Opinion on a notification for prior checking received from the Data Protection Officer of the Council on the Flexitime System

Brussels, 19 January 2006 (Case 2004-258)

1. Proceedings

1.1. On 13 September 2005, the EDPS received by post a notification for prior checking by the Data Protection Officer of the Council of the European Union concerning the prospective introduction of FLEXITIME, an IT system designed to collect and store information by automated means on the working hours, supplementary working hours, and absences of the staff the General Secretariat of the Council (GSC). The notification included several documents:

- Staff Note 2/82 of 04 January 1982 from Secretary-General on adjustment of working hours,
- Staff Note 41/03 of 26 March 2003: Working Hours - Information on the position of the Appointing Authority's representatives,
- Staff Note 19/04 of 17 February 2004: Flexitime - Information on the outcome of the consultation,
- Framework contract on the development, delivery, and installation of software and hardware and the granting of licences to use software products for the Flexitime Information System and the provision of related support and maintenance services and additional development services (contract CUE-DTI-2005/12),
- Conseil de l'Union Européenne - Projet Flexitime- Spécifications Techniques,
- Projet Flexitime- Étude Technique, Problématique, SSO/Active Directory,
- Projet Flexitime- Politique de backups. Version of 23/08/2005,
- Projet Flexitime- Interface Accréditation -Flexitime. Analyse de situation et Proposition de solution. Version of 23/08/2005,
- DTI Security Convention for remote intervention,
- Flexitime- Notification de Traitement des Données à Caractère Personnel - Annexe II: Description Générale des Mesures de Sécurité. Version of 31.08.2005,
- GSC of the EU: Annex 1: functional and technical specifications of the flexitime system and support and maintenance thereof. Tendering specifications (UCA-096/04) for framework contracts (Services) (August 2004).

1.2. On 10 October 2005 additional information was requested from the Controller via the DPO of the Council. On 17 October 2005, the EDPS received a document called "Specifications Fonctionnelles Detaillees des Interfaces" by electronic mail and other pieces of information. One document " Sur l'intégrité des données," sent by the Controller to the EDPS has never arrived at the EDPS office.

On 28 October, on 03 November and on 10 November 2005, additional information was requested from the Controller.

On 11 November, further to the previous question of the EDPS, the controller confirmed which personal data will be imported and exported from the different databases into the central system of flexitime.

On 28 November 2005, the EDPS received an additional document on "Demande d'intégration. Numéro de matricule et Active Directory" via the DPO of the Council of the EU.

On 29 November 2005, the EDPS received by electronic mail the document "Sur l'intégrité des données," which the EDPS was waiting for and never arrived by regular mail, although the Controller sent it. The document was re-sent by the Controller by electronic mail.

On 30 November 2005, the EDPS requested the DPO of the Council to organise a meeting in the context of the prior checking of the Flexitime system with the Controller and the representatives of the technical services responsible for the project (Flexitime meeting). Initially, the date for the Flexitime meeting was fixed on 8 December; however, it had to be postponed until the 15 December 2005.

On 1 December, the EDPS received information on previous questions related to the pilot project. On the same date, additional Staff notes (200/05, 88/05) were sent to the EDPS by the DPO of the Council.

On 2 December 2005, the EDPS received responses to questions asked before and some supplementary documents ("Ecrans information sur l'agent", and other informatico- visual print screens information) from the Controller.

1.3. On 15 December 2005, in the final phase of the prior checking procedure, a meeting took place in the Council's premises between the EDPS (Mrs Eva Dimovne Keresztes, Mr Laurent Beslay, Mrs Sophie Louveaux and Zoi Talidou, stagaire) and representatives of various units responsible for the Flexitime project at the GSC (Mr Jean-Marie Vandeputte - head of unit Administrative solutions (DGA 5), Mr Bruno Massez - Administrative solutions unit (Secretariat), Ms Encarnación Quesada Blánquez - Administrative solutions unit (Central applications, Infrastructure), Ms Mieke Libbrecht - Administrative solutions unit (Applications du Statut), Mr Benjamin Moya Murcia - Personnel management unit (DGA 1 B)) and Mr Plouzeau, on behalf of the external company, GFI; and Mr Pierre Vernhes, DPO of the Council and Ms Gabriella Lodi, assistant to the DPO.

The aim of the meeting was to have an overview of the functioning of the system in the form of the presentation by the GSC and to enable the EDPS to ask for further clarification on those points which the EDPS found less elaborated or contradictory in the documentation at his disposal but which were important for the delivery of the prior checking opinion. The meeting focused on three main themes: technical specifications of the system, interfaces with other databanks and the pilot project. Until the meeting took place between the GSC and the EDPS, the prior checking procedure was suspended.

1. Examination of the matter

1.1. The facts

Objective and general overview of Flexitime system:

Flexible hours has already been in use for years, on an informal basis, in certain sectors of the GSC, particularly in the language and secretarial departments of DGIII. After the informal use of non automated flexitime, the GSC will extend flexitime rules to a broader number of staff. At the time of writing the prior checking opinion, the Appointing Authority has not made the final decision yet on the scope of the staff members to whom flexitime rules will apply; however, in the current stage of planning, as foreseeable, flexitime rules will apply to officials and other

servants referred to in the Staff Regulation (except, maybe, special advisers which would mean 5 persons) and to national experts. Flexitime rules will apply neither to stagiaires (they could only record presences/absences) nor to personnel of external firms (consultants).

