To be filled out in the EDPS' office

REGISTER NUMBER: 556

NOTIFICATION FOR PRIOR CHECKING

Date of submission: 16/12/2009

Case number: 2009-848

Institution: European Union Agency for Fundamental Rights (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

For security and access control purposes. FRA's video-surveillance system is designed to help control access to its building and to help ensure the security of the building, the safety of FRA staff and visitors, as well as property and information located or stored on the premises. The system complements other physical security system, namely Building Access System. It forms part of the security policy measures aimed at preventing, deterring, and if necessary, investigating unauthorized physical access, including unauthorized access to secure premises, IT infrastructure, or operational information. In addition, video-surveillance helps prevent, detect and investigate security incidents, such as theft of equipment or assets owned by FRA, visitors or staff or threats to the safety of personnel working at the office (e.g. fire, physical assault).

Surveillance equipment is located in particularly sensitive areas (entrance-, - delivery, -garage and outer area). It is also 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.
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.In addition, the system is not used for any other purposes, such as monitoring the work of employees or monitoring attendance. The system is also not used as an investigative tool or to obtain evidence in internal investigations or in disciplinary procedures, unless a security incident is involved.

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)*
The video-surveillance system records digital images. It records any movement detected by the cameras in the area under surveillance, together with time, date and location. All cameras operate 24 hours a day, seven days a week. No voice is recorded.

7/ Information to be given to data subjects

Staff members have been informed and the security policy and administrative note have been communicated (see Annex 1).

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

9/ Automated / Manual processing operation

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

13/ retention policy of (categories of) personal data

The data/images are recorded for a maximum of 7 calendar days according to the policy of retention of data collected as part of security procedures. Thereafter, the system starts automatically overwriting previously recorded data. In cases of investigation of security incidents, the data may be retained longer, but only for

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)

Time limits for blocking and erasure of data depend on the maximum retention period of data which is 7 calendar days after the elapse of which the data will be deleted 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:

17/ Comments

The fixed outside cameras are adjusted only to cover the entrances and the windows of the building. For

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, 01/12/2009

DATA PROTECTION OFFICER: Nikolaos FIKATAS

INSTITUTION OR BODY: European Union Agency for Fundamental Rights