Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Commission on "the implementation of flexitime - specific to DG INFSO"

Brussels, 19 October 2007 (Case 2007-218)

1. Proceedings

On 24 March 2007, the European Data Protection Supervisor (EDPS) received by e-mail from the Data Protection Officer (DPO) of the Commission a notification for a consultation on the necessity of prior-checking under Article 27.3 of Regulation (EC) 45/2001 of the processing operations on personal data concerning "Flexitime-specific to DG INFSO - DPO-1611 Version 2". On the 29 March 2007, the EDPS acknowledged that the system had to be prior-checked in accordance with Article 27 of Regulation (EC) 45/2001 (hereinafter the "Regulation"). The two months delay within which the EDPS must render his opinion according to Article 27.4 started to run as from the acknowledgment of the notification by the EDPS, i.e. from the 29 March.

On 4 April 2007 and on 16 April 2007, the EDPS made requests for additional information, to which the Controller replied on 7 May 2007, answering both requests. The EDPS asked for and received some additional clarification by phone on the 24 May. On the same day, it was also announced to the EDPS that the system which was foreseen would be modified, as to integrate it with the TIM module. After further contacts and clarifications, the EDPS decided to suspend the prior-checking case on 31 May, while the new technical specifications were prepared by the data controller. On 16 July, the controller sent the new technical specifications of the flexitime system integrated in the TIM module (the EDPS received 2 technical documents entitled: "Software Requirements Specifications" and "Technology and Infrastructure" as well as the related modifications of the notification for prior checking and a new draft of the specific privacy statement). In the light of the complexity of the case, the EDPS decided, in the respect of Article 27 (4) of Regulation 45/2001, to postpone by one month the deadline for the adoption of his opinion. On 10 September 2007, the EDPS sent his draft opinion to the DPO with a request to comment on it. The comments reached the EDPS on 21 September 2007.

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 63
E-mail: edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax : 02-283 19 50

2. Examination of the matter

Context and Objective of flexitime at the Commission

On 19 December 2006, the Commission adopted the new flexitime system[1] introducing flexitime within Commission services as of 1 April 2007 at the latest[2]. The general framework of Time management is regulated by the "SYSPER 2 Time management system". This system has as its objective the general time management system put in place by the Commission relating to the management of leave and absences by the Commission, notably the management of overtime (Flexitime). It was considered as subject to prior checking by the EDPS on the grounds of Article 27.2.a (presence of data relating to health) and Article 27.2.b (processing operations intended to evaluate personal aspects relating to the data subject). The EDPS issued his opinion on this system on 29 March 2007[3].

In the light of the Guide to Flexitime, the Commission, considering that one of the major elements of its administrative reform is to soften its methods of work in order to facilitate the conciliation of the obligations of the private life and the professional life of its staff, decided to support the application of the flexitime in its services by allowing all Commission personnel to benefit from this opportunity within the framework of the working week of 37 ½ hours, while fully respecting the provisions of the Staff Regulations and the interest of the service. By doing this, the Commission intends to increase the motivation of its personnel while making it more responsible for the organisation of its working time.

DG/Services of the Commission, which choose to apply or try out the flexitime, may use on the basis of the "guide to Flexitime"[4] manual recording systems, electronic files, magnetic cards or similar systems. DG INFSO has decided to implement Flexitime, using the latter possibility.

The present case "SYSPER 2 Time management system - Flexitime-specific to DG INFSO - DPO-1611 Version 2" (hereinafter Flexitime (in) DG INFSO) is related to the abovementioned notification as it adds to the application of Flexitime in DG INFSO an additional and important component in the element of a RFID chip integrated in the personal badge necessary to clock in and out. The inclusion of such a technology into a flexitime system thus reinforces the specific risks already present in the system. On the basis of this crucial new element, the EDPS therefore considered the case as such subject to prior checking.

General description of the system and reasons to implement it

The decision to implement flexitime using electronic badges within DG INFSO was based on the positive results of a pilot project that took place within the DG between May and October 2005. On 28 September 2006 DG INFSO communicated its intention to use electronic badges to DG ADMIN and DG DIGIT and received positive responses.

---

1 Administrative notice SEC(2006)1796 5IA 62-2006 of 21/12/2006 - Guide to Flexitime

2 A Flexitime system has already been developed in another institution, namely the Council, for which the EDPS adopted a prior-checking Opinion (Case 2004-258 of 19 January 2006).

3 See www.edps.europa.eu

4 Administrative notice n° 62-2006 dated 21/12/2006. See also Communication of the Commission on the use of flexitime in the Commission services SEC(2006) 956 of 19.07.2006.

The participation in the flexitime system developed within DG INFSO is made on a voluntary basis and, therefore, the existence of flexitime does not force staff to depart from normal working hours. DG INFSO staff opting for flexitime can choose how to input the arrival and leave times. When the badge system becomes available, they will have the choice to either use the TIM interface or use the badges with the dedicated badge readers.

Nevertheless, a Head of Unit could decide for his/her Unit to use only badges as input for flexitime.

The Commission services in charge of the flexitime application will collect personal data to the extent necessary to help all staff to work the same number of hours they are required to in a flexible manner in order to better conciliate work and private life. Flexitime is based on the principle of time-keeping of worked hours supported by a transparent verification system, which should be easy and fast to use.

The processing, which is developed at DG INFSO consists of 3 parts:

1. Collection of the time registrations

The DG INFSO flexitime situation is represented by the following scenario: one card, two readers. There is one reader which is used for access to the buildings and one reader which is dedicated to the flexitime application. The entry of time registrations for flexitime will be done via badging with the personnel cards. The technology used in the personnel cards is Mifare with a passive component (the model used is the Mifare standard 4K as requested by the Security Directorate). Specific readers will be used for the flexitime (i.e. separate from the readers used for handling the access control).

