To be filled out in the EDPS' office

REGISTER NUMBER: 651

NOTIFICATION FOR PRIOR CHECKING

Date of submission: 20/12/2010

Case number: 2010-1008

Institution: Frontex

Legal basis: article 27-5 of the regulation CE 45/2001(1)

(1) OJ L 8, 12.01.2001

INFORMATION TO BE GIVEN(2)

(2) Please attach all necessary backup documents

1/ Name and adress of the controller

Jose Carreira, Administration Division Director, Controller; Orlin Belchev, Head of Frontex Security Services Sector ("Frontex Security Officer"), Delegated Controller; Frontex, rondo ONZ, 00124 Warsaw, Poland

2/ Organisational parts of the institution or body entrusted with the processing of personal data

Administration Division, Security Services Sector

3/ Name of the processing

Access control system by iris scan technology

4/ Purpose or purposes of the processing

The processing consists of an iris scan technology coupled with a classic badge reader access control. Iris scan technology system is part of the security infrastructure that protects Frontex premises and IT systems which in turn support Frontex information gathering, analysis and operations and all other activities to coordinate the operational cooperation at the external borders of the Member States of the European Union.Frontex intelligence and operational data is subject to the security requirements specified in the Frontex Security Manual adopted with the Frontex Executive Director's Decision 48/2007. The Frontex Security Manual takes into account the principles of the Council Decision 2001/264/EC of 19 March 2001 adopting the Council's security regulation. Moreover, in some cases these data can be classified and corresponding additional EUCI security provisions must be applied. Frontex shall handle EUCI up to SECRET UE. Very stringent confidentiality and security requirements apply to processing such data in this context.
The system is not a multi-purpose system (i.e. will not be used, e.g., for monitoring staff' working hours).
The purpose of the system is twofold: 1) To ensure that only authorised persons have access to certain sensitive Frontex premises. This system is designed to control the identity and permit or deny access of persons entering and in some cases exiting from certain sensitive Frontex premises. Access to Frontex reception areas and to Frontex Administrative area does not require biometric authentication. The use of iris scan authentication is required for entry access to sensitive Frontex areas behind the reception and the Administrative area, such as Frontex Operations Division, Frontex Capacity Building Division, Executive Support, Management Floor and the ICT Unit, which handle sensitive and classified information.2) Be able to use the data to reconstruct events in case of significant security related incidents.The system consists of personal access cards (issued to each member of Frontex) and access readers. There are two types of access readers: the standard type ("card readers") which reads the access card and has it verified by the access point controller, and the "biometric reader" (LG iris camera) which can scan a person's iris pattern and match it with one of those stored in the database. Access will be granted or denied on the basis of the authorisations programmed in the system for that access card and the biometric iris pattern. There are 8 biometric readers in operation. In addition, there are a central database server for storage of access rights and access logging, another database server dedicated to the biometrics processing and two workstations connected to the servers. The workstations are in a secured control room with limited access. The enrolment of the user consists of two independent processes: - the card's unique identification will be registered in the access control system and linked to a person in the database; - the person's iris pattern will be scanned in the system and a digital template representing the pattern will be stored in the database

5/ Description of the category or categories of data subjects

Staff members (TA, CA), SNE, trainees. Regular contractors, consultants or visitors who need to access the sensitive Frontex areas and the secure areas within the Frontex premises. Other contractors, visitors, consultants (i.e. those who do not need to access regularly Frontex premises over a set period of time) are NOT enrolled in the iris scan system and are issued a generic badge while being escorted at all times by a Frontex Staff Member; therefore their personal data will therefore not be recorded in this system.

6/ Description of the data or categories of data*(including, if applicable, special categories of data (article 10) and/or origin of data)*

The categories of personal data collected include the name, biometric eye templates of both eyes, the time when the individual accessed (or tried to access) and the security areas controlled by the system.

7/ Information to be given to data subjects

The data subjects are informed as follows: STAFF MEMBERS: 1.staff members are informed prior to the enrolment, in the mandatory "induction" program;a presentation by Frontex Security Officer (Administrator) is done in which staff members can ask questions. Senior security guards can also provide answers, at a later stage, prior to the enrolment. 2. A mandatory awareness session is held every year, for all staff members (and not only for newcomers) even if they are already familiar with security rules; during this session, information is provided about biometrics. REGULAR VISITORS / CONTRACTORS : they are informed by Frontex Security Officer and or security guards. FOR BOTH STAFF MEMBERS AND REGULAR VISITORS / CONTRACTORS : 1) A privacy statement will be handed out to data subjects. 2) Ultimately, Legal Affairs Unit or the DPO can answer to any concerns regarding the legal basis or the effective exercise of their right to data protection.

