JOAQUIN BAYO DELGADO
ASSISTANT SUPERVISOR

Mr Philippe RENAUDIERE
Data Protection Officer
European Commission
BRU-BERL-08/330
B-1049 Brussels

Brussels, 31 October 2006
JBD/ab D(2006)1155 **C2006-0298**

"INTERNAL AUDIT PROCESS" at DG IAS (Commission)

Dear Mr Renaudière,

We have concluded from our examination of the prior checking notification and the further information received that the "Internal audit process" at DG IAS in the European Commission (EDPS case ref.: 2006-298) is not subject to prior checking by the EDPS.

The case was submitted for prior checking on two grounds, Article 27(2)(b) and Article 27 (2)(a) of the Regulation.

1) Time recording on the use of time by the staff of the Internal Auditor:

This processing was submitted under Article 27(2)(b) of the Regulation. Processing operations which are intended to evaluate personal aspects relating to the data subject, including his or her ability, efficiency and conduct falls under the scope of that article.

From the available information, we conclude that the time recording system is not intended to evaluate the personal aspects of individual staff members, because a) the results of the time-reporting will not form part of the *appraisal process* of the Commission's staff; b) the time recording data are *aggregated* to compare total time reported by staff members compared with scheduled time, which means that the aggregate format does not identify individual users[1]; and c) the IAS does not use the data to see the *proportion of the time spent by the individual staff members* on audit or non-audit activities or their individual use of time within an audit. In addition, the notification form specifically states that the records at present are not used for evaluating the individual members of the staff: "*Staff has 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*".

[1] Note on "Monitoring Time Allocation to Audit Engagements" of 25 January 2005. IAS/FM D(2004).

Since there is no intention to use the time recording data for evaluation purposes, the processing does not present any specific risk in that respect, and it does not fall under prior checking by the EDPS. If the purpose of the time-recording system changes to include evaluation of individual audit staff members, this is likely to fall within the scope of Article 27(2)(b) of the Regulation.

2) Evidence or suspicion of fraud during an audit

The internal audit process was submitted under Article 27(2)(a) of the Regulation. Processing of data relating to suspected offences, offences, criminal convictions and security measures are likely to present specific risks to the rights and freedoms of data subjects.

The Note of the Acting DPO attached to the prior checking notification form specifically mentions that: "*if during the Audit Process IAS has evidence or suspects a fraud it implicates, respectively operates a handover to OLAF as fraud processing is no longer the mandate of IAS".*

The main purpose of the internal audit process is to deal with risks concerning the quality of management and control systems and to issue recommendations for improving upon the situation and to promote sound financial management. It is possible that the internal audit reveals evidence or data on suspected criminal offence or irregularities which may result in further procedures, e.g. internal investigations by the European Anti-Fraud Office (OLAF). The question therefore arises whether any specific risk is involved. The internal audit process does not involve such a risk since information on suspected criminal offences is immediately transferred to OLAF. The internal investigation by OLAF poses specific risks to the rights and freedoms of data subjects, thus fall under Article 27(2)(a). The EDPS already has prior checked the OLAF internal investigations (2005-418)[2].

Therefore the internal audit process itself is not subject to prior checking under Article 27(2)(a).

3) Internal audit as evaluation of individuals

Although the prior checking notification does not mention Article 27(2)(b) as ground for prior checking of the audit process itself, the EDPS has considered this alternative.

The internal auditor advises 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. The internal auditor is 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; and (b) for assessing the suitability and quality of internal control and audit systems applicable to every budgetary implementation operation (Article 86(1) of the Financial Regulation[3]).

[2] Opinion of 23 June 2006 on a notification for prior checking on OLAF internal investigations (Case 2005-418).

[3] Council Regulation (EC, Euratom) No 1605/2002 of 25 June 2002 on the Financial Regulation applicable to the general budget of the European Communities. Official Journal L 248, 16/09/2002 P. 0001-0048.

Since the main purpose of the internal audit is to *evaluate internal management and control systems, not particular individuals (neither managers nor staff members),* the case does not fall under the scope of Article 27(2)(b) of the Regulation.

It should be noted that the findings during an internal audit or the final result of an audit may lead to further consequences on the individuals affected by an audit process. As stated above, investigations may follow, and it is also possible that an internal administrative inquiry and further disciplinary proceedings by the Investigatory and Disciplinary Office (IDOC) take place, which clearly evaluate individual conduct/behaviour. The specific risk is present in the evaluation procedures concerning particular individuals, and not in the internal audit process. The IDOC internal administrative inquiries and disciplinary procedures (2004-187)[4] were already prior checked by the EDPS.

In addition, section 6 of the prior checking notification mentions that: "*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 subject's external activities may be collected".* Should the collection of data on the external activities of a data subject have an element of evaluating personal conduct, it should be noted that this does not justify a prior checking because it is not the major aim of the audit itself and appears to be a mere eventuality which does not happen frequently.

**Due to the above considerations, we have decided to close the case.** However, if you believe that there are other factors justifying prior checking of the internal audit process and the time recording system, we are of course prepared to review our position.

