To be filled out in the EDPS' office

REGISTER NUMBER: 107

NOTIFICATION FOR PRIOR CHECKING

Date of submission: 13/06/2006

Case number: 2006-298

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:MERCHAN CANTOS Francisco

3) Title:Director

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

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

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:

European Commission - DG DIGIT.Data Centre.2
European Commission - IAS.Senior Management
European Commission - IAS.A

3/ Name of the processing

Internal Audit process

4/ Purpose or purposes of the processing

The internal auditor shall advise his/her institution on dealing with risks, by issuing independent opinions on the quality of management and control systems and by issuing recommendations for improving the conditions of implementation of operations and promoting sound financial management.

He/She shall be responsible in particular:

(a) for assessing the suitability and effectiveness of internal management systems and the performance of departments in implementing policies, programmes and actions by reference to the risks associated with them;

(b) for assessing the suitability and quality of the internal control and audit systems applicable to every budgetary implementation operation.

2. The internal auditor shall perform his/her duties on all the institution's activities and departments. He/She shall enjoy full and unlimited access to all information required to perform his duties, if necessary on the spot, including in the Member States and in third countries.

3. The internal auditor shall report to the institution on his/her findings and recommendations. The institution shall ensure that action is taken on recommendations resulting from audits. The internal auditor shall also sub institution an annual internal audit report indicating the number and type of internal audits carried out, the recommendations made and the action taken on those recommendations.

4. Each year the institution shall forward a report to the discharge authority summarising the number and type of internal audits carried out, the recommendations made and the action taken on those recommendations.

5/ Description of the category or categories of data subjects

14) Data Subject(s) concerned:

All agents and contractual staff of the European Commission and its Agencies and Offices.

16) Category(ies) of Data Subjects:

All agents and contractual staff of the European Commission and its Agencies and Offices.

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

The principal types of data concerning auditees collected in the framework of an audit are documents produced or signed by the person, records of transactions within information systems and records of meetings involving the data subject.

The time recording data collected on audit staff are records, filled in by the member of staff, indicating the time spent in audit and non-audit activities.

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

As indicated in Question 18, data collected from the auditee is mainly a collection of documents and records showing his work in an internal capacity. Where appropriate data will be collected on the data subject's external activities if this is relevant to the internal activity. In this latter context more personal data concerning the data subjexts external activities may be collected.

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'

A brochure explaining the principles of internal audit has been distributed to all Commission staff.
The Internal Auditor proposes to give an information to the auditee (the Director-General) on data protection within an audit which could be distributed to all his staff at the beginning of an audit.

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 internal audit process is covered by Article 20 1e which restricts the data subjects rights to access, verify and correct personal data held by the Internal Auditor. In sensitive cases it would not be in the interests of the Institution to inform the data subject spontaneously, or on request, of the exact nature of any personal data gathered in the course of an audit .

Information to audit staff concerning the use which will be made of time reporting data has been made in writing to the staff concerned. Staff have been informed that the data will not be made available in any form which could be used for performance evaluation purposes without the express agreement of the EDPS.

All information held on audit staff is always visible to the staff member and can be contested with the line manager.

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)"

The internal auditor shall advise his/her institution on dealing with risks, by issuing independent opinions on the quality of management and control systems and by issuing recommendations for improving the conditions of implementation of operations and promoting sound financial management.

In the course of his work the internal auditor has access to all data held by the Institution and can request access to data held by third parties who have contractual relations with the Institution. Some of this data may be covered by Article 27 2a of the Regulation.

In the course of his work the Internal Auditor collects data concerning the use of time by his staff. This could be covered by Article 27 2b of the Regulation.

8) Automated Processing operation(s):

The internal audit process is supported by an information system, Audit Management System (AMS) where all data which is collected within a particular audit is stored.

This information system also allows for detailed time recording by audit staff and for a dialogue between audit staff and their line managers concerning their work.

9) Manual Processing operation(s):

As part of the audit process, the auditor will collect background data on the activities of the auditee which will be analysed within the audit team for that particular audit. These documents are often received in paper format which are examined and if appropriate entered into AMS as part of the documentation of the audit.

10/ Storage media of data

The data is mostly stored in an information system, AMS, hosted by the Commission's Data Centre in Luxembourg. Some information which is in electronic format but which is considered too bulky to store in AMS is kept on a protected file system on the IAS servers. A further category of data is stored in paper files in the IAS's offices.

11/ Legal basis and lawfulness of the processing operation

11) Legal basis of Processing:

Articles 85-87 of the Financial Regulation
Articles 109-113 of the Implementing Rules
SEC/2000/1801 Charter of the IAS
SEC/2000/1803 for the Internal Audit Capabilities.
Article 1 of Council Regulation 1700/2003

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)"

Article 86 of the Financial Regulation charges the Internal Auditor to give opinions on the implementation of management and control systems within the Institutions. Article 86.2 gives the Internal Auditor full and unlimited access to all information required to perform his duties.

