Opinion on a notification for prior checking received from the Data Protection Officer of the Court of Auditors related to Internet monitoring

Brussels, 10 November 2008 (Case 2008-284)

1. Proceedings

On 26 November 2007, the European Data Protection Supervisor (**EDPS**) issued comments on the Court of Auditors Internet Security Policy (**ISP**). The EDPS adopted his comments in response to a request for assessment received from the Court of Auditors (**CoA** or **Court**) pursuant to Article 46(d) of Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (**Regulation (EC) No 45/2001** or **Regulation**). In his comments the EDPS asked the CoA, among others, to submit a prior check notification to him concerning the Court's monitoring of its information and communication technology infrastructure, i.e. Internet infrastructure (**ICTI** or **Internet**).

Following the EDPS's request, on 6 May 2008, the Data Protection Officer of the CoA sent to the EDPS a notification for prior checking (**the Notification**) regarding the data processing operations related to monitoring of the Court's ICTI carried out by the Court's Directorate for Informatics and Telecommunications (**I & T Directorate**).

On 3 July 2008, the EDPS sent to the Data Protection Officer (**DPO**) of the CoA a request to confirm and clarify certain factual information regarding the Court's monitoring practices. The EDPS received the answers on 9 July 2008.

On 11 July 2008, the EDPS sent a draft prior checking Opinion to the CoA for comments.

On 3 September 2008, a telephone call took place between EDPS and CoA staff to discuss the recommendations contained in the draft prior checking Opinion sent to the CoA for comments. At the CoA's request, the deadline for providing comments was postponed until 29 September 2008, the date on which these comments were indeed received.

The comments provided by the CoA introduced important changes to the CoA monitoring procedures. In order to be able to examine the new monitoring practices, on 29 September 2008 the EDPS extended the deadline for adoption of a prior checking Opinion for one month. On the same date, the EDPS requested clarification of some aspects related to the new monitoring procedures from the CoA. The CoA sent the requested information on 2 October 2008. On 3 November 2008, the deadline for adoption of a prior checking Opinion was extended for an additional fifteen days.

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

2. Examination of the matter

This Opinion assesses the extent to which the data processing activities related to the monitoring of Court's ICTI are in line with Regulation (EC) No 45/2001. This Opinion does not assess further data processing operations that may take place as a result of administrative and disciplinary proceedings that may be initiated as a result of alleged violations of the CoA ISP.

The CoA data processing activities analyzed in this opinion are described in the Notification, in the Court of Auditors ISP, which was adopted by the Secretary General of the CoA on 29 January 2008, in the Procedure for Internet Monitoring (**MP**), yet to be adopted, and in the Frequent Asked Questions (**FAQs**). The data processing itself towards monitoring the users of the CoA ICTI has not started yet.

2.1. The facts

The data processing mostly consists in monitoring the use of the Internet made by those who employ the ICTI of the CoA. The ***purposes of the processing*** of the data are multiple and include the following: *(i)* to identify which ICTI resources are used at each moment in order to assess the resources that hinder normal traffic; *(ii)* to troubleshoot problems, for example when Internet access is not possible or is slow; *(iii)* to analyse security filters' efficiency in order to verify whether the content filter is not too restrictive or too lax. In addition, the purpose of the processing also includes *(iv)* verifying whether CoA users employ the ICTI in accordance with the allowed uses laid down in the CoA ISP. To avoid repetition hereafter purposes *(i)*, *(ii)* and *(iii)* may be summarised as one single purpose consisting in "ensuring the functionality of the network and avoiding security breaches".

The I & T Directorate has the primary ***responsibility for the data processing*** and some of the data processing operations will be performed by members of this Directorate (system administrators). However, an important part of the data processing will be performed by the IT Security Officer who does not report to the I & T Directorate but to the Director Administration and Finances. It is also important to note that the responsibility for the ISP resides in the Human Resources Directorate. Taken into account the shared responsibilities over the Internet monitoring policies and effective data processing practices, indeed three different Directorates are involved, it can be said that the role of data controller is jointly exercised by the three Directorates. For this reason and to avoid repetition, this Opinion will refer to the three entities that jointly exercise control over the data processing and are therefore the data controllers as the CoA or the Court.

The ***categories of personal data*** to be collected and further processed include all Internet access attempts (successful and unsuccessful) which are first logged and then further analysed. In particular, the information that will be logged includes the following: *(i)* user identification, *(ii)* volume of data exchanged from the Internet (in kbytes), *(iii)* date and time of the attempt to access the Internet, *(iv)* IP address of the PC, *(v)* time taken to process Internet request, *(vi)* content filter category, (vi) content filter result, *(vii)* PC number, *(x)* URL visited, *(xi)* request response and, *(xii)* TCPI P port number. Finally, the logging of unsuccessful attempts will reveal information regarding the cause of the inability to access the Internet (network errors, invalid web site names, timeouts, unknown web addresses, attempt to access filtered web sites, etc.).

The ***manual and automated data processing operations*** are closely interrelated. Whereas some data processing operations such as the initial collection of information are automatic,

later on, this information is processed by system administrators and by the IT Security Officer as follows:

First, the I & T Directorate will systematically register *all* Internet access attempts of the Court's users of ICTI. The content of the information logged includes the personal data described above under "categories of personal data".

