Opinion on a notification for prior checking received from the Data Protection Officer of the Commission related to the Identity Management Service

Brussels, 6 February 2008 (Case 2007-349)

1. Proceedings

On 31 May 2007, the European Data Protection Supervisor ("EDPS") received from the Data Protection Officer of the Commission ("DPO") a notification for prior checking ("the Notification") regarding the data processing operations related to the identity management service ("IMS") carried out by Informatics DG ("DIGIT").

On 19 July 2007, the EDPS extended the deadline for the adoption of an opinion for an additional month, due to the complexity of the data processing operations at stake. On 1 August 2007, the EDPS requested complementary information regarding various aspects of the data processing in point. On 25 September 2007, a meeting took place with staff from the EDPS and of DIGIT and the DPO to discuss the technical features of the IMS. DIGIT responded to the EDPS questions on 6 December 2007. On 20 December 2007, the EDPS sent the draft Opinion to DIGIT for comments which were received on 21 January 2008.

2. Examination of the matter

The current prior checking relates to the processing of personal data that DIGIT carries out to operate the Identity Management Service. This service is used primarily to manage user populations and their rights in the context of information services. In particular, IMS facilitates the authentication and access control of users to different Commission information services, which are managed by different Directorates General (hereinafter "client DGs"). In the off line world this situation would be similar to that of a security company hired by different companies to check the identity and access entitlements of each individual who wishes to enter the premises of such companies.

The personal data processed in the operation of the IMS are used mainly to authenticate and facilitate access control to Commission information services, i.e. client DGs. IMS does not control the personal data that have been or will be collected and further processed once the individual has accessed a given Commission information service. For example, the data collected by client DG X which processes data of users who have subscribed to training courses is not controlled by DIGIT in the context of the operation of IMS. Accordingly, this prior check opinion is limited to the analysis of the data processing used for the purpose of operating the IMS. This can be illustrated by using the above example taken from the off line world insofar as this situation is similar to the security company not having control over the data processing that may take place in each individual company visited by the individual.

Below follows a description of how the Information Management Service operates and the way personal data are processed therein.

2.1. The facts

Overview of how the Information Management Service operates:

IMS' primary objective is to authenticate and to facilitate access control to Commission information services, operated by the Commission, i.e. "client DGs". IMS is used for Commission staff as well as for personnel of other organisations and members of the public.

In addition to the above function, IMS may perform further tasks: firstly, IMS ensures the automatic update of users' access rights and attributes. Secondly, IMS customises user's interfaces according to user's individual characteristics. Finally, IMS offers look up facilities or registries to enable client DGs to provide services such as white pages, e-mail address book, telephone directory, the selection of users from lists, usually based on some selection criteria and the construction of lists of users and primarily e-mail. The construction of e-mail distribution lists is based on attributes of the internal users of the Commission. These lists are usually compiled automatically by batch jobs that are run by the e-mail service overnight. The selection from a list of a user to whom a particular action applies, possibly based on the initial characters of the names, facilitates actions such as sending a fax from a fax machine connected via a client application.

IMS works in combination with various component services. In particular, it works with ECAS (European Commission Authentication Service), a user authentication service with a special user interface, independent of the client site which provides a single sign on experience. It also works with the CED, a directory service. In practical terms this means that IMS authenticates and controls users' access to Commission systems and services through ECAS as well as CED.

Once a user has been authenticated, for example in ECAS, it proceeds to log on to an application operated by a client DG. At this point, IMS will transfer the information it holds about the user which has been authenticated to the client DG. A service level agreement between DIGIT and the client DGs has been drafted for the purpose of establishing the rights and obligations of both parties. Among others, pursuant to the service level agreement, client DGs' usage of data originating from IMS is limited to purposes compatible with that of IMS. In other words, client DGs are bound to use the data for the same purposes for which the data was originally collected by IMS. Further processing must comply with data protection rules.

The way personal data are processed in the operation of IMS:

As further described below, in the context of operating IMS personal data are collected and processed. The ***purpose of the data processing*** coincides with the functions of the IMS as a whole, i.e. to manage user populations and their rights in the context of the Commission's information services. The specific sub-purposes are outlined above in the overview of how the IMS operates.

The primary ***responsibility for the data processing*** lies within DIGIT.

As further described below, ***data processing operations are both automated*** and manual, and they can be summarised jointly as follows:

(i) As far as registration of users external to the Commission is concerned, individuals complete a registration form which is passed on to DIGIT in order to register for access to a given Commission information service. The registration form contains personal information including name, geographical location, e-mail, telephone number, etc. The email address is compulsory whereas the other information, apart from group membership, is optional. For internal users, i.e. for Commission staff, DIGIT registration is completely automatic whereby the information is taken from the human resource database (COMREF) and the telephone and email directories.

