Opinion on a notification for prior checking received from the Data Protection Officer of the European Centre for the Development of Vocational Training (CEDEFOP) related to Internet monitoring (processing of data in connection with a Proxy system)

Brussels, 15 November 2012 (Case 2011-1069)

1. Proceedings

On 22 November 2011, the European Data Protection Supervisor (EDPS) received a notification for prior checking from the Data Protection Officer (DPO) of the European Centre for the Development of Vocational Training (CEDEFOP) related to Internet monitoring (processing of data in connection with a Proxy system) with accompanying documents.

Questions were asked on 16 December 2011 to which the DPO replied on 7 April 2012. Complementary information was requested on 25 April, 28 June and 3 October 2012. The DPO replied on 19 July 2012 and 16 October 2012. Due to the complexity of the matter, the EDPS decided to extend the time limit for issuing the Opinion by two months pursuant to Article 27(4). The draft Opinion was sent to the DPO for comments on 17 October 2012. The EDPS received a reply on 12 November 2012.

2. The facts

The data processing mostly consists in monitoring the use of the Internet made by all CEDEFOP staff and contractors. The **purpose of the processing operation** in connection with the Proxy system is to provide additional security and a mechanism for enforcing the ICT User Policy of the CEDEFOP ensuring thus the functionality of the network and avoiding security breaches.

The use of the ICT equipment of the CEDEFOP is in principle restricted to official use. However, Section 2.1.1. of the ICT User Policy allows for incidental personal use of the e-mail and internet servers as long as such utilisation is not contrary to the interests of the CEDEFOP and the European Unions and remains within reasonable limits. In further exchanges with the EDPS, the CEDEFOP clarified that use which exceeds twice the standard deviation of the monthly use of the Internet is deemed to be excessive. Users over the threshold are considered to have excessively used the Internet for the said period.

The Proxy system is a web security gateway that will be integrated into the ICT infrastructure of the CEDEFOP. The Proxy will be comprised of a durable system that will encompass high availability and resiliency to the users of the CEDEFOP. It will use filtering techniques and automatically block inappropriate websites. Contact persons in ICT are the Proxy administrator and the ICT expert. They will have access to the data as follows: the Proxy

administrator will examine the content of the log files at any time when a technical problem is encountered. Monthly, the ICT expert will generate reports for the Head of Resources based on the data collected (analysis on the Internet usage). Such reports are generated "automatically the first day of each month by the system and submitted to the DPO and the Proxy administrator. The CEDEFOP will start the reporting to the Head of Resources only after the EDPS Opinion is issued.

A working group at CEDEFOP is currently discussing the type and content and creating the reports that the proxy system shall generate to the Head of Resources. Once the Head of Resources agrees to their proposals, the reports will be generated on a monthly basis. The monthly reports will not contain personally identifiable information (user IDs or IP addresses). They may contain information on the following[1]:

- Volume and use percentage of the different Internet protocols (HTTP. HTTPS, FTP, etc.);
- Volume and use percentage of the different types of traffic (volume of data downloaded, executable, multimedia, streaming, etc.);
- Categorisation of the filters errors per reason (filtered because it was non permitted/illegal web sites or file types) and distribution per period of time;
- Calculation of values of Internet usage (lowest, highest, average over a period of 6 months);
- Potentially the examination of malicious/dangerous (based on the categories already provided and maintained by the software vendor) sites or traffic as specified in SANS; CERT or any other warning organisation newsletter;
- Potentially to examine extremely long visited URL (> 250 characters long);
- List of 150 most visited web sites per period (Monthly);
- Distribution of the internet traffic, number of visits and volume per category (sport, economics, science, games), etc.;
- Distribution of internet services traffic against the percentage of users generating the traffic;
- Hits of the user on the Internet.

The parameters (i) volume of traffic (data uploaded and downloaded) and (ii) hits of the user on the Internet (to identify breadth of internet use, how many different pages, etc) are considered for each user and they are measured against the average parameter of all the users. According to the notification, "anonymity" of the user is achieved by covering the identity of each user by a number (user 012, user 120, etc.) (hereinafter referred to as “coded users”). Only the Proxy administrator and the DPO have access to the identity of the users. The indicators are shown for each user next to the average of all users on the specific indicator. The parameter of time is not considered as an indicator due to several reasons. A user may use several browsers at the same time. Multiple sessions (tags) on different sites used at the same time and open sessions during the course of a full day could give a wrong picture for the duration someone has spent on the internet.