Second, *system administrators* will examine the content of the log files at any time when *(i)* a technical problem is encountered and, *(ii)* when one or more performance indicators show an unusual value. They can report unusual patterns or activities suspected of being unlawful or against the ISP to the IT Security Officer.

Third, at the beginning of each month, the *IT Security Officer* will analyse the log files registered the month before. Such analysis is based on the log files of the entire CoA workforce, including failed attempts to log onto the Internet. The analysis will aim at *(i)* ensuring the functionality of the network and avoiding security breaches and, *(ii)* verifying whether CoA users employ the ICTI in accordance with the allowed uses laid down in the CoA's ISP. The outcome of the analysis is a report on the Internet usage. Such report will contain information on the following:

(i) Volume and use percentage of the different Internet protocols (HTTP, HTTPS, FTP, etc);
(ii) Volume and use percentage of the different file types (text files, executable, multimedia, etc);
(iii) Number of errors per a given period of time and categorisation of the errors per type (due to network problems, software problems, authentication, filters);
(iv) Categorisation of the four filter errors per reason (filtered because it was non permitted/illegal web sites or file types) and distribution per period of time;
(v) Depending on the outcome of the previous question, distribution per IP address or per user-ID over a specific period of time;
(vi) Assessment of a sample of 100 log records (including URLs) on whether they represent a danger for the Court's ICTI;
(vii) Visual inspection at about 20 different places in the log file to see if special patterns can be identified (repetitive characters, special characters, etc). Each result will be commented and will receive a qualitative notation varying from "no risk", "low risk", "medium risk", "high risk" and an explanation of how this notation was obtained, making reference to anti-malware references, laws, policies, standards, security information from trusted sources, etc;
(viii) Calculation of values of Internet usage: lowest, highest, average.
(ix) Examination of dangerous sites or traffic as specified in SANS, CERT or any other warning organisation newsletter;
(x) Examination of extreme long visited URLs;
(xi) List of 150 most visited web sites;
(xii) Distribution of the Internet traffic in number of visits and volume per category (sport, economics, science, games).

Fourth, the report will be sent to Director of Human Resources (**HR Director**) for his/her analysis. Depending on the risk classification, the HR Director may decide to request from the IT Security Officer additional information. For example how many people, during which period and how many times a dangerous Web site was accessed or an attempt was made to access such a site. The objective is to identify if an individual or a group of people is deliberately trying to circumvent the filters, accessing or making access attempts to access one or more non-allowed Web sites (pornographic material, xenophobia, etc) or Web sites which could damage the Court's ICTI (pracking, warez, crackz, etc).

Based on the outcome of the analysis, the HR Director will decide whether to lift or not the anonymity of the individual/s alleged to be engaged in a use of the ICTI against the allowed uses. This person will be asked to provide explanations at the end of which the HR Director will decide whether or not to open an administrative enquiry and disciplinary procedure.

Data subjects include everyone who uses Internet services at the CoA. This includes the Court's staff, experts and trainees as well as employees who work for a third party service providers or any other person making use of the Court's Information and Communication Technology infrastructure (hereinafter "users", "Internet users", " ICTI users" and "CoA workforce").

As far **as *conservation of data*** is concerned, according to the Notification log files are deleted six months after they were collected.

The data controller may ***transfer personal data*** to the following types of recipients: *(i)* the HR Director, *(ii)* internal investigators and, *(iii)* to OLAF.

As far as the ***right to information*** is concerned, the Notification says that users have been officially informed of the ISP and the MP with an official paper announcement and with the publication of the ISP, MP and FAQs on the CoA Intranet.

In addition, at the initial connection to the Internet, the user has to confirm that he has read and understood the ISP. A copy of the official announcement of the adoption of the Internet Security Policy, the FAQs and the MP were annexed to the Notification or provided later on, during the period for comments.

According to the MP, the ***right of access*** is guaranteed to the data subjects. According to information provided, the ***right of rectification*** is not applicable as the data is collected automatically.

Security measures are implemented. : [....]

2.2. Legal aspects

2.2.1. Prior checking

This prior checking Opinion relates to the CoA's data processing actions directed at monitoring the use of the Court's ICTI. Accordingly, the Opinion assesses the extent to which the data processing operations described above carried out by the I & T Directorate and the IT Security Officer are in line with Regulation (EC) No 45/2001.

Applicability of the Regulation. Regulation (EC) No 45/2001 applies to the *"processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system*" and to the processing "*by all Community institutions and bodies insofar as such processing is carried out in the exercise of activities all or part or which fall within the scope of Community law*". For the reasons described below, all elements that trigger the application of the Regulation are present:

First, the monitoring of the use of the Internet entails the collection and further processing of

personal data as defined under Article 2(a) of Regulation (EC) No 45/2001. Indeed, as described in the Notification, personal data of Internet users are collected and further processed. This includes user's identification; IP addresses, URLs visited, date and time, content etc.

Second, as described in the Notification, the personal data collected undergo *"automatic processing"* operations, as defined under Article 2(b) of the Regulation (EC) No 45/2001 as well as manual data processing operations. Indeed, the personal information is first collected automatically directly from Internet users (automatic registering of log files) and is then analysed by the IT Security Officer.

Finally, the processing is carried out by a Community institution, in this case by the Court of Auditors, in the framework of Community law (Article 3(1) of the Regulation (EC) No 45/2001). Therefore, all the elements that trigger the application of the Regulation are present in the processing of data for the purposes of engaging in Internet monitoring.

