Opinion on a notification for Prior Checking received from the Data Protection Officer of the Court of Auditors regarding the "Procedure to access private drive - e-mail"

Brussels, 18 January 2010 (Case 2009-0620)

1. Proceedings

On 28 September 2008, the European Court of Auditors (CoA) submitted to the European Data Protection Supervisor (EDPS) a consultation on the need for prior checking (Article 27(3) of Regulation (EC) No 45/2001) on a procedure for accessing users' private drives and e-mails. In the context of his analysis of the case, the EDPS carried out an on the spot check, as part of a larger inspection on 17-19 March 2009. The EDPS examined some specific elements related to the submitted procedure. In his conclusions of 23 July 2009 relating to the consultation, the EDPS requested that a formal notification for prior checking be submitted to him as soon as possible on this processing operation under Article 27 of the Regulation.

On 28 September 2009, the EDPS received from the Data Protection Officer (DPO) of the CoA the notification for prior checking concerning the procedure to access private drive e-mail (hereinafter "the notification").

The notification was accompanied by two annexes. The first annex contains a new version of the procedure (amended in comparison with the initial version received for the consultation) and the second annex is referred to the new e-mail security rules and best practices issued at the CoA by internal Staff Notice on 5 June 2009. The EPDS also benefits from the conclusions of the on the spot check.

On 27 November, the EDPS sent the draft opinion to the Data Protection Officer for comments which were received on 14 January 2010

2. The facts

According to the data controller, the procedure to access private drive - e-mails has been developed by the CoA in order to face different situations which may happen in the day to day activities of the Institution. As explained in the notification, this procedure is to be applied in limited cases where professional information is stored in a user's private drive or e-mail and is required by the controller in the user's absence.

According to the data controller, the procedure has the following **purposes**:

- A) Protect the Court's interests when information is stored on the U: drive (private drive) or e-mail account of an absent user, and that information is necessary in the interest of the service and the information can't be obtained from another source before the users' return.

- B) In cases were users pass away and the surviving family requests to obtain information and documents which are necessary to deal with official instances, school, invoices, etc. and are stored on the U: drive or e-mail account. This purpose does not address the question of the access by the services of the CoA to the business documents of the staff member who passed away.

- C) Upon requests of the user when (s)he has left the Institution but needs to have access to information and documents which are still stored (standard procedure keeps files for 4 weeks after staff member is not anymore at the Court) on his/her U: drive or in his/her e-mail account..

It is necessary to make a clarification here regarding the status of respectively the user's private drive (called U drive at the CoA) and the e-mail accounts used at the CoA.

As was presented during the on-the-spot check, the "U drive" is considered by the CoA as a private drive for each staff member and for which only they should normally have access. Therefore, further access to this drive should be carefully limited. During the on-the-spot check, the controller stated that the users are encouraged to use the S and R network drives for the storage of professional files, instead of the U network drive which is reserved as the users' private space.

On the opposite, the e-mail accounts dealt with are business e-mails (each e-mail ends by eca.europa.eu). Therefore, it is the private use of this e-mail which should be specifically identified and limited. The e-mail remains a business e-mail. This is confirmed in point 4.2 of the e-mail security rules and best practices of June 2009. "*Users are reminded that computer equipment and electronic messaging systems have been installed for official use. However, sending of private messages is allowed as long as business activity is not obstructed*." There is therefore a residual right to use electronic messaging system for private messaging. It is also underlined in point 4.2 of the document that "For private communications users are strongly recommended to use an external private account to exchange private electronic messages to clearly separate work with private communications.

The proposed **procedure** (as described in the annexes to the notification) is as follows: the person[1] requesting the information, which doubtless is stored in the user's private area specified, needs to fill in a standard form (including among other the reasoning for the requested access). The request should contain a detailed description of the reason(s) justifying the access, the file name(s) or e-mail account and/or the subject of the information. The form should be sent to the Information security officer and in his absence to the Physical Security Officer.

The request form to access private drive/E-mail of a user contains the following items to be filled in:

- Reason (i.e. purpose of the processing)
- Files/e-mail requested
- Request order by + box for signature and date
- Boxes for the name, signature of the DPO and date
- Boxes for the name, signature of the Information security officer and date
- Boxes for the name, signature of the System Administrator and date

[1] AIPN, Director HR , line manager

The information security officer will present the request to the Data Protection Officer for a written opinion to be added on the request form. When a favourable opinion is obtained the information security officer will request the system administrator, in the presence of the information security officer, to obtain access to the requested information and deliver the requested information to the requestor.

