To be filled out in the EDPS' office

REGISTER NUMBER: 224

NOTIFICATION FOR PRIOR CHECKING

Date of submission: 31/05/2007

Case number: 2007-349

Institution: European Commission

Legal basis: article 27-5 of the regulation CE 45/2001(1)

(1) OJ L 8, 12.01.2001

INFORMATION TO BE GIVEN(2)

(2) Please attach all necessary backup documents

1/ Name and adress of the controller

2) Name and First Name of the Controller:GARCIA MORAN Francisco

3) Title:Director General

4) Directorate, Unit or Service to which the Controller is attached:.

5) Directorate General to which the Controller is attached:DIGIT

2/ Organisational parts of the institution or body entrusted with the processing of personal data

26) External Company or Directorate General to which the Processor is attached:
25) External Company or Directorate, Unit or Service to which the Processor is attached:

DIGIT.IMS Service Manager

3/ Name of the processing

Identity Management Service

4/ Purpose or purposes of the processing

Manage user populations and their rights in the context of IT systems. The underlying purpose is to ensure the appropriate level of security is applied in a consistent fashion across Commission IT services with the ability to identify the user of the service and / or determine his or her authorisations and roles within the context of their service.
A secondary purpose of the processing is to enable client applications to provide the following services:
- "white pages" services, allowing users contact details to be found (e.g. e-mail address book or telephone directory)
- selection of users from lists, usually based on some selection criteria
- construction of lists of users, primarily e-mail distribution lists
- customisation of user interfaces according to users' individual characteristics

5/ Description of the category or categories of data subjects

14) Data Subject(s) concerned:

Users of Commission IT systems where it is necessary or desirable to know the identity of the user
Persons, not necessarily Commission personnel, whose contact details need to be available to users of Commission IT systems.

16) Category(ies) of Data Subjects:

Personnel employed by or working for the Commission.
Personnel of any other organisation having electronic business with the Commission and individual citizens or members of the public anywhere in the world who have registered with the Commission. Organisations include other European institutions and bodies (for whom its likely that all personnel will be included automatically), member state administrations, other international organisations, as well as private enterprises and non-profit-making organisations.

6/ Description of the data or categories of data (including, if applicable, special categories of data (article 10) and/or origin of data)*(including, if applicable, special categories of data (article 10) and/or origin of data)*

17) Data field(s) of Data Subjects:
Attention: Please indicate and describe in the answer to this question also data fields which fall under article 10

Identifiers (article 10, paragraph 6 of the Regulation): three unique identifiers are stored. The username (or userid); the Commission personnel number (PER_ID) for internal users or, for automatically synchronised external users, a unique key; and the e-mail address (optional for external users).
Other data:
Names; Passwords; group membership; organisational assignment; telephone and office number; date password last changed; date of last authentication; account status (whether active, inactive or locked by an administrator);administrative status (activity and type of employment);job title; job functions; organisational role(s); occupation; place of work or residence; date of birth (used as matching criterion to prevent creation of duplicate entries for a single user)
See the attachment at question 37 for details of the permitted usage of the data fields by client applications.

18) Category(ies) of data fields of Data Subjects:
Attention: Please indicate and describe in the answer to this question also categories of data fields which fall under article 10

Credentials
Contact and location information
Organisational status, assignment and functions
Access rights (group membership and roles)
Authenticated account activity
Error prevention information (to ensure correct matching of data between authoritative source and the identity repository)
Account status

7/ Information to be given to data subjects

15a) Which kind of communication(s) have you foreseen to inform the Data Subjects as described in articles 11 - 12 under 'Information to be given to the Data Subject'

Users of IMS component systems that have a user interface can consult a common service-specific privacy statement (SSPS), which informs the data subject of the information that is available. These systems also have provisions for the user to consult the personal data that is stored regarding his or her user account.
Links to the SPPS are displayed prominently.
The SSPS is attached to this notification.
Client services that process IMS data must provide their own SSPS including a reference to the IMS SSPS.

8/ Procedures to grant rights of data subjects (rights of access, to rectify, to block, to erase, to object)*(rights of access, to rectify, to block, to erase, to object)*

15b) Which procedure(s) did you put in place to enable Data Subjects to exert their rights: access, verify, correct, etc., their Personal Data as described in articles 13 - 19 under 'Rights of the Data Subject' :

The attached SSPS describes the provisions that have been made in this respect.

9/ Automated / Manual processing operation

7) Description of Processing:
Attention: Please describe in the answer to this question if you process personal data falling under article 27 "Prior-Checking (by the EDPS - European Data Protection Supervisor)"

Provide user authentication, access control and authorisation facilities for Commission information systems and infrastructure services.

Includes the European Commission Authentication Service (ECAS), the Commission Entreprise Directory (CED) and the Commons User Directory (CUD).

Serves as master notification for all directories with specific processing characteristics.

8) Automated Processing operation(s):

Collection of information about users from authoritative sources (internal HR databases, transfers from external bodies such as other institutions, and MS administrations ?)

Calculation of access rights based on policies defined by service providers and on the attributes of users.
Assignment of access rights on request by users or service providers.

Input and storage of user information in a common repository or set of repositories

Authentication of users on behalf of and transmission of authorisation data to Commission information systems

9) Manual Processing operation(s):

Register a user external to the Commission
Assign a role or an access right to a user
Validate and execute a user's request to reset their password if they are unable to do it themselves: validation may involve checking personal details supplied by the user against the database
Activate or deactivate a user account or an access right
Check which access rights a user has and which users have access to a given system
Check user information against the data sources for diagnostic purposes
Correct user details in order to resolve conflicts that are preventing automatic processes from working
Create reports, e.g. for a service provider, list who has access to their service

10/ Storage media of data

Electronic storage on disks of the servers in the Commission's Data Centre in DG DIGIT, with backup to the Commission's Data Centre back-up systems

11/ Legal basis and lawfulness of the processing operation

11) Legal basis of Processing:

The processing is necessary for the performance and support of tasks carried out by the institution as mandated by the treaties, in particular articles 5, 7, 211 - 219 of the Treaty of Amsterdam.