The user needs to swipe his/her personnel card in front of one of the readers of the building. According to the notification, this technology only allows a distance of maximum 10 cm for an extremely powerful reader, which is not the case in DG INFSO. Following tests, the installed readers only allow a maximum distance of 3 cm so that any inadvertent swipe is prevented. Moreover, the maximum reading distance specified in the datasheet of the supplier of the card-reader is 5 cm. Each Mifare chip is assigned a unique serial number during its production phase and this number is the only information transmitted to the reader.

2. Transfer of the time registrations

The information of the time registrations (the unique identifier and the time registration) is then passed to the rest of the application where the link is made between the unique identifier of the Mifare chip and a person. The time registrations of a person will be grouped over one day and the next morning inserted into the TIM module of SYSPER 2 via the interface defined by DG DIGIT.

The data transferred are the personnel number, the date and the different time registrations for that person of the previous day. An email will be sent to the person with all his time registrations in case of error in the insertion into TIM. Errors need to be rectified interactively through the TIM module of SYSPER 2 within the first 6 days.

An audit trail of 2 months is foreseen. This will contain the time registrations, the personnel number, the status (error or not) and date of the insertion. A module will be foreseen for the data controller to consult this audit trail (in case of dispute).
The user can verify every data through the TIM module of SYSPER 2.

3. Activation of the badging with personnel cards

An application module will be put in place to activate the personnel cards for badging. This application will register the link between the personnel number of the user and the unique identifier of the Mifare chip on the personnel card. At the same time it will also manage the information if a person has opted in for flexitime – for them the badges will be "activated" as only staff members opting for flexitime are eligible to use the dedicated readers. This application is protected in terms of access and is available to the roles "Administrator" and "Data Controller". DG INFSO will receive information of the link "personnel number – unique identifier of Mifare chip" from the security directorate and the opt-in data will be available from SYSPER 2 (master of the data) and DG INFSO will synchronise its data with both sources.

According to the notification and additional answers provided to the EDPS, the reasons explaining that DG INFSO decided to implement the flexitime through the RFID technology are that:

in terms of necessity, this electronic badging system :

- Offers an up to date system[5] ;
- Ensures fairness, accuracy and reliability of data ;
- DG INFSO manages European research projects on RFID technology. As a result, DG INFSO has some familiarity with the technology in question.

Moreover, in terms of proportionality, this electronic badging system :

- Was authorised by paragraph 5.1 of the "Guide to flexitime" as one possibility among several for time recording in the framework of flexitime ;
- It is simpler and reduces significantly the administrative burden for the staff (Cf. positive results of the pilot project) ;
- Above all, it is considered not invasive as:
    - The reading distance is limited to a few centimetres (the system is technically not able to monitor the movements in a building, nor between different buildings) ;
    - Each individual staff member masters the use of his/her badge and voluntarily (i.e. presents the badge at the reader every time he/she wants the flexitime badge to be read);
    - The card only contains a serial number. According to the notification and the interpretation of DG INFSO, this is no personal information. See analysis under point 3.

Finally, in terms of security, DG INFSO based its technology choice on the Security Directorates recommendations.
The contactless chip technology is the standard adopted by the Security Directorate for a number of reasons such as:

- Private keys managed by the Security Directorate itself (instead of having an external company managing those private keys as it is currently the case) ;
- High level of encryption possible (64bits). The EDPS takes note that the encryption is not implemented in the current flexitime scheme. Therefore, there is no encryption of the card number.

[5] According to the controller, the current badging technology - NEDAP - is now in phasing-out stage and the standard which will be used in DG INFSO (Mifare) amounts for 80% of all "contactless smart cards" in use today

- High security: this technology is used in many other sensitive environments such as credit/bank cards, identity cards.

Characteristics of the badge

The DG INFSO staff members have received a new personnel card, distributed by the Security Directorate, including the double technology (as already mentioned, the one for the use of RFID for flexitime is based on the Mifare standard and the other one to access buildings is based on the currently used technology provided by Nedap). ADMIN DS linked the number of the card to the list of people and sent all the cards to the Local Security Officer of DG INFSO.

There are therefore two numbers associated to these cards: one is the "flexitime number" and the other is the "access number"
The wireless readable tag - so-called "contactless smart card standard" based on the ISO 14443 standard - is integrated in the personnel badge. These tags belong to a specific type of Radio Frequency Identification (RFID) tags (so-called proximity tags). Its operating frequency limits the reading distance to a few centimetres (passive smartcard technology). According to the notification, the installed readers at DG INFSO only allow a maximum distance of 3 cm. The only information used by DG INFSO is the unique identifier of the RFID chip.

Specific readers will be used for the DG INFSO flexitime system (distinct and separated from the readers used for handling the access control to the Commission's buildings under the responsibility of the Security Directorate). Readers are installed in the entrance places where staff members access the buildings. In the buildings BU33 and BU31, there will be 2 readers installed in the entrance hall and 2 readers on each garage floor. In the buildings EUFO and BU25, since staff members have to pass by the ground floor, all readers (4 in total) have been placed on the ground floor. A total of 20 readers are being placed.

DG INFSO staff members who do not participate in flexitime will not have to swipe their badges and, as a consequence, will not use those readers. Since the SYSPER II module accepts these inputs, the local system only stores the monitored "Start" and "End times" until they are transferred to the SYSPER II module.

