EUROPEAN DATA
PROTECTION SUPERVISOR

Opinion on the notification for prior checking from the Data Protection Officer of the Court of Auditors regarding data processing in the Flexitime management and checking system

Brussels, 5 December 2008 (Case 2008-173)

1. Procedure

On 14 March 2008 the European Data Protection Supervisor (EDPS) received notification from the Data Protection Officer (DPO) of the Court of Auditors for prior checking regarding data processing in the Flexitime management and checking system. A number of questions were put to the controller in an e-mail dated 19 March 2008. Replies were given on 26 March 2008. Additional questions were put on 16 April 2008, and replies were given on 9 October 2008.

The draft opinion was sent to the DPO for comments on 6 November 2008. Comments were received on 1 December 2008.

2. Facts

Flexitime was introduced in order to manage staff working hours more effectively and provide greater flexibility. Over a calendar month each official and other servant is required to work a total number of hours corresponding to 37½ hours a week.

The personnel department is responsible for centralised management of the system under the control of the head of the personnel division.

The purpose of the processing operation is as follows:

- FLEXITIME processing = Monitoring and checking staff attendance
- Automatic recording of Court of Auditors staff entry and exit (clocking in and out)
- Automatic recording of authorised absences: leave, absence, mission (batch interface)
- Recording of absences for training by the training department
- Recording of manual corrections and amendments made by flexitime managers
- Consultation of timetables entered, operations and corrections requested by staff
- Consultation by hierarchical superiors of their staff's timetables
- Monthly retrieval of paid overtime for validation and payment authorisation by the hierarchical superior
- Retrieval of overall statistics for the management and evaluation of the system
- Retrieval/print-out of individual clocking records at the request of the Human Resources Director or the directors of the departments concerned.

Arrangements for applying the system

- **Entry and exit**

Staff must clock in or out every time they enter or leave a building, using one of the card readers in the entrance lobby of each building and car park. Clocking is done without contact (the card must be held a few centimetres from the reader), which means that the card contains RFID (radio frequency identification) technology.

- **Information available**

All staff members can see their time credit or debit simply by showing their staff identification at a reader. The balance is always calculated on the basis of an average 7½ hour working day. Staff members can also access their data for the previous two months on a PC. At the beginning of the month a detailed record of all clocking operations over the previous month is sent to each staff member for checking. The head of department must certify records relating to missions or to work exceptionally carried out at home and requiring no mission order.

- **Recording leave and missions**

The personnel department and the staff training department are responsible for entering all information under their remit relating to:
- annual leave and special leave
- sick leave
- missions
- training activities

after the requisite forms have been received (leave applications, mission orders, mission expense forms, declarations of sick leave, training authorisations). Staff does not therefore have to intervene on any of those matters.

Only the code for the type of "non-attendance" for the staff member's day or half-day is recorded in EFFICIENT (the database that manages flexitime): mission, leave, sick leave.

- **Request to have records amended**

The personnel department can be asked at any time to amend data recorded. The request must be made on the relevant form or via a functional mailbox and must indicate:
- the staff number;
- surname and forename;
- telephone number;
- precise details of the reasons for the amendment requested (e.g. loss of card/badge);
- the day concerned;
- the amended timetable.

- **Time debit**

Pursuant to Article 60 of the Staff Regulations, a debit at the end of the month which exceeds 15 hours is deducted from annual leave, each instalment of 3¾ hours being taken as half a day. Any balance below 3¾ hours is automatically kept in the memory.

- **Lunch break**

All staff members are required to clock in and out between 12.00 and 14.30; otherwise the provisions of the last paragraph of point 2.4 of the regulation governing the system will be applied. Staff working in a building other than the main Kirchberg building is allowed 20 minutes "travel time".

- **Absence for medical appointments**

To apply point 2.5 of the regulation governing the system, the system automatically allows 12 minutes per day for absences for medical appointments not requiring special leave.

- **Work activities within the Grand Duchy of Luxembourg**

Staff required to leave the building for work activity in Luxembourg (meetings, liaison between the Court's buildings, etc.) record their entry and exit under "Missions to Luxembourg" (key F1 on the reader). Staff attending authorised training courses in a building other than building they work in are allowed 10 minutes "travel time". Staff members leaving on mission directly from home without having been able to clock out or use the F1 key must inform the personnel department of the duration of the mission using the relevant form, so that it can be recorded.