In order to understand whether the Internet use is within the normal range a monthly threshold is defined. It is based on the overall use of the Internet by all the users for each particular month. In general over a population of ˜150 users, Internet use will be distributed and vary from the users who used the Internet little, the users who used it more, and the users who excessively used it. The threshold is considered to be the number which is 2 times the

[1] cf. Note to the Data Protection Officer Processing of Data in Connection with the Proxy system of 24 August 2011.

standard deviation of the monthly use of the internet.[2] Users over the threshold are considered to have excessively used the Internet for the said period. The monthly reports will capture those (coded) individuals whose internet use is higher than the threshold.

Based on the outcome of this analysis, in case there is adequate suspicion the Head of Resources will ask the ICT Expert to engage in additional in-depth monitoring of the specific coded user over a period of 1 month and at the end of the period to provide a second report with additional information, including URLs[3]. The second report indicates the type of use, per coded user in order to identify the type of content of the excessive use. The new report will confirm or dispel the suspicion. In principle, no further action will be taken before the confirmation of the suspicion through this additional, targeted monitoring.

The report received from the ICT Expert will permit the Head of Resources to decide whether additional information is necessary. Also, the Head of Resources will decide whether to uncover the identity of the individual/s alleged to be engaged in a use of the ICT infrastructure against the allowed uses laid down in the ICT User Policy. This person will be asked to provide explanations. The report will then be forwarded to the Director who will decide whether or not to open an administrative enquiry and disciplinary procedure.

The CEDEFOP has the primary **responsibility for the data processing** as controller. Within the CEDEFOP an important part of the data processing will be performed by the Proxy administrator and the ICT Expert. The Head of Resources is responsible for the Internet monitoring policy and for the decision to open an investigation.

The **data subjects** include everyone who uses Internet services at the CEDEFOP. This includes CEDEFOP's staff and trainees, as well as employees who work for third-party service providers or any other person making use of the CEDEFOP's information and technology infrastructure.

The **categories of personal data** to be collected and further processed include all Internet access attempts, either successful or unsuccessful, which are first logged and then further analysed: In particular, the information to 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)* TCP IP address of the PC, *(v)* browsing time, *(vi)* content filter category, (vi) content filter subcategory, *(vii)* URL visited*), (viii),* Host name visited, *(ix)* TCP IP address of visited URL, and, *(x)* TCPI IP port number.

Failed access attempts are logged for security and troubleshooting purposes. The reason given is that they could identify rogue programs, infected computers and viruses that otherwise could not be easily identified. Although security threats are generally being viewed as coming from the Internet, referring to a past case the CEDEFOP stated that it is possible that a compromised computer either by a person or an infected program may use the Internet to send or receive information. Such attempts when logged would alert the CEDEFOP to the fact that although a particular site is blocked, there are still attempts to access it. It becomes suspicious to look for virus, malware and malicious programs. Data collected by failed attempts are not evaluated or processed in the management reports. Failed access attempts do not affect the traffic statistics of the end user.

[2] In further exchanges with the EDPS, the CEDEFOP provided the following example: if the average use for the month of May is 2.7 GB, the threshold would amount to 21.6 GB (that is at least 10 times over the average use).
[3] Cf Section III of the Note to the Data Protection Officer Processing of Data in Connection with the Proxy system dated 24 August 2011.

The **automated and manual** 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 Proxy administrators and by the ICT expert. All data will be kept in the Proxy system (log and database).

Data processed within the processing operation may be disclosed to the following **recipients:** (i) the Head of Resources, the Director of CEDEFOP, to enable him to decide whether to open an investigation or not, (ii) internal investigators and (iii) to OLAF and investigative bodies if an investigation is launched and if the conditions for the intervention of OLAF or the investigative bodies are met.

As far as **data retention** is concerned, according to the notification and the Privacy Statement log files are deleted six months after they were collected by the Proxy administrator. If monitoring of log files leads CEDEFOP to suspect that an individual has infringed the ICT User Policy, CEDEFOP will keep the incriminating log files as long as these data are necessary to establish, exercise or defend a right in a legal claim pending before the court. Data for statistical purposes will be kept for an unlimited term after being rendered anonymous.

