(To be filled out in the EDPS' office)
REGISTER NUMBER: 1170

(To be filled out in the EDPS' office)

NOTIFICATION FOR PRIOR CHECKING

DATE OF SUBMISSION: 27/09/2013

CASE NUMBER: 2013-1065

INSTITUTION: EBA

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

Adam Farkas
Executive Director
European Banking Authority - EBA
Tower 42 (level 18)
25 Old Broad Street
London EC2N lHQ
United Kingdom

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

EBA Operations Department / Human Resources

3/ NAME OF THE PROCESSING

Health data:
Medical certificates
Pre-employment medical clearances

[1] OJ L 8, 12.01.2001.

[2] **Please attach all necessary backup documents**

4/ PURPOSE OR PURPOSES OF THE PROCESSING

The purpose of the processing is to ensure compliance with the requirements for employment ("physically fit to perform duties") and to justify sickness-related absences.

5/ DESCRIPTION OF THE CATEGORY OR CATEGORIES OF DATA SUBJECTS

Medical certificates:
Staff members (Temporary and Contract Agents, SNEs)

Pre-employment medical checks:
Persons to be recruited under the Staff Regulations and CEOS/newcomers

6/ DESCRIPTION OF THE DATA OR CATEGORIES OF DATA *(including, if applicable, special categories of data (Article 10) and/or origin of data).*

Health data - personal data that have link with the health status of a person:
medical data (e.g. medical examination reports)
administrative and financial data relating to health (medical appointments, invoices, indication of number of sick leave days etc.)

Medical certificates - data regarding health conditionsin the form of a medical certificate of staff member to justify his/her absence due to sickness or accident. Only relevant data for the purpose of justification of medical absence are requested.

1. Identification data:
Administrative data allowing the data subject to be identified (name, surname, birth date, address).

2. Special (sensitive) categories of data:
No additional information than administrative data above should be disclosed on the medical certificate, but in some cases there might be an indication of the medical disease or information on different type of treatment/specialisation of doctor which can lead to sensitive data processing.

Pre-employment medical checks - data in the form of a medical statement following the pre-employment medical check-up for the persons selected for employment with EBA (data subjects), check if the person is fit or not to take up duty at the Authority.

1. Identification data:
Administrative data allowing the data subject to be identified (name, surname, gender, details concerning contract type, nationality and birth date).

2. Special (sensitive) categories of data:
The health data are processed by a health professional (Medical centre of the European Commission) subject to the obligation of professional secrecy. All medical data/results are strictly confidential and kept at the outsourced medical centre. The medical exams are not disclosed to the EBA. HR receives only the information (medical clearance) if the data subject is physically fit or not to perform the duties at the Authority. The medical centre keeps all medical data at the source.

7/ INFORMATION TO BE GIVEN TO DATA SUBJECTS

In order to ensure transparency and fairness of the processing, the following information listed in Articles 11 and/or 12 of Regulation 45/2001 is provided to data subjects:

identity of the controller,
purpose of the processing, data categories,
whether replies to the questions are obligatory or voluntary, as well as possible consequences of failure to reply,
possible data recipients,
existence of rights of access, rectification and recourse to the EDPS,
legal basis of the processing,
applicable data retention periods.

Due to the fact that this information should be provided either at the collection of data or before their first disclosure to a third party, the following communication means were considered as appropriate for the particular procedure:

data protection clause in the respective report form, application form or messages sent to data subjects, and
specific privacy statement made available on the Intranet.

Medical data collected on the basis of the *Staff* Regulations can only be considered as lawful provided that it is based on an informed and freely given consent of the data subject or if the processing is necessary to protect the interests of the data subject. The data subject has a right to refuse and/or withdraw his/her consent with respect to the further processing of his/her medical data for medical follow up purposes.

In case of pre-employment medical check-up the data subjects are informed well in advance (invitation for interview) about the purpose of the processing of health data and the legal basis for this processing is given as well.

8/ PROCEDURES TO GRANT RIGHTS OF DATA SUBJECTS

(Rights of access, to rectify, to block, to erase, to object)

EBA's Implementing Rules on Data Protection relating to the Regulation (EC) No 45/2001 with regards to the processing of personal data lay down the detailed rules pursuant to which a data subject may exercise his/her rights, the procedure for notifying a processing operation and the procedure for obtaining access to the register of processing operations kept by the Data Protection *Officer*.

The data subjects can access their own health data and are entitled to receive copies of their medical file.

Non recruited persons have access to the data processed about their health status.

The right to rectify inaccurate or incomplete data is limited. The data subjects can rectify their administrative data in the medical files only. Or in case that the medical file is not complete, ask to have another opinion of other doctor and have this document added to the medical file.

9/ AUTOMATED / MANUAL PROCESSING OPERATION

Annual medicals:

At the EBA a procedure for the annual medical examinations was established and the staff members were advised to visit doctors of their own choice, submit the results to the medical Centre in Brussels which then reimbursed the cost of the examination up to a ceiling. The results are stored in the medical centre in Brussels.

