GIOVANNI BUTTARELLI
ASSISTANT SUPERVISOR

Ms Zografia PYLORIDOU
Data Protection Officer
European Railway Agency
120 rue Marc Lefrancq
BP 20392
F-59307 Valenciennes Cedex
FRANCE

Brussels, 19 October 2011
GB/IC/kd/D(2011)1807 **C 2011-0671**

Dear Ms Pyloridou,

I refer to your letter of 4 July 2011 by which you submitted to the European Data Protection Supervisor ("EDPS"), amongst other things, a consultation on the need or not to subject ERA policies on mobile telephony, email and internet[1] to prior checking (case 2011-0671).

After having carefully examined the available information, including the information gathered through exchanges of e-mails between you and the EDPS staff, the EDPS has come to the conclusion that specific aspects of the ERA procedures **shall be subject to prior checking**.

The use of electronic communication can be subject to prior checking by the EDPS under two main scenarios:

1) Article 27(1) of Regulation (EC) No 45/2001 ("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, scope or their purposes. Chapter IV of the Regulation contains a specific provision on the confidentiality of communications (Article 36). Where there is a breach of confidentiality of communications, 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.

2) 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

[1] The following documents were provided to the EDPS: "2.0 Use of the ERA ICT owned resources", "2.1 Identity and Access Management Policy", 2.2. Internet Acceptable Use Policy", 2.3 Electronic Communications Policy", and 2.4 E-mail Acceptable Use Policy".

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 at risk, 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.

Although section F11 of ERA policy on the Use of the ERA ICT owned resource provides that "*The Agency shall routinely monitor usage patterns of the ICT resources*", it was clarified through several exchanges of emails between yourself and the EDPS staff 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) in general, neither the content nor traffic data are used to evaluate personal aspects of the individuals, 3) log files are usually kept for 90 days (emails) and 60 days (internet) and are used for problem solving.

On the basis of available information, the EDPS considers that as long as the general monitoring of the use of the ERA ICT owned resources performed by the ERA does not breach the confidentiality of communication and is not aimed at controlling employees' conduct, it does not present the specific risks that would make it subject to prior checking.

Having said that, the EDPS however notes that the Internet Acceptable Use Policy allows, in specific circumstances, the examination of log internet traffic to "identify user's behaviours that are improper and exposing the Agency in serious jeopardy". Since this procedure allows for the evaluation of a person's conduct, it should be subject to prior checking under Article 27(2)(b) of the Regulation.

Furthermore, section V.B of the ERA Electronic Communications Policy sets forth a procedure for accessing emails of staff, with specific conditions depending on whether this is done with or without their consent. This procedure, when applied, may entail a breach of the confidentiality of communications which would affect the rights and freedoms of data subjects in the meaning of Article 27(1) of the Regulation. As a result, ERA's procedure for accessing the content of emails should also be subject to prior checking by the EDPS.

Finally, the EDPS notes that the policies transmitted are not detailed enough as concerns mobile telephony and it is therefore difficult to assess the type of monitoring performed in that respect. The EDPS emphasizes that any monitoring by ERA of the use of mobile telephony which involves a breach of the confidentiality of communication or which is aimed at controlling employees conduct should also be subject to prior checking.

We thereby invite you to submit without delay the relevant data processing operations to prior checking by the EDPS.

Sincerely yours,

(**signed**)

Giovanni BUTTARELLI