**Without prejudice to the above considerations, based upon the notification and the information received on our requests, we scrutinized certain aspects of the processing operations and want to underline the following points:**

A) <u>The internal audit is a more general procedure, and not a particular inquiry.</u>

The controller attached a draft information note on the "Processing of personal data in the course of IAS audits" to the notification form. This draft note aims to give information to the auditee (Director-General) on data protection within an audit, which can thus be distributed to all his staff at the beginning of an audit. The draft note specifically mentions that:

> "*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.*
>
> *In the course of the current audit the auditor may collect personal data concerning the staff of the auditee or contractors with which the auditee has a relationship. This would mainly concern minutes of meetings, transactions in information systems and operational instructions given by or on behalf of the auditee. This information is covered by Council Regulation (EC) 45/2001. The exception specified in article 2(g) of this Regulation confirms the full and unlimited access specified in paragraph 1 above."*

[4] Opinion of 20 April 2005 on the notification for prior checking relating to internal administrative inquiries and disciplinary procedures within the European Commission (Case 2004-187).

Article 2(g) of the Regulation stipulates that "authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients".

As stated above, the internal audit process is of general nature. It can not be regarded as a particular inquiry, because it does not aim to investigate/inquire particular individuals, nor particular conducts, rather it examines systems and potential risks related to them on a more general level. Therefore, Article 2(g) not being applicable to pure auditing activities, not only Article 7 (transfer of data) applies but also Articles 11 and 12 (right of information), which are the only provisions affected by the exception embodied in Article 2(g).

Nevertheless, as concerns Article 7, the EDPS is of the view that, given the nature of the powers entrusted to auditing institutions and bodies, its second point has to be understood in that context and it is up to the requesting auditing authority to assess the necessity of receiving the data requested.

B) On the application of the restrictions in Article 20 of the Regulation

The same draft note states that:

> *"To allow the audit process to be carried out smoothly, this unlimited access to data benefits from the exemption in Article 20.1(e) of Regulation (EC) 45/2001 which restricts the application of Article 4(1) on "DATA QUALITY", Articles 11 and 12(1) on "INFORMATION TO BE GIVEN TO THE DATA SUBJECT", Articles 13 to 17 on "RIGHTS OF THE DATA SUBJECT", but imposes on the Internal Auditor the requirement to inform the data subject under article 20.3 of the data protection Regulation."* Section 8 of the prior checking notification mentions particularly that: "*The internal audit process is covered by Article 20.1(e) 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 interest 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".*

Article 20(1)(e) allows restriction of those rights "where such restriction constitutes a necessary measure to safeguard...(e) a monitoring... or regulatory task connected, even occasionally, with the exercise of official authority in the cases referred to in (a) and (b)". These last two paragraphs concern permitted restriction for the prevention, investigation, detection and prosecution of criminal offences (paragraph (a)); or for an important economic or financial interest... of the European Communities, including monetary, budgetary and taxation matters (paragraph (b)).

Article 20(3) reads as follows: *"If a restriction provided for in paragraph 1 is imposed, the data subject shall be informed, in accordance with Community law, of the principal reasons on which the application of the restriction is based and of his or her right to have recourse to the European Data Protection Supervisor".*

The information in the prior checking notification and in the draft note above seems to be contradictory on whether the restrictions are applied by the controller in a general fashion or only in "sensitive cases". It should be stressed that the restriction in Article 20 (1)(e) applies only in cases where the restriction constitutes a "necessary measure" to safeguard any of the enumerated interests in that article. The "test of necessity" requires that restrictions are applied on a case-by-case basis and are justified. This is to say that a restriction can not be applied to every case and on each and every provision permitted in Article 20 (1) of the Regulation; rather the need for restriction should be demonstrated in every case and for each

specific article (Articles 4(1), 11, 12(1) and 13 to 17 and 37(1)) of the Regulation which is intended to be restricted.

Furthermore, as access rights can be exercised directly by the data subject ("direct access") or under certain circumstances by a public authority ("indirect access"), normally exercised by a Data Protection Authority, being the EDPS in the present context, account should be taken of Article 20(4) of the Regulation:*" If a restriction provided for by paragraph 1 is relied upon to deny access to the data subject, the European Data Protection Supervisor shall, when investigating the complaint, only inform him or her of whether the data have been processed correctly and, if not, whether the necessary corrections have been made".* The indirect access will then have to be guaranteed. This provision will play a role, for instance, in those cases where the data subject has been informed about the existence of the processing, or has knowledge of it, but the right of access is still being restricted in the light of Article 20.[5]

C) In case traffic data are stored for the purposes of audit, the processing should comply with the guidelines laid down in the e-monitoring paper of the EDPS (to be issued shortly).

D) In case the "Absence" section of the time recording system processes particular health related data on maternity or absence due to sickness, the EDPS would find that excessive for the purpose of the system under the data quality requirement of Article 4(1)(c) of the Regulation. An indication that the person was on "leave" (it is not relevant that the reason is health) should be sufficient to achieve the purpose to see the time spent on audit and non-audit activities.

I would be thankful if you could forward these considerations to the controller and keep us informed of the necessary implementation.

Thank you for your cooperation,

Yours sincerely,

Joaquín BAYO DELGADO
Assistant European Data Protection Supervisor

[5] For the concept of indirect access see also part 2.2.8. "Right of access and rectification" of Opinion of 23 June 2006 on a notification for prior checking on OLAF internal investigations (Case 2005-418).