(ii) DIGIT assigns access rights to each user based on the attributes of users and the policies defined by the service providers, i.e. client DGs. An account is therefore created for each user. This information is stored in a repository or set of repositories.

(iii) Once users are registered and have obtained an account and tried to access Commission services that use IMS, the service checks the access rights of the user in order to help client DGs to ascertain whether users have the necessary entitlements to access it. For example, ECAS which gives access to multiple Commission services uses IMS.

(iv) IMS records information about individuals' behaviour or activities, including log files and other information gathered through the use of cookies. The information will be used for verification of authorised use as well as for customisation purposes, for example to display choices based on recent activity or to choose the language for the user interface.

In addition, IMS permits DIGIT to validate and execute a user's request to reset their password if they are unable to do it themselves, to activate or deactivate a user account or an access right as well as correct user details in order to resolve conflicts that are preventing automatic processes from working.

The ***data subjects*** concerned include personnel employed by or working for the Commission ("Commission's staff"), personnel of any other organisation having electronic business with the Commission and individual citizens or members of the public who have registered with the Commission.

The organisations whose staff data may be used in IMS include private enterprises, non-profit organisations as well as Member States.

The ***categories of personal data*** collected include the following:

(i) Identification related information, which includes three unique identifiers (the username referred to as userid, the Commission's personnel number -PER_ID- for internal users or, for automatically synchronised external users, a unique key) and the e-mail address. In addition, the name of the individual is also collected as well as the group membership, organisational assignment, telephone and office number, administrative status (activity and type of employment), job title, job functions, organisational role(s), occupation, place of work or residence, and date of birth (used as matching criterion to prevent creation of duplicate entries for a single user). For external users this information is provided directly by the user through a registration. Sometimes users are registered by their employers. For Commission's staff the information is collected from the Commission's resources particularly from thee human resources database.

(ii) Data related to the use of the Commission information services. As with the above category of data, some of the data related to the use of the Commission information services originates directly from the user, such as the password. Although in fact the password is not

stored by the service. What is stored is a unique hash allowing a supplied password to be verified, but the actual password cannot be computed from it. The hash of the most recent five passwords is stored. The data generated by the service which does not originate from the user includes the date the password last changed, date of last successful authentication, account status (whether active, inactive or locked by an administrator), IP address, time of login and individuals' behaviour or activities when accessing the Commission information services. The recording of behaviour or activities refers principally to the acts of authentication and attempted accesses to systems. User's individual characteristics such as preferred language are also kept in order to customise user interfaces, mainly through the use of cookies. Authentication activity can consist of attempts by an unknown party to guess a user's password.

As far as ***conservation of data*** is concerned there are different data retention periods according to the type of data.

Data referred to as identification related information of outside users is kept for as long as the user is active plus one year. The same type of data as far as the Commission's staff is concerned is kept for the lifetime of the user. This applies to the extent that non active staff is still entitled to access Commission systems and services. The reasons that justify keeping the data are to allow the reuse of the identifier, if the person would require renewed access to Commission IT resources after a long absence.

Two different retention periods are applied to data created by the service in respect of an individual user. Log files that reflect each authentication request are retained for a period of six months. This applies to log files of both outside and Commission staff users (this is referred as "traffic data"). Data created by the service other than log files is maintained for as long as the user is active. Once no longer active, data are retained for a further one year, to allow simpler reactivation of the user during that time. Thereafter, the data is rendered anonymous. The same data created by the IMS which refers to Commission's staff will be maintained for as long as the entry for the person retains a relation with the Commission and therefore has a valid entry in the Commission HR database.

The data controller may ***transfer personal data*** to the following recipients: (i) to Commission services which use IMS and (ii) to IDOC, OLAF, the Security Directorate, the Ombudsman and the EDPS. No other transfers of data take place.

Regarding transfers of user data to client DGs after having been authenticated, according to the privacy policy, the disclosure is authorised by the user by the mere fact of registering with the IMS. An option exists to be notified each time that a Commission service requests the identity of the user and users will have possibility to opt out from disclosure.

Regarding transfers to recipients under (ii) above, DIGIT informed the EDPS that investigation of attempted intrusions might be made by the Security Directorate, IDOC and OLAF. This would involve the transfer of log files containing usernames of those accessing the IMS service or client systems including the relevant times.