The data subjects are granted **rights of access to and rectification of data processed.** All users of the Proxy system have access to the data collected by it by using the "self reporting" function of the system. The data subject is granted the right to be informed and obtain a copy of the data that is being processed about him in an intelligible form. In some instances CEDEFOP will rely on some of the exceptions contained in Article 20.1 of the Regulation (EC) No. 45/2001. CEDEFOP recognises the existence of the right to rectify inaccurate or incomplete data. However, 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 appears unlikely.

As far as the right to **information** is concerned, the notification says that the ICT User Policy (ICTP) is available on the Intranet and every new employee is made aware of the policy on ICT infrastructure during his/her induction. A specific privacy statement and all notes regarding the Proxy system have been posted on the Intranet. When a user tries to get onto a site blocked by the Proxy system, the user's browser shows a screen indicating that the particular site is blocked due to the policy, including an extract of the ICT User Policy.

Furthermore, the monthly average figures and thresholds based on the overall use of the Internet by all the users will be published on the intranet. Each user will have the opportunity to compare his/her traffic data against the averages and become aware of its behaviour on the use of the Internet. The Proxy software logs the Internet activities of the users based on their username. This makes it possible for each user to login onto a "self reporting" page of the proxy system and review the data that the proxy system has collected for this particular user. Furthermore, users over the threshold will get an automatic e-mail of their individual figures from the Proxy system. They will also get as an attachment their Internet activity.

During an information session to all staff on 4 April the proxy working group at the CEDEFOP explained the report formats, the thresholds, standard usage, data categories etc.

According to CEDEFOP; **security measures** are implemented. Both technical and administrative measures are taken to guarantee secure processing. Access to personal data is protected by the fact that the right to access data is granted on a "need to know" basis depending on the duties of the people allowed access. Access to the data is given only to the

proxy administrator and the ICT Expert by means of username and password.

The proxy software system provides an audit trail showing which administrators have accessed TRITON-Web Security, as well as any changes made to policies and settings. The information is available only to Websense administrators who are granted policy permissions. The audit records are saved for 60 days to view the audit log.

3. Legal aspects

3.1. Prior checking

The data processing operations directed at monitoring the use of the internet by the CEDEFOP fall within the scope of Regulation (EC) 45/2001 (hereinafter the Regulation) and are subject to prior checking by the EDPS pursuant to Article 27(2) thereof. Personal data of Internet users are collected and further processed. This includes user's identification, IP addresses, URLs visited, data and time, content, etc. The personal data collected undergo automatic processing operations as well as manual data processing operations.

In the general monitoring phase, the identity of the specific user to which a particular activity refers to is not immediately revealed. According to the notification, “anonymity” of the user is achieved by covering the identity of each user by a number (user 012, user 120, etc.). However, the identity is only temporarily masked and can always be traced back if needed. The EDPS therefore would not refer to these data as “anonymous data” but rather as “coded data”. This is relevant because the application of the Regulation to coded data must be ensured at all times, even before the identity of the user is revealed.

Taking into account that the monitoring of the use of the Internet can lead to the evaluation of users' conduct (to assess whether or not their use of the Internet is in line with the ICT User Policy and that such data 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 are subject to prior checking under Article 27 (2)(a)and (b) of the Regulation.

The notification of the DPO was received on 22 November 2011. According to Article 27(4) of the Regulation, the EDPS Opinion must be delivered within a period of two months. The procedure was suspended for a total of 240 days to request complementary information and to allow for comments on the draft Opinion. Due to the complexity of the matter, the EDPS decided to extend the time limit for issuing the opinion by two additional months pursuant to Article 27(4). Taking the above into account, the present Opinion must be delivered no later than 16 November 2012.

3.2. Lawfulness of the processing

Personal data may only be processed if legal grounds can be found in Article 5 of the Regulation. Of the various legal grounds laid down in Article 5, as pointed out in the Notification, the grounds that justify the processing operations by CEDEFOP 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 the Regulation, 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 CEDEFOP is engaged are the following:

Firstly, CEDEFOP's ICT User Policy sets forth the rules and limits for the proper use of the computing and networking infrastructure at the CEDEFOP. The User Policy foresees the monitoring of the Internet use to protect the security of the ICT infrastructure against network oriented internal and external threats (viruses, malicious software, etc.). However, it does not specifically provide for monitoring of the Internet use to ensure the proper use of the ICT infrastructure in accordance with the allowed use laid down in its point 2.1.

