Biometrics brings together all the techniques used to identify an individual from his physical, biological and behavioral characteristics. These characteristics have the particularity to be unique and almost permanent throughout a person's life.

Biometric data are therefore personal data, the processing of which is subject to the provisions of Law 09-08 on the protection of individuals with regard to the processing of personal data.

The special nature of biometric systems constitutes a risk in terms of the protection of private life.

Certain biometric data may accidentally reveal information that was not provided for in the basic treatment, and which may constitute a serious invasion of the privacy of individuals. For example, the image of the iris used by an access control device is likely to reveal data on the health of the person.

For what purposes?

An organization can, under certain conditions, set up a biometric access control system in order to secure:

• Entrances to buildings and facilities.

• Access to premises subject to traffic restrictions.

Rules specific to biometric devices

A public or private body can use biometric data to control access to sensitive premises and installations subject to traffic restrictions and representing an issue major security, subject to meeting the following conditions:

The organization must justify that the methods access control alternatives are not sufficiently reliable to secure the site.

Biometric data must be recorded on a mobile medium held exclusively by the data subject, such as a smart card or a magnetic card.

In this event, the access control device must be used at authentication purposes and not identification.

Biometric data cannot be used in raw state. Therefore, the organization must carry out a partial extraction of the data as a limited number of elements characteristics (for example for the imprint digital, extract a limited number of points characteristics).

Exceptionally, the CNDP may authorize the creation of a database central biometric data for access control to very sensitive sites.

In this case, only the biometric data of the people whose mission requires a regular or temporary presence in the controlled site.

The duration of the conversation

Raw biometric data should only be kept for as long as necessary to the extraction of their characteristic elements.

When an organization is authorized to set up a central database, the information biometrics of an individual must be deleted as soon as the latter is no longer authorized to access at controlled sites.

Rights of data subjects

The body is required to inform the persons concerned - by means of an information note, for example - before the collection of their personal data.
The briefing note should include the following:
- The identity of the organization.
- The fact that the establishment processes biometric data.
- The purpose of processing (security and access control).
- Contact details for the exercise, by the persons concerned, of the rights of access, rectification and opposition.
- The number of the authorization issued by the CNDP.

Data security processed

The body must take all precautions useful for ensuring security and confidentiality biometric data processed, in particular by educating employees about preservation the integrity of their data on the media mobile.

Insofar as the organization calls on a external service provider authorized to access to employee biometric data, it is obligatory to frame the relationship by an act legal or contract that guarantees confidentiality and data security and, moreover general compliance with the rules relating to Protection of personal data.

Notification formalities at the CNDP

The installation of a biometric device must be the subject of an authorization request with the CNDP.

The authorization request must be accompanied by the following documents:

- A description of the biometric device.
- A commitment that attests that the system to be installed meets the conditions listed in the deliberation of the CNDP N ° 478-2013 and more generally the provisions of law 09-08.
- A model of the information note for persons concerned.
- A document attesting to the power of signature of the person authorized to engage the organization (Copy of the trade register or statutes).

facebook.com/CNDP.Maroc/ twitter.com/CNDP_Maroc

Address: Angle Boulevard Annakhil and Avenue Mehdi ben Barka, Immeuble Les Patios, 3 rd floor Hay Riad - Rabat Morocco - Tel: 05 37 57 November 24 - Fax 05 37 57 21 41
Website: http://www.cndp.ma