As far as the ***right to information*** is concerned, the Notification provides a privacy statement which intends to provide information to users. The privacy statement can be found in the Commission's intranet, particularly when using AIDA and ECAS: https://webgate.ec.europa.eu/ecas/disclaimer.jsp, visible from the link "Privacy Statement" on https://webgate.ec.europa.eu/ecas. The current privacy statement is due to be replaced by the

one that was attached to item 15 in the notification. The privacy statement is supposed to be available to any service that uses IMS.

The privacy statement contains information, among others, on the identity of the data controller, the type of data collected, the purposes of the processing and transfers of the data. It also contains time limits for storing the data, the technical measures to protect the data and the procedures to access and correct the data. It refers to the possibility to consult with the EDPS.

Users can ***access*** their data through the pages of either AIDA or ECAS. It is unclear whether access will be given to *all* the personal data of users or only to registration data, i.e. data of identification nature.

The privacy statement informs that users can exercise ***their right to update*** information on-line. It also informs users that if they were registered by their employers (third parties), the update of the information will need to be done through such third parties.

Security measures have been implemented.

2.2. Legal aspects

2.2.1. Prior checking

This prior check opinion relates to the collection and further processing of personal information carried out by the Commission (DIGIT) to authenticate and control the access to Commission information services.

Applicability of the Regulation. 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 (hereinafter "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*"[1]. For the reasons described below, all elements that trigger the application of the Regulation are present:

First, *personal data* as defined under Article 2(a) of Regulation (EC) No 45/2001 are collected and further processed in order to determine whether individuals have the necessary entitlements to access Commission services using IMS. Second, 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 collected both on paper and electronically and it is used to calculate in an automated fashion users' access rights and is then stored in the Commission servers. Finally, the processing is carried out by a Community body, in this case by the Commission (DIGIT), in the framework of Community law (Article 3(1) of Regulation (EC) No 45/2001). Therefore, all the elements that trigger the application of the Regulation are present in this data processing.

1 See Article 3 of Regulation (EC) No 45/2001.

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 subject by virtue of their nature, their scope or their purposes"*.

The EDPS considers that the processing of user information in order to operate IMS as described in the Notification presents specific risks to the rights and freedoms of the data subject particularly by virtue of its nature and scope. Accordingly, it must be subject to prior checking by the EDPS. The specific reasons that support these views are as follows:

In the first place, there is a question related to the relevance of IMS' main task or objective. Indeed, if one takes into account that IMS' key purpose is to facilitate access control to most Commission services, it is obvious that we are facing a service with huge implications for individuals. This is even more so if one recalls that there is an intention on the part of the Commission for an increasingly broadened use of IMS. IMS is and will increasingly become the tool that opens or closes the 'door' to Commission services.

The implications of the service are even more important in light of the size of the user population. Indeed, currently IMS manages an important number of users which include Commission staff and also personnel from outside the Commission. Furthermore, the intention is for IMS to increase its user population, becoming the manager of user populations from other EU institutions and outside organisations. So, the scope of the processing of the individuals whose data are processed is very large.

Thirdly, there is the question of the type of data collected (log files) and IMS' inherent capacity to monitor individuals' behaviour or activities, which IMS performs currently in order to customise the user interface. IMS records each time users log in to authenticate themselves, the time this happens, the time they spent logged into the service, the applications visited, the time spent on each application, etc. The overall information reflects employees' behaviour very accurately and obviously it could be used to monitor employee conduct for whatever purposes such as assessing performance or others. This possibility does not trigger by itself the application of Article 27.2.b of Regulation (EC) 45/2001 but is in itself a meaningful aspect to take into account.

Fourthly, the service is a common element to many IT systems. Although this does not amount to the interlinking of them, it comes close to it and makes also relevant the criterion set up in Article 27.2.c. As explained above, the legal basis is clear but the specific aspect of interrelation of systems is not foreseen in it, thus adding a new factor.

If one combines the four factors described above, it is evident that because of the scope of the processing (the large number of data subjects), the purposes and nature of the processing (controlling access to an increased number of services and its ability to monitor user behaviour), and the possibility, to some extent, to interlink IT systems, the IMS is a service that presents specific risks for the rights of the data subject supporting the necessity for IMS to be prior checked.

Notification and due date for the EDPS Opinion. The Notification was received on 31 May 2007. The two month deadline for the adoption of an opinion was extended for an additional month. Pursuant to Article 27(4) of Regulation (EC) No 45/2001, the three-month period within which the EDPS must deliver this opinion was suspended for a total of 97 days for the purposes of obtaining information form the data controller, plus the month of August and 32 (14 working) days to allow the data controller to comment on the draft opinion. The Opinion must therefore be adopted no later than 6 February 2008.

