Biometric Access Control
to Professional Premises

1. Definition of Biometric Data

Article 2 of Law No. 1.565 of December 3, 2024 defines biometric data as « *personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that person, such as facial images or dactyloscopic data* ».

Biometrics therefore encompasses:

- physical characteristics: iris, voice, fingerprints, hand vein network, hand outline, etc.;
- behavioural characteristics: gestures, gait, etc.

These data are classified as **sensitive data** when processed for the **purpose of uniquely identifying or authenticating** a natural person. Under **Article 7 of Law No. 1.565**, an employer may only process such data if **strictly necessary for controlling access to workplaces** and to devices and applications in the course of employees' duties.

2. Permitted Purposes

In accordance with the **purpose limitation** principle, personal data may only be collected for purposes that are:

- specified;
- explicit;
- legitimate;
- not further processed in a manner incompatible with those purposes.

The APDP considers that the implementation of such systems is permissible only for the following security imperatives:

- controlling access to premises **specifically identified** by the data controller as requiring restricted circulation;
- where applicable, enabling the gathering of evidence in the event of an offence.

> **!** **Exclusive Purposes**
> These two purposes are exhaustive. Any other use — in particular monitoring attendance, managing working hours or disciplinary oversight — is strictly prohibited.

3. Lawful Bases for Processing

For processing to be lawful, it must be based on at least one of the grounds set out in **Article 5 of Law No. 1.565**. The APDP recognises the following bases for biometric systems in the workplace:

3.1 Legal Obligation

Where sector-specific regulations impose enhanced security requirements, compliance with a **legal obligation to which the data controller or their representative is subject** may constitute the legal basis for processing.

3.2 Legitimate Interest

The pursuit of a **legitimate interest** by the data controller or a third party may justify the system, **provided it does not override the interests or fundamental rights and freedoms** of the data subject. The data controller must document this balancing assessment.

3.3 Consent (Exceptional Basis)

Exceptionally, the consent of the data subjects may be relied upon. However, the APDP applies this basis **particularly strictly** in employment relationships, given the **relationship of subordination** inherent in the employment contract, which compromises the free exercise of consent. This basis may only be used where a non-biometric alternative is offered without any consequence for the professional situation of any employee who refuses to participate.

4. Safeguards for the Protection of Employees' Privacy

Biometric data are unlike ordinary identity data: they originate from the person's own body and identify them in a manner that is **permanent and irrevocable**. Their misuse or diversion may have serious and irreversible consequences. Their use must therefore be strictly regulated.

Biometric access control systems may under no circumstances:

- result in continuous or intrusive monitoring of the persons concerned;
- enable monitoring of employees' working hours or attendance;
- restrict employees' freedom of movement within the premises in the exercise of their duties.

4.1 Necessity Test

The data controller **must demonstrate** that the biometric system is necessary and proportionate. If a non-biometric system (badge, PIN, smart card) is sufficient to ensure the security of the premises, or if those premises present no particular sensitivity, the use of biometrics may not be justified.

4.2 Data Protection Impact Assessment (DPIA)

In accordance with **Ministerial Order No. 2025-361 of July 14, 2025** implementing Article 35 of Law No. 1.565, any biometric system is deemed likely to present a **high risk to the rights and freedoms** of the data subjects (sensitive data, vulnerable persons (employees)). Accordingly:

- a DPIA must be carried out prior to any deployment;
- the data controller must document the reasons and justifications that led to choosing biometrics over a less intrusive technology;
- data controllers who deployed a biometric system before Law no. 1.565 entered into force have, under its **Article 109**, a **3-year transitional period** to carry out a DPIA as part of a risk reassessment.

5. Data That May Be Collected

In accordance with the **data minimisation principle** (Article 4 of Law No. 1.565), only data that is adequate, relevant and limited to the purposes may be collected. The APDP considers the following categories to be admissible:

Category	Admissible Data
Identity	Surname, first name(s), photograph
Professional information	Department, job title, internal employee number, usual authorised time slots, authorised access zones
Timestamps	Date and time of access, date and time of access attempts
Premises access	Name and/or number of the premises
Biometric data	Template of one or more biometric characteristics
Support / authentication	Individual support number, authentication number, secret code (for Type 2 storage)

6. What about Biometric Template?

A template is a mathematical representation of a biometric characteristic. It constitutes the reference model used to subsequently identify or authenticate a person. A template does not reproduce the raw image of the characteristic (fingerprint, iris, etc.) but constitutes an abstract, non-reversible representation of it.