Data subjects

According to the notification, the data subjects covered by the system are all staff of Units of DG INFSO (officials, temporary agents, contract agents, auxiliary staff, DNE). The Guide to Flexitime states that Flexitime is applicable to all staff covered by the Staff Regulations or by the Conditions of Employment for Other Servants, regardless of function group or grade, and to seconded national experts. However, point 1.4 of the same Guide to flexitime states that certain units, parts of units or groups of staff may be excluded from applying flexitime or be subject to restricted use of flexitime owing to particular service requirements.

Informatics experts are not subjects to the rules of the staff regulation and therefore not subject to the flexitime application. By consequence, they will not use RFID enhanced badges for that purpose.

Moreover, DG INFSO will closely follow the Guide to Flexitime. Hence, it will treat interim agents and stagiaires as IT experts and not allow them to use flexitime.

The additional technical specifications which were provided to the EDPS also foresee that the staff members not present in the application but working in DG INFSO according to the information available in Ldap-Directory will be imported in the application. The staff member details which will be imported are: Email, first name, last name, login and personal identifier. It is also added that the imported users will be marked as un-registered and inactive.

Controllers and processors

The controller is the Head of unit INFSO R1 (system owner) and the processor is the Head of unit INFSO R4 (system provider).

The controller is responsible for the IT application. Only he/she can access to the audit trail of the application (time entries and their status of sending them to TIM).

The system administrator is designated by the Controller. He/she can access the links between unique identifiers of the badges and personnel numbers.

The possibility of delegation to a "gestionnaire" within the unit does not exist for the software system developed at DG INFSO. The gestionnaires use the TIM module of SYSPER 2.

On the basis of the above subdivision, the notification defines 2 user classes and three roles for the system:

User Classes:

- Standard user class covers all staff referred to in the "Guide to Flexitime - SEC (2006)1796 §3

- Advanced user class covers all persons having access to the graphical user interface

Access roles:

- Data Controller Role (DC) (advanced user class) who will have access to all the functionalities. The DC is responsible for assigning administrator roles.

- Administrator Role (advanced user class) who will have access to all functionalities except the audit functions. This role is mainly defined for maintenance purposes since holders of such role will receive inconsistent/missing information related to e-mails. They will also be responsible for maintaining the staff member/car link.

- Standard Role (standard user class) who will have no access to the Graphical User Interface.

A person can be assigned several roles simultaneously. There is no hierarchy in the user classes. For example, a person can be assigned the Data Controller role without the Standard role. This specific requirement allows staff members not using their card for time registration purpose to be member of the advanced user class.

Regarding the management of the roles, the application allows three DC and three Administrator roles assignments.

Data required for the processing operation

The data that are collected at the moment the chip is swiped into the reader are the card serial number and the time the card is swiped.

The Controller describes the INFSO system as a "buffer" between the badge readers and the SYSPER 2 TIM module. Therefore, no calculation of balances (between official working time and real working time) is done. This falls under the scope of the SYSPER 2 TIM module. However, other processing operations take place in the flexitime application itself (processing of personnel number, name, ..).

Actually, the data concerned cover more than the unique identifier and the time registration. As the draft privacy statement showed, the information which is eventually collected and subsequently processed on this basis is:
- Badge unique identifier
- Time registrations and their transfer status to TIM
- Personal number in Sysper2
- The opt-in for the flexitime scheme indicator
- Role of the user within the application
- E-mail address
- First name
- Last name
- Login

Information to data subjects

The notification foresees the publication of a specific privacy statement for flexitime which has been developed and will be available on-line on the home page of the Human Resources Unit (Data Controller) that is accessible to all DG INFSO staff members. Drafts have been submitted to the EDPS for review.

It provides a general description of the system, explanation on the transfer of the time registration, information on who has access to information and to whom it is disclosed. It also contains provisions on how the information is protected and safeguarded, as well as on how this information can be verified, modified or deleted. Finally, it contains references to the retention period, legal basis and contact details.

Access, rectification and erasure of personal data

The draft privacy statement specifically for flexitime states that "if you [staff members] wish to verify, modify or delete any of your data registered via the DG INFSO IT flexitime registering application, it can be done via the SYSPER 2 - TIM module, pursuant to the rules defined by DG ADMIN in the SYSPER 2 - TIM notification and annexes".

The prior checking opinion on SYSPER 2 states, regarding flexitime, that: "the right of access, the right of rectification and the right to object are granted in the following ways: all personal data (leave/absences/part-time work/parental and family leave/flexitime) are accessible to the holder (and partly supplied by him or her); he or she can thus check them and if necessary correct them directly or ask for them to be corrected by an HRO manager (data relating to identification) or by his or her immediate superior (flexitime)."

The INFSO flexitime system does not contain any graphical interface accessible for data subjects having "standard role" (standard user class as opposed to advanced user class such as

data controller/administrator). The data subjects use the SYSPER 2 - TIM module (themselves or via the line manager or the gestionnaire) to access, verify and, if necessary, correct their personal data.[6]

DG INFSO introduces a distinction between identification data and data specifically linked to flexitime.