The information security officer specifies, on the request form, which information was made available and signs together with the system administrator the form. A copy of the completed request form is sent to the concerned user and to the Data Protection Officer. The information security officer keeps the original request form and files it.

In the light of the notification, the data controller underlines that the processing operation presents specific risks as there is a risk of breach of confidentiality of communications. The procedure is applied because a person other than the owner of the e-mail account can have access to communications stored in the e-mail account. The EDPS notes that in the notification, there is only a reference to a breach of confidentiality in the case of e-mail communications.

In the framework of his inspection, the EDPS examined some specific elements related to the procedure, as well as to the controller's overall policy towards private drives and e-mail usage. These elements are included below.

The **data subjects** concerned by this procedure are all users which have a private drive (U: drive) and e-mail account at the CoA.

The **data** which are processed are users' data and other information contained into the e-mail messages.

As explained in the notification, different reasons/events may trigger the launch of the procedure. Also the persons requesting the access to the data may vary. The notification mentions that the unit to which belongs the requested information (case A), the surviving family (case B) and, the owner of the data (case C), they all are the possible **recipients** of the data.

According to the notification and the description made by the data controller, it can be interpreted that the recipients are specific to each of the three situations foreseen in the context of this processing.

As regard the **storage of media**, the data retrieved are saved on file server and e-mail server. For the storage of the media, the retrieved data is always an external portable media (USB, CD/DVD in the case the recipient is the owner itself or the family). If the recipient is the ECA itself the data is stored in a shared work related network drive or functional mail box.

No conservation period of data is established in the procedure or in the notification. As is further explained by the data controller in his comments, there is no conservation period for the data necessary because in the case the recipient is the family or the owner itself the data is not kept at the ECA. In the case the retrieved data is stored in a shared work related network drive or functional mailbox the retrieved data is considered as business personal data and follows the normal work related data retention period.

As regards the **information** provided to the data subjects, there is general and specific information provided. The notification states that the users will be officially informed of the access procedure with an official paper announcement and the publication of the procedure on the Intranet of the Court. The procedure states that "if possible" the consent of the user will be requested beforehand and in any case when the procedure has been applied the user will obtain a copy of the official request and a list of documents and messages which have been accessed by and/or transferred to the requestor. It is already important at the stage to underline that every reasonable effort should be made to obtain this consent without constraint (Article 13 of Regulation (EC) No 45/2001). It is more a question of reasonability which needs to be evaluated. It must be mentioned that during the on the spot check, the EDPS inspectors received knowledge of the existence of an internal communication to staff on the use of network and IT resources, which has been available since 1996.

As regards the **rights** of the data subjects, the notification states that users can contact the information security officer (independent to the requestor and serves as observer) to ask which files and or messages have been accessed.

The CoA has adopted [...] **security measures** regarding the processing:

[...]

3. Legal analysis

3.1. Prior checking

This prior checking Opinion relates to the CoA's data processing operation in the context of the procedure to access private drive - e-mail. Accordingly, the Opinion assesses the extent to which the data processing operations described above 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 procedure to access drive e-mails 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 staff members will be accessed, collected and further processed. This includes user's identification, user's data, files and e-mail messages.

Second, as described in the notification, the personal data collected undergo manual data processing operations meant to be part of a filling system, which is compliant with the definition under Article 2(b) of the Regulation (EC) No 45/2001. Indeed, the specific personal information which is retrieved is analysed by the information security officer and system administrator to be part of a filing system.

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".*

The checks carried out during the inspection showed that in the framework of the procedure for accessing users' private drives (called "U drives" in the case of the CoA) and e-mails, there is a risk of breaching the confidentiality of communications. By using this procedure, in a number of cases the private drive or e-mails of absent staff members can be accessed by other members of the services of the CoA. This raises the issue of the confidentiality of data in general. Moreover, in certain cases, it may also involve a breach of the confidentiality of communications under Article 36 of Regulation (EC) No 45/2001. Such situations give rise to a specific risk under Article 27(1) of the Regulation.

Notification and due date for the EDPS Opinion. The Notification was received on 28 September 2009. The period within which the EDPS must deliver an opinion pursuant to Article 27(4) of Regulation (EC) No 45/2001 was suspended for a total of 48 days to allow for comments on the draft EDPS Opinion. The Opinion must therefore be adopted no later than 18 January 2010.

