To be filled out in the EDPS' office

REGISTER NUMBER: 810

NOTIFICATION FOR PRIOR CHECKING

Date of submission: 10/12/2012

Case number: 2011-1149

Institution: ENISA

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
Udo Helmbrecht, Executive Director
P.O. BOX 1309
71001 HERAKLION
GREECE

2/ Organisational parts of the institution or body entrusted with the processing of personal data
ENISAs Administration Department (ADMIN), more specifically HR unit

3/ Name of the processing
Health Data of Staff employed by ENISA

4/ Purpose or purposes of the processing
Fulfillment of legal requirement as per the Staff Regulations upon engagement and on annual basis as well as the development of a preventive culture with respect to health.

5/ Description of the category or categories of data subjects
ENISA statutory and non statutory staff

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

the patient's name and first name; the doctor's name and first name; where the patient is staying; the foreseeable duration of the incapacity for work, specifying the start and end dates; Ability to work certificate (pres-recruitment)

7/ Information to be given to data subjects

Staff is informed about the procedures via intranet announcement.

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

The rights of the data subjects are being granted in their ways of right of access, rectification, rights to block, erase or to object by addressing themselves (by email or orally) to HR or the Medical Adviser

9/ Automated / Manual processing operation

Manual processing of physical medical attestations
Automated processing involves the use of a word processor and spreadsheet that operate on a stand alone PC

10/ Storage media of data

File cabinet
Stand alone PC (PC of the Medical Adviser)

11/ Legal basis and lawfulness of the processing operation

Art 59 and Art 91 CEOS serve as the legal basis for the processing of personal data.
Art. 28 and 33 SR and Art. 12.2 (d), 13 and 83 provide the legal basis for pre-recruitment medical exams.

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

HR staff; medical service of COM and medical advisor.

13/ retention policy of (categories of) personal data

1. Medical certificates are kept by the Medical Adviser in the medical file of staff members for a 1 year;

2. The pre-recruitment certificate is kept in the personal file for an indefinite duration.

3. The results of the annual medical visit are kept for one year by the Medical Adviser (Staff is not obliged to hand over the results of this visit to HR and may directly give them to the medical adviser)

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)
n.a. Data processed can be rectified, blocked and erased upon request by Staff Members.

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,
Processing of anonymous data may be carried out occasionally

15/ Proposed transfers of data to third countries or international organisations
Within the institutions and associated funds (e.g. JSIS)
To designated external medical advisors or medical service providers acting under a specific capacity.

How and when? To control entitlements and specific rights.

16/ The processing operation presents specific risk which justifies prior checking (*please describe*):
Unauthorised access
loss of data
loss / destruction of documents

17/ Comments - ENISA Procedure of processing health data

1) Medical certificates can be either handed (in closed envelope) to :
a. Any of the HR members
i. Medical certificate is subsequently handed to the medical advisor
b. To the reception:
i. In case medical certificate mentions “to be delivered to medical advisor” the guard in service hands it to the medical advisor upon arrival
ii. In case medical certificate mentions “to be delivered to HR” the guard in service hands it to me
iii. I hand the certificate to the medical advisor
c. To HR mail box or pigeon hole:
i. I Medical certificate is subsequently handed to the medical advisor
d. Directly to ENISA’s medical advisor
2) Or submitted electronically:
a. To HR by emailed scanned version
i. The email is then forwarded to the medical advisor and saved under a dedicated email folder
b. Through HR dedicated fax system
i. The fax is printed out by HR, placed in a closed envelope and handed to the medical advisor
3) HR receive validation email issued by medical advisor based on medical certificate. The information issued by the ENISA medical advisor consists, usually, of the following text:
“This is to certify that Mr/Mrs X, according to the fax/scanned/original medical certificate, issued at a medical o
4) The following information is emailed to the respective Head of Department/Section/Unit of the Staff member

18/ Measures to ensure security of processing *(3)*

Please check all points of Article 22 of Regulation (EC) 45/2001.

(3) Not to be published in the EDPS' Register (article 27.5 of Regulation (EC) 45/2001)

PLACE AND DATE: HERAKLION 08/12/2011

DATA PROTECTION OFFICER: Ulrike LECHNER

INSTITUTION OR BODY: European Network Information Security Agency

To be filled out in the EDPS' office