- **Working hours at home**

Work at home (non-permanent) may be recorded, on a purely exceptional basis, provided that it has received prior authorisation and ex post certification from the hierarchical superior. Recording is done by the personnel department using the relevant form.

- **Hours worked at weekends and on public holidays**

Without prejudice to the specific provisions on missions set out in points 2.7 and 2.8 of the regulation governing the system, hours worked at weekends and on public holidays can be recorded *on a purely exceptional basis up to the maximum number of hours per day stipulated in point 2.10 of the basic regulation*, provided that they have received prior authorisation and ex post certification from the hierarchical superior. Recording is done by the personnel department using the relevant form.

<u>Links between databases:</u> the flexitime system is managed by the EFFICIENT database. It imports data relating to individuals, missions and absences (official leave, sick leave, etc.) from the SIC CONGES database but also from the Mission application developed by the Court of Auditors since training absences are recorded by the training department (although processing in that instance is manual). Regarding the import of data by staff members, one item has since been added: a flag to the effect that the person is one of the Drivers or a member of the Helpdesk staff. There is also provision for exporting data to ART (management software for auditors), the purpose being to reconcile ART data and EFFICIENT data[1].

The interfaces between databases use only the staff number. When a person is first entered in the system, the staff number is linked to the staff card number. There is no immediate validation but if a staff number is incorrect the interface will indicate that during the following night and the number will be corrected manually.

<u>The data subjects</u> are all staff members either under the Staff Regulations or on contract to the Court of Auditors or a company working for the Court of Auditors. All those working for the Court of Auditors, on whatever basis, are subject to checking of attendance at work: officials, contractual staff, service providers and seconded national experts.

<u>The data provided are as follows:</u>

* Person:
- Staff number
- Surname

[1] Case 2008-239 currently subject to prior checking.

- Forename
- Site (building)
- Code of the department to which the person is assigned
- Grade
- EFFICIENT checking start date / end date
- Type of timetable
- Electronic staff card number
- Login and password for the consultation interface.

The Court's justification for location data is that its regulation provides for different rates of time compensation depending on which building the person is assigned to (to take account of travel time between the main building and other buildings). Location is one of the parameters for calculating the daily timetable. The following information is added: the place of clocking in/out (identifying the reader) is not currently available via the application (neither to the user, to his/her superior or to the administrator; only a technician may be able to retrieve the information by directly accessing the database tables). The information is nevertheless present in the database but is never visible and is never used.

* Hierarchical superior (Director, head of division/unit)
- Code(s) of the department(s) administered
- Administrator's login / password

* Clocking in/out
- Staff card number + date and time of clocking in/out.

Information to data subjects is provided via the regulation governing the system which is available on the Court's intranet and in the timetable consultation application. Data subjects are informed of the regulation and the system when they take up employment at the same time as their electronic staff card is handed to them in person.

With regard to rights of access and rectification, the application allows all staff members to consult records relating to them for the current month and for the previous month. If they submit a duly substantiated request, data subjects may receive a "clocking in/out table" showing earlier months. Staff may ask managers to correct or amend clocking records for the current month and the previous month via a functional mailbox. (In duly justified exceptional cases, amendments/corrections may be made to older data).

Processing is both automated and manual:

Automated processing:

- Daily synchronisation of basic staff data (surname, staff number, code of the department to which the person is assigned, building, function group, grade) with the personnel database
- Daily synchronisation of "authorised" absences with the SIC-Congés and Mission systems

Manual processing:

- Addition of new staff (assignment of staff card, login and password)
- Recording of training by the training department
- Recording of manual corrections and amendments sent by staff (via the functional mailbox)
- Monthly retrieval of the overtime report for the team in charge of any payments to be made (subject to validation/acceptance)

- Retrieval/print-out of individual clocking records at the request of the Director of Human Resources.

As to the storage medium, flexitime data are managed and stored in a system and an independent database known as "EFFICIENT". That SQL Server database is on a server dedicated to the EFFICIENT application.