This unlimited access to data is carried out in the framework of Article 20 1e where the auditor needs exemptions from the requirement to ask the data subject in advance for permission to acquire personal data and to allow rights of inspection.

The personal data held on audit staff within AMS which could be used for measuring the effectiveness of staff is covered by Article 27 2b.

Considering the legal basis the processing is necessary and lawful under article 5(b) 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:

The processing is used to produce an Audit Report which is delivered to the auditee (either a Commission Directorate-General or an Agency). In this context the auditee refers to the head of the organisation being audited and not necessarily all the individual data subjects. Transmission of this report by the auditee within his own organisation is decided by the auditee. Copies are made available to:
- the Audit Progress Committee
- the European Court of Auditors
- the Data Protection Officer of the European Commission if data protection issues are covered
- Cabinet responsible for the DG(s)
- Central Financial Service
- Assistant of the DG responsible for Budget if associated with the recommendations
- Head(s) of the IAC of the DGs involved
- Control Co-ordinators of the DGs involved
- Persons appointed by the auditee as the contact points
- The Director General of other DGs mentioned in the report as responsible for implementation

Details of the recommendations (which are a subset of the audit report) and their follow up in affected
21) Category(ies) of recipients:

The auditee, some of his staff and responsible cabinet, DGs involved in implementation, the Audit Progress Committee, the European Court of Auditors and in certain circumstances the Data Protection Officer of the European Commission. The information system of the Audit progess Committee receives electronic copies of recommendations.

13/ retention policy of (categories of) personal data

The audit report will be kept indefinitely. This type of document is considered to be a 'document of administrative value' as defined in Article 1 of Council Regulation 1700/2003 setting out the categories of documents which would be placed in the historical archives of the European Union.

Article 85 of the Financial Regulation requires the internal auditor to operate in compliance with the relevant international standards. The Institute of Internal Auditors, which is the relevant international body, produces 'practice advisories' which recommend to audit bodies how they should operate to meet international standards. In the case of time limits for retention of supporting documentation, the IIA does not suggest a particular time period but says that they should be maintained long enough for the issues raised to be resolved and that the records should then be destroyed. The Internal Auditor of the Commission has decided to work on a three year audit cycle. In these circumstances the audit documentation should be available for consultatation throughout the following audit cycle to measure to what extent issues have been resolved in the in the previous audit cycle. The maximum period of retention would then be 6 years unless an issue remained unresolved at that point in which case the documentation on that issue would be retained for a longer period.

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

Not applicable as the data subject has no rights to consult the data held on him/her. (article 20 1e)

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

Not applicable

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.

Not Applicable

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

Not Applicable

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)"

The internal auditor shall advise his/her institution on dealing with risks, by issuing independent opinions on the quality of management and control systems and by issuing recommendations for improving the conditions of implementation of operations and promoting sound financial management.

In the course of his work the internal auditor has access to all data held by the Institution and can request access to data held by third parties who have contractual relations with the Institution. Some of this data may be covered by Article 27 2a of the Regulation.

In the course of his work the Internal Auditor collects data concerning the use of time by his staff. This could be covered by Article 27 2b of the Regulation.

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)"

Article 86 of the Financial Regulation charges the Internal Auditor to give opinions on the implementation of management and control systems within the Institutions. Article 86.2 gives the Internal Auditor full and unlimited access to all information required to perform his duties.

This unlimited access to data is carried out in the framework of Article 20 1e where the auditor needs exemptions from the requirement to ask the data subject in advance for permission to acquire personal data and to allow rights of inspection.

The personal data held on audit staff within AMS which could be used for measuring the effectiveness of staff is covered by Article 27 2b.

Considering the legal basis the processing is necessary and lawful under article 5(b) 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,

Some of the processing operations of the procedure and system concerning the "Internal Audit Process" are submitted under this paragraph.

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

Some of the processing operations of the procedure and system concerning the "Internal Audit Process" are submitted under this paragraph.

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

None

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

None

Other (general concept in Article 27.1)

None

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.

no

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

Senior Management and the Unit IAS/A/2 responsible for communication with the Audit Progress Committee have access to audit documentation to allow validation and reporting activities. Neither of these two entities are under the direct control of the data controller. The AMS database is managed by officials in Unit IAS/A/1.

PLACE AND DATE:13/06/2006

DATA PROTECTION OFFICER: HILBERT Nico

INSTITUTION OR BODY:European Commission