Given the specific risks of the processing, the EDPS recommends that CEDEFOP expressly refers to the monitoring of the proper Internet use in the ICT User Policy, including the logging of each attempt to access the Internet carried out by the users of the CEDEFOP's ICT infrastructure and the respective procedure. This would also provide clarity and certainty to staff members. The legal basis, and other related documents, should therefore be reconsidered with a view to specifying this essential aspect.

Secondly, the EDPS notes that the Regulation contains in itself certain provisions that are relevant for the legitimacy of the monitoring of Internet usage by CEDEFOP. In particular, Recital 30 of the Regulation 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 CEDEFOP when it engages in monitoring of the internet is to prevent the use of the internet against the rules set forth in the ICT User Policy. Also, Article 37(2) of the Regulation provides for an additional legal ground authorising the CEDEFOP to keep traffic data, in this case, log files. 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. In particular, it allows the use of traffic data beyond traffic and budget management to ensure the security of the system/data and respect of the Staff Regulations or other provisions such as those included in the ICT User Policy. In this case, the monitoring is carried out to verify whether users employ the ICT infrastructure for the uses that the CEDEFOP has authorized in its ICT User Policy.

Finally, the EDPS notes that the CEDEFOP 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 a necessary, transparent and proportionate processing. For example, CEDEFOP's right to protect itself from the liability of the harm that workers' actions may create may also justify the processing. In some cases, subject to certain conditions, this may include the processing of sensitive data (see Section 3.3.).

Necessity: As outlined above, the necessity of the data processing is linked to the purpose that such processing intends to achieve. 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 is necessary for the purposes indicated in the ICT User Policy.

As described above, there are two purposes of the processing operation. The data are collected and processed to provide additional security on the one hand and a mechanism for enforcing the ICT User Policy of the CEDEFOP on the other.

The EDPS notes that in order to achieve the purpose pursued by the ICT User Policy, i.e. to ensure the functionality of the network and avoid security breaches, CEDEFOP considers as necessary to engage in data processing. Otherwise, CEDEFOP would not be able to identify the ICT infrastructure resources used at each moment and to troubleshoot problems. The EDPS also notes that according to the Agency, without monitoring the Internet use the CEDEFOP may not detect any use of the ICT against CEDEFOP's ICT User Policy. Therefore, it appears that the registration of log files and their analysis, at least to some extent, could be considered as necessary for the purposes of carrying out the task of ensuring a use of the internet in accordance with the ITC User Policy.

Finally, some monitoring is also necessary for the purpose of enabling the employer where appropriate to exercise its rights and obligations derived from employment law. If the CEDEFOP would not be able to monitor the use of an individual suspected of engaging in behaviour against the ICT User Policy (for example, downloading pornography) it may not have the necessary evidence to open disciplinary proceedings.

In the light of the above, the EDPS notes that the monitoring of CEDEFOP's computing and networking infrastructure as such could be considered as necessary towards achieving the intended purpose. Thus, the EDPS is convinced that the requirements for compliance with Article 5(a) of the Regulation are satisfied in principle.

3.3. 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 the Regulation.

Article 10(2)(b) of the Regulation 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*".

As mentioned in Section 3.2., some monitoring of the Internet use may be deemed necessary to ensure compliance with the Staff regulations and other provisions including employment law. This would comprise, for example, preventing the viewing of sexually offensive information in the workplace which would justify CEDEFOP'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 an employer such as his right to initiate disciplinary procedures including dismissing employees who engage in unlawful activities such as viewing and downloading materials that promote crime. Therefore, the EDPS considers that the CEDEFOP, as an employer, is subject to rights and obligations derived from employment law that justify CEDEFOP's processing of sensitive data of users of the ICT infrastructure that cannot be avoided.

