EUROPEAN DATA PROTECTION SUPERVISOR

WOJCIECH RAFAŁ WIEWIÓROWSKI
ASSISTANT SUPERVISOR

Mr Jorge DOMECQ
Director-General
European Defence Agency (EDA)
Rue des Drapiers 17-23
1050 - Brussels

Brussels, 16 February 2016
WW/XK/sn/D(2016)0422 **C 2013-0740**
Please use edps@edps.europa.eu for all correspondence

Subject: **Prior-check Opinion on the processing of health data and administrative data related to health at the European Defence Agency (case 2013-0740)**

Dear Mr Domecq,

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 and administrative data related to health at the European Defence Agency (**EDA**). The purpose of this processing is to ensure compliance with the requirements foreseen in the EDA Staff Regulations in the context of pre-recruitment medical visits, annual check-ups, sick leave and special/family/parental leave of the agency's staff members.

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 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 notes that the notification refers briefly to the invalidity procedure. The Guidelines do not cover the processing operation related to the invalidity procedure. EDA 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.

[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.

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

1) Services of a private practitioner in the context of the annual check-up

The notification states that with regard to the annual medical visits, "*no medical data in the strict sense contained in the medical examination report is sent to the HR Unit*".

The EDPS reminds EDA that as per the Guidelines, 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 also mention any special accommodations or working conditions the staff members might need.

EDA should therefore adopt the above good practice and indicate it in the notification.

2) Recipients and processors

EDA lists in the notification the Council's medical service as recipient.

EDA has concluded a Service Legal Agreement (SLA) with the Council's medical service for carrying out the pre-recruitment medical visits and annual check-up visits. In light of Article 23 of the Regulation, the Council's medical service is acting on behalf of the agency and is therefore classified as processor rather than recipient. This is because it is obliged to carry out the processing only on instructions from the controller - EDA (Article 23(2)(a)). Their obligations regarding confidentiality and security measures are also laid down in the SLA (Article 23(2)(b)).

The EDPS therefore recommends that EDA clarify that the Council's medical service acts as processor on behalf of EDA in light of the requirements of Article 23 of the Regulation.

Furthermore, the notification and the privacy notices mention a number of possible recipients of personal data, such as the Civil Service Tribunal, the Internal Auditors and the College of Auditors, the European Ombudsman and the EDPS. For your information, with regard to Article 2(g) of the Regulation, authorities which would only receive data in the context of specific targeted inquiries are not considered "recipients" and do not need to be mentioned in the notification and the privacy statement[3].

3) Retention periods

The privacy notice on the pre-employment medical check-up indicates that the medical files are stored at the European Council and data processing linked to medical files is notified to

[3] This is an exception to the information obligations in Articles 11 and 12, but not to the rules on transfers in Articles 7 to 9. In practice, this means that authorities such as the OLAF, the European Ombudsman or the EDPS do not need to be mentioned in the privacy statement (unless the processing operation in question involves transfers to these organisations as part of the procedure); however, the applicable rules on transfers will always need to be respected.

the EDPS under n° 2004-254. As to the pre-recruitment aptitude certificates, it is stated that the "apt for duty" note is kept *"as long as the personal file exists"*.

The EDPS recalls that **medical data** of the pre-recruitment and annual visits (if the staff member chooses to carry out the medical check-ups with the Council's medical service) should be kept for a maximum period of 30 years after the last document has been inserted to the medical file.

Pre-recruitment aptitude certificates should be kept in the personal files for ten years after the end of the period during which a staff member is in active employment or the last pension payment.

EDA should therefore state clearly in the notification the above retention periods.

4) Security measures

EDA's HR officers process personal data related to health, namely aptitude certificates and administrative information on sick leave and special leave. In EDA's e-mail of 3rd December 2015, it was stated that a confidentiality declaration template was attached among other documents submitted to the EDPS. However, this declaration was missing.

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.

5) Information to be given to the data subject

Privacy notice on annual check-ups

EDA has not prepared a privacy notice regarding the processing of personal data in the context of annual check-ups. EDA should prepare a clear and concise privacy notice including all information required under Articles 11 and 12 of the Regulation. The EDPS recommendation in point 1 should also be included. The privacy notice should be easily accessible to all staff members as soon as they request to carry out their annual check-up either with the Council's medical service or with a private practitioner.

Rights of access and rectification

On the basis of Articles 11(1)(e) and 12(1)(e) of the Regulation, EDA should explain in the privacy notices on pre-recruitment medical visit and annual check-ups how affected individuals are entitled to exercise their rights of access and rectification so that they fully understand their rights.

EDA should mention that staff members 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, EDA should mention that staff members are entitled not only

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

to correct administrative errors in their medical file but also to supplement it by adding opinions of other doctors to ensure completeness of the file.

Finally, the privacy notices do not seem to inform staff members of any time limits for requests and responses. It is a good practice to include information on time limits within which a reaction can be expected (e.g. 3 months for access request, without delay for rectification, etc.). Consequently, the EDPS recommends that these time limits are added to the privacy notices.

The time-limits for storing the data

In light of Articles 11(1)(f)(ii) and 12(1)(f)(ii) of the Regulation, EDA should clearly indicate in the privacy notice on pre-recruitment medical visit the retention period for medical data as well as for pre-recruitment aptitude certificates (see point 3 above).

The right to recourse to the EDPS

In light of Articles 11(1)(f)(iii) and 12(1)(f)(iii), EDA should indicate in the notice on personal data processing of health data and administrative data linked to health that data subjects have a right to recourse to the EDPS **at any time** following the model of the privacy notice on personal data in the context of the pre-employment medical check-up.

EDA should adopt all EDPS recommendations in order to comply with the Regulation. In the context of the follow-up, the EDPS expects EDA to send all updated relevant documents within a period of three months, to demonstrate that EDA has implemented the above recommendations.

Yours sincerely,

(signed)

Wojciech Rafał WIEWIÓROWSKI

Cc: Mr. Jan-Paul BROUWER, Head of Human Resources, EDA
Ms. Silvia POLIDORI, Data Protection Officer, EDA