Whatever the technology used, there is a card number. That number is not used for any purpose other than flexitime. The staff card number is used only in EFFICIENT. A Windows programme runs on the server permanently, transferring data between the card readers and the database. Whenever the connection between the server and a card reader fails, the card reader stores the data.

Recipients are: the Human Resources Division and all the Directors and Heads of Unit for the staff assigned to each department, the appointing authority, the payment officer responsible for overtime payments, internal and external auditors in the case of an audit and, where applicable, the legal service. Only the DB Administrator and his/her backup have full access to the database. All other access is via the application's web interface.

There are several user groups: Administrators (consultation and amendment of application parameters and staff timetables), Training Department (consultation and addition of training courses), Manager (consultation of data relating to staff in his department), User (consultation of own clocking in/out data for the current month and the previous month).

Data may be stored until all rights are extinguished and appeals are no longer possible (five years). When a staff member ceases work and financial rights have been determined and no appeal is being made, data are erased within 18 months of cessation of work. The EFFICIENT software stores all data, including clocking in/out data, in a centralised database constructed on an incremental basis: today's data are based on the data for last month, which in turn are based on those for the previous month, and so on. There is no provision in the software for erasing certain items of individual data (e.g. individual clocking in/out): data erased must be the whole set of data covering a period in the past. (If an individual's clocking in/out data for a date or dates in the past are erased, the system will consider that the person did not clock in or out on those dates and will recalculate all the data up to the current date). For that reason, the arrangement is that when the appointing authority concludes that all of the data for a particular year are no longer needed, or in any event after five years at most, all the data for that year will be erased from the database, including the "not present" codes for days or half days and the clocking in/out data for all staff members. Card reader data are stored only temporarily until they are loaded into the database. Management regularly requires that details of clocking in/out be accessible far into the past: the most obvious case is when a person returns from lengthy leave or a long absence (leave on personal grounds often extends over several years) and is either reintegrated (the situation as it was before the person left needs to be recovered) or leaves the institution (it may, in certain instances, be necessary to pay him/her for hours worked, or with the appropriate substantiation ask him/her to refund hours, and to respond to any appeals).

Erasure of personal data is a procedure which takes place between three and six months after departure, it being necessary to allow time for financial effects to be settled. In certain exceptional cases, the procedure may take longer. By application subject to appeal, a person no longer working at the Court of Auditors may request that data relating to him/her be erased. Erasure is carried out within 18 months. In the case of staff still at work, data contested may be **blocked** immediately at the request of the data subject.

At the request of the appointing authority, overall statistical reports may be produced in order to monitor developments in the use of flexitime: they do not contain individual data. At this stage, in the absence of computer capability, no reporting environment has been put in place for EFFICIENT: analysis of management needs for such statistical reports should begin in 2009. They would in any event only be anonymous overall statistical reports (average arrival/departure time, length of "standard" break, number of hours per day, etc.) designed to evaluate the flexitime system as a whole, e.g. when the rules are being reviewed. Provision was made for that when EFFICIENT was launched but it does not appear to be a priority or an urgent requirement; however, the appointing authority wishes to retain the possibility of resorting to it in the future if it finds it necessary.

Security measures are guaranteed and dealt with by the IT department. Export is generated via a script operating directly on the EFFICIENT server (access limited to the system administrator and his/her backup). Access to the Oracle database is also protected by login/password (access limited to the ART Administrator and his/her backup). The administrator and his/her backup who manage the EFFICIENT database belong to the IT and Telecommunications Directorate, **Development** Department.

- Security measures for the whole of the system are [...].

3. Legal aspects

3.1. Prior checking

Management of data relating to absences, the different types of leave and attendance timetables constitutes processing of personal data ("any information relating to an identified or identifiable natural person (…)": Article 2(a) of Regulation (EC) No 45/2001). The data processing in question is carried out by an institution in the exercise of activities which fall within the scope of Community law.

Data managed by EFFICIENT, a Court of Auditors application, are processed both automatically and manually. Processing is thus partly by automatic means (Article 3(2) of the Regulation).

It therefore comes within the scope of Regulation (EC) No 45/2001.

