Resolution No. 478-2013 of 1 st November 2013 on the conditions necessary for the use of biometric devices for the control access.

The National Commission for the Control of Personal Data Protection , held on 1 st November 2013, under the chairmanship of Mr. Said Ihrai;

Were present Mrs. Souad El Kohen, Messrs Driss Belmahi, Abdelaziz Benzakour and Omar Seghrouchni;

Considering the Law n ° 09-08 promulgated by the Dahir 1-09-15 of February 18, 2009, relating to the protection of natural persons with regard to the processing of personal data (BO n ° 5714 of 05/03/2009);

Considering the Decree n ° 2-09-165 of May 21, 2009 taken for the application of the aforementioned Law n ° 09-08 (BO n ° 5744 of 06/18/2009);

Having regard to the Internal Regulations of the CNDP (approved by decision of the Prime Minister n ° 3-33-11 of March 28, 2011 / BO n ° 5932 of 04/07/2011);

Has adopted the following decision:

1. General framework

Biometrics brings together all the techniques used to identify an individual based on its physical, biological and behavioral characteristics. These characteristics have the particularity of being unique and almost permanent throughout life.

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

Aware of the impact of biometric techniques on the privacy of individuals and risks of violation of fundamental human rights and freedoms, the CNDP has defined certain rules that comply with international standards in the field, rules that must be observed by data controllers operating such systems.

The special nature of biometric systems constitutes a risk in terms of Protection of private life. Among other things, certain biometric data can reveal fortuitous way of information which was not provided for in the basic processing, and which can 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.

2. Rules for using biometric data for access control

The CNDP assesses, on the basis of the principle of proportionality, the advisability of authorizing the use of biometric data for access control depending on the nature of the site that the controller intends to secure.

The CNDP may authorize the use of biometric data for access control to sensitive premises and installations subject to traffic restrictions and representing a major security issue exceeding the strict interest of the organization under the following conditions:

1) The controller must justify that the alternative methods of access controls are not reliable enough to secure the site;

2) Only biometric data of a limited number of people, whose mission requires a regular or temporary presence in the site;

3) Biometric data cannot be used in the raw state. Therefore, the data controller must carry out a **partial extraction** of the data in the form of a limited number of characteristic elements (for example for fingerprint, extract a limited number of characteristic points);

4) The controller must not set up a database for store the collected biometric data. Moreover, in some cases individuals, and subject to very strict security measures, the constitution a database could be authorized by the Commission; As a general rule, the data should be recorded on a medium held exclusively by the data subject, such as a smart card or a magnetic card;

5) The biometric device must be used for authentication purposes and not identification.

3. Excluded purpose

Due to the excessive and disproportionate nature, the management of the attendance time of officials and employees may not be retained as the finality for the processing of biometric data.

4. Retention period of biometric data

The controller can only keep the biometric data in its raw state the time necessary for carrying out the operation of extracting the characteristic elements.

The biometric data used by the device must be deleted as soon as the the person concerned is no longer authorized to be present on the secure site.

5. Rights of data subjects

The data controller proceeds to:

a. The designation of the service (s) allowing the persons concerned to exercise their right of access, rectification and opposition guaranteed by articles 7, 8 and 9 of law 09-08 mentioned above.

b. Informing the persons concerned prior to the collection of their data personal and this, in accordance with article 5 of law 09-08 relating to the protection of natural persons with regard to the processing of personal data, in particular specifying in particular:

- ✓ the identity of the data controller and, where applicable, of his representative;
- ✓ the purpose of the processing,
- ✓ the recipients or categories of recipients;
- ✓ the compulsory or optional nature of the measures used to collect data;
- ✓ the existence of rights of access, rectification and opposition for persons concerned and the contact details of the service to which they should be sent to be worth ;
- ✓ the characteristics of the receipt for the authorization request of the National Commission for the Protection of Personal Data Staff ;

6. Security of biometric data

The data controller takes all necessary precautions to preserve the security and the confidentiality of the biometric data processed and, in particular to prevent them from being are destroyed, distorted, damaged or that unauthorized third parties can use them for misuse, in accordance with article 23 of the aforementioned law 09-08.

7. Formality of notification of processing to the CNDP

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

The aforementioned authorization request must be accompanied by a description of the device, biometric and a commitment that certifies that the system to be installed meets the conditions listed in this deliberation and more generally the provisions of Law 09-08.

Done in Rabat, November 01, 2013

President

Said Ihrai