Grounds for prior checking. Article 27(1) of Regulation (EC) No 45/2001 subjects to prior checking by the EDPS *"processing operations likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes".* Article 27(2) of the Regulation contains a list of processing operations that are likely to present such risks. This list includes, under paragraph (a) "*processing of data relating to health and 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*".

Taking into account on the one hand that the monitoring of the use of the Internet as described in the ISP leads to the evaluation of users' conduct (to assess whether or not their use of the Internet is in line with the ISP) and, on the other hand, that such monitoring may entail the collection of data related to suspected offences (if there is a suspicion of unlawful behaviour) as well as other types of sensitive data, in principle, such monitoring and related data processing operations must be subject to prior checking *ex* Article 27 a) and b) of Regulation (EC) 45/2001.

Notification and due date for the EDPS Opinion. The Notification was received on 6 May 2008. The period within which the EDPS must deliver an opinion pursuant to Article 27(4) of Regulation (EC) No 45/2001 was extended for one month due to the major changes introduced in the data processing operations during the initial two months period and subsequently for an additional fifteen days. The procedure remained also suspended during the month of August. The overall period within which the EDPS must deliver an opinion was suspended for a total of 58 days to obtain additional factual information and allow for comments on the draft EDPS Opinion. The Opinion must therefore be adopted no later than 18 November 2008.

2.2.2. Lawfulness of processing

Personal data may only be processed if legal grounds can be found in Article 5 of Regulation (EC) No 45/2001. Of the various legal grounds laid down in Article 5, as pointed out in the Notification, the grounds that justify the processing operation are based on Article 5(a), pursuant to which data may be processed if the processing is "*necessary for 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*".

In order to determine whether the processing operations comply with Article 5(a) of

Regulation (EC) No 45/2001 two elements must be taken into account: first, whether either the Treaty or other legal instruments foresee a public interest task on the basis of which the data processing takes place (*legal basis*), and second, whether the processing operations are indeed necessary for the performance of that task, i.e. necessary to achieve the intended goals (*necessity*).

Legal basis. The legal instruments that legitimise the data processing in which the Court is engaged are the following:

In the first place, the EDPS notes that the CoA adopted an ISP. Among others, the ISP sets forth the rules for the use of the Internet towards ensuring the appropriate use of the CoA Information and Communications System. The ISP foresees the monitoring of the Internet usage, including the logging of each attempt to access the Internet carried out by the users of the CoA's ICTI in order to ensure the functionality of the network as well as to ensure the use of the ICTI in accordance with the allowed uses laid down in the ISP. In sum, the adoption of this Policy and its communication to users of the CoA ICTI constitute for the EDPS a relevant element in determining whether there is an adequate legal basis for the purpose of Article 5(a) of Regulation (EC) No 45/2001.

In the second place, the EDPS notes that the existing data protection legislation, Regulation (EC) 45/2001, contains in itself various provisions that legitimise the monitoring of Internet usage for certain purposes which coincide with the purposes sought by the CoA's monitoring. In particular, Recital 30 of Regulation (EC) 45/2001 establishes that "*It may be necessary to monitor the computer networks operated under the control of Community institutions and bodies for the purposes of prevention of unauthorised use"*. As outlined above, one of the purposes sought by the CoA when it engages in monitoring of the Internet is to prevent the use of the Internet against the rules set forth in the ISP. Also, Article 37(2) of Regulation (EC) 45/2001 provides for an additional legal ground authorising the CoA to carry out a very specific data processing activity, i.e. to keep traffic data, in this case, log files. In particular, Article 37 (2) provides that traffic data may be processed for the purpose of telecommunications budget and traffic management, including the verification of the authorised use of the telecommunications systems. 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 Staff Regulations or other provisions such as those included in the Internet Security Policy. Precisely in this case, the monitoring is carried out to verify whether users employ the CoA's ICTI for the uses that the Court has authorized in its ISP. In this context a key issue further discussed under Section 2.2.4 is to determine how much monitoring is necessary in order to verify authorized use. The EDPS considers that authorized use can be determined in different ways. It may be determined in terms of volume (size of document downloaded), time spent on the Internet or web sites visited. Authorized use can also be determined through other means such as third party complaints, unusual low efficiency of a staff member, etc.

Finally, the EDPS notes that the CoA in its role as employer has certain rights and is bound by certain obligations derived from employment law that can be considered as appropriate legal grounds that could justify the processing. For example, the CoA's right to protect itself from the liability of the harm that workers' actions may create may also justify the processing. This includes the processing of sensitive data, in certain circumstances (see Section 2.2.3).

Necessity. As outlined above, the necessity of the data processing is directly linked to the purpose that such processing intends to achieve. In other words, whether a data processing is

necessary or not depends on the intended purposes of the processing activity at stake. In this case, in order to make such assessment one must consider the extent to which the registration of Internet usage and subsequent analysis of log files (altogether "monitoring") is necessary for the purposes indicated in the Internet Security Policy.