Article 27(1) of Regulation (EC) No 45/2001 requires prior checking by the EDPS processing for operations likely to present specific risks to the rights and freedoms of data subjects. The EDPS considers that the insertion of technologies such as radio frequency identification (RFID) presents a specific risk. That is why files dealt with by the EFFICIENT interface are to be regarded as personal data processing coming under Article 27(1) of the Regulation.

In principle, checks by the EDPS should be performed before the processing operation is implemented. Failing that, checking necessarily becomes ex post. This does not make it any the less desirable that the recommendations issued by the EDPS be implemented.

The formal notification was received by e-mail on 14 March 2008. The DPO was given 25 days in which to comment on the draft EDPS opinion. In accordance with Article 27(4) of the Regulation, the EDPS will therefore deliver his opinion by 8 December 2008 at the latest (15 May + 145 days' suspension + month of August + 25 days for comments).

3.2. Lawfulness of the processing

The lawfulness of the processing must be considered in the light of Article 5(a) of Regulation (EC) No 45/2001 which reads: "*processing is necessary for the 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*".

In this case, the persons in charge of managing the EFFICIENT database are performing a task in the public interest on the basis of the Staff Regulations of the European Communities and the Conditions of Employment of Other Servants of the European Communities.

The legal basis for the data processing under consideration is to be found in the following articles:

Legal basis for part-time work:

- Article 55a and Annex IV to the Staff Regulations, Article 55b of the Staff Regulations on part-time work

Legal basis for flexitime:

- Article 55 of the Staff Regulations
- Regulation amending the basic regulation introducing a flexitime system - COM PER 34/2005 of 17 June 2006

Legal basis for flexitime:

Article 56 of the Staff Regulations.

All these legal bases are thus appropriate and back up the lawfulness of the processing.

3.3. Data Quality

"Personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed" (Article 4(1)(c) of the Regulation).

The data processed in this case as described above appear to be generally relevant and adequate.

The data regarding location require particular analysis. The justification provided by the Court of Auditors is that the regulation provides for different rates of compensation depending on which building the person is assigned to (to take account of travel time between the main building and other buildings). Location is one of the parameters for calculating the daily timetable. The data are present in the system but are accessible only to a technician. The way in which they are processed, i.e. with no access for the hierarchical superior, complies with the principle of data quality set out in Regulation No 45/2001. Moreover, retaining such data in the system while preventing access by the hierarchical superior allows rectification where there is a problem or dispute.

The overall statistical reports which may be produced at the request of the appointing authority in order to monitor developments in the use of flexitime do not contain individual data. It should be remembered that EFFICIENT does not yet have a reporting function: analysis of management needs for such statistical reports should begin in 2009. They would in any event only be anonymous overall statistical reports (average arrival/departure time, length of "standard" break, number of hours per day, etc.) designed to evaluate the flexitime system as a whole, e.g. when the rules are being reviewed.

The EDPS welcomes the fact that that development is being envisaged with provision for making data anonymous and considers that Article 4(1)(e) is being complied with.

Furthermore, data must be "processed fairly and lawfully" (Article 4(1)(a) of the Regulation). Lawfulness has already been analysed in point 3.2 of this opinion. Fairness relates to the information which must be transmitted to the data subject (see point 3.9 below).

Finally, the data must be "accurate and, where necessary, kept up to date; 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" (Article 4(1)(d) of the Regulation). The Windows programme which runs on the server permanently, transferring data between the card readers and the database, ensures that data are up to date. Whenever the connection between the server and a card reader fails, the card reader stores the data. The purpose of using the staff number to facilitate the link between databases is to eliminate data inaccuracies which could occur in the central system, if the other databases feeding it are not synchronised and if the central system is not updated. Linkages between the different systems are intended to establish greater consistency and accuracy of data. The EDPS considers that Article 4(1)(d) has been complied with.

Rights of access and rectification by the data subject are also a way of ensuring the accuracy and updating of the data concerning him or her (See also "right of access and rectification", point 3.8).

