Opinion on a notification for Prior Checking received from the Data Protection Officer of the Court of Auditors regarding "ART: Audit Reconciliation Tool".

Brussels, 9 February 2009 (Case 2008-239)

1. Proceedings

On 25 September 2007, the Data Protection Officer ("*DPO*") of the Court of Auditors ("*The CoA*") consulted by e-mail the European Data Protection Supervisor ("*EDPS*") on the need for prior-checking of the Audit Reconciliation Tool ("*ART*"). This tool is linking two databases of the CoA together: EFFICIENT and ASSYST.

A meeting was held on 6 November 2007 between the DPO of the CoA and members of the staff of the EDPS to discuss this consultation. On 6 December 2007, the EDPS replied by e-mail concluding on the need for prior-check of the ART processing operations.

Moreover, the EDPS decided that the ASSYST database did not have to be prior-checked (on the basis that although it contains personal data relating to time spent by data subjects on specific tasks, it does not include evaluation of the data subjects themselves), but that the EFFICIENT system needed to be prior-checked (because of the specific risks created by the inclusion of RFID technology into the badging system of the Court).

On 15 April 2008, the DPO of the CoA sent by email the notification for prior checking of the processing operations relating to "ART/Assyst Reconciliation Tool" ("*ART*"). On 17 April 2008, the EDPS requested additional information from the CoA. The CoA replied on 21 May 2008. On 23 May 2008, the EDPS requested further information to which the CoA responded on 30 May 2008. On 9 June 2008, the EDPS requested further documentation regarding the legal basis of the processing. The information was provided on 10 June 2008. The procedure was again suspended from 11 July 2008 until 17 July 2008, when answers were provided by the data controller.

Finally, on 24 July 2008, the EDPS decided to suspend the ART procedure until he adopted his opinion on the EFFICIENT processing operations. This opinion was adopted on 5 December 2008[1].

Finally, the EDPS sent to the CoA his draft Opinion for comments on 11 December 2008. The procedure was suspended until 4 February 2009, when the CoA provided its comments.

[1] See Case file 2008-173 on "Avis sur la notification d'un contrôle préalable reçue du délégué à la protection des données de la Cour des Comptes à propos du traitement des données "Système de gestion et de contrôle du Flexitime ", available on the EDPS website.

2. The facts

2.1 Scope of the Notification

The purpose of the processing operation is to facilitate individual auditors and their Heads of Unit to reconcile their time recorded in ASSYST (the Audit Management System) with EFFICIENT (the Flexitime system) through the so called ART tool. More specifically, according to the notification, the purpose of ART is to verify (by the superior as well as the staff member concerned) that the information entered in ASSYST and the one contained in EFFICIENT (Flexitime) do match and, in case there would be a discrepancy, to allow the verification of the reason(s).

2.2 Description of the processing:

- The Court has a Flexitime system (time recording tool) called EFFICIENT in which the staff clock-in when arriving and clock-out when leaving. The system is used by the staff by badging when entering the Court or when leaving it. The system also contains information about leave, missions, sick leave. The total of hours per day is recorded in this system. An individual person has read-access only to his or her personal record. The Heads of Unit have read access to the data for his or her staff.

- The Court also has an Audit Management system called ASSYST in which the auditors document their audits which includes recording time spent in audit tasks. This system allows ensuring a constant and complete follow up of the work performed on a specific audit topic (or specific audits topics). The system also includes a "timesheet" allowing the hierarchy (and the auditor) to have an overview of the time spent on the audit topic. The information contained in the timesheets is introduced by the auditors concerned. Each auditor has read access only to his or her time reports in ASSYST. The Heads of Unit and those who have so called management access have read access to the time reports in that unit concerned. The total time recorded in ASSYST per person and per day should more or less reflect the hours per day in the Flexitime system.

- According to the notification, the ART tool will facilitate the reconciliation of the data between the two systems (the time recording tool and the management tool). Data from ASSYST are used by staff to compile a six-month Annual Work Programme Implementation Report. A reconciliation of the records of ASSYST and EFFICIENT by staff allows them ensuring that their ASSYST records (and hence the Implementation Report) are complete and accurate for the current month and the previous month. Since EFFICIENT only shows the current and previous month, ART can only display the current and the previous month. As it is presented by the controller and in the documentation provided, ART is not a database but an application which pulls the data from the two source databases and displays the data in table format. It is just a reconciliation of the time recorded in ASSYST and EFFICIENT. The ART tool will not give read access to more data than the person has in the two source systems. As presented in the notification, ART is mainly a supervising tool.

The data and categories of data collected are: Family name, First name, Division/Unit, time recorded in ASSYST and number of hours from the Flexitime system.