As described above, one of the main purposes of the processing in the context of the Internet monitoring is to verify whether CoA users employ the ICTI in accordance with the allowed uses laid down in the CoA ISP. The EDPS is of the view that if the CoA does not engage in some monitoring of the use of the ICTI, the CoA is likely to fail in preventing use of the ICTI against the CoA ISP. Indeed, without such monitoring, the CoA may not detect such uses and it will not be able to prevent them. Therefore, it appears that the registration of log files and their analysis, at least to some extent, are necessary for the purposes of carrying out the task of ensuring a use of the Internet in accordance with the Internet Security Policy and thus, ensuring the overall security of the CoA ICTI. The EDPS also considers that in order to achieve the second purpose pursued by the Internet Security Policy, i.e. to ensure the functionality of the network and avoid security breaches, it is necessary for the CoA to engage in data processing. For example, the logging of Internet access and a certain amount of monitoring is necessary in order for the CoA to be able to identify the ICTI resources used at each moment and also in order to troubleshoot problems. Finally, some monitoring is also necessary for the purposes of enabling the employer, in this case the Court, where appropriate to exercise its rights and obligations derived from employment law. For example, if the Court would not be able to monitor the use of an individual suspected of engaging in behaviour against the ISP (for example, downloading pornography) it may not have the necessary evidence to open disciplinary proceedings.

In the light of the above, the EDPS is of the view that the monitoring of the CoA ICTI as such is necessary towards achieving the CoA intended purposes. Thus, the EDPS is convinced that the requirements for compliance with Article 5 a) of Regulation (EC) No 45/2001 are satisfied in principle.

This being said, it should be noted that monitoring across the board or very thorough monitoring of the use of the Internet by each individual, as opposed to a more selective monitoring (for example, when a suspicion exists), is not necessary at all times. Therefore, if the CoA engages in such type of monitoring across the board/very thorough monitoring, it may lack the legal grounds under Article 5 a) of Regulation (EC) No 45/2001 to perform it. This is why in the context of assessing the necessity it is more accurate to state that "***certain***" monitoring is necessary to comply with Article 5 a) of Regulation (EC) No 45/2001. Section **2.2.4** below suggests some limitations to the monitoring practices carried out by the CoA so that only really necessary monitoring takes place, in compliance with the "data quality principle".

2.2.3. Processing of special categories of data

The monitoring of the Internet use may reveal "sensitive" personal data. These data are qualified by the Regulation as any personal data "*revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life*" (Article 10). For example, trade-union membership may be revealed in access logs which show that an official routinely accesses a particular trade-union Web site. Access to certain Web sites may indicate sexual preferences. The processing of sensitive data is in principle prohibited unless grounds can be found under Article 10 of Regulation (EC) 45/2001 justifying their use.

Article 10(2)(b) of Regulation (EC) 45/2001 establishes that the prohibition shall not apply where the processing is "*necessary for the purpose of complying with the specific rights and obligations of the controller in the field of employment law insofar as it is authorised by the treaties establishing the European Communities or other legal instruments adopted on the basis thereof*".

Some monitoring of the Internet usage may be deemed necessary for the CoA to ensure the security of the system/data, as well as compliance with the Staff Regulations and other provisions. This includes compliance with the right and obligations derived from employment law. This would comprise, for example, the Court's obligation to prevent the viewing of sexually offensive information in the workplace which would justify the Court's processing of sensitive information, such as certain URLs visited, that may reveal that an employee is engaged in this type of activity. Monitoring of sensitive information may also be justified in certain cases in order to enable the employer to exercise his rights as employer such as his right to initiate disciplinary procedures including terminating employees who engage in unlawful activities such as viewing and downloading materials that promote crime. In sum, the EDPS considers that the Court, as employer, is subject to rights and obligations derived from employment law that justify the Court's processing of the sensitive data of users of the ICTI which can not be avoided beforehand (see additional considerations under section 2.2.4, *Collection of URLs visited*).

2.2.4. Data quality

Adequacy, relevance and proportionality. Pursuant to Article 4(1)(c) of Regulation (EC) No 45/2001, personal data must be adequate, relevant and non excessive in relation to the purposes for which they are collected and/or further processed. This is referred to as the data quality principle.

A priori, the EDPS considers that overall the data registered in log files seems appropriate in the light of the purposes sought by the processing. However, regarding the following two categories of information collected in the log files, the EDPS doubts whether their processing for purposes of establishing whether CoA users employ the ICTI in accordance with the allowed uses complies with the quality principle.

Log files of failed attempts to log to the Internet. EDPS notes that the CoA registers *all* log files without exception. The EDPS understands that for technical purposes, to ensure the functionality of the network and avoiding security breaches, including for purposes such as debugging, identifying DNS errors, etc., the CoA must register failed attempts to log on to the Internet. The EDPS considers that this processing is in line with the data quality principle.

However, he notes that the CoA *uses* these logs not only for ensuring the functionality of the network and avoiding breaches but also for the purposes of establishing whether CoA users employ the ICTI in accordance with the allowed uses. In particular, the IT Security Officer categorizes the filter errors according to the reasons that trigger the filter (filtered because it was non permitted/illegal Web sites or file types) and assesses the period of time when the filter was activated (i.e. when it went on). Depending on the outcome, the IT Security Office links each failed attempt to access the Internet to the IP address or user ID from which the attempt was made.

The EDPS recalls that technologies exist that may be utilised to diminish the need for a broad, full monitoring of *all* Internet access attempts. Among such technologies there is the filter software which filters the access to web sites previously deemed inappropriate or unlawful.

