EUROPEAN DATA PROTECTION SUPERVISOR

COMMENTS ON THE COURT OF AUDITORS'S INTERNET SECURITY POLICY

I. INTRODUCTION

1. This paper contains comments on the ECA Internet Security Policy that aim at ensuring the full respect of the right to protection of personal data and privacy.

2. The comments are divided in two sections. The first section analyses whether the ECA Internet Security Policy is subject to prior checking. The second section assesses the extent to which the ECA Internet Security Policy is in line with the main data protection and privacy principles and proposes amendments to the Policy to ensure full consistency with them.

II. THE INTERNET SECURITY POLICY AND THE QUESTION OF ITS PRIOR CHECKING

3. The purpose of the Internet Security Policy is to identify and prevent information security breaches and misuse of the ECA Information and Communication Technology Infrastructure ("ICTI"). Towards this end, the Internet Security Policy contains, among others, rules of conduct that apply to users[1] who utilise the Court's ICTI. In particular, it describes the availability and restrictions to the use of Internet services and connections. The Internet Security Policy also informs users about the systems set up to prevent access to certain types of content as well as the monitoring practices that the ECA will put in place in order to verify compliance with the Internet Security Policy.

4. The Internet Security Policy does not cover email monitoring. A separate policy applying to email monitoring is under preparation. The EDPS expects to be consulted under Article 28(1) of Regulation (EC) 45/2001 before the adoption of such a policy.

5. The EDPS has analysed the extent to which the Internet Security Policy must be prior checked under Article 27 of Regulation (EC) 45/2001. Prior checking is designed to address situations that are likely to present certain risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes. Processing operations likely to present such risks are specified in Article 27.2 and notably cover a) "*processing of data relating to {...}suspected offences, offences...*" and b) "*processing operations intended to evaluate personal aspects relating to the data subject, including his or her ability, efficiency or conduct*".

[1] Users include the ECA staff, experts and trainees as well as employees who work for a third party service provider or any other person making use of the ECA Information and Communication Technology Infrastructure.

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 63
E-mail : edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax : 02-283 19 50

6. Taking into account on the one hand that the monitoring of the use of the Internet as described in the Internet Security Policy leads to the evaluation of users' conduct and, on the other hand, that such monitoring entails the collection of data related suspected offences, in principle, such monitoring and related data processing operations are likely to be subject to prior checking ex Article 27 a) and b) of Regulation (EC) 45/2001.

7. The EDPS understands that ECA is still fine tuning the technical details regarding the monitoring of Internet usage and the related data processing operations that this activity will entail. Therefore, the EDPS recommends that ECA submits the prior check notification when ECA will have reached a decision on all the details regarding how the monitoring operations and concomitant data processing operations will take place.

8. In completing the prior check notification, the ECA should describe the data processing operations carried out towards monitoring the Internet usage to ensure compliance with the Internet Security Policy. Further uses of the information should not be included. In particular, the EDPS notes that as a consequence of the monitoring of the Internet usage, ECA may become aware of information pointing towards the perpetration of infringements of the Internet policy and other unlawful actions. Later, ECA may process some of this information for the purposes of opening administrative enquires and disciplinary procedures. ECA's further processing of information for the purpose of administrative enquires and disciplinary procedures are not part of the prior check on the monitoring of the Internet. In fact, ECA's administrative enquires and disciplinary procedures have already been prior checked by the EDPS[2].

III. SUBSTANTIVE COMMENTS

9. The EDPS welcomes the ECA's decision to put in place an Internet Security Policy for users of the ECA Information and Communication Technology Infrastructure. Employees at the ECA and other users need to know not only what they are allowed to do when they use the ICTI but also which personal information is collected about them when ECA engages in the monitoring of their usage of the Court's ICTI. The EDPS attaches a great deal of importance to ensuring transparency of the employers' activities.

III.1 Communication of the Internet Security Policy to Users: The communications channel.

10. As important as having a policy is its communication to its intended users. It is important that the channel used to communicate the policy enables individuals to take notice of its content in an effective way. This is a consequence of the principle of transparency *ex* Article 11 and 12 of Regulation (EC) 45/2001. Regarding the communication of the ECA Internet Security Policy to users, Paragraph 2 of the Policy says "*This policy will be delivered to, and accepted by all users prior to using the Internet services at the Court*".