The data subjects are officials and temporary agents who have access to ASSYST (for instance individual auditors and their Heads of Unit). Therefore, it does not concern all staff of the Court.

Automated/manual processing: The ART tool will retrieve total hours recorded per day per person in ASSYST and compare these with the total hours per person from EFFICIENT. The result is presented in a table format. No further details are available. It is an automated operation triggered by the users. At present, this reconciliation is being done manually by individual auditor staff.

Recipients of the data: Only the individual auditors and their Heads of Units who will in any case have the same access to the tool.

Information to data subjects: The notification foresees that everybody will have access to the tool will be given a guideline on how to use it and the possibility to attend a presentation on it.

Rights of the data subjects: An auditor logging on to the ART tool will have the same read access as the one of the two underlying system sources, for instance only data for her- or himself. A Head of Unit or someone who the Head of Unit has delegated will have read access to the data of the Unit.

A staff member may change or request that the records in ASSYST or EFFICIENT be changed.

Regarding time limit for blocking and erasure of the different categories of data on justified legitimate request from the data subject, EFFICIENT displays the data for the current and previous month. The data in ASSYST is available for three years.

Storage: The table can be printed by the auditor or the Head of Unit (or his/her delegate). No other storage is foreseen. It will be up to each user to save her or his tables as needed. The system does not store any data at all. According to the notification, the ART tool cannot store any data.

Security: This tool will have the same security set up as the two underlying system sources.

Giving access to the tool and handing out passwords will be managed centrally by the IT & T department through signed Network forms to ensure the security of the subsequent processing. The tool will not give access to more information than the individual source systems already provide.

3. Legal aspects

3.1. Prior checking

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 of*

which fall within the scope of Community law"[2]. 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.

Second, the personal data collected undergo[3] *"automatic processing"* operations, as defined under Article 2(b) of the Regulation (EC) No 45/2001. Indeed, the personal data such as personal identification data (Family name, First name), time recorded in ASSYST and number of hours from the Flexitime are collected and undergo "automatic processing".

Finally, the processing is carried out by a Community body, in this case by the Court of Auditors, in the framework of Community law (Article 3(1) of the Regulation (EC) No 45/2001). Therefore, all the elements that trigger the application of the Regulation are present in this data processing.

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".* Article 27(2) contains a list of processing operations that are likely to present such risks, for example "*processing operations allowing linkages not provided for pursuant to national or Community legislation between data processed for different purposes*" (Article 27(2)(c). Indeed ART allows interconnections not provided for under national legislation or community between data processed for different purposes.

Since prior checking aims at addressing situations that are likely to present certain risks, the opinion of the EDPS should be given prior to the start of the processing operation. The current opinion constitutes a **true prior check**. Therefore, such processing should not be implemented until the recommendations of this opinion are taken into account and the EDPS is informed of the measures of implementation.

The notification was received on 15 April 2008. Pursuant to Article 27(4) of Regulation (EC) No 45/2001, the two-month period within which the EDPS must deliver an opinion was suspended for a total of 48 days to obtain additional information plus 134 days to adopt the opinion on the EFFICIENT processing operations. It was also suspended 55 days to allow comments on the draft Opinion. The Opinion must therefore be adopted no later than 9 February 2009.

3.2. Lawfulness of the processing

Personal data may only be processed if grounds can be found in Article 5 of Regulation (EC) No 45/2001.

Of the various grounds listed under Article 5 of Regulation (EC) No 45/2001, the processing operation notified for prior checking falls under Article 5 a), pursuant to which data may be processed if the processing is "*necessary for 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 or in the legitimate exercise of official authority vested in the Community institution or body or in a third party to whom the data are disclosed"*

---

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

3 Before the deployment of the interface, the reconciliation is done manually by individual auditor staff.

In order to determine whether the processing operations comply with Article 5 a) of Regulation (EC) No 45/2001, the first issue under Article 5(a) is to determine whether there is a specific legal basis for the processing: a Treaty provision or another legal instrument adopted on the basis of the Treaties. The second issue is to determine whether the processing operation is necessary for the performance of a task carried out in the public interest. To address this second issue in the present case, Recital 27 of the Regulation needs to be taken into account, which specifies that "*processing of personal data for performance of tasks carried out in the public interest includes the processing necessary for the management and functioning of those institutions and bodies*". Thus, the second issue in the present case is whether the processing is necessary and proportionate for the management and functioning of the CoA.

Legal basis: The legal basis of the processing is to be found in the European Court of Auditors Information Technologies strategy document (DEC 56/077 adopted by the Court on April 26th, 2007). Especially in article 30 a) and b), a reference is made to ASSYST where it is said that "*an upgrade of ASSYST is proposed*" and that ASSYST has to be enhanced. It is in this context that the implementation of ART was decided.