2.2.2. Lawfulness of the processing

Personal data may only be processed if legal grounds can be found in Article 5 of Regulation (EC) No 45/2001. 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 the performance of a task carried out in the public interest on the basis of the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof"*. In order to determine whether the processing operations in question 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 that entails the processing of personal data (legal basis), and second, whether the processing operations are indeed necessary for the performance of that task (necessity test).

In ascertaining the *legal grounds* in the Treaty or in other legal instruments that legitimise the processing operations that take place in the context of the operation of the Identity Management Service, the EDPS takes note of the following:

In various Commission Communications, the Commission has stated that it will take a series of measures to strengthen the security of its information and communications systems. In particular, is relevant Decision C (2006) 3602 which deals with security of information systems used by the European Commission. This document obliges directorates general to "*draw up, implement and develop the relevant measures for their information systems in accordance with their security requirements in order to give them appropriate protection*". Along the same lines, the Commission communication COM (2001) 298 on Network Information and Security, paragraph 3.7 on security in Government use, states that *"In the framework of the e-Commission, the Commission will take a series of measures to strengthen the security requirements in its information and communications systems"*. By providing authentication and access control to a number of Commission sites, IMS facilitates the implementation of the Commission policies set out above consisting of putting into operation measures towards reinforcing the security of the Commission's information services and systems.

Furthermore, the e-Commission implementation strategy (SEC(2001)924) states the need for officials to easily access in a secure way the information stored in the Commission networks from anywhere. In particular, the Communication reads: "*every official should be able to access information easily at any time and from anywhere using secure desktop or portable computing facilities and secure communication networks*". By enabling the on-line access to different Commission services, using a single sign on, IMS helps to put in place this policy consisting of ensuring easy and secure access to information for Commission staff. Furthermore, because IMS is used not only for Commission staff but also for members of the public, it also contributes to the Commission's goal consisting in setting forth a "*secure and robust on-line systems [....] to allow electronic tendering for procurement, contract and payment tracking systems and electronic invoicing and funds transfer* - "*An e-administration depends on a secure technical infrastructure*". Furthermore, for users outside the Commission, the Decision 2004/387/EC of the European Parliament and of the Council regarding the IDABC programme, Annex II, paragraph h) IMS is also relevant insofar as it states the need to provide identification, authorisation, and authentication and non-repudiation services for projects of common interest.

All in all, IMS contributes towards the goal summarised by DIGIT's communication to the Commission e-Commission 2006-2010: Enabling Efficiency and Transparency "*Better, more*

cost-effective, transparent and secure services will benefit staff, national administrations, partners, business and citizens. [This] also necessitates:... Implementing enhanced security mechanisms".

Clearly, the data processing operations notified for prior checking take place on the basis of this legal framework which all in all aims to put in place the e-Government defined as "*the use of information and communication technologies in public administrations combined with organisational change and new skills"*. IMS is set up under this umbrella and is a step that contributes towards this goal.

As to the necessity of the processing (*necessity test*), the EDPS considers that the IMS can be regarded as a building block or additional step towards achieving the goal of e-Government. Taking into account the Commission's commitment towards e-Government as a general objective and the more concrete measures outlined above, such as the need to ensure the secure on-line access to information for Commission's staff, it appears that the IMS is a necessary measure to achieve both the general and more specific objectives.

The use of data collected through IMS for customisation purposes: As described above, various legislative measures foresee the setting up of measures to strengthen the security of the Commission's information and communications systems. Clearly, the use of IMS for the purposes of authenticating and facilitating access control and related functions falls within these measures. Thus, the use of IMS for such purposes fulfils Article 5a of Regulation (EC) No 45/2001.

However, in the EDPS view, the use of IMS for customisation purposes may be deemed as falling beyond what is purely a measure aiming at enhancing the security of the Commission's information and communications systems. For this reason, the use of IMS data for purposes other than authenticating and facilitating access control may require additional legal grounds. In other words, Article 5a of Regulation (EC) No 45/2001 and the legislation described above are not sufficient to legitimise the use of IMS data for purposes other than authenticating and facilitating access control.

These views are further confirmed if one takes into account Article 6.2 of Regulation (EC) No 45/2001 which establishes that "*personal data collected exclusively for ensuring the security or the control of the processing systems or operations shall not be used for any other purpose, with the exception of the prevention, investigation, detection and prosecution of serious criminal offences"*. This article implies that the data stored in log books so as to ensure the security of the service by tracing the entries into the system should not be used for any other purpose such as the monitoring of the behaviour of the staff member unless in the frame of the prevention, investigation, detection and prosecution of serious criminal offences.