The first type (identification) is linked to SYSPER 2 and can, when needed, be changed following the procedure described in this system's notification; for the second type of data (flexitime related), changes are made via the SYSPER 2 - TIM module, pursuant to the rules defined by DG ADMIN in the SYSPER 2 - TIM notification and annexes. In the case of a dispute, the person could request conservation or blocking of the data by the data controller (in this case the Head of Unit of the human resources unit within DG INFSO)

Data Storage

The data are stored in an Oracle database. Within the first 6 days, there are no specific paper file registers involved. The application transfers the registered swipes to TIM manager pursuant to the rules defined by DG ADMIN in the SYSPER 2 - TIM notification and annexes. Following the rules of the SYSPER 2 - TIM module corrections, completions within a period of 6 days can be done by the data subject him/herself (provided that the line manager did not decide to centralize encoding). In this case the incident is not registered on a standard paper form.

Hence a paper file registers the incidents in the procedure in order to complete/correct the SYSPER 2 - TIM data if an elapse time of 6 days is exceeded or if the access to the SYSPER 2 - TIM module is centralized by the line manager.

The INFSO IT flexitime registering application is functioning like a buffer of time registrations to be transferred to the TIM module. In this context and considering the necessity to keep an audit trail of the registering of data, DG INFSO foresees an audit trail with a retention period of 2 months (see above page 3 on the presentation of the system),

Automated processing operation

The automated processing operations are the following:
- time registration of the swipes for each person ;
- transfer of the time registrations to the TIM module of SYSPER 2. In case of error send an email to the user with the registered time entries ;
- a management user/card function (user synchronisation with SYSPER 2, unique identifier synchronisation with the personnel card database, create / modify / remove user, create / modify / remove cards) ;
- a reporting function (audit trail: list of time registrations together with the status and date for one person).

Manual processing operation

In line with the technical specifications, within the DG INFSO application, there is no specific manual processing involved.

[6] See on this aspect, prior-checking 2007-0063: "SYSPER 2 : module Time management "

When errors occur during the insertion of the time registration, they need to be corrected via the SYSPER 2 - TIM module, pursuant to the rules defined by DG ADMIN in the SYSPER 2 - TIM notification and annexes. Where an individual change is possible, data subjects can do this themselves within 6 days. Once this 6 days period has passed, the line manager or the unit "gestionnaire" can correct the information. In the case a centralized approach is chosen, all corrections need to be asked to the unit "gestionnaire".

Depending on the choice of the line manager, this can be done via a standard paper form. The forms need to be destroyed once the monthly timesheet is validated.

Security

The model of Mifare used is the Mifare standard 4K one, as requested by the Security Directorate.

According to the additional information provided by DG INFSO, "*As a result of an analysis of the different scenarios, the potential trifling risks have been mitigated by the security measures adopted such as technology choice, secure location of hardware, no personal data stored on the cards, extremely limited action range of the readers, controlled access to the application*".

The data collected in the flexitime application is not accessible by anyone outside the Commission. Inside the Commission the data can be accessed by the person concerned or designated Commission officials, using a UserID and a password.

The system is hosted on servers, managed by the IRM staff of DG INFSO (Unit R4), and which are physically located in secure server rooms under the control of Unit R4.

Controllers are located in the secure PABX room (Private Automatic Branch eXchange). Access to the PABX room requires either a call to DIGIT along with opening justification or specific access card for authorised personnel only (maintenance). Access to the computer room requires specific access card with associated PIN code.
The controllers for the readers are placed in secure PABX (Private Automatic Branch eXchange) rooms, which are under the control of DG DIGIT.

Concerning logical access to the server, 2 groups of persons are identified: DBAs (database administrators) and LSAs (local system administrators). Only those 2 groups of persons have logical access to the server. DBAs perform database maintenance tasks (Oracle) such as performance optimization and backup actions. LSAs perform maintenance tasks on the server computers such as upgrading and installing security patch applications.

DBA staff and LSA staff are strictly different persons, and they are out of the functional scope of the (any) application. The list of DBA staff and LSA staff will be made available to the Data Protection Coordinator ("DPC").

3. Legal aspects

3.1 Prior checking

In view of the specific operation taking place in this processing, the EDPS deems it important to refer to the definition of personal data. According to Article 2 (a) of the Regulation 'personal data' shall mean "*any information relating to an identified or identifiable natural*

person" hereinafter referred to as 'data subject'; "*an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity".*

The system being analysed, that is the specific flexitime application of DG INFSO, does indeed process personal data because the data relate to natural persons who are identifiable, for instance by the use of names, personal numbers. Even the serial number, which in itself is non personal data, becomes, in the system, a personal number from the moment it is linked or is linkable to identification data and is used to record that a badge issued to a particular staff member has passed the reader. The natural person can be identified, directly or indirectly by reference to an identification number.

The processing operation by the Commission is carried out in the exercise of activities falling within the scope of Community law (Article 3(1) of Regulation (EC) No 45/2001).

The Flexitime in DG INFSO concerns both automatic and manual processing. Thus this is partly automated processing. Therefore Article 3(2) of the Regulation applies.

According to paragraph 5.1 of the "Guide to flexitime"[7] manual recording systems, electronic files, magnetic cards or similar systems can be used for time recording. Article 27 (1) of Regulation (EC) 45/2001 subjects to prior checking by the EDPS all "*processing operations likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes*". The TIM management system, of which flexitime is part, was prior-checked by the EDPS on the basis of Articles 27 (2) a and 27 (2) b. Besides, the EDPS considers that the inclusion of such a technology (the RFID chip embedded in the badge) into a flexitime system constitutes an important innovation in the system already prior checked and reinforces the specific risks already present in the system. Therefore, the current prior checking falls under Article 27(1) of the Regulation.

Since prior checking aims 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 real prior check. In this respect, the EDPS welcomes the internal note of DG INFSO (e-mail to DG INFSO staff dated 30 March 2007) by which DG INFSO acknowledged that it will not implement the badging system until formal clearance is granted by the EDPS.