3.4. Data storage

Personal data must be "*kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. (…)*" (Article 4(1)(e) of the Regulation). In accordance with Article 4(1), where personal data are to be stored for longer periods for historical, statistical or scientific use, they should be kept either in anonymous form only or only with the identity of the data subjects encrypted.

Data may be stored until all rights and appeal rights are extinguished (five years). The EFFICIENT software stores all data, including clocking in/out data, in a centralised database constructed on an incremental basis.

The Court of Auditors also justifies the five-year period on the grounds that management regularly requires that details of clocking in/out be accessible for a long time in the past: the most obvious case is when a person returns from lengthy leave or a long absence.

The EDPS regards that data storage period as excessive having regard to the purposes of the processing. It would remind the Court of the rule applicable to data storage presented in the various cases relating to flexitime[2]. We would emphasise that data relating to flexitime must be stored for the current calendar year and must be deleted once the process of transfer of unused leave to the following year has been completed, and no later than the end of March of the following year.

[2] Case 2007-063 Sysper 2: Commission Time Management module, Case 2007-218 Flexitime DG INFSO (EDPS web site).

The EDPS considers the argument that a five-year period is necessary for purposes of appeal inadmissible. The fact is that appeals are made in the year following the year in which data were recorded, and where an appeal is made the data relating solely to the person concerned are retained (blocked) until such time as the appeal proceedings have been completed. That does not justify retaining all the data on the database for five years. Nor is there any basis for the argument regarding a person returning from lengthy leave or absence. It is for the Human Resources Department to produce a record of hours worked before the data subject leaves.

The EDPS recommends that the Court of Auditors establish a different period, preferably three months. The procedure for the exceptional cases envisaged would arise only where data were disputed. In such a case, the data will have to be flagged as being disputed.

By application subject to appeal, a person no longer working at the Court of Auditors may request that data relating to him/her be erased. Erasure is carried out within 18 months. In the case of staff still at work, data may be blocked immediately at the request of the data subject. Blocking can take place within a day. Erasure of personal data is a procedure which takes place between three and six months after departure, it being necessary to allow time for financial effects to be settled. In certain exceptional cases, the procedure may take longer.

The EDPS also regards that period of 18 months for erasing data relating to data subjects who have left the Court of Auditors as excessive. In other cases, the EDPS considered that a period of 15 days would be proportionate to the purposes of the processing. The EDPS also recommends reviewing the period necessary for erasing data relating to data subjects who have left the Court of Auditors.

3.5. Change of purpose / compatible use

Data are retrieved from or entered in the staff databases. The purpose of processing the data is to manage and monitor flexitime (flexitime rules and management of working hours and absences via an automated system). The linking of the databases (EFFICIENT - SIC CONGES - the Court's Mission application) is a technical tool to facilitate the transfer of personal data between various services (leave department, human resources, immediate hierarchical superior, person responsible for training). This processing is necessary for the legitimate performance of tasks covered by the competence of those departments: overtime, administration of leave, human resources planning in the narrow sense, and compensation for overtime, training and missions.

The processing being reviewed involves no general change to the specified purpose of staff databases, and the management of timetables and absences is only part of that purpose. Accordingly, Article 6(1) of Regulation (EC) No 45/2001 is not applicable to the case in point, and Article 4(1)(b) of the Regulation is complied with, given that the purposes are compatible.

3.6. Transfer of data

The processing operation should also be scrutinised in the light of Article 7(1) of the Regulation. Article 7 of the Regulation provides that "*personal data shall only be transferred within or to other Community institutions or bodies if the data are necessary for the legitimate performance of the tasks covered by the competence of the recipients*".

The recipients are: the Human Resources Division and all the Directors and Heads of Unit for the staff assigned to each department, the appointing authority, the payment officer responsible for overtime payments, internal and external auditors in the case of an audit and, where applicable, the legal service. Only the DB Administrator and his/her backup have full access to the database. All other access is via the application's web interface.

The EDPS considers that this sharing of information is *necessary for the legitimate performance of tasks covered by the competence of the recipients*. Such processing is indeed within the competence of the Court's various departments (Human Resources, IT, etc.) and transfer is lawful insofar as the purpose is covered by the competence of the recipients.