The EDPS notes that the CoA uses filter software and other techniques to restrict access to inappropriate information such as material that is obscene, racist, sexually or religiously offensive, which the EDPS welcomes. The use of such techniques entails a preventive approach to the misuse of the Internet rather than a detective or repressive one. Furthermore, such techniques are more privacy friendly because they render unnecessary or a least drastically diminish the need of monitoring failed attempts to visualise the blocked information. Indeed, if the individual never succeeded in accessing and viewing the content of a given blocked Web site, there does not seem to be a legitimate need to register such a failed attempt.

In this regard, the EDPS is negatively surprised that while the CoA uses filter software, it does not, at the same time, take into account the use of such technology to reduce the need for Internet monitoring of the Court's ICTI.

In the EDPS' view adopting both approaches at the same time, a preventive (filter software) and a detective or repressive one (monitoring) may be deemed *excessive*, both in terms of processing and in terms of data collection and may violate the data quality principle.

In the light of the above, the EDPS calls upon the CoA to ***reconsider*** its approach towards monitoring failed attempts to access the Internet or provide justifying reasons otherwise. In the event that the CoA were to conclude, based on sound reasons, that there is a need to analyze failed attempts to log to the Internet, the EDPS calls upon the CoA to implement at least the following safeguards and notify the EDPS thereof:

(i) A policy should be set up establishing a percentage of filtering use (activation of the filter), per period of time, per individual which is deemed normal, in other words, establishing what is a regular number of failed attempts per individual. When the filtering use is above the threshold mentioned above, the policy should foresee the possibility for the IT Security Officer to monitor failed attempts to access Web sites. For example, if the filter use is above 10 per individual, per a given period of time, activating the filter 11 times would trigger the possibility for the IT Security Officer to link the failed attempts to access the Internet to the user ID or IP address from which the failed access has been sought.

(ii) Given the potential consequences of linking failed attempts to an IP address or user ID, the EDPS considers that for the processing to be fair, some information should be provided to the ICTI user. In particular, the EDPS is of the view that the CoA should set up an automatic email or pop up window, for example, after a certain number of failed attempts to access the Internet, informing individuals that given the high number of failed attempts (per period of time), the IT Security Officer may engage in an enhanced monitoring of his or her ICTI use. This of course applies without prejudice of the information about the monitoring practices provided in the MP.

Monitoring of URLs visited. As pointed out above, the EDPS is aware that the collection of URLs is necessary for ensuring the functionality of the network and avoiding breaches. URLs visited reveal not only traffic data *per se* but also the specific content likely to have been viewed, including sensitive information. The CoA processes URLs visited both for ensuring the functionality of the network and for assessing abuse of the Court's ICT. The latter function is achieved through assessments made on a monthly basis of a sample of 100 log records for the whole workforce. The outcome of the assessment is a record establishing whether they represent "no risk", "low risk", "medium risk" or "high risk" for the Court's ICTI.

In this context two key questions arise: **First**, the extent to which the ***monitoring of URLs by the CoA is necessary*** for the purposes of assessing compliance with the ISP must be determined. In other words, to be in compliance with the data quality principle, how and to what degree can monitoring of URLs be carried out? **Second**, if an adequate suspicion exists that an individual is engaged in misuse (revealed through monitoring or through other off line means), ***what procedural steps should be set up*** to ensure that potential enhanced monitoring of this alleged behaviour is not excessive and that only those monitoring activities are undertaken that are necessary for the intended purposes?

On the first point (**monitoring without suspicion vs. use of indicators**), the EDPS views can be summarised as follows:

(i) In the absence of adequate suspicion, the monitoring of *all* the URLs visited by *all* the users is deemed unnecessary and excessive; this is particularly the case when such monitoring affects the entire workforce. Even randomly limited monitoring when there is no suspicion appears unnecessary. This is the case, for example, of fishing expeditions such as that proposed by the CoA consisting of monitoring samples of 100 URLs log records per month. In the EDPS view, this practice is avoidable because, as further described below, other less intrusive means exist, such as the use of other types of indicators, which may reveal suspicious behaviour, thus, making unnecessary the complete or even randomly limited monitoring of URLs, which is a more intrusive practice.

(ii) The EDPS concedes that in certain circumstances it may be necessary for the CoA to monitor URLs visited of *specific* individuals. In particular, when there is an *adequate suspicion* that a given user is engaged in behaviour against the ISP (e.g. downloading paedophilic materials) it is clear that the collection of information related to the URLs visited by such user is appropriate insofar as it will help to establish whether the user in question is engaged in such behaviour.

(iii) Exceptions may be made to the principle formulated under (i), for example, the danger associated with extremely long URLs outweighs the privacy invasion associated with their monitoring[1]. Therefore, the EDPS considers that their monitoring, linking this type of URLs to users' IDs or IP addresses is not excessive. The same reasoning applies to dangerous sites or traffic as specified in SANS, CERT or any other warning organisation newsletter.

(iii) In addition to monitoring long URLs, the CoA may use other indicators in order to detect misuse. The EDPS advises the Court to make use of these indicators. Examples of indicators include the collection of information regarding the volume of data downloaded, time spent surfing the Internet, as well other possible variables that do not involve the monitoring of URLs (collection of suspicion triggered by other, off-line means, e.g. unusually low efficiency). As described above, patterns of filter activation may also play the same role. In order to use indicators, the CoA should draft usage patterns and related deviations in use. In this regard, usage patterns based on volume may be more practical than other types of patterns such as the time spent on the Internet insofar as some tasks may require surfing the Internet and therefore may lead to false suspicions. In drafting usage patterns based on volume (or another relevant criterion), the CoA should ensure that it does not lead to a disproportionate control and monitoring.