In general, special categories of data may be processed in the framework e-monitoring practices under two different scenarios. First, special categories of data may relate to the very

subject-matter of the investigation (e.g. alleged viewing of pornographic materials). In this case, the processing could be considered as necessary for the purpose of investigating an alleged illegal activity and therefore complying with the rights and obligations of the controller in the field of employment law (Article 10(2)(b)). Second, special categories of data may *accidentally* be processed in the framework of the monitoring of authorised use, for example when the Internet traffic data include particular websites of a sensitive nature (a political party or religious institution), although these do not relate to the subject matter of the investigation. In these cases, adequate safeguards should be put in place to ensure that processing of such data is kept to a minimum and occurs only where it is really unavoidable. Furthermore, such data should not be recorded or further processed in the further steps of the procedure.

3.4. Data quality

Adequacy, relevance and proportionality: According to Article 4(1)(c) of the Regulation *"personal data must be adequate, relevant and non excessive in relation to the purposes for which they are collected and/or further processed"*.

The EDPS notes that overall the data registered in log files are considered as appropriate in the light of the purposes sought by the processing.

Log files of failed web access attempts. The EDPS notes that the CEDEFOP uses filter software which automatically blocks inappropriate web sites. He also understands that, in addition, for technical purposes, to ensure the functionality of the network and to avoid security breaches, including for purposes such as identifying infected computers and viruses, the CEDEFOP must register failed web access attempts. Otherwise, CEDEFOP would not be able to identify hacked computers or rogue programs which try to connect to the internet from inside the network. The EDPS considers that this processing is in line with the data quality principle.

However, it should be pointed out that log files of failed web access attempts should not be used to establish whether internet use is in accordance with user policy. As highlighted in a previous Opinion,[4] the EDPS considers that filtering technologies entail a preventive approach to the misuse of the Internet rather than a detective or repressive one. Whenever the access to a prohibited website is blocked, the EDPS takes the view that monitoring and punishing the mere attempt to access those websites would go beyond what is necessary for the intended purpose. If the individual user never succeeded in accessing or viewing the content of a given blocked website, there does not seem to be a legitimate need to register such a failed attempt. The EDPS welcomes that failed attempts are not evaluated or processed in the management reports by the CEDEFOP. He recommends complementing the ICT User Policy in this regard and informing the staff accordingly**.**

Monitoring of URLs visited. The Proxy system will systematically log all Internet access of the CEDEFOP's users of ICT infrastructure. The content of the information collected includes URLs visited and may thus reveal not only traffic data but also the specific content likely to have been viewed, including sensitive information. As indicated above, the collection of URLs is considered as necessary for ensuring the functionality of the network and avoiding security breaches. However, the URLs visited are also processed for assessing abuse of the CEDEFOP's ICT User Policy.

[4] cf EDPS Opinion of 10 November 2008 on Internet monitoring (European Court of Auditors'), available on EDPS website, p. 8-9.

In this context, two questions have to be addressed: first, the extent to which the monitoring of URLs by the CEDEFOP is necessary for the purpose of assessing compliance with the ICT User Policy; second, in case there is an adequate suspicion of misuse, what procedural steps should be set up to ensure that further monitoring of this alleged behaviour is not excessive and that only those monitoring activities are undertaken that are necessary for the intended purposes.

As regards the monitoring of URLs by the CEDEFOP for the purpose of assessing compliance with the ICT User Policy, the EDPS welcomes that the CEDEFOP does not monitor all URLs of all users. He notes that the proportionate collection of information regarding the volume of traffic (data uploaded and downloaded) and the hits of the user on the Internet (to identify the breadth of Internet use) could be considered as appropriate tools to achieve the purpose without monitoring of all the URLs visited[5].

As regards monitoring when a suspicion exists, the EDPS took good note of the procedure set up by the CEDEFOP establishing when, how and under which conditions an additional monitoring will be performed[6]. The procedure consists of several steps, gradually increasing the monitoring. It involves the blocking of certain websites and the use of automatic e-mail warnings to users over the threshold. The monthly Internet usage reports for the Head of Resources do not reveal the identity of the user. They enable the Head of Resources to request an in-depth monitoring of a specific user over a period of one month. Only after this additional targeted monitoring the Head of Resources will decide whether to lift or not the anonymity of the individual/s alleged to be engaged in a misuse of the ICT infrastructure. At this stage the alleged person will be asked to provide explanations. The EDPS welcomes this gradual approach which is aimed to ensure that the monitoring is not excessive.

