To be filled out in the EDPS' office

REGISTER NUMBER: 360

NOTIFICATION FOR PRIOR CHECKING

Date of submission: 25/04/2008

Case number: 2008-270

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

Contantinos Manolopoulos
European Union Agency for Fundamental Rights
Rahlgasse 3, 1060 Vienna
tel: +43 1 58030611, email: constantinos.manolopoulos@fra.europa.eu

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

Unit Administration / IT

3/ Name of the processing

Firewall - Monitoring of internet connections

4/ Purpose or purposes of the processing

To ensure security and stability for the FRA's network. To detect attacks from out and inside, to measure loads. All incoming/outgoing data has to pass through a security firewall where the source IP and destination IP are being recorded.

5/ Description of the category or categories of data subjects

Data subjects are staff members, DNEs, interim staff and trainees. All system users.

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

Data relating to security measures
Data relating to system functioning

Collected data are:
Date, Time, Gateway,Internal IP address, Outside IP address, Port information (See Annex 1 - Example log file)

7/ Information to be given to data subjects

New staff members are receiving on their first day a letter containing their default login credentials(see Annex 2). Within this letter users are informed about the data stored within the systems. The list is also being published on FRAs intranet side.

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

To have Access: On request to the IT
To Rectify: Not possible
To Block: Not possible
To Erase: Not possible
To Object: Not possible
This is due to the nature of the automatically created log files.

9/ Automated / Manual processing operation

Logging process is fully automated. The system is keeping only the latest 100 entries in a cache.
In case of attacks all activities are being logged to a file. FRA IT administartion staff will investigate the attack by using the log files.

10/ Storage media of data

Cisco ASA local cache, Log files are stored in a resticted area on the SYSLOG server.
Access is provided to IT administartion staff members only.

11/ Legal basis and lawfulness of the processing operation

Article 5(a), (b), (d), (e) of Regulation 45/2001
"Standards of the use of IT systems at FRA" - Annex 3

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

All computer users

13/ Retention policy of (categories of) personal data

The local cache stores only the latest 100 action entries.
The log files abe being stored for a max. period of three months.

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 local cache stores only the latest 100 action entries.
The log files abe being stored for a max. period of three months.

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 - Letter given to staff members
Annex 2 - Mail server log file (Example)
Annex 3 - Chapter B and D of "Standards of the use of IT systems at FRA"

PLACE AND DATE: 25/04/2008

DATA PROTECTION OFFICER: Nikolaos Fikatas (Data Protection Officer of FRA)

INSTITUTION OR BODY: FRA