



JOAQUIN BAYO DELGADO
ASSISTANT SUPERVISOR

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

Brussels, 26 January 2007
JBD/EDK/ktl D(2007) 117 C 2006-0507

Dear Ms Candellier and Ms Fierro,

After carefully examining the available information on the "**E-mail system** of the European Economic and Social Committee (EESC) and the Committee of the Regions (CoR)", the European Data Protection Supervisor ("EDPS") concludes that **the case is not subject to prior checking and he closes the case.**

The prior checking notification was submitted under Article 27(1) of Regulation (EC) 45/2001 noting that the case involves e-monitoring.

As the forthcoming e-monitoring paper of the 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 the 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.

The 22-01-2007 meeting with the controller clarified that: 1) No regular or random monitoring of the use of the email system is put in place to check for the inappropriate use of emails. 2) Neither the content nor traffic data are used in any ways to evaluate personal aspects of the individuals. 3) Log files are kept for a maximum of six months and are used for problem solving and preparing anonymous statistics. They could be made available to the competent authorities in the context of an official investigation.¹

Since the confidentiality of communication is not breached and the IT infrastructure does not have a monitoring mechanism which aims to control employees conduct, the email system in itself does not present the specific risk that is required for a prior checking by the EDPS. However, if you believe that there are other factors justifying prior checking of the email system of the EESC and CoR we are, of course, prepared to review our position.

Without prejudice to the above considerations the EDPS will examine access to log files or to content data in the course of prior checking those procedures where the authorities can access to those data with the purpose of evaluating the behaviour or conduct of the individuals or where data on (suspected) offences are concerned, e.g. in the course of a disciplinary procedure. Disciplinary procedure is among the priority themes for *ex-post* prior checking and it is most important to receive the notification as soon as possible.

In the course of our analysis we have spotted an aspect the EDPS would like to draw the attention of the controller of the email system on. In the context of the Spamcheck application, the controller should reconsider whether it is necessary to keep the email addresses to which users have sent emails and from which they have received emails (that were not tagged as spams) in a database, with the aim to use those for filtering against spam as a "white list". These lists rise doubts as to their proportionality and excessiveness and, in any case, as to their being kept for an unlimited duration, instead of linking their storage period to the end of term in service of the employee concerned. The EDPS requests the controller to inform him about his conclusions, after his considerations on the ways the system is established.

Aside from the email system, I take the occasion to address the issue whether **Internet use**² is subject to prior checking, because the memo of the abovementioned meeting of 22-01-2007 with the controller clarified the crucial issues. Now it is clear that "*[t]here is no monitoring mechanism put in place to check for violations of the Internet security policy. Internet log files are not used to evaluate employee conduct. Log files are kept for a maximum of 6 months and are used for solving problems and preparing anonymous statistics. They could be made*

¹ "...access may be granted where the written request has a legal basis and where access is necessary in the context of an ongoing investigation," in particular, for OLAF, AIPN, EDPS, European Ombudsman, DPOs of the two Committees, judicial authorities in the exercise of their competence. Part C of *Système Informatique Regles d'Utilisation*, decision of 23 August 2006 of the EESC and CoR. Decisions No 451/06 (EESC) and Decision No 280 (CoR).

² This question was raised in the EDPS final answer to the controller in the context of the "User account management" at EESC and CoR (EDPS case ref.: 2006-506).

available for competent authorities in the context of an official investigation." With similar considerations as above, the EDPS concludes that it is not necessary to submit a prior checking notification to the EDPS on the use of Internet.

I would appreciate if you could share these considerations with the controller. We remain available for any further consultation on the above matters.

Yours sincerely,

Joaquín BAYO DELGADO