EUROPEAN DATA PROTECTION SUPERVISOR

WOJCIECH RAFAŁ WIEWIÓROWSKI
ASSISTANT SUPERVISOR

Mr Adam FARKAS
Executive Director
European Banking Authority
One Canada Square, Floor 46
Canary Warf - London E14 5AA
UNITED KINGDOM

Brussels, 26 February 2016
WW/XK/sn/D(2016)0506 **C 2013-1065**
Please use edps@edps.europa.eu for all correspondence

Subject: **Prior-check Opinion on the processing of health data at the European Banking Authority, case 2013-1065.**

Dear Mr Farkas,

We have analysed the updated notification and revised documents you have provided to the European Data Protection Supervisor (EDPS) for prior-checking under Article 27(2)(a) of the Regulation (EC) n° 45/2001 (the Regulation) on the processing of health data at the European Banking Authority (**EBA**). The purpose of this processing is to ensure compliance with the requirements for pre-employment, annual medicals and sickness-related absences.

As this is an ex-post case, the deadline of two months for the EDPS to issue his Opinion does not apply.

The notification and the relevant documents are analysed in light of the EDPS Guidelines on health data in the workplace (the Guidelines)[1]. The EDPS Joint Opinion related to the processing of health data by 18 agencies[2] is also applicable in the present case**.**

The EDPS will identify EBA's practices, which do not seem to be in conformity with the principles of the Regulation and the Guidelines, and then provide EBA with relevant recommendations.

[1] Issued in September 2009 and published on the EDPS website.
[2] Issued on 11 February 2011 and it concerned 18 agencies, case 2010-0071.

1) Legal basis

The legal basis is one of the conditions for a processing operation to be lawful under Article 5(a) of the Regulation.

EBA indicated in the notification the legal basis of the processing operation related to occupational diseases and accidents. The Guidelines do not cover such processing operation related to this procedure. EBA should therefore submit for prior-checking a separate notification with a privacy notice and other relevant documents under Article 27(2)(a) of the Regulation.

However, the processing operation on special leave is similar to a processing operation on sick leave. The EDPS invites EBA to include in the notification under analysis the relevant legal basis of the processing related to special leave.

The notification and the privacy statement should be updated accordingly.

2) Services of a private practitioner

The notification is silent on the possibility for staff members to have their annual check-up visit carried out by a private practitioner.

The EDPS reminds EBA that a declaration from the staff member's private practitioner should be considered sufficient in terms of the preventive purpose of the annual check-up. This declaration can confirm that the medical exams were carried out and if necessary, it can specifically mention any special accommodations or working conditions the staff members might need.

EBA should therefore inform staff members of their entitlement to choose the private practitioner who will perform their annual medical check-up and of the practical steps they must take to have the check-up carried out by the private practitioner of their choice.

3) The placement screening questionnaire

The purpose of the questionnaire

It is not clear whether the placement medical screening questionnaire is used for the annual check-up[3]. The Staff Regulations do not foresee that the pre-recruitment medical examination serves for prevention purposes. The EDPS acknowledges that data collected during the pre-employment medical visits could additionally serve to alert a future member staff of a specific health issue concerning his/her health and therefore could eventually serve for prevention purposes. This does not however imply, however, that additional data should be requested for the purpose of prevention.

The EDPS recommends that EBA clarify this issue in the notification and inform data subjects accordingly in the privacy statement (see point 8).

[3] The Staff Regulations do not seem to specify the purpose of the annual medical check-up. However, the EDPS recognises that a medical service at work, as a measure of preventive medicine, can be seen as beneficial for the employer as it helps maintain human resources in better health. It also serves staff members who benefit from a medical service at their disposal.

The issue of consent in the questionnaire

The placement medical screening questionnaire asks data subjects to tick in the box "yes" or "no" by giving their consent for a further processing, namely "*I consent to the information on this form being disclosed to the Company's insurers for underwriting purposes*". The term "*underwriting purposes"* means with respect to any group health plan, or health insurance coverage offered in connection with a group health plan.

This is not the purpose of a pre-employment medical examination, which is to process medical data in view of assessing whether the data subject is physically fit to perform his duties. Furthermore, under Article 2(h) of the Regulation, consent is not valid unless it is freely given, specific and constitutes an informed indication of the data subject's wishes. In this particular case, in an employment context, consent is a sensitive matter as it is doubtful that such consent is freely given and most importantly, data subjects are not informed to what exactly they should consent.

EBA should therefore erase the above statement from the questionnaire.

4) Recipients and processors

EBA lists the external medical providers and the Commission's medical service as recipients.

EBA has concluded a Service Level Agreement (SLA) with the Commission's medical service and a contract with two external medical providers in London for carrying out the pre-recruitment examinations and annual check-up visits, as well as sick leave consultations.