3.2. Lawfulness of the processing

As explained in the facts, there are 3 specific purposes for which such procedure will be implemented: First, in the case of an absent user, who has information necessary in the interest of the service and the information cannot be obtained from another source before the user's return; Second, when users pass away and the relatives request to obtain information and documents; Finally, when users who have left the institution require copy of the data.

These cases are interpreted by the EDPS in a restrictive way. Moreover, each purpose is motivated by a specific reason which must be analysed separately.

According to Regulation (EC) No 45/2001, personal data may only be processed if legal grounds can be found in its Article 5. The notification states that, of the various legal grounds laid down in Article 5, 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".*

The EDPS does not agree that Article 5(a) would be relevant in all cases as the legal ground. Indeed, in the light of the procedure foreseen, the EDPS considers that the first legal ground to be applied should be the consent of the user. Article 5(d) states that personal data may be processed if "*the data subject has unambiguously given his or her consent*".

For instance, as regards the third purpose of accessing drive e-mails of users (i.e. users who have left the institution but ask for their data) the processing would definitely be based on Article 5(d). Indeed, in such situation, the user will necessarily have consented to the processing of his/her data in order to receive them.

The EDPS also considers that in the case of the first purpose (absent user whose information is necessary for the Institution before the user comes back to the office), the consent of the user could also be obtained beforehand or a back-up procedure could be envisaged. Another possibility could be that users are entrusted with the faculty to designate a colleague/third party which might be delegated to assist to the operations or even have direct access to the data on behalf of the user, therefore without starting the more complex foreseen procedure. If adopted, such alternative procedure should, of course, be subject to a password change and implement a corresponding security policy.

Examples of such cases were discussed during the inspection, like e.g. the case where a user organising a conference falls sick and relevant e-mails (sent to the user's personal account) need to be retrieved by the controller so as to proceed with the event's organisation. The EDPS considers that in such case (e.g. in the view of organising a conference) the CoA should provide a back-up procedure or more simply, make use of a functional e-mail account, which would be accessible to several staff members. By implementing this simple organisational measure, the implementation of the procedure would not be necessary if such case was arising. This measure is partly implemented in point 4.8 of the e-mail security rules and recommendations, as it foresees a procedure of delegation for users with managerial responsibilities.

It would only be in the case of the impossibility to obtain the user's consent (if the user is not reachable or not in the capacity to consent), or the impossibility to implement alternative organisational or technical solutions that Article 5(a) should be considered as the legal basis.

Finally, as regards the case of death of staff members (case B), the Institution can not presuppose that a user wanted his/her relatives to have access to his private drive/e-mail account. Therefore, the processing, in this case, cannot be based on consent.

In order to determine whether the processing operations would 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 CoA is engaged are the following:

In the first place, the EDPS notes that the CoA adopted a new e-mail security rules and best practices. Among others, the document sets forth the rules and guidelines to be applied by electronic messaging systems' users. It also sets rules to guarantee the availability, integrity and performance of the electronic messaging systems. It also aims at protection personal data stored in electronic messaging systems.

As regards the specific procedure to access drive e-mails, the document only touches upon e-mails by stating: "*An emergency procedure will be implemented in case users are absent and there is a justified need to access (sic) urgently access the user's account for work related purposes. This procedure will also respect the Data Protection Regulation 45/2001*". Therefore, this document only relates to e-mail and not to the use of private drives as they are not part of the e-mail system. The use of the network drives is defined and available on the Intranet of the CoA, in the welcome package of every new arrived user, and is in the User Management Policies document. According to the notification, a second document forming

the legal basis for the processing is the "Procedure to access private drive - e-mail", which will also be part of the Information Security Policy of the CoA. Moreover, the EDPS thinks that the abovementioned statement should have listed the different cases under which the procedure would apply.

On the basis of the information available, the EDPS considers that the legal basis of the processing is not sufficient and lacks clarity. Indeed, the new e-mail security rules and best practices do not cover the use of drives at the CoA. Moreover, the general procedure to access private drive - e-mail accounts is lacking complementary information, as it does not fully cover the planned processing.