6.1 Authorised Storage Methods

For premises access control systems, two types of storage are permitted:

Type	Description	Example
Type 1 — Individual support (preferred)	Support held exclusively by the data subject (badge, smart card). The template is never stored in a centralised system.	The employee presents their badge: their fingerprints are compared to the template stored on that support.
Type 2 — Encrypted centralised database (exceptional)	Encrypted templates stored on a centralised server controlled by the employer. Authentication is two-factor: biometrics (something the person is) + individual secret code known only to them (something they know). Templates are unusable without that code. The biometric reader retains no data.	The employee first enters their PIN on the reader — the server identifies which template to retrieve. The employee then presents their biometric data. The server compares the two templates and, if both factors match, grants access.

! **General Rule**
Unless exceptional circumstances are duly documented and justified (premises of extreme sensitivity), Type 1 storage must be used. Type 2 may only be adopted as a last resort.

7. Data Retention Periods

In accordance with **Article 4 of Law No. 1.565**, data may only be retained in a form that permits identification for as long as necessary for the purposes pursued. The APDP sets the following periods:

Type of Data	Maximum Retention Period
Temporal information (timestamps)	3 months after recording — unless a duly documented sector-specific justification applies
Biometric template	Duration of the authorisation of the data subject. Immediate deletion upon expiry of that authorisation.
Other data (identity, professional information, premises access, support/authentification)	Duration of the authorisation of the data subject. Immediate deletion upon expiry of that authorisation.

8. Persons Authorised to Access the Data

Access to data must be limited to those persons who, in the course of their duties, may legitimately need it in light of the system's objectives.

8.1 Biometric Data (Templates)

Access to templates is strictly reserved for persons authorised to:

- manage the enrolment of data subjects;
- delete templates (upon departure or revocation of authorisation);
- carry out technical maintenance of the system.

8.2 Other Data

The following may in particular be authorised:

- the IT manager, for enrolment and modification or deletion of access profiles;
- personnel responsible for premises security;
- the maintenance contractor (data processor), strictly within the limits of their service contract. The APDP recalls that such a contractor is subject to the **same security and confidentiality obligations** as the data controller, and that their access rights must be limited to what is strictly necessary for the performance of their contract.

8.3 Disclosure to the Direction de la Sûreté Publique

Disclosure of data to the Direction de la Sûreté Publique (Police Department) may be justified for the purposes of a judicial investigation. Any such transfer must be strictly limited to the scope of the legally conferred duties of that Directorate and must be logged and documented.

9. Informing Data Subjects

In accordance with **Article 10 of Law No. 1.565** any system for controlling access to professional premises using biometric authentication must be brought to the attention of the data subjects (employees, visitors, contractors). This information must be provided **in writing** prior to the enrolment of biometric data and must contain at least the following:

- **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.**

10. System Security

The data controller must take all appropriate precautions to preserve the security of the data and prevent unauthorised access, in accordance with **Article 31 of Law No. 1.565**. Prior to any deployment, the following questions must be addressed:

10.1 Access Organisation and Control

- Are there particularly sensitive areas whose access should be restricted to certain employees only?
- How are access profile requests and the enrolment procedure managed?
- Does each authorised person have an individual username and password (no shared accounts)?
- Is automated logging (audit trail) of system access in place?

10.2 Protection of Biometric Data

- Are biometric data encrypted (at rest and in transit)?
- Is biometric template storage Type 1 (individual support) or Type 2 (centralised server + secret code)? If Type 2, are all security requirements met (encryption, two-factor authentication, no data retained on the reader)?

10.3 Equipment Security

- What is the security level of the biometric access control server (strong authentication, antivirus, firewall, etc.)?
- What is the security level of the workstation(s) connected to the system?

10.4 Remote Access

- Which profiles have remote access, and by what secure means (VPN, point-to-point link, etc.)?
- What is the security level of the equipment used for remote access?

10.5 Business Continuity

- In the event of a system failure, how are access points openings opened securely?
- Is an incident response procedure in place (deletion of compromised templates, re-enrolment)?

11. Applicable Legal References

Text	Subject Matter
Law No. 1.565 of 3 December 2024	Law on the Protection of Personal Data — Principality of Monaco
Article 2 — Law No. 1.565	Definition of biometric data
Article 4 — Law No. 1.565	Data processing principles: minimisation, storage limitation
Article 5 — Law No. 1.565	Lawful bases for processing
Article 7 — Law No. 1.565	Conditions for processing sensitive data
Article 10 — Law No. 1.565	Obligation to inform data subjects
Article 31 — Law No. 1.565	Security obligation for processing
Article 35 — Law No. 1.565	Data Protection Impact Assessment (DPIA)
Article 109 — Law No. 1.565	Transitional provisions — 3-year period to carry out a DPIA for existing systems
Ministerial Order No. 2025-361 of July 14, 2025	Implementation of Article 35 — criteria for determining whether a processing operation is subject to the AIPD