If DIGIT wishes to use data collected trough IMS for other purposes, such as customisation, it is necessary that DIGIT complies with additional legal grounds.

Of the various legal grounds foreseen in Article 5 Regulation (EC) No 45/2001, consent of the data subject may be the most appropriate one. In practice, in order to obtain user's consent, individuals must be given the choice as to whether they want their personal data to be used for customisation purposes. This option can be provided upon accessing the Commission services that use IMS, interactively and on screen. For example, it could be provided using the technique of a "pop up" window. Taking into account that such data will be retained for one year after the user is active, when individuals are asked whether they agree to their personal information being used for customisation purposes, they must be informed that these

type of data will be kept for one year after the user has ceased to be active (see below under 2.2.5)

It should be noted that the fact that an individual does not agree to his/her personal information to be used for customisation purposes does not preclude IMS to use his/her data for the purposes of authenticating and facilitating access control. This is because, as explained above, the use of the personal information for security and access control is legitimised under Article 5(a) of Regulation (EC) No 45/2001, in particular by the specific legal instruments described without the need for any additional legal ground such as consent.

If DIGIT were to decide that IMS will not engage in customisation and instead let the client DG decide to carry out the customisation function, then it would be up to the client DG to obtain consent from the users.

2.2.3. Processing of special categories of data

The notified data processing does not involve data falling under the categories of data referred to in Article 10.1 of Regulation (EC) No 45/2001.

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.

In analysing whether the processing described above is in line with this principle, the EDPS notes the following:

First, data collected can be categorised as identification related data on the one hand and data related to the use of the Commission information services on the other. As far as Commission staff is concerned, identification related data will be collected from human resources databases kept by the Commission. Identification data from outside users will be collected through registration forms.

Second, identification data collected from human resources databases, which according to the Notification, includes three identifiers, work related information, access rights and date of birth seem proportionate to the users for which is collected. Indeed, in order to control access and manage user populations it seems necessary for IMS to collect identifiers, contact and location information, organisational status and functions and access rights. Only if IMS is in possession of this information, will it be possible to deny or allow access to individuals according to their entitlements.

Third, identification data collected from outside users are collected through registration forms. The EDPS understands that the type of information collected through such forms and further input in IMS will not go beyond the categories of data referred to above as 'identification related data'. The data collected from this category of users is also proportionate for the purposes of the collection. If additional data were to be collected through registration forms and such data would be used in IMS, it is doubtful as to whether they would be necessary for the purpose of the service. Furthermore, special care should be taken in collecting such types of data in the light of the fact that registration data by default will be made available to sites other than the one for which users originally obtained the

account. The transfer of registration data other than of identification nature would likely be considered as not proportionate and unnecessary.

Fourth, additional data collected includes data related to the use of the Commission information services, such as the activity on the user account. According to the Notification and privacy policy such data are collected to protect the identity and the integrity of the Commission services accessed by the user. Additionally, such data are also used for customisation purposes. The type of data collected in this context seems necessary for the purposes sought. In other words, the categories of data collected from the use of IMS seem adequate vis-à-vis the purpose consisting of authenticating and facilitating access control as well as for customisation purposes. Although the type/categories of data are appropriate to the purposes, there is an issue about the retention time for this type of data (see below under 2.2.5).

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 respect, the EDPS notes that the service foresees automatic updates of information, particularly of user attributes and calculation of user rights. In other words, IMS is set up in a way that it regularly and automatically updates staff related information obtained through human resources databases. The service level agreement foresees certain deadlines for the updates to take place. The EDPS finds it positive that the service has built-in procedures for the update of information. As further illustrated below, for the information to be fully accurate it is also important to ensure the proper application of the right of access and rectification, which is discussed further below under Section 2.2.7.

The EDPS notes that whilst the procedures exist to update staff related information, a similar system does not appear to exist regarding information of outside users. Such users may have been registered by third parties such as their employers with the enhanced risk for information to be inaccurate. It is therefore important for IMS to put in place a system that ensures the accuracy of the data of outside users. Of course, the possibility of accessing and requesting an update of one's information is in itself an excellent tool towards ensuring the accuracy of the data. But relying only on access rights may not necessarily ensure the accuracy of the data. Accordingly, it would be appropriate to set up a system that will verify the accuracy of the data. For example, such a system could consist of the following: Upon receiving a registration request from an employer, IMS could send an automatic confirmation request to users (i.e. the employees) in order for them to verify that their personal information initially provided is accurate. This should happen the very first time they are or have been registered.

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. This is usually referred to as the 'conservation principle'.