However, it is important to underline that the EDPS promotes (in his opinions as well as in his annual reports) the idea that the development of 'privacy by design' technologies could favour better data protection. That is the reason why the EDPS would have appreciated that he or the DPO had been involved at an earlier stage in the process foreseen in DG INFSO, for instance when the pilot project was under development[8].

In the abovementioned prior checking case of 29 March 2007, the EDPS underlined that there is no reason to believe that there is a breach of the provisions of Regulation 45/2001 providing the considerations he makes are fully taken into account. Therefore, the general as well as the specific-flexitime related recommendations of that prior checking remain valid for the current prior checking under scrutiny.

---

7 Administrative Notice 62-2006 dated 21/12/06

8 For instance, this was the case of the Flexitime system developed by the Council, where the EDPS is involved since the pilot project

The notification of the DPO was received on 29 March 2007. A request for information was sent on 4 April 2007 and a subsequent request for information on security aspects was sent on 16 April 2007. The period of two months during which the EDPS must render his opinion for prior checking was suspended. The Commission replied on 7 May 2007, answering both requests. On 24 May, the EDPS requested by phone additional clarifications, which were provided on the same day. The controller also announced that the technical aspects of the system would be changed. In view of the changes that would be made on the notification, the EDPS suspended the case on 31 May, in order for the controller to prepare the technical specifications. The documents were received on 16 July. In the light of the complexity of the case, the EDPS decided, in the respect of Article 27 (4) of Regulation 45/2001 to postpone by one month the deadline for adopting his opinion. On 10 September 2007, the EDPS sent the draft opinion to the DPO with a request to comment on it. The Commission's comments reached the EDPS on 21 September 2007 and a meeting between staff members of the EDPS, the data controller of the flexitime system and the DPO of the Commission took place on 12 October 2007, the procedure being suspended till the meeting. The prior checking procedure was suspended for a period of 100 days + 11 days (for comments) + one month of extension (Article 27.4.). The EDPS will deliver his opinion on 19 October 2007.

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"*

In order to determine whether the processing operations comply with Article 5 a) of Regulation (EC) No 45/2001 three elements must be taken into account: First, whether either the Treaty or other legal instruments foresee the data processing operations carried out, second, whether the processing operations are performed in the public interests and, third, whether the processing operations are necessary. Obviously, the three requirements are closely related.

Relevant legal grounds in the Treaty or other legal instruments

The legal basis for the processing is to be found in:
- the Staff Regulations of officials and Conditions of employment of other servants (especially Article 55)
- the Communication of the Commission on the use of flexitime in the Commission services SEC(2006) 956 of 19.07.2006
- the Administrative notice n° 62-2006 dated 21/12/2006 : Guide to flexitime.

The EDPS underlines that the "Guide to flexitime" provides, in its Article 5.1 on the recording of worked hours, that: "*The head of unit has to ensure that the working hours of his/her staff are recorded following the procedure referred to in point 3.1. For this purpose DGs and Services may use manual recording systems, electronic files, magnetic cards or similar*

systems. *Any time recording system must be proportionate and in conformity with the regulation (EC) 45/2001 on the protection of personal data processed by Community institutions and bodies*".

Processing operations are carried out in the legitimate exercise of official authority

The EDPS notes that the Commission carries out the processing activities in the legitimate exercise of its official authority. Indeed, the processing operations are taking place in the framework of a mission carried out in the public interest on the basis of Staff Regulations of the officials of the European Communities and the conditions of employment of other servants of the European Communities. The admissibility of the treatment is thus respected.

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. In this respect, recital 27 states 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*".

As presented by DG INFSO, in terms of necessity, this electronic badging system :

- Offers an up to date system ;
- Ensures fairness, accuracy and reliability of data ;
- DG INFSO manages European research projects on RFID technology. As a result, DG INFSO has some familiarity with the technology in question.

The EDPS considers that there is not a specific need to develop a badging system using RFID to implement a flexitime system, as the same purpose (management of working hours) could be reached by other, less intrusive, means.

However, the EDPS also accepts that "need" does not mean that it is unavoidable but that it can be considered reasonably necessary in the specific context for fulfilling the purpose aimed at. Therefore, there is a margin of appreciation left at the discretion of the administration in deciding to implement this system using RFID. If the safeguards and proportionality are present, it can be considered that such a system fulfils the conditions of need.

Finally, the participation in the flexitime system itself is made on a voluntary basis.

As to the specific system to input arrival and leave times, i.e. either by using the TIM interface or the badges with the dedicated badge readers, it has to be chosen in principle by each participant, but the head of Unit can decide to have a homogeneous system in his/her unit.

3.3 Data Quality

Data must be "*adequate, relevant and non excessive in relation to the purposes for which they are collected and/or further processed*" (Article 4(1)(c) of Regulation (EC) No 45/2001).

The data collected are a magnetic card number (serial ID number) and daily events such as arrival and departure. Moreover, the ID number of the reader is never collected nor processed with the daily events. The EDPS considers this adequate and relevant. Those data are not considered excessive.

The additional technical specifications which were provided to the EDPS also foresee that the staff members not present in the application but working in DG INFSO according to the information available in Ldap-Directory will be imported into the application. The staff member details which will be imported are: Email, first name, last name, login and personal identifier. It is also added that the imported users will be marked as un-registered and inactive.