The data controller should review the current e-mail policy in line with the following considerations:

The institution should adopt a specific legal basis on the use and storage of private e-mail and establish sound user guidance on the use of network resources and e-mail. It should:

- Include information about the need to keep private and professional information as distinct as possible, using different types of best practices, like: use of a specific password-protected folder for the storage of private e-mails (both incoming and outgoing), marking of private messages as such, deleting private e-mails that are no longer needed, etc.
- Clarify the status of some terms. For instance, the meaning of "private" is not clear with regard to drive U. As it was concluded from the on the spot check, although U drive is declared as private it was at the same time stated that *official documents* might also be stored there. Local drive D was also declared as "private" but the difference of access rights with regard to U drive is not explained (during the inspection the controller stated that the users are only recommended not to use the D drive). Therefore, the legal basis should clarify what the CoA considers as a private drive and what the business drives are.
- Inform the users about the consequences of not applying the private and professional e-mail best practices, like e.g. the fact that access to their e-mail in their absence might be needed when a specific document or e-mail is urgently required and the controller has no other way to get it.
- Be made public more visibly. The controller should communicate the above information/advice in written form, e.g. via the overall policy or using e-mail, and should also post it visibly on the internal ECA network.

Moreover, the controller should include in the proposed document containing the procedure to access private drive - e-mail accounts a chapter about the obligation for each staff member to distinguish between private and professional information as a means to avoid the application of the procedure. A link to the relevant guidance on the use of network resources and e-mail should also be provided.

Finally, the controller should review the steps of the procedure and add user information and consent as the basic step of control with regard to granting access or not. As an example the procedure could be modified as follows: after the access request has been sent to the information security officer, he/she should first try to contact the user in order to inform him/her and obtain his/her consent. This action together with its result (i.e. whether user was reached and if he/she consented) should also be included in the access form

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 processing aiming at accessing user's data and subsequent processing is necessary for the purposes indicated in the procedure.

As described above, the main purposes of the processing in the context of the procedure are threefold: Protect the Court's interest in case of an absent user and the information is necessary in the interest of the service, answer to requests of surviving family of a user and answer on the request of the user when he/she has left the Institution.

In the light of these purposes, the EDPS is of the view that the access by the CoA information security officer (and IT Administrator) in the context of the procedure could only be considered as necessary towards achieving the CoA intended purposes if the CoA can demonstrate that the staff member received a clear and complete information regarding the use of private/professional e-mail and private drive, that the matter of urgency of the access requested could be demonstrated and that the consent of the user could not be received. These aspects of the necessity would need to be demonstrated on a case by case basis.

It is also important to underline that such procedure of access shall not be considered as part of an administrative enquiry procedure against a staff member. To be more precise, this procedure shall not serve as a way to circumvent the rules established in the case of an administrative enquiry procedure or disciplinary procedure against a staff member. The DPO of the CoA should demonstrate, in his written opinion, that he analysed this aspect.

As regards the case of the death of staff members, the EDPS would like to stress that other alternative solutions have already been proposed by other institutions. For instance, other institutions have, in such cases, established the possibility of implementing other procedures aiming at the destruction of the private electronic files previously managed by the dead staff member.

In this case, the storage of data would be of a technical nature and therefore access by the institution should not be authorised, unless the conditions set under Article 7 of Regulation (EC) 45/2001 are established. As regards the family, the conditions set under Article 8 of Regulation (EC) No 45/2001 would apply (see point 3.6 below).

In the case of staff having left the CoA, other institutions have also foreseen a specific procedure for the departure of staff. In such cases, before leaving the institution, the IT department may contact the person and provide a copy of the content of the private drive in a CD/DVD format. It may also ask him/her to empty the concerned drives before leaving.

Moreover, as regards private e-mails, a copy of them may also be provided to the person in a CD/DVD format. The staff would also be asked to empty his/her e-mail account of its private content, so that the e-mail account will only contain personal data that will be considered by the institution as business data for the remaining period of retention (in the case of the CoA, it would be for 4 more weeks). The staff members also need to be informed that, even if their data have been copied or if they, personally, have deleted the personal data from their e-mail accounts, copies may remain for some time on the institution's servers. This should be part of the information provided to staff members (see also point 3.8) It must also be ensured that the institution will not make use of these data, unless in the framework of a disciplinary procedure.

Implementing such procedure and specific measures would greatly limit problems of access to

private information of staff whether in a private drive or in the e-mail account after their departure, as they would have received a copy of the data and personally ensured that the respective folders are empty.

The EDPS considers that such solutions could be developed by the CoA, as to mitigate the applicability of the procedure to its minimum.