Fairness and lawfulness. Article 4 (1)(a) of the Regulation requires that data be processed fairly and lawfully. This issue of lawfulness was analysed above (Section 3.2.). The issue of fairness is closely related to what information is provided to data subjects which is further addressed in Section 3.8.

Accuracy. Under 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 linked to users ID and IP addresses. They are logged automatically. Nevertheless, the ICT unit must take every reasonable step to ensure that data are accurate, complete and up to date.

The EDPS welcomes that an adequate suspicion is required for the Head of Resources to engage in depth-monitoring. In this respect, the EDPS stresses that according to Article 19 of the Regulation providing that the data subject should not be subject to automated individual decisions, i.e. decisions producing legal effects or significantly affecting the data subject which is based solely on automated processing of personal data intended to evaluate certain personal aspects. Any such decision cannot be taken on the basis of mere automated means but must be the result of a specific assessment by the competent hierarchical level.

[5] cf EDPS recommendation in Opinion on Internet monitoring (ECA), cited above, to consider indicators such as volume of data downloaded to discover abuse of the ICT user policy.
[6] cf Opinion on Internet monitoring (ECA), cited above; the procedure set up by CEDEFOP appears to be in line with the proposals of the EDPS in case 2008-284.

3.5. Data retention

Article 4(e) of the Regulation states that personal data must be "*kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed*".

The EDPS is of the view that keeping log files for a maximum period of six months after collection by the proxy administrator is in line with Article 37 of the Regulation which provides for specific measures as concerns the conservation of traffic and billing data, and log files are included in such a definition.

As regards the retention of log files in individual cases that led the CEDEFOP to suspect that an individual has infringed the ICT User Policy, the EDPS considers that keeping data within the specified period may be justified under Article 37 (2) of the Regulation.

3.6. Transfer of data

Articles 7, 8, and 9 of the Regulation 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) EU institutions or bodies (based on Article 7), (ii) recipients subject to Directive 95/46/EC (based on Article 8), or (iii) other types of recipients (based on Article 9).

3.6.1. Transfers within or between EU institutions and bodies

The transfer of data that takes place within the processing of personal data related to the use of the proxy system network includes the following recipients: (i) the Head of Resources and the Director of CEDEFOP, to enable him or her to decide whether to open an investigation or not, (ii) internal investigators and (iii) OLAF and investigative bodies if an investigation is launched and if the conditions for the intervention of OLAF or the investigative bodies are met. The EDPS considers that in some cases, where the monitoring activity leads to suspicion of criminal offences, CEDEFOP may also need to transfer personal data to the national authority in charge of investigating and prosecuting crimes. This is not clearly specified in the notification, but may concretely happen.

The EDPS considers that the transfer of personal data to the Head of Resources which occurs when he has decided to uncover the identity of the user (i.e. decode the data) complies in principle with Article 7. The transfer of personal data is considered by CEDEFOP as necessary for the legitimate performance of tasks covered by the competence of the Head of Resources in relation to ICT monitoring. Similarly, the transfer to the Director is considered justified with a view to allow him or her to decide whether or not to open an administrative enquiry and disciplinary procedure.

Also, the EDPS considers that the transfers of personal data to internal investigators and OLAF for the purposes stated above comply in principle with the requirements of Article 7. In order to be considered competent for the purposes of Article 7, internal investigators should be officially appointed by CEDEFOP in accordance with the official procedures of the Agency. Under these conditions, the recipients can be considered as having the competence to perform the task assignment for which the data is transferred. In both cases, the data transfers could thus be considered in principle as necessary for the addressees to perform their tasks. A case by case analysis must however be carried out. Furthermore, the controller should remind all recipients of their obligation not to use the data received for purposes other than those for which they were transmitted as it is explicitly stated in Article 7(3) of the Regulation.

Moreover, account should be taken of Section 4.1.3. of the ICT User Policy. The latter provides that "*[t]´he Administration of CEDEFOP may access the personal accounts of any staff members at any time for justified reasons, namely suspected illegal activities, suspected irregularities, improper conduct or other suspected wrongdoings*". This provision appears too widely formulated with regard to both its personal and material scope. Access to personal accounts should be framed as an exception rather than the rule. It should be foreseen only in particular circumstances and limited to a closed number of competent persons under a strict need to know basis. In particular, whenever the access is performed with a view to investigating suspected irregularities, it can be performed only in the presence of adequate suspicion of wrongdoing (which is supported by initial evidence).[7] Furthermore, it should take place in the framework of an internal investigation. The ICT User Policy should be amended to reflect these limitations.

