EUROPEAN DATA PROTECTION SUPERVISOR

GIOVANNI BUTTARELLI
ASSISTANT SUPERVISOR

Mr Jan KILB
Data Protection Officer
European Court of Auditors
12, rue A. de Gasperi
L - 1615 LUXEMBOURG

Brussels, 21 December 2009
GB/RB/ktl D(2009)1826 **C 2009-639**

Dear Mr. Kilb,

I am writing to you regarding the prior check notification concerning the Court of Auditors Identity & Access Management ('CoA I&A Management System'), which you submitted to us for prior checking on 8 October 2009 ('notification'). The notification was given the case number C 2009-639.

The CoA I&A Management System entails the use of certain information (name, surname, birth date) in order to grant users with application accounts and access rights access to such accounts. After an examination of the notification and additional information provided by the data controller we consider that **there are is basis under Article 27 of the Regulation (EC) No 45/2001 to subject the processing at stake to prior checking.**

The potential legal basis for prior checking of the CoA I&A Management System are Article 27.1 and 27.2 (b) of Regulation 45/2001. Article 27.1 subjects to prior checking "*processing operations likely to present specific risks to the rights and freedoms of data subject by virtue of their nature, their scope or their purposes*". Article 27.2 (b) subjects to prior checking processing operations *"intended to evaluate personal aspects relating to the data subject, including his or her ability, efficiency and conduct*". For the reasons described below, we have concluded that the CoA I&A Management System does not meet the criteria of Article 27.1 and Article 27.2 (b).

Regarding Article 27.2 (b). The CoA I&A Management System assigns access rights and manages the effective access to applications on the basis of such rights. Whether individuals (for example, CoA staff) have certain access rights depends on pre-defined rules, based on the attributes of a user (i.e.., A is an AD civil servant that belongs to Unit Y and accordingly has access to application 1 and 2). CoA I&A Management System will not "evaluate" individuals but rather check their access rights in order to authenticate those who have access rights. The mere checking of the rights based on pre-defined rules as described above does not entail a *de*

facto evaluation of user's, of their efficiency, competences, ability to work, behavior (see below).

Regarding Article 27.1. The CoA I&A Management System will not log/retain user activity which may have enabled the evaluation of his/her behavior for different purposes. This reinforces our view that the processing does not *present specific risks to the rights and freedoms of data subjects.* If, on the contrary, the CoA I&A Management System had recorded users' activities, such risk may have been present insofar as the recording itself would have produced detailed information of employees' behavior (use of applications, timing of such use, etc), particularly in the light of the potential uses of such information.

For the reasons described above, the EDPS considers that the data processing is not subject to prior checking. However, if you believe that we have overlooked factual information or there are other factors justifying our checking of the CoA I&A Management System, we are of course prepared to review our position. It goes without saying that the remaining provisions of Regulation (EC) No 45/2001 are fully applicable. In this context, we want to stress the importance of ensuring that individuals are fully informed of the data processing; in this context, information campaigns and direct notices are essential.

I would be thankful if you could forward these considerations to the data controller.

I remain at your disposal should you have any questions concerning this matter.

Yours sincerely,

(Signed)

Giovanni BUTTARELLI