---

[1] Overly long URLs may indicate an attempt to engage in a URL attack whereby the hacker uses the Internet Explorer address bar as a mechanism for hacking the site.

***To sum up,* the EDPS considers that the combination of using filtering software, the collection of information regarding time spent using the Internet, possibly, the collection of failed attempts to access the Internet (subject to the safeguards described above) as well as other off-line indicators should be sufficient tools for the I & T Directorate and IT Security Officer to achieve the purposes of monitoring without monitoring URLs except in limited cases.**

In this case, the EDPS is particularly pleased that the CoA does not monitor *all* the URLs of *all* CoA users. The EDPS finds the CoA reliance on user indicators such as volume of data downloaded and percentage of use of Internet protocols and file types positive. However, the EDPS regrets the CoA plans to engage in the monitoring of samples of 100 URLs log records per month and he finds it unnecessary. Therefore, he calls upon the CoA to ***reconsider*** this practice or provide justifying reasons otherwise.

In addition to the above, it should be taken into account that the monitoring of URLs may reveal sensitive information. As discussed under 2.2.3, the CoA has legal grounds to process sensitive information in order to exercise his rights and obligations derived from employment law. In particular such grounds may exist when the CoA wishes to exercise certain rights and obligations derived from employment law such as initiating disciplinary proceedings based on a suspicion that a user is engaged in wrongdoing. In these circumstances, the monitoring may be necessary in order to initiate administrative enquiries or disciplinary proceedings against the user. However, lacking a suspicion and lacking the exercise of rights and obligations under employment law, the legal grounds for collecting such types of information are not crystal clear. This would be an additional argument in support of the views calling for a limited collection of URLs, which takes place in those cases where a suspicion of wrongdoing exists based on indicators and/or off-line means.

On the second point (**monitoring when a suspicion exists**), the EDPS views can be summarised as follows:

(i) Once the IT Security Officer has an adequate suspicion that an individual is engaged in misuse (from the application of the above criteria), the EDPS suggests implementing a policy consisting in *gradually* increasing the monitoring depending on the circumstances. This will ensure that the monitoring is not excessive since only those data would be processed which would be necessary for the intended purposes. In this context it is important to remember that because the URLs are nevertheless collected and registered for their use for technical purposes, should a suspicion of misconduct arise, it will always be possible for the IT Security Officer to analyse URLs kept in log files that belong to the individual engaged in suspicious behaviour.

To apply the above, in other words, to engage in additional monitoring when the IT Security Officer has an adequate suspicion of misuse, a procedure should be set up establishing when, how and under which conditions this additional monitoring will be performed. To this end, the EDPS has the suggestions described below.

(ii) The discovery by applying the criteria outlined above of suspicious behaviour may be deemed relevant enough to justify the next step which consists in reporting the suspicion, without revealing the identity of the individual, to the relevant hierarchy. In this case, CoA plans to deliver monthly reports to the HR Director which may reveal suspicious behaviours. The EDPS is satisfied with this practice. The report is not supposed to reveal the identity of the user. In this context, the EDPS suggests removing any user ID or IP addresses that could

eventually be linked to the user.

(iii) The information on the suspicious behaviour must enable the competent person, in this case, the HR Director, to request an in-depth monitoring of the suspected individual, for example, for a period of two to four weeks. At the end of the two or four weeks the IT Security Officer should provide a new report which will confirm or dispel the suspicion. In principle, no action should be taken before the confirmation of the suspicion through this additional, targeted monitoring.

In this case, it is foreseen that the report received from the IT Security Officer will permit the HR Director, after informing the DPO, to decide whether additional information is necessary. Based on the outcome of the analysis, the HR Director will decide whether to lift or not the anonymity of the individual/s alleged to be engaged in a use of the ICTI against the allowed uses laid down in the ISP. This person will be asked to provide explanations at the end of which the HR Director will decide whether or not to open an administrative enquiry and disciplinary procedure. The EDPS considers this practice to be appropriate.

Fairness and lawfulness. Article 4(1)(a) of the Regulation requires that data be processed fairly and lawfully. The issue of lawfulness was analysed above (see Section 2.2.2). The issue of fairness is closely related to what information is provided to data subjects which is further addressed in Section 2.2.8.

Accuracy. According to Article 4(1)(d) of the Regulation, personal data must be *"accurate and, where necessary, kept up to date",* and *"every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed , are erased or rectified"*. In this case, the data include log files I & T Directorate must take every reasonable step to ensure that data are up to date and relevant. In this respect, see also Section 2.2.8.

2.2.5. Conservation of data

Pursuant to Article 4(1)(e) of Regulation (EC) No 45/2001 personal data may be kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which the data are collected and/or further processed.

According to the Notification and the ISP, log files are deleted six months after collection. Six months must be a maximum period. This timing is in line with Article 37 of Regulation (EC) 45/2001 which provides for specific measures as concerns the conservation of traffic and billing data, and 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.

If monitoring of log files leads the CoA to suspect that an individual has infringed the ISP, the CoA 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 ISP or the Staff Regulations and the CoA 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.