3.6.2. Transfers to recipients subject to Directive 95/45/EC

As far as the transfer of personal data to investigative bodies of the Member States is concerned, Article 8 of the Regulation is relevant. Many national laws in the Member States have broadened the scope of application of their national law implementing Directive 95/46/EC so as to include public authorities when carrying out their judicial or police duties.

Article 8 provides that "*Without prejudice to Article 4, 5, 6 and 10, personal data shall only be transferred to recipients subject to the national law adopted for the implementation of Directive 95/46/EC, (a) if the recipient established that the data are necessary for the performance of a task carried out in the public interest or subject to the exercise of public authority, or (...).* In the view of the EDPS, this provision should be construed as meaning that if the information is not being sent at the recipient's request, it is the sender's task to verify that the transfer is necessary. Thus, where CEDEFOP sends personal data to investigative bodies in a Member state, it should establish that those data are necessary for the performance of a task carried out in the public interest.

3.6.3. Transfers to recipients not subject to Directive 95/45/EC

For recipients which are not subject to the Directive, Article 9 of the Regulation provides that "*personal data shall only be transferred to recipients [not subject to Directive 95/46/EC], if an adequate level of protection is ensured in the country of the recipient or within the recipient international organisation and the data are transferred solely to allow tasks covered by the competence of the controller to be carried out*". In those cases, the Council of Europe Convention 108, which for the matter under analysis can be considered in principle as providing a presumption of adequate level of protection, is in any case applicable to judicial authorities. Furthermore, the controller may consider the exception under Article 9 (6)(d) "*the transfer is necessary or legally required on important public interest ground, or for the establishment, exercise or defence of legal claims*". In any case, the EDPS recommends within this context that CEDEFOP should carefully establish that the personal data to be transferred is necessary for such purposes.

[7] The facts which raise a suspicion need not be of the same level as those necessary to justify a conviction or even the bringing of a charge. However, a reasonable suspicion presupposes the existence of facts or information which would satisfy an objective observer that the person concerned might have committed an offence. See ECtHR, *Murray v. United Kingdom* (14310/88) judgment of 28 October 1994, paragraphs 55-63.

3.7. Rights of access and rectification

The data subjects' rights of access and rectification are enshrined in Articles 13 and 14 of the Regulation.

In the case at hand, the users of the Proxy system have access to the data collected by it by using the "self reporting" function of the system. They also have the right to be informed and obtain a copy of the data that is being processed about them. If the Head of Resources decides to uncover the identity of the individual, the individual will be informed and if he requests so, a copy of the data being processed about him will be provided. In individual cases where a restriction of the right of access is necessary to safeguard *"(a) the prevention, investigation, detection and prosecution of criminal offences*", the CEDEFOP may be able to rely on some of the exceptions in Article 20 (1) of the Regulation. The EDPS notes, that this procedure seems to ensure compliance with Article 13 of the Regulation.

Under Article 14 of the Regulation individuals have the right to rectify inaccurate or incomplete data. Due to the nature of the data and the way in which they are collected (logged automatically), the possibility of rectification of the data may in some cases be necessary. This may be the case for instance where a computer is shared by more than one individual user. Qualifying the possibility of rectification as highly unlikely may, under this perspective, be misleading. The EDPS recommends therefore to amend the privacy statement and related documents accordingly. For the rest, the EDPS notes that the CEDEFOP recognises the existence of such right.

3.8. Information to the data subject

Articles 11 and 12 of the Regulation provide that data subjects must be informed of the processing of data relating to them and list a range of general and additional items, *inter alia,* the purposes of the processing, the recipients of the data and the specific rights that data subjects are entitled to.