As far as conservation of data is concerned, there are different data retention periods according to the *type* of data. In particular, there are data retention periods for *(i)* identification data; *(ii)* data linked to the use of IMS and the Commission information services that constitutes traffic data and *(iii)* data linked to the use of IMS and the Commission information services that does not constitute traffic data.

Data referred to as ***identification related information*** of outside users are kept for as long as the user is active plus one year. The additional one year is justified for those cases where the person would require renewed access to Commission IT resources, for example, if his/her contract is renewed.

The same type of data as far as the Commission's staff is concerned is kept for the life of the user. This applies to the extent that non-active staff is still entitled to access Commission systems and services.

The above retention periods seem appropriate insofar as information is kept only to the extent and during the time that is necessary for the purpose for which it was collected. Regarding identification related data of the Commission's staff, the EDPS considers that it may be appropriate to keep it for the lifetime of the user, but only provided that the user is entitled to such continued access after he moves from active to inactive status. In other words, if non active users are not entitled to have access to services under the IMS umbrella, information from such users should be erased or removed.

As far as the ***data linked to the use of the Commission information services that constitute traffic data,*** mainly log files, the EDPS notes that the retention period is 6 months. Regarding the storage period for log files the EDPS notes that Article 37 of Regulation (EC) 45/2001 provides for specific measures as concerns the conservation of traffic and billing data. 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. The concept of "*verification of authorised use*" ex Article 37.2 of Regulation (EC) 45/2001 covers all measures adopted by the institution/body to ensure the security of the system/data and respect of the law, Staff regulations or other provisions in a contract with an external subcontractor. Authorised use can be determined in terms of applications visited, web site visited or number called; volume (size of document downloaded, number of e-mails, for example), cost or duration (for example, time spent using a given application).

In the light of the above, the six months period of storage of log files is in line with Article 37.2 of Regulation (EC) 45/2001. However, the EDPS questions whether there is a real need for storing the data for such a long period of time and calls upon DIGIT to shorten it or provide reasons justifying such a need. The EDPS understands that it may be necessary for DIGIT to keep log files for a certain time to verify authorised use of user accounts as defined above. Yet, it seems unlikely that six months old log files will be useful for this purpose and considers that a one/three months period should be sufficient to verify authorised use of user accounts/attempted intrusions unless DIGIT can justify otherwise. Of course, if the monitoring of log files leads the DIGIT to suspect that an individual is engaged in other unlawful activity, the DIGIT will be allowed to keep the incriminating logs files. This measure should only take place on a case by case basis, when there is a legitimate suspicion

that an individual is engaged in other unlawful activity and DIGIT 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. In this regard, it should be noted that the EDPS has interpreted Article 20 to include disciplinary or administrative enquiries.

The EDPS notes that whereas the data used for access control and security, mainly log files, are subject to the storage period mentioned above, additional *information* ***linked to the use of the Commission information services but which does not constitute traffic data is also collected and it is subject to a different retention period.*** Data created by the service other than log files is maintained as long as the user is active. Once no longer active, data are retained for a further one year, to allow simpler reactivation of the user during that time. Thereafter, the data are rendered anonymous. As far as data created by the IMS which refers to personnel employed by the Commission, the information will be maintained for as long as the entry for the person retains a relation with the Commission and therefore has a valid entry in the Commission HR database. The type of information that is kept also includes information obtained through cookies, which is kept for customisation purposes.

In the EDPS' view, this period appears to be justified. Indeed, as it is the case regarding identification data discussed above, it also appears appropriate to keep customisation related data as long as the user is active plus an additional year to allow reactivation so that the user will log in and be able to visualise in a customised way the Commission Services provided through the umbrella of IMS.

Independently of the above, the EDPS considers that the retention policy for such a type of data (i.e. data linked to the use of the Commission information services that constitute traffic data, mainly log files) as described in the privacy statement is not sufficiently precise. To start with, it seems unclear whether the retention time described for identification related data also applies to data linked to the use of the Commission information systems. Whereas the policy for log files is expressly described in the privacy statement, for the rest of such types of data, the situation is not clear. Furthermore, regarding data storage and particularly the types of data stored, the privacy statement says that *"We also store certain additional information relating to the activity on the user account that we create for you.... Data of this kind is not considered personal."* The sentence does not allow individuals to know which kind of information related to the use of the service is stored. Furthermore, any information related to the use of the service which can be traced back to an individual is likely to be deemed personal. The statement that these data are not personal should be deleted.