The controller must nevertheless define precisely the roles and responsibilities of each user in relation to the criterion of necessity for the performance of their tasks. The EDPS recommends that users should have access only to data which can be reasonably regarded as being necessary for the performance of their tasks. There must be safeguards so that only persons authorised to access personal data can actually do so. Moreover, persons accessing data in the central information system must be informed that they may not use them for purposes other than those compatible with the purpose of the Flexitime system.

3.7. Processing including the personal or identifying number

Article 10(6) of the Regulation stipulates 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*".

The EDPS has already clarified the status of the RFID chip number[3]. The identification number associated with the RFID chip is personal data covered by Regulation No 45/2001. This identification number, when used to record a staff member’s behaviour and linked to the personal number (which means linked to the name of a person, as is the case here), means that the processing is processing of personal data, which requires compliance with the data protection principles.

The Court of Auditors uses both the personal number and the staff card number in the Flexitime system. The staff card number is necessary because the card is used to clock in/out at the card readers. In this instance, the use of the staff member's personal number for the purpose of recording data in the system is reasonable since that number is used to identify the person in the system and keep track of his/her records, thus facilitating processing and helping ensure that the data are accurate. Article 10(6) has thus been complied with.

3.8. Right of access and rectification

Article 13 of the Regulation makes provision, and sets out the rules, for right of access at the request of the data subject. Article 14 of the Regulation deals with the data subject's right of rectification.

The application allows all staff members to consult records relating to them for the current month and for the previous month. If they submit a duly substantiated request, data subjects may receive a "clocking in/out table" showing earlier months. Staff may ask managers to correct or amend clocking records for the current month and the previous month via a functional mailbox. (In exceptional and duly substantiated cases, amendments/corrections may be made to older data).

[3] See Case DG INFSO 2007-218 on flexitime.

The EDPS considers that the conditions set out in Articles 13 and 14 of the Regulation have been complied with, provided that the necessary correction is made to the duration (see point 3.4, data storage) For the rights of access of persons other than the data subject, see security measures below (point 3.11).

3.9. Information to data subjects

Regulation (EC) No 45/2001 provides that the data subject must be informed when his or her personal data are processed and lists a series of specific items of information that must be provided. In the present case, some of the data are collected directly from the data subject and other data from other persons.

Article 11 (*Information to be supplied where the data have been obtained from the data subject)* applies in the case in point since the data subject encodes his or her own data.

Article 12 (*Information to be supplied where the data have not been obtained from the data subject*) also applies in the case in point, as information can be encoded by the head of unit, or his or her secretariat if the task has been delegated.

Information to EFFICIENT data subjects is provided via the regulation governing the system which is available on the Court's intranet and in the timetable consultation application. Data subjects are informed of the regulation and the system on taking up employment when their electronic staff card is handed to them in person. Nevertheless the regulation governing the system includes none of the points covered by Articles 11 and 12 of Regulation No 45/2001 other than right of access and rectification. The EDPS recommends that all the provisions of Articles 11 and 12 of Regulation No 45/2001 be added to the regulation so that information to data subjects is complete and exhaustive.

3.10. Security

Under Article 22 of Regulation (EC) No 45/2001 on the security of processing "*the controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected*".

The Security measures are […].

Conclusion

The proposed processing operation would not appear to involve any breach of the provisions of Regulation (EC) No 45/2001, provided that account is taken of the observations made above. This means, in particular, that:

- the Court of Auditors should review the period necessary for the erasure of data relating to persons who have left the Institution, should set a specific period for erasing data relating to staff working at the Court and should make provision for flagging data which are disputed
- users should have access only to data which can be reasonably regarded as being necessary for the performance of their tasks
- there should be guarantees that access to personal data is reserved solely for those authorised to receive them and that persons accessing data in the central information

system are informed that they may not use them for purposes other than those compatible with the purpose of the Flexitime system

- all the points covered in Articles 11 and 12 of Regulation No 45/2001 should be added to the regulation governing the EFFICIENT system so that information to data subjects is complete and exhaustive
- the Court of Auditors should establish security measures […].

Done at Brussels, 5 December 2008

(Signed)

Joaquín BAYO DELGADO
Assistant European Data Protection Supervisor