8/ Procedures to grant rights of data subjects*(rights of access, to rectify, to block, to erase, to object)*

Data subjects have access at all time to the DPO; they can also ask to the data controller whether and how Executive Director Decision 2008 36 of 8 September 2008 adopting implementing rules concerning data protection at Frontex, has been applied and complied with in the processing at stake. In addition, data subjects will be provided a specific privacy statement informing them of the purpose of the processing, the way to exercise effectively their rights, inter alia, right of access and rectification and possibility to have recourse to internal bodies and to the EDPS. This will be done just before the enrolment process.

9/ Automated / Manual processing operation

The automated processing operation consists of the reading of personal access card by standard/biometric card reader; the transmission of data from reader to access point controller; the controller's storage and forwarding of the access logs to a central database server and the storage of information by the central database server. Regarding the manual processing, this will only happen in case of a security incident, in which case the Security Officer or the Senior Security Guard will log on to the access control database and retrieve the information as to who has entered or left Frontex premises at a certain time.

10/ Storage media of data

Digital media

11/ Legal basis and lawfulness of the processing operation

Based on Article 5(a) of the Data Protection Regulation (" necessary for the performance of a task carried out in the public interest on the basis of [the Treaties] or other legal instruments adopted on the basis thereof"). In addition, other relevant instruments are mentioned as follows: COUNCIL DECISION of 19 March 2001 adopting the Council's security regulations (2001/264/EC), 2001/844/EC,ECSC,Euratom: Commission Decision of 29 November 2001 amending its internal Rules of Procedure, Frontex Security Manual, The Frontex Regulation (Council Regulation (EC) No 2007/2004 of 26 October 2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union, Frontex Executive Director decision 48/2007

12/ The recipients or categories of recipient to whom the data might be disclosed

Frontex Security Services Sector; Director of Administration; Executive Director, Deputy Executive Director. Normally the data is processed solely within the Security Services Sector. Theoretically, in exceptional cases when a serious security breach has occurred and when Frontex Executive Director or Deputy Executive Director has issued a specific written instruction, some data related to the specific case at stake may be made available to the duly authorised internal investigation body as well as to authorised EU body (OLAF e.g.). It may exceptionally be disclosed to MS law enforcement or judicial authorities solely in case of criminal proceedings. However there has not been any case up to the moment.

13/ retention policy of (categories of) personal data

The retention period of the biometric personal data is for the duration the authorised stay of the relevant person inside sensitive Frontex areas premises. The iris biometric template is deleted immediately after the length of this stay, i.e. transfer of the data subject to a non secure area with no need to visit the secured areas, expiration of work contract or service contract (for contractors) etc. In such cases, Frontex Security Sector commits to delete the personal data until a maximum of three months after expiry / termination of contract or transfer above mentioned.

13 a/ time limits for blocking and erasure of the different categories of data
(on justified legitimate request from the data subject)
(Please, specify the time limits for every category, if applicable)

See above

14/ Historical, statistical or scientific purposes
If you store data for longer periods than mentioned above, please specify, if applicable, why the data must be kept under a form which permits identification,

Not envisaged so far

15/ Proposed transfers of data to third countries or international organisations

No transfers

16/ The processing operation presents specific risk which justifies prior checking (*please describe*):

AS FORESEEN IN:

X Article 27.2.(a)
Processing of data relating to health and to suspected offences, offences, criminal convictions or security measures,

□ Article 27.2.(b)
Processing operations intended to evaluate personal aspects relating to the data subject,

□ Article 27.2.(c)

Processing operations allowing linkages not provided for pursuant to national or Community legislation between data processed for different purposes,

□ Article 27.2.(d)

Processing operations for the purpose of excluding individuals from a right, benefit or contract,

□ Other (general concept in Article 27.1)
17/ Comments
PLACE AND DATE: Warsaw, 16 December 2010 DATA PROTECTION OFFICER: Sakari Vuorensola INSTITUTION OR BODY: Frontex