EUROPEAN DATA PROTECTION SUPERVISOR

WOJCIECH RAFAŁ WIEWIÓROWSKI
ASSISTANT SUPERVISOR

Mr Carlo des DORIDES
Executive Director
European Global Navigation Satellite Systems Agency (GSA)
Janovskeho 438/2
170 00 Prague 7
Holesovice, Czech Republic

Brussels, 17 March 2016
WW/XK/sn/D(2016)0662 **C 2015-1129**
Please use edps@edps.europa.eu for all correspondence

Subject: **Prior-check Opinion on the processing of health data at the European Global Navigation Satellite Systems Agency (case 2015-1129).**

Dear Mr Dorides,

On 22 December 2015, the European Data Protection Supervisor (EDPS) received an updated notification and revised documents for prior-checking under Article 27(2)(a) of the Regulation (EC) n° 45/2001 (the Regulation) from the Data Protection Officer of the European Global Navigation Satellite Systems Agency (**GSA**). The notification concerns the management of health data at GSA[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 visits, annual check-ups, and sick leave of the agency's staff members.

According to Article 27(4) of the Regulation, this Opinion must be issued within a period of two months, that is, no later than 24 March 2016, taking into account a suspension due to a request for further information[2].

The notification and relevant documents are analysed in light of the EDPS Guidelines on health data in the workplace (the Guidelines)[3]. The EDPS Joint Opinion related to the processing of health data by 18 agencies[4] is also applicable in the present case**.**

[1] The present notification (case 2015-1129) replaces the notification submitted in the case 2014-0472. The contracts with the external contractors have been signed, but the provision of the medical services has not started yet.
[2] The case was suspended for further information from 14 January 2016 to 22 January 2016 and for comments from the DPO and the controller from 26 February 2016 to 11 March 2016.
[3] Issued in September 2009 and published on the EDPS website.

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

1) Lawfulness of the processing

GSA's notification, along with the privacy statement on pre-recruitment, annual medical visits and sick-leave, refers to Articles 5(a) and 5(d) of the Regulation as lawful grounds for the processing operations.

As the EDPS Guidelines explain, the legal basis for GSA to carry out pre-recruitment and annual medical visits and to collect sick-leave certificates is found in the EU Staff Regulations. These processing operations are necessary for assessing the staff members' ability to carry out their duties and of managing their sick leave. The processing operations under analysis are therefore necessary for the performance of GSA'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.

As to whether Article 5(d) of the Regulation is applicable, the EDPS considers that consent is a difficult issue, as it is doubtful whether data subjects can freely provide *"unambiguous consent*" in an employment context. However, Article 5(d) of the Regulation may be considered as an additional ground for legitimising 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. In such cases, it is fundamental that GSA informs its staff members to what exactly they should consent, as under Article 2(h) of the Regulation, consent is only valid if it is freely given, specific and constitutes an informed indication of the data subject's wishes.
The EDPS therefore recommends that GSA include the above clarification on Article 5(d) of the Regulation in the notification and in the privacy statement.

2) Processing of personal data on behalf of controllers

GSA has concluded two contracts with two external medical centres and a SLA with the Commission's medical service.

In both contracts with the two contractors respectively, Article II.6 on the processing of personal data is confusing. The first three paragraphs of this provision (Article II.6.1 to Article II.6.3) relate to the obligations of the controller (GSA) vis-à-vis the personal data of the contractor and of the contractor's rights. The other paragraphs (Article II.6.4 to Article II.6.6) describe the obligations of the contractor bound by the contract with GSA in compliance with the requirements of Article 23 of the Regulation. In order to avoid confusion, GSA should have included in both contracts two separate paragraphs, namely the contractor's rights/GSA's obligations on the one hand and the contractor's obligations towards GSA as to the processing of the personal data of its staff members on the other hand.

[4] Issued on 11 February 2011 and it concerned 18 agencies, case 2010-0071.

Moreover, GSA has chosen to use a standard data protection clause in both contracts whereas a tailor-made clause could have been developed due to the sensitivity of the processing operations under analysis. Although, regrettably, both contracts have already been signed, the EDPS recommends that GSA clarify the above distinction of rights and obligations via the channel of a privacy statement or any other appropriate channel it considers appropriate.

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

The notification states that staff members may be informed on the GSA intranet about the procedure with regard to the annual medical visits carried out by a private practitioner.

The EDPS reminds GSA 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 also mention any special accommodations or working conditions the staff members might need.

GSA should therefore adopt the above good practice and include it in the notification.

4) Quality of data

It is not clear from the notification, whether staff members send their sick leave certificates to one of the external contractors or whether the HR of GSA collects them and keeps them in their personal files.

Sick 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 GSA should therefore, 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.

GSA should ensure that its staff members send their sick leave certificates directly to one of its external contractors and should specify which one. The external contractor will then inform the HR about the administrative related data, such as the name, surname and duration of absence of the staff member.

5) Retention periods

The retention periods regarding the medical data and the aptitude certificates in both the notification and in the privacy statement seem to be confusing.

The EDPS recalls that the **medical data** of the pre-recruitment and annual visits (if the staff member chooses to carry out the medical check-ups with the Commission's medical service)

should be kept for a maximum period of 30 years after the last document has been inserted to the medical file.

As to the **pre-recruitment aptitude certificates,** they 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.

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

Furthermore, GSA should indicate clearly in both the notification and in the privacy statement, which contractor keeps the medical files of its staff members.

6) Security measures

GSA'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.

7) Information to be given to the data subject

Rights of access and rectification

On the basis of Articles 11(1)(e) and 12(1)(e) of the Regulation, GSA should explain in the privacy statement 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, GSA 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[5].

As to the right of rectification, GSA should mention that staff members are entitled not only 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.

The time-limits for storing the data

In light of Articles 11(1)(f)(ii) and 12(1)(f)(ii) of the Regulation, GSA should clearly indicate in the privacy statement the retention period for medical data as well as for pre-recruitment aptitude certificates and which external medical contractor keeps its staff members' medical files. The recommendations under point 5 should be adopted.

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

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

Yours sincerely,

(**signed**)

Wojciech Rafał WIEWIÓROWSKI

Cc.: Mr Olivier LAMBINET, Head of Administration (and acting Head of Human Resources Department).
Ms Triinu VOLMER, Data Protection Officer.