [Installation of cameras in the workplace](#)

BIOMETRIC DEVICES: CAN I USE A BIOMETRIC DEVICE BASED ON FINGERPRINT RECOGNITION TO MONITOR MY EMPLOYEES' WORKING HOURS?

No. The APDP expressly excludes the use of fingerprints for the purpose of managing employee schedules and attendance times.

It considers that fingerprint recognition poses specific difficulties in that it is a particularly traceable form of biometrics.

This is because it is not assigned by a third party or chosen by the individual, but comes directly from the individual's body and identifies them definitively. Consequently, the misuse or misappropriation of such data can have serious consequences.

The APDP therefore strictly regulates this method. Thus, while it authorises the use of fingerprint recognition devices in certain circumstances, the APDP considers that the implementation of such processing can have no other function than to control access to certain areas within the company or organisation that are subject to restricted access for reasons of security of property and persons working there.

BIOMETRIC DEVICES: CAN I INSTALL A BIOMETRIC DEVICE (FINGERPRINT, FACIAL RECOGNITION, OR OTHER) FOR AUTHENTICATION PURPOSES TO UNLOCK IT DEVICES SUCH AS A LAPTOP OR MOBILE PHONE?

The APDP authorises the use of biometric devices for the purpose of controlling access to professional IT equipment and applications that have been **specifically identified** by the data controller.

The implementation of such a device may be justified by the pursuit of a **legitimate interest** by the data controller or a third party, **provided that it does not infringe on the fundamental rights and freedoms of the data subject**.

In exceptional cases, the use of a biometric device may also be based on the consent of the data subjects. However, the APDP assesses this justification **particularly strictly**, especially when an employment contract establishes a **relationship of subordination** between the employer and the employee.

In any event, the data controller must **demonstrate the necessity** of the device. If a non-biometric system (e.g. a badge system) is sufficient to guarantee the security of the devices and/or

applications, or if these are not particularly sensitive, the use of biometrics is not justified.

In accordance with Ministerial Order no. 2025-361 of July 14, 2025 implementing Article 35 of Law no. 1.565 of December 3, 2024 on the protection of personal data, such a system is deemed likely to present a **high risk to the rights and freedoms of the individuals concerned**.

Consequently, the data controller is required to carry out an **impact assessment on personal data protection** prior to any deployment and to **document the reasons and justifications** for choosing biometrics over a less intrusive technology.