2.2.6. Transfers of data

According to the Notification, information may be transferred (i) to IDOC, the Security Directorate, the Ombudsman and OLAF and (ii) to Commission systems and services which use IMS. The EDPS notes that the privacy statement only refers to the second transfer, but not to potential transfers to IDOC, OLAF and Ombudsman**.**

*Transfers to IDOC, the Ombudsman**, the Security Directorate,** and OLAF:* Articles 7 of Regulation (EC) No 45/2001 which sets forth certain obligations that apply when data controllers transfer personal data to Community institutions or bodies, which is the case for transfers to IDOC, Ombudsman and OLAF. In particular, Article 7 requires that personal data

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, DIGIT must ensure that *(i)* the recipient has the appropriate competences and *(ii)* the transfer is necessary.

Whether a given transfer meets such requirements will have to be assessed on a case by case basis. If *transfers to the IDOC, the Ombudsman and OLAF* are carried out for the specific purpose of each of the three institutions, they are likely to fulfil the requirement (i) insofar as the three institutions will have the appropriate competences to carry out their respective tasks. However, it will be necessary to assess on a case by case basis whether the transfer of such information is necessary in the light of the specificities of the case. In order to materialise this requirement, the EDPS considers that it would be appropriate for each set of data transfers to describe the reasons why the necessity criteria is fulfilled. In addition to the above, pursuant to Article 7 of Regulation (EC) No 45/2001 a notice has to be given to the recipient in order to inform him/her that personal data can only be processed for the purposes for which they were transmitted[2].

Transfers to the Commission systems and services which use IMS: In addition, data transfers are made to the Commission systems and services which use IMS. As opposed to the above type of transfers, which happen occasionally, transfers to the Commission services/systems using IMS are a recurrence. As a matter of fact, by virtue of being an IMS client, an automatic transfer of the data gathered through IMS is passed on to the IMS client unless the individual objects to the transfer. Client DGs' usage of data originating from IMS is limited to purposes compatible with that of IMS. If a user objects to the transfer, he/she may be able to access the Commission service/system anonymously, although, in some cases, access will not be possible without authentication, thus, in fact, the transfer is carried out provided that the user did not opt out.

In the light of the above facts, these data transfers appear to satisfy the requirements of Article 7 of Regulation (EC) No 45/2001: The recipients, the different Commission services will use the data in order to perform tasks for which they are competent. The data will be used, among others, to enforce decisions as to user entitlements (i.e. allow or deny access to users to their own applications), customisations of users experience, etc. These are legitimate and necessary tasks for a client DG that is responsible for a Commission service/system which is accessible only to those who have the necessary access rights. The transfer may not fulfil the requirements of Article 7 if the client application is not subject to access rights, i.e. application is available to anyone. This is because in such case it seems uncertain as to whether the Commission would be performing a task for which it is competent and also whether the transfer is necessary. Indeed, if the client application is open to everyone, it seems uncertain whether there is any need to process data of visitors. In this context, the possibility for users to opt out from the transfers offered by IMS is particularly appropriate. Indeed, the EDPS considers that it is correct to provide an opt out for data transfers to client DGs that run applications not subject to access rights and for which Article 7 may not be fulfilled.

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

[2] This issue has been discussed in the EDPS Opinion of 8 March 2006 on a notification for prior checking on "Disciplinary cases (including related administrative reviews of complaints and grievances, Ombudsman and Court cases)" (Case 2004-270).

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 Notification and the privacy statement provide the right of access to the information collected through IMS. Individuals are notified of the possibility to exercise such a right and they are given information about whom to contact to do so. In particular, this right can be exercised through the user registration service AIDA and ECAS. It is unclear whether access will be given to *all* the personal data of users or only to registration data, i.e. data of identification nature. However, the language used in the privacy statement seems to suggest that access is limited to registration information, which the user can access directly on-line. It does not refer to the possibility to access, for example, indirectly, data created by IMS such as log files. Thus, it appears that this type of data, including log files will not be provided if individuals exercise their access rights.

In this regard, the EDPS recalls that individuals are entitled to access *all* personal data ("*any information relating to an identified or identifiable natural person*"), and this includes data that identify the individual, directly and indirectly, and also data generated by the service which relate to the user. This includes data such as log files. The EDPS urges DIGIT to ensure that individuals have the right of access to all their personal data. For data that individuals can not access directly which could be for example log files, in order to ensure that such access will be dealt with in a timely fashion and without constraints, it may be appropriate for DIGIT to set up a procedure with reasonable time limits.

Article 14 of the Regulation provides the data subject with the right to rectify inaccurate or incomplete data. The privacy statement informs that users can exercise this right on-line. It also informs users that if they were registered by their employers, the update of the information may need to be done through these third parties. If the update is done by the Commission and the third parties re-submit the information, it will be re-instated. The EDPS does not object to a procedure where rectification/erasure rights are carried out through a third party, provided of course that the rights can be effectively exercised.