In light of Article 23 of the Regulation, these parties are acting on behalf of EBA and are therefore classed as processors. This is because they are obliged to carry out the processing only on instructions from the controller - EBA (Article 23(2)(a)). Their obligations regarding confidentiality and security measures are also laid down in the SLA and contract respectively (Article 23(2)(b)).

The EDPS therefore recommends that EBA clarify in the notification and in the privacy statement that the external medical providers and the Commission's medical service act as processors on behalf of EBA in light of the requirements of Article 23 of the Regulation.

5) Quality of data

Staff members are required to send their sick leave certificates to EBA's Human Resources to justify their leave.

Sick leave and some special leave certificates are considered as data concerning health. Although the exact type of illness is not indicated, staff members can be identified as having been absent due to a short or long term illness on medical treatment or due to special sick leave of a medical nature.

The HR of EBA should, under Article 4(1)(c) of the Regulation, only keep information which is adequate, relevant and necessary for the purpose for which it needs to collect them, that is, to be able to manage the absences of the agency's staff members. The HR should hence collect only administrative data related to an absence of a staff member and not the sick leave certificate as such.

The EDPS recommends that EBA modify its policy and requires its staff members to send their sick leave certificates directly to the external medical providers or to the Commission's medical service. The latter or the external medical provider will then inform the HR about the administrative related data, such as the name, surname and duration of absence of the staff member.

6) Retention periods

EBA keeps aptitude certificates in the personal file for a period of 20 years after the end of the period during which a staff member is in active employment or the last pension payment.

The retention period of 20 years seems to be excessive to the purpose for which aptitude certificates are collected. The EDPS has always recommended a 10-year-retention period after the end of the period during which a staff member is in active employment or the last pension payment. The EDPS invites EBA to adopt the recommended retention period. The notification should be updated accordingly.

7) Security measures

EBA's HR officers process personal data related to health, namely aptitude certificates and administrative information on sick leave.

Due to the sensitive nature of such data, the EDPS recommends that the HR Officers sign confidentiality declarations mentioning that they are subject to an obligation of professional secrecy equivalent to that of a health professional. This organisational measure aims at maintaining the confidentiality of personal data and at preventing any unauthorized access to them within the meaning of Article 22 of the Regulation.

8) Information to be given to data subjects

Identity of the controller
Both the notification and the privacy statement mention the Executive Director as the controller of the present processing operations. The EDPS reminds EBA that from a legal perspective, EBA is the responsible controller of these processing operations. The Executive Director legally represents EBA. In practice, EBA's HR is responsible for internally managing the processing operations under analysis, as it is correctly indicated in point 2 of the notification. A contact person of HR should also be indicated, so that data subjects may contact the appropriate case officer directly, allowing written requests and confidentiality.

Purpose of the processing for which the data are intended
EBA should inform in the privacy statement, under Articles 11(1)(b) and 12(1)(b) of the Regulation whether the placement medical screening is used in the context of an annual check-up and for preventive purposes (see point 3 above).

Legal basis
As it was recommended in point 1 above, EBA should include the legal basis of special leave, under Articles 11(1)(f)(i) and 12(1)(f)(ii) of the Regulation.

The recipients of the data
In light of Articles 11(1)(c) and 12(1)(d), EBA should list the Commission's medical service

and the external medical providers as processors (see point 4 above).

The time-limits for storing the data
In light of Articles 11(1)(f)(ii) and 12(1)(f)(ii), EBA should modify the retention period for aptitude certificates (see point 6 above).

Rights of access and rectification
On the basis of Articles 11(1)(e) and 12(1)(e), EBA should provide more specific information as to the meaning of the rights of access and rectification in the context of the processing operations under analysis, so that affected individuals fully understand their rights.

With regard to the right of access, EBA should also indicate that:
- non-recruited candidates and trainees may also exercise their rights of access and
- data subjects can have indirect access - instead of direct access - to their psychiatric and psychological reports via a doctor appointed by them[4].

As to the right of rectification, EBA should mention that staff members are entitled to correct administrative errors in their medical file and to supplement it by adding opinions of other doctors to ensure completeness of the file.

In the context of the follow-up procedure, please send all updated relevant documents (notification, privacy statement and screening questionnaire) within a period of three months, to demonstrate that EBA has implemented the above recommendations.

Should you have any questions, please do not hesitate to contact us.

Yours sincerely,

(**signed**)

Wojciech Rafał WIEWIÓROWSKI

Cc: Mr Peter MIHALIK, Director of Operations (Human Resources).
Mr Joseph MIFSUD, Data Protection Officer.

[4] In that regard, EBA should refer to the Conclusion 221/04 of the Board of Heads of Administration of 19 February 2004.