2.2.6. Transfers of data

Articles 7, 8 and 9 of Regulation (EC) No 45/2001 set forth certain obligations that apply when data controllers transfer personal data to third parties. The rules differ depending on whether the transfer is made to (i) Community institutions or bodies (based on Article 7), (ii) recipients subject to Directive 95/46 (based on Article 8), or (iii) other types of recipients (based on Article 9).

The transfers of data that take place within the context of the activities consisting in monitoring the Internet include the following: (i) Transfers of data to the HR Director to enable him to decide whether to open an investigation or not; *(ii)* transfers to internal investigators and, *(iii)* transfers to OLAF if an investigation is launched and if the conditions for the intervention of OLAF are met.

All the above transfers are made within or to Community institutions or bodies, thus, Article 7 of the Regulation applies. Article 7 of Regulation (EC) No 45/2001 requires personal data to be transferred "*for the legitimate performance of tasks covered by the competence of the recipient"*. In order to comply with this provision, in sending personal data, the IT Security officer must ensure that *(i)* the recipient has the appropriate competences and *(ii)* the transfer is necessary.

The EDPS considers that the transfer of information to the HR Director which occurs when there is a well founded suspicion of use of the ICTI against the ISP complies with Article 7. The Director of HR has the competence to perform the task assignment for which the data is transferred, to know the facts and assess the extent to which they constitute a solid suspicion of acting against the ISP and the Staff Regulations that support a decision to initiate an administrative enquiry and disciplinary procedure. It should be ensured that the transfer of such information takes place on solid grounds, after the suspicion has been confirmed with a second report, following the enhanced monitoring carried out during two or four weeks (see above under Section 2.2.4 Monitoring of URLs visited). This means that the first report should not contain personally identifiable information such as user IDs or IP addresses.

The EDPS considers that the transfers of information to internal investigators *(ii)* and OLAF *(iii)* for the purposes stated above comply with these requirements. In both cases, the recipients have the competence to perform the task assignment for which the data is transferred. Also, in both cases, the data transfers are necessary for the addressees to perform their tasks.

2.2.7. Right of access and rectification

According to Article 13 of Regulation (EC) No 45/2001, the data subject shall have the right to obtain, without constraint, at any time within three months from the receipt of the request and free of charge, from the controller, communication in an intelligible form of the data undergoing processing and any available information as to their source. The MP states that individuals have the right of access but is silent on the subject of rectification.

The EDPS recalls that the right of access is of mandatory nature, unless an exception applies, and the CoA has to put in place the procedures allowing its exercise. The right of access comprises, among others, the right to be informed and obtain a copy of the data that is being processed about an individual in an intelligible form. The CoA must implement the appropriate procedures to ensure the possibility for users to exercise their right of access.

In some instances the data controller, here the CoA, may be able to rely on some of the exceptions contained in Article 20.1 of Regulation (EC) No 45/2001 to defer the provision of the right of access or rectification. Notably, in this case, this may be lawful where such a restriction constitutes a necessary measure to safeguard *"(a) the prevention, investigation, detection and prosecution of criminal offences"*. In deciding whether to rely on an exception, the CoA must engage in a case-by-case assessment of the circumstances of the particular data processing at stake.

If the CoA uses an exception to defer the provision of access, it should take into account that the restrictions to a fundamental right can not be applied systematically. The CoA must assess in each case whether the conditions for the application of one of the exceptions. In addition, as foreseen in Article 20 of the Regulation, the measure has to be "necessary". This requires that the "necessity test" has to be conducted on a case-by-case basis. If the CoA uses an exception, it must comply with Article 20.3 according to which *"the data subject shall be informed, in accordance with Community law, of the principal reasons on which the application of the restriction is based and of his or her right to have recourse to the European Data Protection Supervisor*". However, the CoA may avail itself of Article 20.5 to defer the provision of this information as set forth in this Article: *"Provision of the information referred to under paragraphs 3 and 4 may be deferred for as long as such information would deprive the restriction imposed by paragraph 1 of its effect."*

According to Article 14 of Regulation (EC) No 45/2001 individuals have the right to rectify inaccurate or incomplete data. Due to the nature of the data (log files linked to users ID and IP addresses) and the way in which they are collected (logged automatically), the possibility of rectification of the data would appear highly unlikely. Therefore, it is unlikely that there will be scope for the exercise of this right. However, as a matter of principle, the CoA must recognise the existence of such right which, in some limited cases may apply, for example, if someone makes use of someone else's user ID.

2.2.8. Information to the data subject

Pursuant to Articles 11 and 12 of Regulation (EC) No 45/2001, those who collect personal data are required to inform individuals that their data are being collected and processed. Individuals are further entitled to be informed of, *inter alia*, the purposes of the processing, the recipients of the data and the specific rights that individuals, as data subjects, are entitled to. Below follows an analysis of whether the communication channel to make this information available to individuals is the appropriate one and also guidance on the content of the information to be provided to users to ensure conformity with Regulation (EC) No 45/2001.

The communication channel: In order to ensure compliance with Articles 11 and 12, according to the Notification and follow up information received from the CoA, ICTI users have been officially informed of the monitoring procedure with *an official announcement* and the publication of the ISP and the FAQs on the CoA Intranet. The MP will be published in the same way soon. Furthermore, at the initial connection to the Internet, the user has to confirm that he/she has read and understood the ISP. Finally, users trying to access a

prohibited Web site are told that access has been refused and the reasons for refusal (the Web site belongs to a non desired category with the name of the category). The message tells the user to contact the Help Service desk of the IT Security Officer for more information.