The EDPS considers that the data controller should comply with the above mentioned measures in order to comply with Article 5 a) of Regulation (EC) No 45/2001.

3.3. Processing of special categories of data

The EDPS considers that the procedure to access private drive e-mails of users at the CoA may also imply the process[2] of "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, in some cases users may have lawfully (according to the CoA Policy) stored e-mails or documents that reflect any of the above mentioned data (a document referring to a medical result, a document stating the subscription to a political party, exchanges of e-mails with a doctor which would mention health related data in the header of the messages, etc). Therefore, by accessing the private drive or e-mail of a user, sensitive personal data may be revealed. 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. However, the EDPS considers that access to the special categories of data would normally take place incidentally (access is given for some specific data and the special categories of data would be processed incidentally).

After careful analysis of the possible exceptions, one basis for processing can be found in Article 10(2)(b) if "*the data subject has given his or her express consent to the processing of those data*". This would only be applicable in the case of the user having left the institution (third case) or also when the person is absent and is not returning before the information is needed but is able to provide a valid consent (first case).

However, concerning the other cases (death of the user or absence of the user and impossibility to receive a valid consent) the EDPS considers that only Article 10(4) can form a basis for the processing of sensitive data. This article states that : "*Subject to the provision of appropriate safeguards, and for reasons of substantial public interest, exemptions in addition to those laid down in paragraph 2 may be laid down by the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof or**, if necessary, by decision of the European Data Protection Supervisor***." (emphasis added)

The EDPS considers that this prior-checking opinion, including the specific safeguards mentioned, shall be considered as fulfilling the requirements of Article 10(4). However, if such access is necessary, the substantial public interest, as described in Article 10(4) needs to be demonstrated, on a case by case basis.

[2] According to Article 2 (b) of the Regulation, 'processing of personal data' shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, **consultation**, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction (emphasis added);

3.4. Data Quality

Adequacy, relevance and proportionality. Pursuant to Article 4(1)(c) of Regulation (EC) No 45/2001, personal data processed in the context of the procedure 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.

By consequence, it must be ensured that only the data which are adequate, relevant and non excessive will be retrieved. In this context, the written opinion of the DPO of the CoA, which will be added to the request form, is an important element for verification of the data quality, as the description of the documents which were accessed. Moreover, the EDPS considers that the separation made between private personal data (according to the CoA policy) and business personal data contributes to ensure data quality.

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 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. 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 e-mails and files. The information security officer (or the Physical Security Officer in his absence) must take every reasonable step to ensure that data processed in the context of the procedure are up to date and relevant. In this respect, see also Section 3.8.

3.5. Data retention

Pursuant to Article 4(1)(e) of Regulation (EC) No 45/2001 personal data processed in the context of the procedure 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.

As a general principle, the data retrieved from the e-mail accounts or private drive must be stored no longer than necessary to fulfil the purpose for which they were accessed. The data must then be erased.

In the case of staff leaving the CoA or the death of staff members, data in e-mail accounts and the private drive are normally erased within 4 weeks. In the case of log files, the same procedure should apply. However if logs can not be destroyed within the prescribed time limit, because the life cycle of logs is longer, there should be a legal provision by which the institution states that the logs will not be used for other purposes.

Then, they must be erased or made anonymous as soon as possible and in any case no longer than 4 weeks 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.

3.6. Transfer 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 Community institutions or bodies (based on Article 7), recipients subject to Directive 95/46 (based on Article 8), or other types of recipients (based on Article 9).

As explained in the facts, the recipients of the data vary, according to the purpose of the processing: unit to whom belongs the requested information; surviving family; Owner of the data (staff member).

Most the above transfers are made within 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 information security officer must ensure that *(i)* the recipient has the appropriate competences and *(ii)* the transfer is necessary.

In complying with the procedure established and the recommendations of the current opinion, the EDPS considers that the transfer of information to the unit to which belongs the requested information complies with Article 7 of Regulation (EC) No 45/2001.

In the situation where the CoA is confronted with the death of a staff member, a transfer of data to the family member would have to comply with Article 8 of the Regulation

Justifications that the data are necessary to deal with official instances, school, invoices, etc. will have to be presented and should be added to the request form for evaluation of the whole request by the DPO. Moreover, this procedure could only take place within 4 weeks after the death of the staff member, according to the conservation period set for e-mail accounts and private drives.

