(To be filled out in the EDPS' office)
REGISTER NUMBER: 1445

(To be filled out in the EDPS' office)

NOTIFICATION FOR PRIOR CHECKING

DATE OF SUBMISSION: 09/03/2017

CASE NUMBER: 2017-0284

INSTITUTION: European Insurance and Occupational Pension Authority EIOPA

LEGAL BASIS: ARTICLE 27-5 OF THE REGULATION CE N° 45/2001([1])

INFORMATION TO BE GIVEN[2]

1/ NAME AND ADDRESS OF THE CONTROLLER

Executive Director
European Insurance and Occupational Pension Authority EIOPA
Westhafenplatz 1
60327 Frankfurt am Main
GERMANY

2/ ORGANISATIONAL PARTS OF THE INSTITUTION OR BODY ENTRUSTED WITH THE PROCESSING OF PERSONAL DATA

Human Resources Unit

3/ NAME OF THE PROCESSING

1) Medical files processed by the in-house medical advisor, the external medical service, as well as the medical service of the European Commission.

2) Health related administrative documents processed by the Human Resources Unit.

4/ PURPOSE OR PURPOSES OF THE PROCESSING

The purposes of processing such data are, among others, depending on the recipients (see point 12), to:

[1] OJ L 8, 12.01.2001.
[2] **Please attach all necessary backup documents**

- determine medical fitness of staff members to take up duties and provide certain accommodations at the workplace when necessary;
- apply preventive medicine;
- manage sick and special leave requests, as well as invalidity and occupational illness procedures;
- intervene in/investigate/justify cases of absences because of sickness or accident;
- review compliance with internal rules regarding medical reimbursement requests.

5/ DESCRIPTION OF THE CATEGORY OR CATEGORIES OF DATA SUBJECTS

Staff Members: Temporary Agents (TA) and Contract Agents (CA); Seconded National Experts (SNEs); trainees; successful candidates for the before-mentioned positions; family members of the before-mentioned persons (such as spouses, children and other relatives).

6/ DESCRIPTION OF THE DATA OR CATEGORIES OF DATA (INCLUDING, IF APPLICABLE, SPECIAL CATEGORIES OF DATA (ARTICLE 10) AND/OR ORIGIN OF DATA)

1. Identification data: name, date of birth, gender, personnel number, address etc.

2. Health data found in administrative documents processed and kept with the Human Resources Unit, such as: medical appointments scheduling, invoices for healthcare service provision, sick leave management, special leave applications, medical certificates (e.g. documents certifying medical aptitude for work).

3. Health data contained in the medical files kept with the in-house medical advisor, the external medical service, as well as the medical service of the European Commission, such as: medical reports, laboratory tests, medical questionnaires (e.g. at the pre-recruitment medical examination phase or at the annual medical check-up).

7/ INFORMATION TO BE GIVEN TO DATA SUBJECTS

All the information listed in Articles 11 and 12 of Regulation (EC) 45/2001 is provided to the data subjects:

(a) In the Commission's "Information Note on Data Protection" that is attached to the invitation of successful candidates to the pre-recruitment medical check-up;

(b) In the Privacy Statement attached to the invitation of staff members to the annual medical check-up. The Privacy Statement is also published on the "InCiderNet", EIOPA's intranet. There, it is made clear that the medical practitioners involved will not forward the results of the medical examinations to EIOPA, unless the staff member concerned consents to that. Only a proof/document stating the aptness (or not) of the employee for service will be provided to the Authority.

8/ PROCEDURES TO GRANT RIGHTS OF DATA SUBJECTS
(Rights of access, to rectify, to block, to erase, to object)

EIOPA's Data Protection Implementing Rules lay down the rules and procedures pursuant to which data subjects may exercise their rights of access, rectification, erasure and objection with regards to the processing of any kind of personal data, including health related data. In addition to that, the Privacy Statement relevant to the processing of health data explains those rights in detail.

Data subjects may address any request regarding the exercise of their rights to EIOPA's DPO, by sending an email to the respective functional mailbox (dpo@eiopa.europa.eu). An e-mail can also be sent to the data controller, the Executive Director of EIOPA, as well as the medical advisor. A reply is given to such requests normally within 15 working days.

As specifically regards the *right of rectification*, the results of medical examinations and the diagnosis cannot be altered. However, data subjects are entitled to correct administrative errors found in their medical file and supplement the file by adding opinions of other doctors, in order to ensure the completeness of the file.