Manual and semi-automated processing operation for medical certificates:
The medical requests (sick leave with/without certificate, medical examination or special leave requests) are registered via HR leave management tool Allegro. Only limited number of HR staff (HR ASSistants) have the full rights to access all staff applications/medical entries. The data subject can only see, access and modify his/her own entries.
Hard copies of the medical certificates are held and stored in a separate file per staff member. The access to these data is strictly limited to HR staff.

Manual processing operation for pre-employment medical checks:
Structured set of personal data in the form of medical clearance is held in a hard and electronic copy per data subject. The file is filed in the personal file of staff member. The access both to the hard and electronic copies is strictly restricted to a few HR. The medical data are processed and stored by the medical centre of the European Commission. No medical data in the strict sense is processed by Authority.

A legally binding contract (SLA) with the EC medical centre is established, and rules governing the communication of health data are explained within that document.

10/ STORAGE MEDIA OF DATA

The medical certificates to justify absences are stored on paper (hard copies) in a dedicated HR folder, locked in a special cabinet with restricted access rights.
The pre-employment medical clearances are stored in personal files, locked in a special cabinet with restricted access rights.

11/ LEGAL BASIS AND LAWFULNESS OF THE PROCESSING OPERATION

Compliant with Article 5(a) of the Regulation 45/2001, the personal data may be processed if "processing is necessary for the performance of a task carried out in the public interest on the basis of the Treaties ... or other legal instrument adopted".

Temporary/Contract Agents, SNEs, Trainees:

Regulation (EU) No 1093/2010 of the European Parliament and the Council of 24 November 2010 establishing EBA.

Medical certificates:

For the EBA staff members: Staff Regulations of Officials (SR) and the Conditions of Employment of Other Servants of the European Communities (CEOS), and in particular Art. 59(1) (SR).
For SNE: EBA Management Board Decision EBA DC 017 dated 12 January 2011 on Secondment of National Experts.

Pre-employment medical clearances:

Staff Regulations of Officials (SR) and the Conditions of Employment of Other Servants of the European Communities (CEOS), and in particular Art. 28-33 (SR) and Art. 12(d), 13(2) and 83(2) (CEOS).

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

The access rights to the personal data of data subject are restricted to HR staff. Recipients within Authority:

HR staff
Executive Director of the EBA/Appointing Authority
Data subjects themselves, for the data that concerns them individually.

Recipients outside Authority, if requested (European Union institutional bodies):

Medical service of the European Commission (for possible advice when foreseen in the Staff Regulations)
Internal Audit Service of the Commission and the Court of Auditors (for audit purposes)
OLAF
Court of Justice of the European Union
European Ombudsman.

13/ RETENTION POLICY OF (CATEGORIES OF) PERSONAL DATA

Article 4(1)(e) of Regulation 45/2001 states that personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.

The pre-employment medical clearances are stored on paper (hard copies) in personal files in line with Article 26 of the Staff Regulations, locked in a special cabinet with restricted access rights, for up to 10years after the termination of the employment.

The medical certificates are stored until the end of year N+2 (i.e. for max 3 years period of time).

The medical clearance for staff considered physically unfit (and hence not recruited) is kept only for the period of time during which is it possible to challenge the negative decision taken on the basis of such clearance.

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)

According to the EBA Implementing Rules, Article 12:
If the ground for the request of blocking data is the inaccuracy of the data, as referred in paragraph (1) letter(a), the Data Controller shall immediately block the data for the period necessary for verifying the accuracy and completeness of the data. A data subject who has requested and obtained the blocking of data shall be informed thereof by the Data Controller. He or she shall also be informed of the fact that data are to be unblocked at least 15 working days before they are unblocked. The Data Controller shall take a decision as soon as possible and at the latest within 15 working days of receiving a request for data to be blocked. If the request is accepted, it shall be acted upon within 30 working days and the data subject notified thereof. Should the request for blocking be rejected, the Data Controller shall have 15 working days within which to

inform the data subject by means of a letter stating the grounds for the rejection. In automated filing systems, blocking shall be ensured by technical means. The fact that personal data are blocked shall be indicated in the system in such a way as to make it clear that the data may not be used. Personal data blocked pursuant to this Article shall, with the exception of their storage, only be processed for purposes of proof, or with the consent of the data subject or for the purpose of protecting the rights of third parties.

According to the EBA Implementing Rules, Article 13: The data subject shall have the right to obtain from the Data Controller the erasure of data if the processing thereof is unlawful. If the request is accepted, it shall be acted upon immediately. If the Data Controller deems the request unjustified, he or she shall have 15 working days within which to inform the data subject by means of a letter stating the grounds for the decision.

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):*

The selection procedure is a processing operation that:

relates to health and therefore falls under Article (27) paragraph 2. letter (a) of the Regulation;

17/ COMMENTS

PLACE AND DATE: London, 27/09/2013

DATA PROTECTION OFFICER: Joseph Mifsud

INSTITUTION OR BODY: EBA