Non-biometric access to business premises, with or without time controls

In an increasingly secure environment, and faced with the growing risks of industrial espionage, the number of access control systems in the workplace is on the rise.

These systems use means of varying degrees of complexity, requiring the use of digital and/or IT tools, and even electronic communications systems. They may involve magnetic cards, with or without contact, combined with a device for reading the cards, which may or may not record the information they contain. Other types of device are also used, such as secret codes issued only to authorized persons.

The very essence of such systems lies in the **need to identify** people in order to monitor those who enter the workplace or certain restricted areas. This surveillance therefore extends to their identity, as well as the date, time and door through which they gained access to the premises.

For what purposes can an employer set up an access control 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 access control systems, the implementation of such devices is permissible only in the context of the following security requirements:

- control access to the entrances and exits of a company, organization or apartment building;
- control access to certain premises identified as being subject to traffic restrictions, justified by the safety of goods and people working there;
- manage employee schedules and attendance times;
- control visitor access;
- enable evidence to be gathered in the event of an offence.

What justification is needed for the implementation of an access control 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 an access control system can be justified by:

- compliance with a **legal obligation** to which the controller or its representative is subject;
- the performance of a **contract** or **pre-contractual measures** with the data subject;
- 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 installation of an access control 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 employees?

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

These systems must not be diverted from their intended purpose. Under no circumstances may they :

- lead to **permanent and inappropriate monitoring** of the data subjects;
- enable **monitoring of the number of hours** allocated by law to **staff and trade union representatives** for the performance of their duties;
- enable the **monitoring of movements within the entity**, with the exception of areas specifically identified as being subject to traffic restrictions.

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 : surname, first name, internal registration number, photograph ;
- informations relating to professional life: department, function, time slots usually authorized, authorized access areas, holidays, telephone extension number ;
- time information or time stamps: date and time of entry, date and time of exit, date and time of passage to a restricted area ;
- access to premises : name and/or number of the entrance or exit door, or of the point of passage;
- car park : vehicule registration number, parking space number ;
- visitors : surname, first names, dates and times of visit, company, identity of the employee greeting the visitor;
- badge or card : badge or access car number, date of issue, date of validity.

How long can data collected and processed by an access control system be kept?

In accordance with article 4 of Law no. 1.565 of December 3, 2024, personal data which are the subject of processing may only be kept in a form which allows the data subjects to be identified for as long as is necessary to achieve the purposes for which they are processed.

The APDP therefore requests that :

- the badge be immediately deactivated as soon as the employee is no longer authorized to access the premises;

- the photo be deleted as soon as the badge is handed over;

- access data be deleted 3 months after they are recorded;

- data used to monitor working hours be kept for 5 years.

Who can access the data from the access control system?

Access to access control 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**.

Internally, this may be the IT manager for creating/deactivating badges, the Human Resources department for consulting timetables, or the service provider who has access to the system for maintenance purposes.

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 system is only set up for the purpose of accessing premises **without monitoring working hours**, the APDP points out that access for consultation by the Human Resources Department may only be carried out as part of a disciplinary procedure in line with the **purposes** of the processing.

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 access control system must be brought to the attention of the data subjects, whether employees, visitors or service providers.

As a minimum, these persons must receive the following information:

- **the identity and contact details of the data controller**, and where applicable, its **representative** established in Monaco or, failing that, within a Member State of the European Union;
- the **purposes** and **legal basis** for the processing**;**
- the **legitimate interests pursued by the data controller** or a third party where legitimate interests is the legal basis;
- the **categories of personal data** concerned;
- the **period for which the data will be stored** or, where that is not possible, the criteria used to determine that period;
- where processing is based on **consen**t, the right to withdraw consent **at any time;**
- the **recipients** or **categories** of recipients;
- the means of exercising **rights of access, opposition, rectification, deletion, limitation** or **portability**;
- the right to **lodge a complaint with the Autorité de Protection des Données Personnelles (APDP) ;**
- where applicable, the **contact details of the Data Protection Officer.**

The employer is **free** to decide how to communicate this information. In the case of employees, for example, this information could be posted or communicated by means of an internal company memo.

In the case of visitors, this information could, for example, take the form of a statement on the personal data collection form that they fill in, where applicable.

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 a non-biometric access control device:

- Are there authorized/unauthorized access zones depending on the type of people involved (employees, service providers, etc.)?

- What is the procedure for:
  - requesting a badge?
  - enrolling/creating a badge?
  - delivering a badge?

- How do the authorized person(s) connect to the access control system?

- Does each authorized person have an individual identifier and password?

- Is there an automated log (traceability) of access to the system?

- What is the security (login with individual identifier/password, anti-virus, etc.) :
  - of the access control server ?
  - of the workstations ?

- In the event of remote access (from outside) :
  - who has this access ?
  - by what means (VPN, point-to-point link, etc.)?
  - How secure is the equipment used?

- If the system breaks down, how do the doors « *open* »?