The EDPS has reviewed the content of the ICT User Policy, the Privacy Statement, the Note to the Data Protection Officer of 24 August 2011 and all notes regarding the Proxy system. The combination of the above documents provide information about the purpose of the processing, the identity of the data controller, existence of the right of access, the time limits for storing the data and the recourse to the EDPS. However, a detailed description of the process, including the disclosure of data to the Head of Resources, is only given in the Note to the Data Protection Officer and not, as one might expect, in the ICT User Policy or the Privacy Statement. Also, the Privacy Statement contains no link to the ICT User Policy or the Note to the Data Protection Officer. The content and relationship between the ICT User Policy, the Privacy Statement and the Note to the Data Protection Officer is somewhat unclear. Therefore, the EDPS recommends to provide all relevant information in a unified document.

The EDPS is of the opinion that the ICT User Policy should contain a clear definition of what constitutes abusive use of the Internet. In particular, users must know the parameters against which they will be monitored. In addition, they must be informed about the details of the monitoring procedure, in particular when, how and under which conditions an additional monitoring will be performed. The Privacy Statement should contain a link to the ICT User Policy.

Moreover, the ICT User Policy and the privacy statements do not contain a description of the procedures followed in the framework of the verification. In the light of the particular risks

connected with Internet monitoring, the EDPS considers that the staff needs to be specifically informed about it.

As regards the way of communicating the information to the data subjects, the EDPS highlights the need for the CEDEFOP to ensure that individuals are effectively informed about the monitoring of their Internet use and the respective data processing. In this case, the combination of the official announcement, the information session to all staff on 4 April 2012 and the publication of the ICT User Policy and the Privacy Statement on the intranet could be considered as appropriate tools to inform individuals about the monitoring practices. However, this may not always be sufficient, as not all users may read the documents published on the Intranet. It is therefore essential that all staff members are individually informed. One way to do so would be to send the ICT User Policy document and the privacy statement by e-mail. To ensure proper information of all individuals, the EDPS also recommends implementing a system to oblige users, when they first attempt to access the internet using the CEDEFOP ICT infrastructure, to read and accept the ICT User Policy.

The EDPS welcomes that the monthly average figures and thresholds based on the overall use of the Internet by all the users will be published on the intranet and that users over the threshold will get an automatic e-mail of their individual figures from the Proxy system. He also notes that users trying to access a prohibited website are told that access has been refused and a link to the ICT User Policy is provided.

3.9. Security measures

On the basis of the available information, the EDPS has no reason to believe that the security measures implemented by the CEDEFOP are not adequate in light of Article 22 of the Regulation. CEDEFOP confirmed that it adopted the security measures required under Article 22 of the Regulation and has described some of these measures. As regards the audit trail, the EDPS considers that it guarantees integrity and confidentiality and complies with the requirements of Article 22 of the Regulation.

4. Conclusion

There is no reason to believe that there is a breach of the provisions of the Regulation, provided that the considerations in this Opinion are fully taken into account. In particular, the CEDEFOP should:

- reform the legal basis (ICT User Policy) so as to expressly foresee the monitoring of the proper Internet use in the ICT User Policy, including the logging of each attempt to access the Internet carried out by the users of the CEDEFOP ICT infrastructure and the respective procedure and inform the staff accordingly (Section 3.2. and 3.4.);
- put in place technical safeguards to ensure that the accidental processing of special categories of data (not related to the investigation) is kept to a minimum and occurs only where it is really unavoidable. In such cases, the data should not be recorded or further processed in the further steps of the procedure (Section 3.3.);
- reform Section 4.1.3. of the ICT Policy by stating the principle that access can take place only in cases where there is a reasonable suspicion of wrongdoing in the framework of an administrative investigation and that access should be limited to a closed number of competent persons under a strict need to know basis (Section 3.4);
- establish that personal data are necessary for the performance of a task carried out in the public interest if disclosure to an investigative body in a Member State is envisaged (Section 3.6.);

- whenever data are transferred under Article 9(6)(d) of the Regulation, clearly establish that personal data are necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims (Section 3.6.);
- amend the Privacy Statement and related documents in the parts where the rectification is qualified as "highly unlikely" (Section 3.7);
- revise information to data subjects as outlined in Section 3.8.;
- individually inform the users, for example by sending the Internet policy document and the privacy statement by e-mail (Section 3.8);
- implement a system to oblige users, when they first attempt to access the Internet using the CEDEFOP ICT infrastructure, to read and accept the ICT User Policy (Section 3.8).

Done at Brussels, 15 November 2012

(**signed**)

Giovanni BUTTARELLI
Assistant European Data Protection Supervisor