EUROPEAN DATA PROTECTION SUPERVISOR

JOAQUIN BAYO DELGADO
ASSISTANT SUPERVISOR

Ms. Petra CANDELLIER
Ms Elena FIERRO
Data Protection Officer
EESC/COR
Rue Belliard 101
B - 1040 BRUXELLES

Brussels, 24 November 2006
JBD/ZB/ktl D(2006)1278 **C 2006-0506**

Subject : "USER ACCOUNT MANAGEMENT" at (EESC) and (CoR)

Dear Ms Candellier and Ms Fierro,

We have concluded from our examination of the prior checking notification that the "User account management" at the European Economic and Social Committee (EESC) and the Committee of the Regions (CoR) (EDPS case ref.: 2006-506) is not subject to prior checking by the EDPS.

The Notification was submitted under Article 27(1) of Regulation (EC) 45/2001 ("Regulation"), noting that the case involves e-monitoring. As the forthcoming e-monitoring paper of the European Data Protection Supervisor ("EDPS") will highlight, electronic communications can be subject to prior checking by the EDPS under two main scenarios:

A) Article 27(1) of the Regulation subjects to prior checking all processing operations which are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes. Chapter IV of the Regulation contains a particular provision on the confidentiality of communication (Article 36). Where there is a breach of confidentiality of communication, a specific risk to the rights and freedoms of data subjects may exist, and therefore, the processing operation is subject to prior checking by the EDPS.

B) Article 27(2) of the Regulation contains a non-exhaustive list of processing operations that are likely to present specific risks. The list includes, *inter alia*, (i) processing of data "relating to suspected offences or offences or security measures" (Article 27(2)(a)) and (ii) processing operations "intended to evaluate personal aspects relating to the data subject, including his or her ability, efficiency and conduct" (Article 27(2)(b)). Where a mechanism is in place to monitor the communication network for purposes of Articles 27(2)(a) and/or 27(2)(b) of the Regulation, the processing operations must be submitted to EDPS for prior checking.

This means that not all electronic communication systems are necessarily subject to prior checking. In fact, if the confidentiality of communications is not breached, and the IT infrastructure is not used to monitor employee conduct, there is often no reason to submit the electronic communication systems for prior checking.

Based on the foregoing consideration, in the current case, although the user account management system is clearly part of the electronic communication system of the EESC and the CorR, this fact alone does not mean that the user account management system, in itself, should be subject to prior checking.

We reviewed the Notification and its various attachments to see whether they contain any information that would suggest that the user account management system would need to be prior checked based on the grounds discussed above. In particular, we looked for elements of breach of confidentiality, or indications that the system is used to monitor offences, ability, efficiency, or conduct, as described above. We have not found any such indications. Therefore, **we have decided to close the case.** However, if you believe that there are other factors justifying prior checking of the user account management, we are, of course, prepared to review our position.

On a different note, aside from the matter of the user account management, we point out that the various attachments submitted along with your Notification suggest that other aspects of the IT infrastructure (rather than the user account management itself) might be used for e-monitoring purposes, and thus, certain operations carried out using the IT infrastructure might require prior checking by EDPS.

For example, the Internet Security Policy, attached to the Notification as Annex IV prohibits, among others, downloading software from the Internet, or using the network for illegal activities. The Internet Security Policy also provides that the system keeps log files of Internet use for a period of six months. The documents attached do not describe whether there is a monitoring mechanism put in place to check for violations of the Internet Security Policy, or whether Internet use, in general, is subject to any monitoring. In order to know whether there is a ground for prior-checking, the question whether the content and/or traffic data related to the Internet use (e.g. sites visited, duration of visits) are monitored and used to evaluate employee conduct must be answered. If the answer is yes, a prior checking notification needs to be submitted and needs to describe, in detail, the circumstances of monitoring and the related data protection issues.

Based on the information available to us at this stage, we are not in a position to tell whether there is, in fact, a need for submitting a new notification for prior checking on grounds of monitoring Internet use or on grounds of monitoring use of other aspects of the IT infrastructure; the assessment is for you to make. Of course, if, after your internal assessment, you are unsure whether to submit a new notification for prior checking, EDPS is available for you to consult under Article 27(3). In case of doubt about the need for prior checking or the exact scope of prior checking, we always encourage you to take advantage of the opportunity of consulting EDPS.

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

Thank you for your cooperation,

Yours sincerely,

Joaquín BAYO DELGADO
Assistant European Data Protection Supervisor