As concerns *access to psychiatric and psychological reports*, data subjects can only have an indirect right of access via a doctor appointed by them.

Data subjects have the right to recourse to the EDPS at any time, in accordance with Articles 11(1)f(iii) and 12(1)f(iii).

9/ AUTOMATED / MANUAL PROCESSING OPERATION

The processing of health data found in medical files and administrative documents will be both manual and automated.

10/ STORAGE MEDIA OF DATA

1) Medical files kept at EIOPA are securely stored in a safe with restricted access rights only to the parties involved (e.g. the medical advisor him/herself). The in-house medical advisor sits in a closed room.

The medical files produced at the external medical centre are stored securely in a locked cupboard that is located there.

As concerns the medical files kept at the medical service of the European Commission, we invite the EDPS to refer to the Commission's relevant Notification for prior checking.

2) Health related administrative documents are securely stored either in a locked cupboard of the Human Resources Unit or in electronic folders saved on EIOPA server – "I Drive" and on Outlook, with restricted access rights only to persons that are defined by the Appointing Authority on a "need-to-know-basis".

11/ LEGAL BASIS AND LAWFULNESS OF THE PROCESSING OPERATION

Legal basis:

Health data are processed in fulfilment of legal obligations imposed on EIOPA by the Staff Regulations and the CEOS for the management of people working at the Authority.

Lawfulness:

A. Processing of health related data falls under article 5(a) of Regulation (EC) 45/2001.

B. Since the processing of such sensitive data is necessary for the management of the staff and is provided for in the Staff Regulations and the CEOS, this processing operation also falls under Article 10(2)b of Regulation (EC) 45/2001.

C. As concerns the processing of medical data by health professionals, the lawfulness of the processing could also fall under Article 10(3) of Regulation (EC) 45/2001.

D. Any further processing of medical data will be based on an informed and freely given consent of the data subject, in light of Articles 5(d) and 10(2)a of Regulation (EC) 45/2001, and will be only performed provided that this is necessary for protecting the interests of the latter.

12/ THE RECIPIENTS OR CATEGORIES OF RECIPIENT TO WHOM THE DATA MIGHT BE DISCLOSED

- Personal data contained in:
1) Medical files: the medical advisor, the external medical service, as well as the medical service of the European Commission.

2) Health related administrative documents: Human Resources Unit.

- Recipients of health-related data could also be EIOPA's Confidentiality Counsellor, EIOPA's Executive Director, EIOPA's legal advisors, and in case of complaint, the internal investigators for administrative/disciplinary proceedings, OLAF, the Court of Justice of the EU, the European Ombudsman, as well as the EDPS.

- Sick leaves and their duration may be communicated to other staff member(s) on a need-to-know basis and and/or for business-related purposes.

13/ RETENTION POLICY OF (CATEGORIES OF) PERSONAL DATA

In compliance with Article 4(1) of Regulation (EC) 45/2001, health related data contained in:

1) Medical files are retained for a period of maximum 30 years after the end of employment.

In the case of non-recruited candidates, their medical data are kept for a period of 1 year following the conclusion of the relevant recruitment procedure, or up until the expiration of the validity of the respective reserve list, unless a relevant dispute or appeal is underway.

2) Health related administrative documents (such as sick and special leave requests, as well as requests for reimbursement of medical expenses), are retained for 3 years, unless a relevant dispute or appeal is underway.

13 A/ TIME LIMIT TO BLOCK/ERASE ON JUSTIFIED LEGITIMATE REQUEST FROM THE DATA SUBJECTS

(Please, specify the time limits for every category, if applicable)

The rights of blocking and erasure can be exercised at any point in time.

EIOPA's DPO will react to such requests within the time-limit provided in EIOPA's Data Protection Implementing Rules (i.e. 15 working days).

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.

The storing of health related data for such purposes is only done on an anonymous basis.

15/ PROPOSED TRANSFERS OF DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

When health data need to be transferred to third countries (e.g. to doctors established in a third country), it is ensured that such a transfer will only be performed if the respective national legislation applies a level of protection of personal data that is at least equivalent to Directive 95/46/EC. If this is not the case, the data subject needs to unambiguously give his/her consent.

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 27.2.(b): Processing operations intended to evaluate personal aspects relating to the data subject.

17/ COMMENTS

N/A

PLACE AND DATE:
FRANKFURT, 7 MARCH 2017

DATA PROTECTION OFFICER:
CATHERINE COUCKE

INSTITUTION OR BODY:
EIOPA