As to the **necessity** of the processing (necessity test), according to Article 5 a) of Regulation (EC) No 45/2001, the data processing must be "*necessary for performance of a task*" as referred to above.

ART is a tool which allows the necessary supervising task of the superior. At the same time, ART allows the staff member to verify/ensure that the information contained in EFFICIENT do match with the one in ASSYST.

Although the necessity of supervision exists, the EDPS considers, as he already explained in previous cases[4] that this aggregation of databases also increases the risk of "function creep" when the interlinking of two databases designed for two distinct purposes will provide a third one for which they have not been built, a result which is in a clear contradiction of the purpose limitation principle". Therefore, such purpose must be clearly limited and the necessity be demonstrated. In this specific case, the necessity is not clearly established and should be further developed.

Concerning the legal basis, the EDPS considers that a more specific one should be elaborated. The new text should define the purpose and explain the necessity of the processing.

As regards the necessity of the processing, the EDPS considers that there are many ways to achieve the purpose of the planned processing but that, in order to ensure consistency of the data present in the two databases, it makes sense to link the two databases via the ART tool. In this case, the quality of data of the interlinked systems is ensured.

The EDPS considers that the notified processing operation is lawful, as long as the Court of Auditors complies with the recommendations made in this Opinion, especially regarding the legal basis, the purpose and the necessity of the processing.

[4] See EDPS comments on the Communication of the Commission on interoperability of European databases, 10 March 2006 available on the website.

3.3. 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*".

Based on the information provided to him (Family name, First name, Division/Unit, time recorded in ASSYST and number of hours from the Flexitime system), the EDPS does not challenge the adequacy, relevance and proportionality of the data processed in the framework of the ART tool.

Fairness and lawfulness. Article 4(1)(a) of Regulation (EC) No 45/2001 requires that data must be processed fairly and lawfully. The issue of lawfulness was analysed above (see Section 3.2). The issue of fairness is closely related to what information is provided to data subjects (see Section 3.10 below).

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*."

Based on the information provided to him, the EDPS does not challenge the accuracy of the data collected through ART. Moreover, the prior-checking of the EFFICIENT database demonstrated the compliance of the processing operations with Article 4.1.d .

Nevertheless, where rectification takes place in one of the databases linked through ART (see 3.8), the quality of data in ART could be at stake if, for instance, the Head of unit has checked the table before a rectification took place, has printed the table and has not checked it afterwards. Therefore, by using the facility of printing the table, the Head of unit could have wrong data if these data were rectified afterwards. Therefore, together with the argument regarding the conservation period (see below 3.4) it is one of the reasons why the EDPS considers that the printing facility should be removed.

3.4. Conservation of data

Article 4(1)(e) of Regulation (EC) No 45/2001 sets forth the principle that "*personal data must be kept in a form which permits identification of data subjects for no longer that is necessary for the purposes for which the data were collected or for which they were further processed". "The Community institution or body shall lay down that personal data which are to be stored for longer periods for ... statistical use should be kept either in anonymous form only or, if that is not possible, only with the identity of the data subject encrypted."*

According to the notification, the ART tool cannot store any data. However, the information is available as a table which can be printed by the auditor or by the Head of Unit (or his/her delegate). No other storage is foreseen. As data from EFFICIENT can store the data for the current and previous month and that the ASSYST allows conservation of data for three years, the ART tool does not allow recovering older data than those of the previous month. However, given that the table created through ART can be printed, this leads to a possible unrestricted storage of data, which the EDPS can not accept. The EDPS considers that the CoA must implement a function by which the Heads of Unit will only have reading access and no printing possibility of the tables.

Moreover, as already underlined above, the removal of the printing facility is also an issue pertaining to the quality of data (3.3) and not only to the conservation of data.

3.5. Compatible use / Change of purpose

As explained in the facts, the goal of the processing operation is to facilitate individual auditors and their Heads of Unit to reconcile their time recorded in ASSYST with EFFICIENT through the ART tool. The purpose of ART is to verify (by the superior as well as the staff member concerned) that the information entered in ASSYST and the one contained in EFFICIENT (Flexitime) do match and, in case there would be a discrepancy, to allow the verification of the reason(s).

When the data from the two databases are connected via ART, it is in the framework of a new purpose, different from the original purposes of both processing operations, but which may be considered as compatible and acceptable with these purposes. Article 4(1) (b) of Regulation 45/2001 provides that personal data must be *"collected for specified, explicit and lawful purposes and not further processed in a way incompatible with those purposes"*. After analysing the elements, the processing operation analysed does not entail any general change in the intended purpose of the databases from where some data are collected, nor are they incompatible with that purpose. The management within an institution is an activity falling within the general remit of a human resources department. Moreover, the EDPS underlines that Article 6 § 1 provides that, without prejudice to Articles 4, 5 and 10 "*Personal data shall only be processed for purposes other than those for which they have been collected if the change of purpose is expressly permitted by the internal rules of the Community institution or body*".