In principle, the EDPS would find this inclusion excessive for the processing operation because the information concerns persons who are falling outside the flexitime system. No reasonable justification has been given to the EDPS to keep these staff in the database (Oracle database) and therefore the EDPS does not see any reason to import into the application the staff members who are not present in the application but are working in DG INFSO. This concerns not only IT experts, interim agents and stagiaires but also, in the respect of the data minimization principle, the staff members of DG INFSO who decide not to opt for the flexitime system. The EDPS recommends that DG INFSO analyses the means and frequency of updates of the database in order to implement this recommendation regarding the categories of people that have to be kept outside the flexitime database and informs the EDPS on the outcome.

Furthermore, the notification states that no data falling under the categories of data referred to in Article 10.1 (special categories of data) are processed in the context of the data processing operation notified for prior checking. Taking into account the overall purpose pursued by DG INFSO when it engages in the flexitime data processing operations, the EDPS considers that the collection of special categories of data is not DG INFSO's intention.

The data must be processed "*fairly and lawfully"* (Article 4(1) (a) of the Regulation). The lawfulness of the processing has already been discussed (See 3.2 above). As regards fairness, this relates to the information given to the persons concerned (See 3.9 below).

Data must be accurate, and where necessary, kept up to date" (Article 4 (1) (d). The system in general must ensure data accuracy and the updating of the data. This is the case here.

When errors occur during the insertion of the time registration, they need to be corrected via the SYSPER 2 - TIM module, pursuant to the rules defined by DG ADMIN in the SYSPER 2 - TIM notification and annexes. Where an individual change is possible, data subjects can do this themselves within 6 days. Once this 6 days period has passed, the line manager or the unit "gestionnaire" can correct the information. In the case a centralized approach is chosen, all corrections need to be asked for to the unit "gestionnaire".

Further, on the right of access and rectification, see 3.8 below.

3.4 Data retention

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."*

The EDPS wants to confirm the rule applicable to the retention of data, as presented in the Prior checking case regarding SYSPER 2 - module Time management. Indeed, on the data

retention aspect of SYSPER 2, it is underlined that data concerning flexitime are stored during the ongoing calendar year. They will be deleted once the transfer of unused days of annual leave to the following year has been closed, and at the latest by the end of March. In the case where the computing of daily work is done at the level of the head of unit/sector and is based on intermediate statements, they will be destroyed after the validation of the monthly assessment by the head of unit/sector, and for the 15th of the following month at the latest.

As to the specific conservation of data in the application of DG INFSO, the draft specific privacy statement states that the application could be described as a simple buffer of time registrations to be transferred to the TIM module and that, considering the necessity to keep an audit trail of the registering data, all data received are stored for a maximum of two months.

The same time applies for the time limit to block/erase data on justified legitimate request from the data subjects.

The EDPS considers that these retention periods comply with the requirements set in Article 4(1)(e) of the Regulation.

The EDPS understands from the notification that no statistics on personal data are allowed after the retention period of one year, therefore complying with Article 4(1)(e). Nevertheless, the EDPS would emphasise that where such data are used beyond the retention period, they must be made anonymous (Article 4(1)(e) of the Regulation).

3.5 Compatible use / Change of purpose

Article 4(1)(b) of the Regulation provides that personal data must be "*collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes*". The purpose of the processing is that, based on the principle of time-keeping of worked hours, flexitime helps all staff to work the same number of hours they are required to in a flexible manner in order to better conciliate work and private life. The Commission does not use the data processed in the analysed context for any purposes other than for the purpose it sought to fulfil. Moreover, it is strictly underlined by the Commission that the "magnetic card number" is not used for any other purposes than the flexitime framework and that it is only stored in the DG INFSO flexitime application for linking the card to the person. It is the understanding of the EDPS that there is no change of purpose to the processing. Therefore, Article 6.1 of Regulation 45/2001 is not applicable to the case and Article 4.1.b of the Regulation is respected.

3.6 Transfer of data

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 tasks covered by the competence of the recipient"*.

The specific privacy statement explains the categories of persons who could have access to the registered data via the IT registering application of DG INFSO. Two categories are mentioned: the controller (responsible of the processing) and the system administrator.

Such transfers are legitimate since they are necessary for the legitimate performance of the tasks covered by the competence of the recipient.

Regarding the deployment of the cards, another transfer of data takes place. DG INFSO implemented the changes of cards in one general step by sending a list of the people for whom the cards have to be changed and by receiving the corresponding cards. The EDPS understands that the cards prepared by the Security Directorate have been sent, for security purposes, to the Local Security Officer of DG INFSO. The EDPS recommends that the Local Security Officer does not keep the listing(s) of people associated with the flexitime number of the card. Indeed, the situation existing in the flexitime application is different from the security purpose attached to the other number of the card, which is meant to control access to the building. In the case of flexitime, access to the flexitime number of the card has to be limited to the relevant persons of DG INFSO and the local security officer is not one of them. DG INFSO should therefore ensure that the LSO does not have this list. This recommendation is also applicable in the case of lists of new users.

The EDPS also understands that there will be no data transfer outside of the Commission. The data collected in the flexitime application is not accessible by anyone outside the Commission.

3.7 Processing of personal number or unique identifier

Article 10(6) of the Regulation provides that "*the European Data Protection Supervisor shall determine the conditions under which a personal number of other identifier of general application may be processed by the Community institution or body"*. The present opinion will not establish the general conditions of such a use of a personal number, but consider the specific measures necessary in the context of Flexitime.

The EDPS already clarified the status of the RFID chip number in the current processing. The identification number associated to the RFID chip is personal data covered by Regulation 45/2001. Indeed, this identification number when used to record a staff member's behaviour and linked to the personnel number (which means linked to the name of a person, as it is the case here), makes the processing fall under a processing of personal data, which requires compliance with the data protection principles.