The EDPS highlights the need for the CoA to ensure that the channel selected to communicate the monitoring must enable individuals to take notice of its content in an effective way. Covert monitoring, where users are unaware that the monitoring is taking place, is not permissible. In this case, the combination of the official announcement, the publication in the Intranet of the ISP, MP and the FAQs are appropriate tools to make individuals aware of the existence of the monitoring practices. The content of these documents is relatively clear, the documents are available on a permanent basis to ICTI users for further consultation and, very importantly, their content is reminded to users through the pop up messages sent to individuals when they are denied access to certain Internet sites.

A concern regarding these documents is the fact that they provide the relevant information in a very disperse manner; indeed, to have access to the legally mandatory information, the ICTI user has to read three separate documents, the ISP, the MP and the FAQs. Furthermore, at first sight, the content and relationship between the three documents is somewhat unclear.

It would have been preferable to provide the relevant information, including the content of Article 11 and 12 of Regulation (EC) No 45/2001, in a unified way (rather than in three different documents). In order to minimise the effects of the possible confusion, the EDPS makes two suggestions: First, a new FAQ could be drafted highlighting the existence of the two basic documents (ISP and MP) and clarifying how they fit together. Second, when users are denied access to a Web site, together with the information regarding the reasons for refusal, they could be provided with a link to the ISP and MP.

As an additional measure, in order to raise awareness of the ISP, the EDPS also recommends that the CoA conducts periodic audits of usage practices to establish whether current procedures are well understood by users.

The content of the policy: The EDPS has reviewed the content of the ISP, the MP and the FAQs in order to assess whether they contain the information requested under Articles 11 and 12 of Regulation (EC) No 45/2001. The combination of the above documents provide information about the purpose of the processing, the identity of the data controller, the existence of the right of access, the time limits for storing the data and the recourse to the EDPS. Both the ISP and the MP refer to the disclosure of data to the HR Director. The EDPS is satisfied that this information complies with Article 11 of Regulation (EC) No 45/2001 provided that a reference is included to the possibility to transfer data to OLAF which is currently missing in the three documents.

The description of what constitutes abusive use of the Internet.- In addition to the above, it is essential that the privacy statement contains a clear definition of what constitutes abusive use of the Internet. In particular, users must know the parameters against which they will be monitored, for example, the volume used or time spent using the Internet. In addition, users must be informed of the type of sites which are deemed inappropriate so that individuals are well aware of what is or is not permissible.

The EDPS notes that the initial description of how the monitoring takes place in the ISP has been completed with a list of categories of Web sites whose access is prohibited. This list is part of the FAQs. Albeit that the list has some overlaps (i.e. Web sites on nudity, adult content and sex seem to refer to the same type of content) and is sometimes imprecise (it is

uncertain what is deemed as tasteless Web site), for the sake of transparency the drafting of this list is welcome.

2.2.9. Security measures

According to Articles 22 and 23 of Regulation (EC) No 45/2001, the controller and the processor must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected. These security measures must in particular prevent any unauthorised disclosure or access, accidental or unlawful destruction or accidental loss, or alteration and prevent all other forms of unlawful processing.

The IT& T Division of the CoA confirms that it adopted the security measures required under Article 22 of the Regulation and has described some of these measures. The EDPS has no reason to believe that these technical and organisational measures are not appropriate to ensure a level of security in line with the risks represented by the processing and the nature of the personal data to be protected.

However, the EDPS considers that, because these logs are used not only for pure security purposes but also for evaluation of behaviour, the security measures might need to be reinforced. In particular, the EDPS recommends the following measures: [....]

3. Conclusion

The intended data processing activities give rise to serious doubts about their compatibility with Regulation 45/2001, especially as to their necessity and proportionality in different situations. To ensure compliance with Regulation 45/2001 the EDPS recommends the CoA:

1. to do its utmost to continue using filtering techniques that entail a preventive approach to the misuse of the Internet rather than a repressive one;
2. to reconsider the policy consisting in monitoring URLs of failed access attempts to Internet sites whose content was blocked because of software filters or other techniques;
3. if monitoring of failed access attempts were to be deemed absolutely essential, to ensure that the data processing safeguards described in this Opinion are implemented when monitoring URLs of failed attempts to access the Internet and inform the EDPS thereof;
4. in the absence of an adequate suspicion, to abstain from monitoring URLs of visited Web sites unless there is a justified reason for such an activity, namely, in case of (i) extremely long URLs, and (ii) dangerous sites as specified in SANS, CERT, and similar publications;
5. to consider using other indicators such as volume of data downloaded to discover abuse;
6. to make sure that, monthly reports to the HR Director do not contain personally identifiable information (user IDs or IP addresses);
7. to see that appropriate procedures exist to ensure the possibility for users to exercise their right of access and rectification, subject to the application of the relevant exceptions;
8. to amend the FAQs and ISP as suggested in this Opinion;
9. to conduct periodic audits of usage practices to establish if monitoring practices are well understood by users;
10. to insert a link pointing to the privacy statement in the pop-up message that informs

users that access to a given Web site is blocked;

11. to reinforce security measures with regard to log files and ensure the conservation of the above identified documents.

Done at Brussels, 10 November 2008

(Signed)

Peter HUSTINX
European Data Protection Supervisor