11. Whereas the mere fact of delivering the policy to users is a positive step towards communicating its content to users and, thus, providing transparency, the EDPS would like to insist on the further need to raise awareness of the Internet Security Policy. To do so, many different actions are possible. For example, it may be appropriate for the ECA to distribute summaries of the main points of the Internet Policy (i.e., when and how monitoring takes place) on paper and also electronically. It may also be appropriate to ensure that the policy or its main points are available on line in a prominent place. Also, when users receive personal messages informing them of the reasons why access to a web site is refused, it may be appropriate to include a link to the Internet Security Policy for

[2] Opinion of 22 December 2005 (case 2005-0316)

further information about how the monitoring takes place.

12. Furthermore, in order to raise awareness of the Policy, the EDPS also recommends that once the policy is in place, the ECA conducts periodic audits of usage practices to establish whether current procedures are in line with the stated policy, and consistently enforces breaches of the policy. The policy should inform users of such practices. The acceptance of the policy by users is discussed in paragraph III.3 below.

III.2. Necessary content of the Internet Security Policy

13. Necessary information to be provided in an Internet security policy includes *(i)* the systems implemented to prevent access to certain sites *(ii*) the systems implemented to detect misuse and *(iii)* whether the private use of the Internet services is allowed. The extent to which the ECA Internet Security Policy provides this information is discussed below.

14. In providing this information is important to ensure that the policy can be easily understood by users. To achieve this, it should be drafted in a clear and concise way. In this regard, the EDPS finds the Internet Security Policy reasonably accessible and comprehensible, so as to enable its users upon reading to have an accurate understanding of the existing rules and also of the ECA monitoring practices towards enforcing the policy. The EDPS appreciates various features of the policy that serve this purpose. For example, the Policy clearly delineates what type of conduct is expressly prohibited (Paragraph 5 "Downloading of software is not allowed"). However, as further illustrated below, the EDPS considers that some improvements towards providing more clarity and accuracy are possible.

15. As far as informing users of the **systems aiming at preventing access** is concerned, the ECA Internet Security Policy says that *"The Court will use software filters and other techniques whenever possible to restrict access to inappropriate information (racism; terrorism; sexual; obscene or religiously offending; etc). When access is denied to information, the user will get a clear and personal message showing the reasons why the access was refused"*. The EDPS welcomes the provision of this information.

16. As to the concrete content to which the Court has banned access, Paragraph 17 says: "*Viewing racist, sexual, terrorist, obscene or religiously offending sites is inappropriate*". The EDPS notes that in addition to the mere viewing of such types of information it may be necessary to add that the *creation* of such types of information would likewise be deemed inappropriate. Some web sites allow individuals to post material. In such cases the posting of information which is racist, sexist, terrorist, obscene or religiously offending will also be considered as inappropriate.

17. As outlined under Paragraph 13 above, an Internet Policy must also inform users about the **systems implemented to detect misuse**. In other words, if the employer engages in monitoring of the Internet usage, this must be clearly indicated in the policy. Paragraphs 25 to 29 describe the monitoring of ECA ICTI for the purpose of managing and protecting the Court's information system. The EDPS considers that the Internet Security Policy fails to inform clearly and completely about the monitoring of the Internet use. The fact that monitoring occurs at three levels (Paragraph 25, monitoring of the traffic volume to detect abuse; Paragraph 26 monitoring for technical reasons or for investigation procedures and Paragraph 27 monitoring of access to inappropriate information) should be made more transparent. As the text stands, the way in which monitoring takes place is not absolutely clear.

18. More specifically, this section does not define what is included in the log files. It is

unclear whether the ECA logs only the web sites that the user successfully accessed or also those whose access was denied (because they were deemed to have improper content).

19. Furthermore, taking into account the common misconception that the private usage of ICTI is not controlled, it may be necessary to include a statement to reinforce awareness that any use of ECA internet services will be monitored. Such a statement should stress the fact that monitoring will also take place regarding the private use of the system, in other words, during the time when private use is allowed. Furthermore, in order to ensure that users do not forget that their usage of the Internet is monitored, it may be appropriate to set up automatic pop-up messages that are sent to employees whenever they access the internet from their PCs. The messages could say that "ECA will conduct routine monitoring of its ICTI, and employees should be aware that their use of the ECA ICTI is subject to monitoring ".

20. The EDPS notes that Paragraph 25 refers to anonymous monitoring: "*The Court automatically, anonymously logs all attempts to visit web sites or download files*". The EDPS appreciates the deletion of the word anonymous from a second version of the Internet Security Policy because the reference to "anonymous" is misleading. Indeed, taking into account that by analysing the log file the Court can ascertain the identity of a user who has accessed the web site; it means that the logs are not anonymous.