It must be noted that the transfer of data to the staff member who has left the institution (regardless of whether he is still working in a EU institution or not) would be covered by his/her consent to the processing;

3.7. 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, confirmation as to whether or not data related to him or her are being processed, information at least as to the purposes of the processing operation, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed as well as communication in an intelligible form of the data undergoing processing and any available information as to their source.

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 for those entitled to. 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.

The notification foresees that users can contact the information security officer (independent to the requestor and who serves as observer) to ask which files and or messages have been accessed. This would comply with Article 13(b) of Regulation (EC) No 45/2001. Moreover, it also states that the users will be officially informed of the access procedure with an official paper announcement and the publication of the procedure on the Intranet of the Court. The consent of the user will be requested and in any case when the procedure has been applied the user will obtain a copy of the official request and a list of documents and messages which have been accessed by and/or transferred to the requestor. As already underlined above, every reasonable effort should be made to obtain this consent without constraint of the user 45/2001.

In the light of the elements provided, the EDPS considers that the current procedure complies with article 13.

According to Article 14 of Regulation (EC) No 45/2001 individuals have the right to rectify inaccurate or incomplete data. As the data will normally be collected without the staff member being present or even without his/her knowledge, it is important to ensure this right retrospectively for those entitled to. This possibility should be provided in addition to any other solution which would be suitable in the day to day activities to rectify directly the data,

As a matter of principle, the CoA must recognise the existence of such right which, even if it may not be exercised frequently, may apply in some limited cases.

3.8. 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.

The procedure contains the following elements. The users will be officially informed of the access procedure with an official paper announcement and the publication of the procedure on the Intranet of the Court. As explained above, every reasonable step should be taken to obtain the consent of the user and in any case when the procedure has been applied the user, upon return, will obtain a copy of the official request and a list of documents and messages which have been accessed by and/or transferred to the requestor. The procedure also foresees that the user has at any time the right to contact the EDPS.

As a consequence of the described procedure, most of the information will be provided to the data subject after the processing has taken place.

After analysing the request form described in the facts and which shall be handed to the data subject, the EDPS has the following comments:

- it should be clearly underlined that the purpose of the access should be motivated in the request form, i.e. by providing other documents (i.e. request by the staff member, elements provided by the family, elements provided by the unit which prove that the required files are stored on the private drive or in the e-mail account). Resuming this aspect under the heading "reason" in the request form is not a sufficient element to comply with article 11(1)(b) of the Regulation.

- the data controller should add a box which contains a summary of the documents attached to the request form.
- the data controller should add a box which includes the different recipients who may receive the data. Referring to the requestor of the access (most of the time not the final recipient of the data) is not sufficient to comply with article 11(1)(c) of the Regulation.
- the data controller should add the reference to the right of access of the data subject in the context of this procedure.

Finally, as a good practice, the data controller should ensure that the written opinion of the DPO is attached to the request form.

3.9. 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 data controller of the procedure detailed in the notification the security measures implemented.

[...]

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.

[...]

Conclusion:

The proposed processing operation does not appear to involve any infringement of the provisions of Regulation (EC) No 45/2001 provided that the comments made above are taken into account. This means, in particular, that:

- The institution must adopt a specific legal basis on the use and storage of private e-mail and establish sound user guidance on the use of network resources and e-mail. This legal basis should :
    - Include rules about the need to keep private and professional information as distinct as possible.
    - Clarify the status of the drives in use at the CoA and especially, clarify what the CoA considers as private drives and what are the business drives.
    - Inform the users about the consequences of not applying the private and professional e-mail best practices.
    - Be communicated more visibly.

- The request form should be modified in the light of the comments in this opinion.

- The requestor must demonstrate a substantial public interest, when access to special categories of data is foreseen. It shall be analysed on a case by case basis

- The procedure can not be used as a way to circumvent the rules established by a disciplinary procedure.

- A retention period of conservation of data retrieved should be established without exceeding the normal retention period.

- In the case of impossibility to destroy the log files within the time limit prescribed, the institution should ensure that they will not be used for other purposes.

- Complete the request form as to include:
    - justification documents
    - the elements of article 11 or Regulation (EC) No 45/2001

- The logs on the log file server must only be accessible by a third party like the DPO (in addition to the information security officer and system administrators).

Done at Brussels, 18 January 2010

(signed)

Giovanni BUTTARELLI
Assistant European Data Protection Supervisor