To be filled out in the EDPS' office

REGISTER NUMBER: 509

NOTIFICATION FOR PRIOR CHECKING

Date of submission: 20/5/2009

Case number: 2009-382

Institution:FRA

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
Costantinos MANOLOPOULOS (Head of Administration), European Union Agency for Fundamental Rights (FRA), Schwarzenbergplatz 11, A-1040 Vienna

2/ Organisational parts of the institution or body entrusted with the processing of personal data
De[partment Administration: Head of Administration, Security staff of the Agency (Roland Frankovics)
External security company G4S.

3/ Name of the processing
Security: Building Access System

4/ Purpose or purposes of the processing
1. To prevent unauthorised entry to FRA's offices and if necessary to investigate unauthorized entry to the FRA's offices
2. To ensure secure access to offices
3. To provide the Auditing services (CoA and IAS) when requested with figures on the attendance of staff members, in order to check correctness with the attendance sheets (known as holiday table). Data is available on request by the Head of Administration.

5/ Description of the category or categories of data subjects

Data subjects are staff members. They are provided with badges that enable staff member's identification.

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

Name of the staff member and his/her individual identification number are logged.

7/ Information to be given to data subjects

Staff members have been informed and the security policy and administartive note have been communicated to them (see Annex 1).
The security policy is available at the Agency's intranet and internet sites (see Annex 2).

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

§ Right to access data – Data Subjects have the right to access their data.
To exercise this right, data subjects have to:
1. Send a request to the Head of Administration, who will assess if the reason is legitimate in accordance to the Staff Regulations, Regulation 45/2001 and other related regulations and no restrictions apply.
a. Once the reason is proved valid, the Head of Administration will pass the request to the security staff member.
b. In case the reason is not proved valid, a response to the data subject will be given mentioning why access can not be provided.
2. A response mentioning whether the access request is valid or not should be provided within 10 working days upon official receipt of the request.
3. The security staff member must ensure, before providing access to the staff member, that information including only
the staff member in question is accessible for view. If another data subject is included then access to such footage will
not provided before receiving the consent of the involved staff member. Access to information will be provided within 5 working days upon approval of the request.

§ Right to block – The data subjects can request from the Data Controller the blocking of their personal data. Blocking is not possible in case of an official investigation.

§ Right to rectify – Rectification is not allowed due to the nature of the automatically recorded data following actions of the data subjects. However, the data subject can exercise his right of rectification on the report written by security staff in connection with a security incident.

9/ Automated / Manual processing operation

Automated processing operation.
The access data is recorded on a software called "ALPHwin". The data is taken out of the software and copied to the Security folder by the Security staff of the Agency where restricted access is given.

10/ Storage media of data

The access data is stored in a security folder accessible only by the Security Guards, Security staff and IT Administrator of FRA and will be deleted after 2 months. In accordance with Article 1.10.1 and 1.10.2 of the Framework Contract between FRA and Group 4 (see Annex 4). Group 4 can only act upon the instruction of FRA security staff. Therefore, FRA has control of access to data recorded as part of its security procedures.

11/ Legal basis and lawfulness of the processing operation

Art. 5 (a), (b), (d) and (e) of Reg. 45/2001

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

Data is disclosed to company Group 4 staff members working at the premises of the Agency. No data is transferred to external parties.

13/ retention policy of (categories of) personal data

The data will be deleted after 2 months according to the policy of retention of data collected as part of security procedures.

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)

Data subjects have access to their data as defined in Annex 1 and they have their right to block but can not modify or erase any data.

The data will be deleted after a maximum period of 2 months according to the policy of retention of data collected as part of security procedures.

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 applicable

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

Not applicable

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

AS FORESEEN IN:

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

17/ Comments

Annex 1 - Administrative note providing information to staff members
Annex 2 - Security policy
Annex 3 - Plan of installed access points and infrared detectors
Annex 4 - DP clause included in the FWC between FRA and G4S

Preventing unauthorised persons from using data-processing systems is guaranteed as the access to the recording tools is strictly limited.
Access to data is password protected and any action to the system is logged.
The security system is a stand-alone system so no access from the remaining IT systems is possible.

Data is only provided for on the spot inspection to Auditing services when a specific request for a staff member on a specific date is requested.
Therefore there is no transfer of data as such but access to view as part or auditing inspection.

PLACE AND DATE: Vienna, 18/05/2009

DATA PROTECTION OFFICER: Nikolaos FIKATAS

INSTITUTION OR BODY: European Union Agency for Fundamental Rights