The use of the personal number has already been analysed in the prior checking of SYSPER2 Tim management. The badge number will be necessary because the personal badge will be used to clock in/out via the use of the badge readers. The badge number and the personal number should co-exist in the Flexitime system for practical reasons. For the case in hand, the use of the staff personnel number for the purpose of recording data in the system is reasonable considering that this number is used to identify the person in the system and thus helps ensure that the data are accurate.

3.8 Right of access and rectification

Article 13 of Regulation (EC) No 45/2001 establishes a right of access- and the arrangements for exercising it- upon request by the data subjects. Article 14 provides for a right of rectification of inaccurate or incomplete personal data.

The prior checking notification and the supplementary information submitted by the controller describe the possibility of access to and mention the possibility of rectification of personal data by a staff member.

Regarding access, the EDPS welcomes the distinction by DG INFSO between two categories of data: the identification data and the data specifically linked to flexitime. Identification data

are linked to SYSPER 2 and can, when needed, be changed following the procedure relating to this system (see the prior checking opinion on SYSPER 2 - TIM module, mentioned above). This access by the data subjects is only authorised with a login and password. This login and password are based on the European Commission Authentication Service (ECAS), which is also used to access other Commission's applications. The data subjects (users of the application) could access, verify and, if necessary, correct their data.

As concerns data linked to the flexitime application, the data subjects use the SYSPER 2 - TIM module (themselves or via the line manager or the gestionnaire) to access, verify and, if necessary, correct their personal data. Therefore, if the line manager agrees to individual access, staff members can correct/complete the time registrations themselves within a time period of 6 days via the SYSPER 2 - TIM module. After that period, or if the line manager opted for a centralized approach, the corrections/completions need to be requested to the line manager or a designated gestionnaire.

Taking into consideration both the right of correction and blocking, the EDPS considers that in certain occasions, the right of rectification of the data (Article 14) is exercised jointly with the right of blocking of these data (Article 15), for example when the data subject disputes their accuracy. Article 14 of the Regulation stipulates that "*the data subject shall have the right to obtain from the controller the rectification without delay of inaccurate or incomplete personal data*". During period which allows the controller to check the accuracy of the data, these must be blocked (at the request of the data subject).

In his opinion of 29 March 2007 in the case of the TIM module integrated in SYSPER 2, the EDPS agreed with a solution which is also applicable in this case.
Similar to the TIM module integrated in SYSPER 2, the data blocking inside the DG INFSO flexitime application could only be applied in a selective way as a complete blocking would obstruct the totality of the data processing. DG INFSO explains that each time a blocking is requested to prove the facts, DG INFSO will be able to take a "photo" of the data by means of a printout, a backup or a CD Rom the same way as in SYSPER2 - TIM. Two copies are made available, one for the requesting person (complainant) and one for the data controller.

As explained in his prior checking case on SYSPER 2, the EDPS can accept this solution only because it is for evidence purposes (Article 15.1.b and 15.1.c of the Regulation) and because the IT consequences of modifying SYSPER 2 so that it can block data selectively cannot be implemented at present. Blocking would have indeed in this case the consequence to affect even more the data subject.

In the case of the blocking procedure, the EDPS would like a third copy of the printout, backup or CD Rom to be made available to the DPC of DG INFSO. Indeed, in the case of a complaint, it would facilitate his/her intervention.

The EDPS notes that, according to the notification Article 20 of Regulation 45/2001 is not to be applied, in principle, in the context of this data processing operation.

In conclusion, the EDPS considers that the conditions of Articles 13 and 14 of the Regulation are met.

3.9 Information to the data subject

Articles 11 and 12 of Regulation (EC) 45/2001 list information that must be provided to the data subjects. These articles list a series of compulsory items and another set of information.

The latter are applicable insofar as, taking into account the particular circumstances of the treatment in question, they are necessary in order to ensure a fair data processing with regard to the data subject. In this case, part of the data is collected directly from the data subject and another part from other people.

Article 11 (*Information to be supplied where the data have been obtained from the data subject)* should be observed in the present case. Staff members will personally click in and out in the system, thus data subjects provide the data themselves.

Article 12 (*Information to be supplied where the data have not been obtained from the data subject)* should also be observed as the list of identification information is retrieved from SYSPER2 about DG INFSO staff members.

Data subjects are informed by the following instruments:
- Guide for flexitime (Administrative Notice No 62 of 21.12.2006 SEC(2006)1796)
- Communication of the Commission on the use of flexitime in the Commission services SEC(2006) 956 of 19.07.2006
- A specific privacy statement for flexitime at DG INFSO, on-line on the home page of the application where everybody could read it.

The draft of the specific privacy statement, annexed to the original notification, has been replaced by another privacy statement in the course of the analysis of the processing operations and contains most of the dispositions of Articles 11 and 12 of Regulation No 45/2001.