More specifically, 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?.

Commission Decision C(2006) 3602 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". The processing provides mechanisms and data to facilitate this.

Furthermore, the e-Commission implementation strategy (SEC(2001)924), states:
- "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
- "secure and robust on-line systems need to be put in place to allow electronic tendering for procurement, co
- "An e-administration depends on a secure technical infrastructure"

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;"

For users outside the Commission, decision 2004/387/EC of the European Parliament and of the Council reg

12) Lawfulness of Processing:
Answering this question please also verify and indicate if your processing has to comply with articles 20 "Exemptions and restrictions" and 27 "Prior checking (by the EDPS)"

The processing is necessary and lawful based on article 5(a) of Regulation (EC) 45/2001.

12/ The recipients or categories of recipient to whom the data might be disclosed

20) Recipient(s) of the Processing:

Any Commission IT service registered within the Identity Management Service's database for the purposes described in paragraph 13, with the exception of freely available data which, subject to volume restrictions, can be accessed by any clent system. (The latter usage is being phased out.)
Entities authorised by the Data Protection Officer to obtain historical data in justified cases (see response to 22(a)) such as Ombudsman, IDOC, OLAF

21) Category(ies) of recipients:

Other systems forming part of the Identity Management Service
Client applications within the Commission
Privileged clients within the Commission, such as the e-mail service
Entities specially authorised by the DPO on a case by case basis

13/ retention policy of (categories of) personal data

Data created by the system in respect of an individual user is maintained as long as the user is active. Once no longer active, data is retained for a further year, to allow simpler reactivation of the user during that time. Thereafter, the data is rendered anonymous. Nevertheless, for personnel employed by or working for the Commission, the user's identifier (userid), personnel number and, to prevent errors, date of birth are retained in order to:
(1) allow the reuse of the identifier, if appropriate, should the person require renewed access to Commission IT resources after a long absence.
(2) determine the real world identity of a user. Systems relying on the authentication service may record the identifier used when performing an action - in cases of litigation, dispute or investigation, the personnel number linked to an identifier will be disclosed to an appropriate authority, subject to the prior authorisation of the Data Protection Officer.
Since it is possible for users to change their identifiers, a history of changes must also remain accessible. The limited information is maintained for a period of three years.

13 a/ time limits for blocking and erasure of the different categories of data (on justified legitimate request from the data subject) (Please, specify the time limits for every category, if applicable)
(on justified legitimate request from the data subject)
(Please, specify the time limits for every category, if applicable)

22 b) Time limit to block/erase data on justified legitimate request from the data subjects

Data that is obtained by IMS from external systems can only be modified by changing the data in the source. Any modification will be reflected automatically in IMS.
Data that is maintained by IMS itself can be corrected by the individual participating system, in line with its own notification to the DPO.

14/ Historical, statistical or scientific purposes
If you store data for longer periods than mentioned above, please specify, if applicable, why the data must be kept under a form which permits identification,

22 c) Historical, statistical or scientific purposes - If you store data for longer periods than mentioned above, please specify, if applicable, why the data must be kept under a form which permits identification

15/ Proposed transfers of data to third countries or international organisations

27) Legal foundation of transfer:

Only transfers to third party countries not subject to Directive 95/46/EC (Article 9) should be considered for this question. Please treat transfers to other community institutions and bodies and to member states under question 20.

28) Category(ies) of Personal Data or Personal Data to be transferred:

16/ The processing operation presents specific risk which justifies prior checking (please describe):*(please describe)*):

7) Description of Processing:
Attention: Please describe in the answer to this question if you process personal data falling under article 27 "Prior-Checking (by the EDPS - European Data Protection Supervisor)"

Provide user authentication, access control and authorisation facilities for Commission information systems and infrastructure services.

Includes the European Commission Authentication Service (ECAS), the Commission Entreprise Directory (CED) and the Commons User Directory (CUD).

Serves as master notification for all directories with specific processing characteristics.

12) Lawfulness of Processing:
Answering this question please also verify and indicate if your processing has to comply with articles 20 "Exemptions and restrictions" and 27 "Prior checking (by the EDPS)"

The processing is necessary and lawful based on article 5(a) of Regulation (EC) 45/2001.

Article 27.2.(a) Processing of data relating to health and to suspected offences, offences, criminal convictions or security measures,

Processing of data relating to suspected offences,

Article 27.2.(b) Processing operations intended to evaluate personal aspects relating to the data subject,

Processing operations intended to evaluate personal aspects relating to the data subject

Article 27.2.(c) Processing operations allowing linkages not provided for pursuant to national or Community legislation between data processed for different purposes,

n/a

Article 27.2.(d) Processing operations for the purpose of excluding individuals from a right, benefit or contract,

n/a

Other (general concept in Article 27.1)

n/a

17/ Comments

1) Date of submission:

10) Comments if applicable:

36) Do you publish / distribute / give access to one or more printed and/or electronic directories?
Personal Data contained in printed and/or electronic directories of users and access to such directories shall be limited to what is strictly necessary for the specific purposes of the directory.
If Yes, please explain what is applicable.

yes
Please see the attachment at question 37

37) Complementary information to the different questions if applicable, including attachments to this notification which should not be public :

PLACE AND DATE:31/05/2007

DATA PROTECTION OFFICER: RENAUDIERE Philippe

INSTITUTION OR BODY:European Commission