21. In addition to informing users about the systems to prevent access and misuse of the Internet services, a policy must inform about **conditions under which private use of the Internet is permitted.** In this regard, the EDPS welcomes paragraph 18 which provides for the use of ECA ICTI facilities for private use. A policy of zero tolerance for the private use of ECA ICTI may be considered to be impractical and unrealistic as it fails to reflect the degree to which the Internet can assist employees in their daily life. Furthermore, the Court of First Instance itself has recognised that communication networks including the Internet can be reasonably used for personal purposes[3].

22. Paragraph 18 states the timing during which individuals can use ECA ICTI facilities for private use which is before 8:00 and after 18:00. In the same paragraph 18, it may be helpful to indicate what may constitute an abuse of private use of the ECA ICTI not only in terms of timing (abuse is the use of the ECA ICTI outside the defined hours) but also in terms of amounts of data. For example, it may be useful to indicate that downloading of large non-work-related large audio or video streams/files is abusive.

III.3 Legitimacy

23. This principle means that any data processing operation can only take place if the Court fulfils/meets one of the legal grounds provided in Regulation (EC) 45/2001, and thus has legitimate purposes. Of the various legal grounds provided for in Article 5, the Internet Security relies on users' consent. In this regard, Paragraph 2 of the Policy says "*This policy will be delivered to, and accepted by all users prior to using the Internet services at the Court*". The EDPS is uncertain about how the acceptance will be sought and calls for clarification. In this regard, it is important that the acceptance is express, not implied.

24. In relying on consent as legal ground to legitimise the data processing, the ECA must realise that in order to be valid, this consent, whatever the circumstances in which it is given, must be a freely given, specific and informed indication of the individual's wishes. In the case in point it is uncertain whether consent will meet this standard. In particular,

[3] Case T333/99 X. European Central Bank.

the EDPS questions whether individuals will be able to make a real choice. If an individual refuses to give consent, is the Court in a position to refrain from monitoring the Internet usage of such an individual? If the answer is no, the alternative is that this person probably will not be able to use the Internet, which in some cases may raise the issue of whether he/she can perform his/her tasks which may jeopardise its job position. In sum, if users are compelled to consent because otherwise their ability to perform their job and even their job may be at stake, consent cannot be considered as freely given.

25. As further described below, the EDPS considers that the existing data protection legislation foresees legal grounds other than consent that legitimise the monitoring of Internet usage for the purposes stated in the Internet Security Policy.

26. In particular, Article 5 a) of Regulation (EC) 45/2001 establishes that personal data may be processed if "*processing is necessary for the performance of a task carried out in the public interest on the basis of the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof or in the legitimate exercise of an official authority vested in the Community institution or body...".* According to recital 27 "*processing of personal data for the performance of tasks carried out in the public interest by the Community institutions and bodies includes the processing of personal data necessary for the management and functioning of those institutions and bodies".*

27. The EDPS notes that the main purpose of the processing of personal data in the context of the Internet Security Policy is to identify and prevent information security breaches and misuse of the ECA Information and Communication Technology Infrastructure. If the ECA ICTI were to collapse, it would be difficult for the Court to function properly. In this regard, it appears that protecting the Court's computer network from Internet dangers and abuse is necessary for the management and functioning of the ECA as an institution. Hence, by processing personal data through the monitoring its ICTI, ECA is carrying out a task or function necessary for its management and functioning, which falls under the allowed purposes *ex* Article 5 a) of Regulation (EC) 45/2001.

28. Furthermore, Article 37(2) of Regulation (EC) 45/2001 provides for an additional legal ground authorising ECA to keep traffic data, in this case, log files[4]. In particular, Article 37 (2) provides that traffic data, as indicated in a list agreed by the EDPS, may be processed for the purpose of telecommunications budget and traffic management, including the verification of the authorised use of the telecommunications systems.

29. The concept of "*verification of authorised use*" is central as it concerns the possible use of traffic data beyond traffic and budget management. In particular, it allows the use of traffic data to ensure the security of the system/data and respect of the law, Staff regulations or other provisions. Authorised use can be determined in terms of web site visited; volume (size of document downloaded), cost or duration. Precisely in this case, the monitoring is carried out to verify whether users employ the ECA ICTI for the uses that the Court has authorised.