However, in this case, the EDPS considers that the procedure could be improved to ensure the effective application of the right. As it is currently proposed, the procedure may lead to situations when in fact individuals have to waste time and energy to exercise their right to no avail. Users whose data have been provided by a third party may not know whom to contact to exercise the rectification right. Furthermore, they are forced to go through a double procedure, first try to update the information by themselves and then if it is unsuccessful (for example, because the third party re-instates it), go through the third party. In order to improve the procedure the EDPS considers that it would be more straightforward if DIGIT took over the responsibility to contact the third party who had supplied the information in order to ensure the effective application of the rights, particularly to avoid situations where the information would be re-instated. In other words, it should be up to DIGIT to ensure the accuracy of the data that it holds about individuals. If an individual erases/updates some information, it seems appropriate for DIGIT to have procedures to ensure the verification of this information. Thus, the EDPS encourages DIGIT to set up a procedure to ensure the effective application of the right of rectification/erasure.

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.

In order to ensure compliance with these provisions, a copy of a privacy statement was annexed to the Notification. The data controller has informed the EDPS that the privacy statement provided with the Notification will be available when using AIDA and ECAS and is also supposed to be available before the use of any Client service or system that uses IMS through a user interface.

The EDPS calls upon DIGIT to ensure that individuals whose personal data are processed through IMS (i.e. individuals who have an account) are provided with the privacy policy. The privacy policy can be made available by displaying it prominently in ECAS, AIDA or any other user interface. Furthermore, the statement not only has to be displayed when the user first registers but must also remain available at any time for further consultation. Finally, it is also important to avoid confusion between this statement and the privacy statement of the application operated by the client DG. Individuals may not expect their data to be collected by an interface between themselves and a client application. Thus, DIGIT should do its utmost to clarify that a collection of user data occurs that is independent from the collection that may occur in the application itself.

The EDPS also reviewed the content of the information provided in the privacy statement to verify whether the content satisfies the requirements of Articles 11 and 12 of Regulation (EC) No 45/2001. The privacy statement contains information, among others, on the identity of the data controller, the type of data collected, the purposes of the processing and transfers of the data. It also contains time limits for storing the data, the technical measures to protect the data and the procedures to access and correct the data. It refers to the possibility to consult with the EDPS. The EDPS considers that the privacy statement contains most of the information required under Articles 11 and 12 of the Regulation. However, several amendments would contribute to ensure full compliance with Articles 11 and 12, in particular:

(i) The description of the purposes of the processing should be ameliorated, because it now contains paragraphs that are confusing or somehow misleading. For example, the use of the data for customisation purposes as such is not clearly indicated. Also, section 2 says that registration is required "*if there is a simple need for the site to remember you between visits and adapt itself to your needs or wishes*". In this regard, it appears doubtful whether there is a real *need* for a site to remember individuals or whether this is in fact an optional element. The statement that certain data related to the use of the site are not personal should be deleted.
(ii) The types of information collected should be clarified. In particular, it should be explained what "*additional information relating to the activity on the user account*" means. The statement that this information is not personal data should be deleted.
(iii) Information on data retention periods should be clarified.
(iv) It would be appropriate to indicate that, if necessary, the information may be transferred to OLAF, IDOC, Security DG, the Ombudsman and EDPS.

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 technical and organisational measures appear to be suitable in order to ensure a level of security appropriate to the risks represented by the processing and the nature of the data protected.

3. Conclusion

There is no reason to believe that there is a breach of the provisions of Regulation 45/2001 provided that the considerations in this Opinion are fully taken into account. In particular, DIGIT must:

- Obtain users' consent to process data processed through IMS for customisation purposes (interactively and on screen, for example, using the technique of a "pop up" window).
- Put in place a system that ensures the accuracy of personal information of non Commission staff members who have been registered in IMS by third parties such as their employers.
- Consider shortening the data retention deadlines for log files.
- Erase or remove identity data of non active Commission staff users, not entitled to have access to services under the IMS umbrella.
- Set up reasonable time limits to deal with access requests.
- Ensure that access is given to all types of data, including personal data generated by IMS.
- Set up a system to ensure the effective application of the rectification right, probably by DIGIT taking over the verification of data provided by third parties.
- Amend the privacy statement as recommended in this Opinion and ensure its display before the use of IMS as well as the possibility to consult it at any time.

Done at Brussels, 6 February 2008

Peter HUSTINX
European Data Protection Supervisor