EUROPEAN DATA PROTECTION SUPERVISOR

WOJCIECH RAFAŁ WIEWIÓROWSKI
ASSISTANT SUPERVISOR

Dr Udo HELMBRECHT
Executive Director
European Union Agency for Network and Information Security (ENISA)
P.O. Box 1309,
710 01 Heraklion,
Crete
GREECE

Brussels, 31 March 2016
WW/XK/sn/D(2016)0756 **C 2011-1149**
Please use edps@edps.europa.eu for all correspondence

Subject: **Prior-check Opinion on the processing of health data at the European Union Agency for Network and Information Security (case 2011-1149).**

Dear Dr Helmbrecht,

On 15 December 2015, the European Data Protection Supervisor (EDPS) received a notification on the processing of health data for prior-checking under Article 27(2)(a) of the Regulation (EC) n° 45/2001 (the Regulation)[1]. The purpose of this processing is to ensure compliance with the requirements foreseen in the Staff Regulations in the context of pre-recruitment medical exams, annual check-ups, and sick leave of the agency's staff members. The documents sent to the EDPS are the following:
- a draft policy concerning the processing of health data at ENISA,
- a privacy statement on the protection of personal data in relations to health data,
- a snippet copy of ENISA confidentiality declaration with references to Article 10(3) and 7(3) and
- copies of extracts of contracts (on confidentiality and data protection) with the external medical supplier.

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

[1] The notification was sent to the EDPS on 10 December 2011, but important information and documents were missing. There was an exchange of correspondence between the EDPS and the former Data Protection Officer. On 19 June 2015, the EDPS carried out a visit to ENISA.

The notification and relevant documents are analysed in light of the EDPS Guidelines on health data in the workplace (the Guidelines)[2]. The EDPS Joint Opinion related to the processing of health data by 18 agencies[3] is also applicable in the present case**.**

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

1) Processing of personal data on behalf of controllers

ENISA has concluded a contract with an external medical supplier and under this contract; a medical advisor has been selected for the provision of medical services to ENISA's staff members.

Article I.9 of the contract on data protection refers to the external contractor's rights. Indeed, ENISA has obligations vis-à-vis the processing of personal data of the contractor and the latter has also rights under the Regulation. The object of the contract is nevertheless the provision of medical services to ENISA's staff members. ENISA should therefore add a paragraph on the contractor's **obligations** as to the processing of the personal data of the agency's staff members.

Due to the sensitivity of the processing operations under analysis, ENISA could have developed a tailor-made clause, instead of using a standard data protection clause. Although, regrettably, the contract has already been signed, the EDPS recommends that ENISA revise the contract and add a clause on the contractor's **obligations** as to the processing of personal data of the agency's staff members. As to the contractor's rights under the Regulation, ENISA should better inform the contractor via the channel of a privacy notice or any other appropriate channel it considers appropriate.

2) Retention periods

The notification states that the **pre-recruitment aptitude certificates** are kept in the personal file in an indefinite duration**.** In light of Article 4(1)(e), ENISA should set up a maximum retention period which is necessary for the purpose for which the aptitude certificates were collected. The EDPS recommends that aptitude certificates be kept in the personal file for ten years after the end of the period during which a staff member is in active employment or the last pension payment.

As to the **medical data of the pre-recruitment visits**, ENISA should indicate in the notification that they are kept by the Commission's medical service for a maximum period of 30 years after the last document has been inserted to the medical file.

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

With regard to the **medical data kept by the external medical advisor**, the notification states that they are kept for one year, whereas the draft policy refers to a period of 30 years in compliance with EDPS rules. This inconsistency should be clarified.

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

3) Information to be given to the data subject

ENISA has prepared a thorough draft policy on the processing of health to be published on the intranet, explaining the procedure and the good data protection practices in the context of pre-recruitment medical visits, annual check-ups and medical certificates. Nevertheless, under Article 11 of the Regulation, staff members should be informed about the processing of their personal data **before** they are collected for fairness and transparency.

Privacy notices on pre-recruitment and annual check-ups

The privacy notice provided to the EDPS concerns only the processing of medical certificates in cases of absences. ENISA should prepare two clear privacy notices on the pre-recruitment medical visits and on annual check-ups including all information required under Articles 11 and 12 of the Regulation.

The privacy notice on pre-recruitment medical visits should be attached to the invitation letter sent to the successful candidate to carry out the pre-recruitment medical visit.

As to the privacy notice on annual check-ups, it should be easily accessible to all staff members as soon as they request to carry out their annual check-up either with ENISA's external medical advisor or with a private practitioner.

Identity of the controller

Under Articles 11(1)(a) and 12(1)(a), it is important that a contact person of HR is indicated in all three privacy notices (including the one on medical certificates) so that staff members may contact the appropriate case officer directly, allowing written requests and confidentiality. The EDPS recalls that in practice, ENISA's HR is responsible for internally managing the processing operations under analysis. From a legal perspective, ENISA is the responsible controller of these processing operations.

Rights of access and rectification

On the basis of Articles 11(1)(e) and 12(1)(e) of the Regulation, ENISA should explain in all privacy notices how staff members are entitled to exercise their rights of access and rectification so that they fully understand their rights.

As to the right of access, ENISA should mention that staff members could 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, ENISA should mention that staff members are entitled not only to correct administrative errors in their medical file but also to supplement it by adding

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

opinions of other doctors to ensure completeness of the file.

The time-limits for storing the data
In light of Articles 11(1)(f)(ii) and 12(1)(f)(ii) of the Regulation, ENISA should clearly indicate in the relevant privacy notices the retention period for medical data as well as for pre-recruitment aptitude certificates.

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

Yours sincerely,

(**signed**)

Wojciech Rafał WIEWIÓROWSKI

Cc: Mr Aidan RYAN, Head of Administration.
Ms Athena BOURKA, Data Protection Officer