GIOVANNI BUTTARELLI
ASSISTANT SUPERVISOR

[redacted]
Director
European Police College (CEPOL)
Bramshill, Hook
Hampshire RG27 0JW
United Kingdom

Brussels, 26 March 2014
GB/[redacted]/D(2014)0745 **C 2013-0893**
Please use edps@edps.europa.eu for all correspondence

Subject: Notification on the processing of health data in the workplace, case 2013-0893

Dear [redacted],

We have analysed the notification you have provided to the EDPS for prior-checking under Article 27(2)(a) of Regulation 45/2001 ("the Regulation") on the processing of health data at the European Police College **("CEPOL").** This will be analysed in light of the EDPS Guidelines on health data in the workplace ("the Guidelines").

The EDPS points out that the analysis and principles laid down in the EDPS Joint Opinion on the same topic ("the Joint Opinion")[1] are also applicable in the present case**.**

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

1) Lawfulness of the processing

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

As the Guidelines explain, the legal basis for CEPOL to carry out pre-recruitment and annual medical visits are found in the EU Staff Regulations. These processing operations are necessary for the purpose of managing and monitoring the sick leave of CEPOL's staff members, and to

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

assess their ability to carry out their role effectively in light of any medical issues. The processing operations in question are therefore necessary for the performance of CEPOL'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.

With regard to whether Article 5(d) of the Regulation is applicable, the EDPS considers that consent is a difficult issue here, 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 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.

The EDPS therefore recommends that CEPOL includes the above clarification on Article 5(d) of the Regulation in the notification and privacy statements.

2) Retention periods

In light of the Guidelines and Joint Opinion, the EDPS recommends that retention periods should be clarified in the notification, and in the privacy statements on pre-recruitment and annual check-up medical visits. The text should make clear that on one hand, ***medical results and reports*** are kept in the medical files for a maximum period of 30 years after the last document has been inserted in the file. On the other hand, personal files, where the ***aptitude certificates*** are stored, are kept for 10 years after the end of the period during which a staff member is in active employment or the last pension payment.

CEPOL should also indicate whether it is the Commission's medical service or the external medical service provider which keeps the medical files of CEPOL's staff members.

The retention period of the administrative data related to sick leave certificates should also be indicated in the privacy statement.

3) Right of access and rectification

In the notification, CEPOL has explained how the rights of access and rectification are granted, in light of the EDPS Guidelines.

However, the privacy statements on pre-recruitment and annual check-up medical visits simply make reference to the existence of these rights. The EDPS recommends that CEPOL supplements the privacy statements with the explanations contained in the notification, so that data subjects fully understand their rights.

4) Recipients and processors

The EDPS notes that in both privacy statements on pre-recruitment and annual check-up medical visits, CEPOL lists the Commission's medical service and the external medical provider as recipients.

CEPOL has implemented an SLA with the Commission's medical service for carrying out the pre-recruitment medical visits and has contracted an external medical provider in London to carry out the pre-recruitment and annual check-up visits. In light of Article 23 of the Regulation, both parties are acting on behalf of the agency and are therefore classed as processors rather than recipients. This is because they are obliged to carry out the processing only on instructions from

the controller - CEPOL (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 CEPOL clarifies that the Commission's medical service and the external medical provider act as processors on behalf of CEPOL in light of the requirements of Article 23 of the Regulation.

In the context of the follow-up procedure, please send revised versions of the notification and privacy statements within a period of 3 months, to demonstrate that **CEPOL** has implemented the above EDPS recommendations.

Yours sincerely,

(signed)

Giovanni BUTTARELLI

Cc : [redacted] Data Protection Officer
[redacted] Head of Corporate Services Department