To be filled out in the EDPS' office

REGISTER NUMBER: 233

NOTIFICATION FOR PRIOR CHECKING

Date of submission: 01/06/2007

Case number: 2007-360

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:JORTAY Marcel

3) Title:Head of Unit

4) Directorate, Unit or Service to which the Controller is attached:C.02

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:

3/ Name of the processing

Log files of DIGIT operational environment

4/ Purpose or purposes of the processing

Log files are used exclusively by system administrators. They are very useful and, when well designed, are powerful tools to understand and follow the behaviour of a system. As such, log files are used to trace events in an information system and to help debugging and repair. Log files are part of the systems and are essential tools to provide the security and an efficient support when information systems are not working correctly.

5/ Description of the category or categories of data subjects

14) Data Subject(s) concerned:

Anybody who uses an information system of the Commission may have his user ID recorded in the corresponding log file.

16) Category(ies) of Data Subjects:

Categories of Data Subjects are EC Officials, Officials from other European Institutions, "Experts Nationaux Détachés", subcontractors, European & world citizens.

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

- Logging of user ID, IP addresses, logon time, logoff time and program used. In some cases, sequences of actions performed on the information system are also recorded.

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

NA

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 have to enter their user ID to use an information system. No specific communication is in place.

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' :

No specific procedure has been put in place to enable Data Subjects to exert their rights directly on their personal data in log-files. The creation of a log files results when starting an application. Information to users has to be given at application level.
Note that the only personal data of the Data Subject present in the log files are his own user ID he must enter at logging time. If an incorrect user ID is used, the user cannot log on.

What regards incorrectly encoded user ID, Data Subjects are instructed to take contact with their Local informatics' support who can initiate the corresponding change procedures.

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)"

Operational environment of the Data Center and telecommunications, more precisely processing personal data related to operation and administration of servers, storage and telecommunications (information systems themselves are notified by the system owner).

Log files are created to record elements that trace any operation or event on a system. These elements may be the name, the user id, the logical address (IP address), a time stamp giving the beginning and the end of the operation. Other more technical information are also associated in the records but they are not data falling under article 27, they are collected and used to understand the behaviour of the system.

Examples of log files:

- Logging into Europa proxies, Intracomm and application server's proxies (access to web applications not
8) Automated Processing operation(s):

Log files are generated automatically; they are embedded into the function of the system. Each time a system is started, a log file is created automatically; data is recorded and stored in well defined area.

9) Manual Processing operation(s):

There is no manual data processing.

10/ Storage media of data

Log files are recorded on the system disks and saved on tape every day during system back up.

11/ Legal basis and lawfulness of the processing operation

11) Legal basis of Processing:

The processing of the log files are the result of running information systems. Information systems are necessary for the performance and the support of the numerous tasks carried out by the institution as mandated by the treaties, and more specifically articles 6, 7, 211 - 219 and 255 of the Treaty of Amsterdam.

Implementing the Treaty, the e-Europe Action Plan, including the derived policy measures and actions on e-Government, and the e-Commission implementation strategy based on actions 7, 8 and 9 of the Commission Reform White Paper called for a modern & efficient communications infrastructure including equivalent office automation technology.

As almost all institutional tasks have multiple "communication" aspects, which, considering the current state of the art in use in almost every organisation in a global networked environment around Europe and the world, these tasks must be supported by the appropriate functionalities of a modern, diversified and performing information systems.
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 for the efficient functioning of the European Commission. The lawfulness of the processing is based on article 5(a) of the regulation.

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

20) Recipient(s) of the Processing:

EC officials responsible of the information system and System administrators who are responsible of the support of the information system.

21) Category(ies) of recipients:

- EC officials,
- Subcontractors under EC officials guidance.

13/ retention policy of (categories of) personal data

Log files are retained on disks no more than 10 days. Tapes used for back up are reused after 30 days.

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

NA

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

Some log files of information systems on Oracle may be used for statistics to follow the performance of the system. In this case, log files are treated to be anonymous before generating statistics.
Log files older than 30 days are no more used since tapes are not trusted after that delay.

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.

NA

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

NA

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)"

Operational environment of the Data Center and telecommunications, more precisely processing personal data related to operation and administration of servers, storage and telecommunications (information systems themselves are notified by the system owner).

Log files are created to record elements that trace any operation or event on a system. These elements may be the name, the user id, the logical address (IP address), a time stamp giving the beginning and the end of the operation. Other more technical information are also associated in the records but they are not data falling under article 27, they are collected and used to understand the behaviour of the system.

Examples of log files:

- Logging into Europa proxies, Intracomm and application server's proxies (access to web applications not

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 for the efficient functioning of the European Commission. The lawfulness of the processing is based on article 5(a) of the regulation.

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

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

Article 27.2.(b) 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:

Generally, log files are consulted when there is a problem on a system, to provide support to a user, to verify the behaviour and performance of a system, to guaranty the security of the systems by tracking unauthorised accesses. The system administrators used them only as tools in the framework of their tasks.

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.

no

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

PLACE AND DATE:01/06/2007

DATA PROTECTION OFFICER: RENAUDIERE Philippe

INSTITUTION OR BODY:European Commission