To be filled out in the EDPS' office

REGISTER NUMBER: 508

NOTIFICATION FOR PRIOR CHECKING

Date of submission: 20/5/2009

Case number:2009-381

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

Department Administration: Head of Administration, Security staff of the Agency (Roland Frankovics)
External security company G4S.

3/ Name of the processing

Security: CCTV System

4/ Purpose or purposes of the processing

To prevent and if necessary to investigate unauthorized entry to the FRA's offices. The level of protection at specific areas needs to be improved to strengthen prevention measures.
Surveillance equipment is needed in order to monitor more closely the particularly sensitive areas (entrance-, -delivery, -garage and outer area). It will also be used to observe access and exit to and from the staff zone. CCTV cameras are only installed in areas highlighted in Annex 4 - CCTV building plan. The CCTV cameras are installed following consultation of the Security services of DG ADMIN and after an on the spot visit of DG ADMIN's Security expert at the building.
The CCTV footage can also be used to investigate security incidents which have occured.
No further cameras are installed inside the building. All floors include infrared detectors which are enabled after the closing hours of the Agency to ensure no trespassing.

5/ Description of the category or categories of data subjects

Data subjects are staff members and any other third party that enters the premises of the FRA.

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

Images caught on camera. No voice is recorded.

7/ Information to be given to data subjects

Staff members have been informed and the security policy and administartive note have been communicated (see Annex 1).
A notice on the wall at the entrance area is available to alert staff and passers-by to the fact that monitoring takes place. The information on the notice includes the following: the name of the controller, the purpose, the fact that recording takes place, the rights of data subjects, contact information, availability of further information on the internet and at the reception building (see Annex 2).
The security policy is available at the Agency's intranet and internet sites (see Annex 3).
A hard-copy of the security policy is also available at the building reception upon request.

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. No fees for access will be charged.

§ 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 of CCTV footage is not allowed. However, the data subject can exercise his right of rectification on the report written by security staff in connection with a security incident.

§ Right to object – This right is not applicable due to the Legal basis under which the data are processed.

9/ Automated / Manual processing operation

Depending on the level of recorded activity the system will store data only for a maximum period of 2 months, after which it will automatically begin to overwrite previously recorded data.

10/ Storage media of data

The CCTV data is stored on a hard-disc recorder accessible by a Security Guard of G4S or Security staff of the Agency. The system is protected by a password given by the security staff of the Agency. In accordance with Article 1.10.1 and 1.10.2 of the Framework Contract between FRA and Group 4 (see Annex 5). Group 4 can only act upon the instruction of FRA security staff. Therefore, the FRA has control of access to data recorded as part of 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 the security guards of G4S working at the premises of the Agency. Only the security staff of the Agency will be granted access to the data via password and the password will be changed frequently. All security equipment is based at the reception area. The security staff consists of one security officer, but it could be more in the future as the Agency is growing. No data will be transferred to external parties.

13/ retention policy of (categories of) personal 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.

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)

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.
Staff members are informed.

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

Article 27.3 - Consultation

17/ Comments

The fixed outside cameras are adjusted only to cover the entrances and the windows of the building. For security reasons, the moveable outside camera will only be used if the security guard has to monitor/observe the area around the building. (e.g. demonstration).

Cameras are adjusted to only cover the entrances and windows of the buildings. Unnecessary monitoring of people who do not want to enter the buildings is avoided.

Annex 1 - Administrative note providing information to staff members
Annex 2 - Information notice available at the entrance area
Annex 3- Security policy
Annex 4 - Plan of installed cameras
Annex 5 - DP clause included in the FWC between FRA and G4S

PLACE AND DATE: Vienna, 18/05/2009

DATA PROTECTION OFFICER: Nikolaos FIKATAS

INSTITUTION OR BODY: European Union Agency for Fundamental Rights