EUROPEAN DATA PROTECTION SUPERVISOR

WOJCIECH RAFAŁ WIEWIÓROWSKI
ASSISTANT SUPERVISOR

Ms Verena ROSS
Executive Director
European Securities and Markets Authority (ESMA)
103, rue de Grenelle
75007 Paris
FRANCE

Brussels, 18 May 2016
WW/XK/sn/D(2016)1069 **C 2013-0927**
Please use edps@edps.europa.eu for all correspondence

**Subject: Prior-check Opinion on the processing of health data at the European Securities and Markets Authority (ESMA), case 2013-0927.**

Dear Ms Ross,

We have analysed the revised notification and attached updated documents you have provided to the 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 Securities and Markets Authority (**ESMA**). The purpose of the processing operations under analysis is to assess the aptness of successful candidates and staff members in the context of pre-recruitment and medical check-ups respectively and to manage their absences in case of sick leave and special leave.

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**.**

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

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

**1) Legal basis and lawfulness**

The notification states that "*Moreover, as in line with the Regulation (EC) 45/2001, the data subjects are giving their consent for data processing by providing their personal data voluntarily*".

The legal basis for ESMA to carry out pre-recruitment and annual medical visits and, to process sick leave certificates is found in the EU Staff Regulations. These processing operations are necessary to assess the data subjects' ability to carry out their role effectively in light of any medical issues and for the purpose of managing the sick leave of ESMA's staff members. The processing operations in question are therefore necessary for the performance of ESMA's mission carried out in the public interest on the basis of the EU Staff Regulations in conformity with Article 5(a) of the Regulation.[3]

However, the data subjects' consent cannot be considered as a legal basis for the processing operations under analysis. 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, consent is a sensitive matter as it is doubtful whether data subjects can freely provide *"unambiguous consent*" in an employment context, taking into account the power imbalance between employee and employer.

Article 5(d) of the Regulation may be considered as an additional ground for legitimising any further processing of medical data collected on the basis of the provisions of the Staff Regulations or other legal instruments adopted on the basis of the Treaties, for the purpose of ensuring medical follow up. Of course, data subjects should be adequately informed before the further processing of their medical data and they should have the possibility to withdraw their consent at any time without prejudice to their rights.

The EDPS therefore recommends that ESMA clarify the issue of consent in the notification, as explained above.

**2) Recipients and processors**

ESMA lists the Commission's medical service as recipient.

ESMA has concluded a Service Level Agreement (SLA) with the Commission's medical service for carrying out the pre-recruitment examinations and annual check-up visits.

In light of Article 23 of the Regulation, the Commission's medical service is acting on behalf of ESMA and is therefore classed as processor. This is because it is obliged to carry out the processing only on instructions from the controller - ESMA (Article 23(2)(a)). The Commission's medical service's obligations regarding confidentiality and security measures are also laid down in the SLA (Article 23(2)(b)).

[3] Recital 27 of the Regulation explains that this provision is meant to also cover processing necessary for the internal management and administrative functioning of the institutions.

The EDPS therefore recommends that ESMA indicate in the notification and in the privacy statement that the Commission's medical service acts as processor on behalf of ESMA in light of the requirements of Article 23 of the Regulation.

**3) Quality of data**

ESMA pointed out that the agency has no access to medical information of its staff members and the Commission's medical service keeps the medical files of the agency's staff members.

However, two administrators from the HR Team of ESMA collect sick leave certificates from the staff members and keep them in a folder, which is only accessible to them.

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 Team of ESMA 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. 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 notes that confidentiality declarations are signed by the administrators in charge and sufficient security measures seem to have been adopted for the storage of the sick leave certificates. Nevertheless, ESMA should consider modifying its policy so that staff members send their sick leave certificates directly to the Commission's medical service. The Commission will then inform the HR administrators in charge about the administrative data, such as the name, surname and duration of absence of the staff member. This is a best practice followed by a significant number of agencies.

**4) Information to be given to the data subject**

In light of Articles 11 and 12 of the Regulation, ESMA has to provide all necessary information to all data subjects before a processing operation is launched in order to guarantee a fair and transparent processing in respect of the data subjects. ESMA should therefore attach the "*privacy statement on health*" to the document entitled "*annual medical check-up's - ESMA provisional procedure*".

***Identity of the controller***
The privacy statement mentions ESMA as controller. The EDPS reminds ESMA that from a legal perspective, ESMA is the responsible controller of these processing operations. In practice, the Operations Division (HR Team) is responsible for internally managing the processing operations under analysis, as it is correctly indicated in point 2 of the notification. A contact person from the HR should also be indicated in the privacy statement, so that data subjects may contact him/her directly, allowing written requests and confidentiality.

***The recipients of the data***
In light of Articles 11(1)(c) and 12(1)(d), ESMA should list the Commission's medical service as a processor (see point 2 above).

***Right of access***

On the basis of Articles 11(1)(e) and 12(1)(e), ESMA should also 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 data subjects fully understand their rights.

With regard to the right of access, ESMA should indicate that:
- non-recruited candidates and trainees may also exercise their rights of access and
- 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, ESMA 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.

ESMA should revise the privacy statement accordingly.

**Conclusion**

In light of the accountability principle, the EDPS trusts that the ESMA will duly implement the above recommendations so that the processing under analysis is in conformity with the Regulation.

We have therefore decided to close the case.

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

Yours sincerely,

(**signed**)

Wojciech Rafał WIEWIÓROWSKI

Cc: Mr Andrea LORENZET, HR Team leader.
Ms Sophie VUARLOT-DIGNAC, Acting Data Protection Officer.
Mr Panagiotis PAPAPASCHALIS, Deputy Data Protection Officer.
Mr Enrico GAGLIARDI, Assistant Data Protection Officer.

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