The privacy statement is entitled: "*specific privacy statement for IT flexitime registering application in DG INFSO*". The EDPS believes that the use of the term "registering" is not accurate as the flexitime application is a system in itself and not only a registering function. So, the privacy statement does not refer only to the registering but also to the application which processes and acts as a buffer for the TIM Management Module. This specific privacy statement is an additional privacy statement to the general privacy statement about Flexitime (from DG ADMIN) to which the staff of DG INFSO is also entitled

However, in this particular case, insofar as such information is necessary to guarantee the fair processing and considering the specificities of this technology and the concerns it can create, the EDPS advises to provide the following additional information:

- Modify the reference which is made to the EDPS Opinion as regards the wording "who delivered a favourable opinion" and replace it by "who delivered an opinion." The EDPS would also appreciate, in view of transparency, that the privacy statement contains a link to this opinion ;
- For completeness and given the possibility for Heads of Units to delegate their rights to a "gestionnaire" within the Unit, the EDPS would like this category of persons who can be recipient to be added in the privacy statement, together with the Data Controller and System Administrator ;
- As explained on the point 3.1 above, delete the sentence: "*This is not related to any personal data*";
- Add a paragraph specifying clearly the people or categories of people of DG INFSO who are allowed to use the flexitime application (i.e. the staff members concerned) ;
- The draft of the specific privacy statement is not clear on the information which can be directly changed by the data subjects and the information for

any of their data registered via the DG Infso IT flexitime registering application can do it via their access to the SYSPER 2 - TIM module". It should be redrafted ;

- Following the EDPS recommendation on a third copy, the Data Protection Coordinator of DG INFSO should also be mentioned in the privacy statement of the system ;
- Mention whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply. For instance, the consequences of failure to clock in and out. By analogy with a questionnaire, the staff should be informed of the practical consequences to clock in and out and to failure to do so (i.e. report by writing in a paper file document) ;
- Mention the legal basis, besides the Guide to flexitime ;
- Mention the retention period of the audit trail of 2 months ;
- Add a specific paragraph on the blocking of data, pursuant to Article 15 of Regulation 45/2001, in line with point 3.8 of the current Opinion ;
- Add a paragraph on the right to have recourse at any time to the European Data Protection Supervisor.

3.10 Security measures

According to Article 22, 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.

Given the possible risks developed in the use of RFID embedded badges, the EDPS had a careful analysis of the security measures implemented.
[...]
After careful analysis by the EDPS of the security measures adopted, and given that the above recommendations will be implemented, the EDPS considers that these measures are adequate in the light of Article 22 of Regulation (EC) 45/2001".

Conclusion:

There is no reason to believe that there is a breach of the provisions of Regulation 45/2001 providing the following considerations are fully taken into account:

- The EDPS finds the inclusion into the flexitime application of staff members who are not using it but who are working in DG INFSO excessive and recommends that DG INFSO analyses the means and frequency of updates of the database and informs the EDPS on the outcome;

- The EDPS requests that the Local Security Officer of DG INFSO does not keep the listing(s) where staff members' names are associated with the flexitime number of the card;

- Regarding the procedure on blocking foreseen by DG INFSO (by way of a "photo" of the data by means of a printout, a backup or a CD Rom), the EDPS would also like a third copy be made available for the DPC of DG INFSO ;

- The EDPS considers that DG INFSO should implement the following changes to the draft of the privacy statement:

    - Delete the term "registering" in the title of the Privacy statement;
    - Modify the reference which is made to the EDPS Opinion as regards the wording "who delivered a favourable opinion" and replace it by "who delivered an opinion." The EDPS would also appreciate that the privacy statement contains a link to the opinion;
    - Delete the sentence: *"This is not related to any personal data"*;
    - The EDPS would like the category of persons who can be recipients (i.e. delegated controller) to be added in the privacy statement, together with the Data Controller and System Administrator;
    - Add a paragraph specifying clearly the people or categories of people of DG INFSO who are allowed to use the flexitime application (i.e. the staff members concerned);
    - Redraft the specific privacy statement on the information which can directly be changed by the data subjects and the information for which the data subjects must contact the system administrator to implement the changes;
    - Following the EDPS recommendation on a third copy, the Data Protection Coordinator of DG INFSO should also be mentioned in the privacy statement of the system;
    - Mention whether replies to the questions are obligatory or voluntary, as well as the practical consequences of failure to reply. For instance, the consequences of failure to clock in and out;
    - Mention the legal basis, besides the Guide to flexitime;
    - Mention the time-limits (retention period) of the audit trail of 2 months;
    - Add a specific paragraph on the blocking of data, pursuant to Article 15 of Regulation 45/2001, in line with point 3.8 of the opinion;
    - Add a paragraph on the right to have recourse at any time to the European Data Protection Supervisor.

About the security measures:

- The EDPS recommends that DG INFSO sets specific rules in order to define the people having logical access to the servers;

- The EDPS suggests clarifications on the persons who will have to ensure the role of Data Controller, System Administrator, delegated controller, by adopting a list of defined staff members and to have this list available at the DPC office. This list should, at least, define the quality of the person in charge. Moreover, the EDPS would like to suggest that those people be familiar with Data Protection issues;

.

- The EDPS recommends that DG INFSO reconsiders the decision taken in terms of technological choices through a new assessment, including a viable timetable to implement the change of technology, taking into consideration the choice of the best available techniques: In the interim period, full application of available possibilities within the actual technological choice has to take place as described in point 3.10 above;

- The EDPS advises, at least, to ensure that the minimum reading distance specified by the supplier between the reader and the chip is the one used in the system and that this reading distance can not be changed;

- The EDPS considers it important to differentiate, in ECAS, between the functions of the application relating to the staff member him/herself and the functions of the application relating to the flexitime system of other people under the staff member having advanced rights. Therefore, the EDPS would favour a solution requiring the implementation of a double identification while entering the application.

Done at Brussels, 19 October 2007

Joaquín BAYO DELGADO
Assistant European Data Protection Supervisor

Follow-up of 6 November 2007:

The European Data Protection Supervisor welcomes the fact that the Institution (DG INFSO) has implemented, as regards the security measures, an interim solution which is in accordance with his recommendation.