30. It would thus be more appropriate to replace "acceptance by users" as envisaged in Paragraph 2 of the Policy by a feature simply confirming that the user is aware of its existence and has taken note of its main provisions. However, in practice, this could still not serve as evidence that the user has read the complete policy and has fully understood its consequences.

[4] Log files containing the IP address of user, web address connection can be deemed to be traffic data as they are used for traffic purposes.

III.4. Necessity and finality principles

31. The EDPS considers that the monitoring activities for the purposes outlined in the Internet Security Policy respect the necessity and finality principles according to which monitoring can only take place when it is absolutely necessary and for specified purposes.

32. The application of the above principles requires a balanced approach between the right for the institution to monitor Internet usage and the right for the user to see their privacy respected. The EDPS welcomes the following features of the monitoring which favour such balance.

33. In the first place, the EDPS is positive towards the practice of using filter software which entails a preventive approach to the misuse of the Internet rather than a detective one. The interest of the Court is better served in preventing Internet misuse through technical means, including software and other techniques, rather than expending resources on detecting misuse. At the same time, the use of filters and similar techniques constitutes a less privacy invasive solution than engaging in continuous monitoring.

34. Secondly, the monitoring by Department managers of traffic volume by department rather than by individual usage also favours a balanced approach (despite of the fact that individual consumption can be determined if abuse is suspected).

35. On the other hand, the EDPS considers that the balanced approach has not been respected as regards the use of the Internet for private purposes. While the EDPS welcomes the Policy's provision for the private use of ECA ICTI facilities, he finds that the private use allocated to individuals is too restrictive (only before 8:00 and after 18:00). This schedule would preclude some staff from exercising the right to use the ECA facilities at all. For example, it is well known that parents often have a 8:00 to 18:00 pm schedule which coincides with school hours. The EDPS considers that some private use should be allowed in the course of the day, for example, between 12 and 2 pm.

III.5. Data retention

36. Article 37 of Regulation (EC) 45/2001 provides for specific measures as concerns the conservation of traffic and billing data. As pointed out under Paragraph 18 above, log files are included in such a definition. Article 37.2 of Regulation (EC) 45/2001 provides that traffic data may be processed for the purpose of budget and traffic management, including the verification of authorised use of the telecommunications systems. However they must be erased or made anonymous as soon as possible and in any case **no longer than six months** after collection, unless they need to be kept for a longer period to establish, exercise or defend a right in a legal claim pending before the court.

37. The EDPS notes that Internet Security Policy does not refer to the time period during which log files will be kept in order to perform monitoring. Hence, he calls upon the ECA to fix a deadline in accordance with the rules outlined above and to communicate this deadline to users in the Internet Security Policy.

38. In setting up a retention policy in line with Article 37.2 of Regulation (EC) 45/2001, ECA must take the following into account:

39. First, as a general rule the ECB must set up a deadline during which it will keep log files. In doing so, the ECB may decide to keep the logs for a maximum period of 6 months. As a general rule, the data can not be kept for a longer period[5]. To comply with this rule, it

[5] In complaint 2007/597, the EDPS has called upon the ECA to shorten the storage time of email communications in order to respect

would be appropriate to delete the data periodically and automatically.

40. Second, if monitoring of log files leads the ECA to suspects that an individual has infringed the Internet Security Policy or is engaged in other unlawful activity, the ECA will be allowed to keep the incriminating logs files in order to "*establish, exercise or defend a right in a legal claim pending before the court*". It should be noted that this measure should only take place on a case by case basis, when there is a legitimate suspicion that an individual has infringed the Internet Security Policy or is engaged in other unlawful activity and the ECA has opened an administrative inquiry. In this context Article 20 of the Regulation is also relevant insofar as it provides for possible restrictions to the principle of immediate erasure of the data as established in Article 37. 1 notably when the restriction constitutes a necessary measure to safeguard "*the prevention, investigation, detection and prosecution of criminal offences"*. Thus where relevant, log files may be processed in the frame of an administrative inquiry, whether it be a criminal or disciplinary offence.

III.6. Enforcement

41. Details of any enforcement procedures outlining how and when individuals will be notified of breaches of the policy and how they will be given the opportunity to respond to any such claims against them should be further developed.

Done at Brussels, 26 November 2007

Peter HUSTINX
European Data Protection Supervisor

Article 37. The EDPS calls upon the Court to take this into account in the drafting of the new email policy.