As a consequence, the EDPS underlines the importance of adopting a specific legal basis for the processing operation of ART, which should contain the specific purpose of the processing.

3.6. Transfer of data

The system does not foresee any transfer of data outside the institution. Within the institution, A Head of Unit or someone who the Head of Units has delegated will have read access to the data of the Unit. Access by the Heads of Units is consistent with Article 7 (1) of the Regulation. According the Article 7(3) they should be reminded that the data cannot be used for any other purpose than assuring consistency between the two linked databases.

3.7. Processing of personal number or unique identifier

Article 10(6) of the Regulation states that "*the European Data Protection Supervisor shall determine the conditions under which a personal number or other identifier of general application may be processed by a Community institution or body*".

In order to link the EFFICIENT database with the ASSYST database through the interface, it is necessary to use the data subject's staff number. Use of the staff number is justified in this case for reasons of practicality. Rather than having to enter a series of data to interconnect the systems, it can be done more readily using the staff number as an identifier. The staff number serves only to link the databases for purposes clearly set out in the project and directed towards a common end, as indicated above.

The need to use a single identifier to make connections between files thus appears to be justified and presents no specific risks given the measures to restrict access.

3.8. Right of access and rectification

According to Article 13 of the Regulation, the data subject shall have the right to obtain without constraint from the controller, communication in an intelligible form of the data undergoing the processing and any available information as to their source.

Article 14 of the Regulation provides the data subject with a right to rectify inaccurate or incomplete data.

As described in point 2.2 of the present Opinion, an auditor logging on to the ART tool will have the same read access, for instance only data for her- or himself. There is thus only a reading access to the information provided by the interface. The tool will not give access to more information than the individual source systems already provide.

Therefore, to respect articles 13 and 14, it is necessary that these rights be granted in the two systems EFFICIENT and ASSYST being linked through the interface. As ART is a tool to access data from the two other systems, access right is guaranteed. For the right of rectification, EFFICIENT has been prior-checked by the EDPS and considered as compliant regarding the right of rectification. Therefore, the CoA should guarantee the same right of rectification in the case of the ASSYST system.

Finally, it must also be guaranteed that the changes taking place in any of the two databases will be reflected in the table created by the interface.

3.9. Information to the data subject

Under Articles 11 and 12 of the Regulation, certain information must be provided to the data subject. In the case in question, many data are not obtained directly from the data subject since the system is fed from various sources. That said, some data may be provided by the data subject. Therefore, both Article 11 and Article 12 apply.

The notification states that everybody who will have access to the tool will be given a guideline on how to use it and the possibility to attend a presentation of it. The EDPS considers that to implement the right of information of the data subjects, there is a need to inform each users of the ART not only on the way to use the system but also on the specific provisions of articles 11 and 12. Therefore, the EDPS advises to develop a privacy statement containing the elements of Articles 11 and 12 and that this privacy statement be provided to the concerned data subjects, also regarding a reference to a clear legal basis.

Moreover, it is also necessary to include a mention in the privacy statements relating to the EFFICIENT and ASSYST systems in the sense that their data can be further used in the framework of ART processing operation and that these privacy statements be distributed to the data subjects concerned.

3.10. Security measures

The ART tool will have the same security set up as the two underlying system sources.

Conclusion:

The EDPS considers that the proposed processing does not infringe Regulation (EC) No 45/2001 because the Court of Auditors has already implemented the draft recommendations made by the EDPS during the period which was provided to it to comment on the draft opinion. These recommendations that had to be taken into account were the following:

- The CoA must adopt a specific legal basis to the planned processing operation, where the purpose and the necessity of the data processing should be clearly defined;
- As regard the conservation of the data and the quality of data, the CoA must implement a function by which the Heads of Unit will only have reading access and no printing possibility of the tables created through ART;
- Head of Units should be reminded that data of ART cannot be used for any other purpose than assuring consistency between the two linked databases;
- The CoA should ensure that the right of access and rectification should be implemented in the two databases which are linked by ART;
- A privacy statement containing the elements of Articles 11 and 12 should be developed;
- The CoA should include a mention in the respective privacy statements relating to the EFFICIENT and ASSYST systems in the sense that their data can be further used in the framework of ART processing operation.

Done at Brussels, 9 February 2009

(signed)

Giovanni BUTTARELLI
Assistant European Data Protection Supervisor