The GSC creates an automated system to manage Flexitime rules. Using flexible hours will be an option: "The existence of flexitime does not force staff to depart from normal working hours. On the contrary, officials who wish to work normal hours (...) will have the right to do so." Normal working hours as a main rule will be one of the possible variants of flexitime, but in that case the recording system will thus apply. (Point 3 and Annex to CP 41/03). As staff notes emphasize, the purpose of introducing flexitime is to contribute both to modernising of the working conditions and to improving human resources management within the GSC. It is designed to enable staff to achieve a better balance between their private and professional life within the framework of a transparent and fair system which aims to promote equal opportunities. Flexitime is also designed to enable the institution to manage attendance more effectively in accordance with work requirements and to manage human and budgetary resources-including overtime-more efficiently (Staff note 88/05, CP 41/03,).

Flexitime system offers individuals an opportunity under specified conditions to follow a personal working timetable and enjoy the flexibility margin which enables them to reclaim a certain number of hours worked in excess of normal working hours (37,5 hours/week). Examples of the flexibility elements of the new system are: building up a credit up to 25 hours worked beyond normal working time, claiming up to 15 hours of the credit per month as time off, and to be allowed a debit of up to 10 hours bellow normal working time. The number of staff present and the flexibility margin is calculated by an electronic recording system. Officials will be granted special compensation for working at weekends, on public holidays or for long hours, and time off for health reason in certain circumstances. Due to the computerised system, individuals can monitor their hours worked and the supplementary hours to be compensated from their computer screen.

An internal regulation, which is in drafting stage at the time of writing the prior checking opinion, will specify flexitime rules.

Flexitime information system includes the use and recordings of the working hours by the badge readers, and the use of intranet managing leaves and absences.

The badge recording:

Officials/servants of the GSC will be recording their working hours in a central information system (flexitime system).

Officials/servants will record their working hours by clocking in and out using their personal badge at one of the badge readers that will be installed near entrances to the buildings. On a normal working day each staff is required to have at least four recordings: clock in, clock out for lunch, clock in after lunch, clock out. When clocking in and clocking out using the personal badge of staff members, the badge reader registers the identification of the badge, the identification of the badge reader and the start/finish time and sends it to the central flexitime information system. The system automatically calculates the working hours and updates the personal flexitime balance.

The personal service card already required for access to the building will also serve as the flexitime badge, with the access (security) and flexitime components remaining separate at the level of databanks, at the level of badge readers, and at the level of software. The only common

element between the flexitime system and the security system will be the currently used personal badge.

Use of Intranet managing leaves and absences:

Officials/servants will be required to set up an individual timetable. Based on this timetable and the recordings of leave in the flexitime system, the system will generate an overview of resource availability. Individual timetables are established on a 4-week basis, but the accounting period for calculation of overtime compensation is one calendar month.

Officials will be able to submit requests for time off (holidays, flexi-leave, special leave or recuperation of overtime and compensatory hours) in the flexitime system. The immediate superiors must validate these requests, after which the requests will be sent to the Leave Office for processing.

All electronic recordings within the framework timetable (7:00-20:00) will be automatically validated if the total hours worked (not including lunch) are up to the maximum length of a flexitime day (9 hours). All other recordings are exceptions or requests and need to be validated electronically in the flexitime system by the immediate superior of the staff member involved. Examples of recordings that need to be validated and authorised by the immediate superior:

- individual timetables;
- working hours outside the framework timetable (7:00-20:00);
- requests for leave;
- requests for correction;
- working hours that lead to compensation for working overtime;
- working hours at weekends or on public holidays;
- working hours that lead to compensation for working long hours (longer than 12 hrs at a stretch);
- request for time off for health reasons.

The immediate superiors have the possibility to decline a request or recording. The system notifies the staff member of any recordings that have been declined by the immediate supervisor. The staff member then can amend his request.

If a staff member is unable to perform his/her duties owing to illness or accident, he/she must notify his/her immediate superior. In case of an absence with a medical certificate, the staff member has to send this certificate to the secretariat of the Medical Service who will record this absence in the flexitime system. In case of an absence without a medical certificate the staff member has to enter a manual recording of the absence into the flexitime system when he or she returns to the office. This recording is subject to validation by the superior.

In certain cases, not only the immediate superior, but also the Leave Office is involved, as a second tier, in checking and validating data of staff. For example: After validation by the immediate superior, the Leave Office may perform checks and validate requests for annual leave, special leave or compensatory leave. If the Leave Office finds errors, they will inform the staff member and agree on corrective measures. After this second validation, the requests for leave are entered in the Congés system where the annual leave entitlement or the personal balance for compensatory hours are updated. The staff member can view the status of his/her requests in the flexitime system. Requests for leave that are validated by the Leave Office are automatically recorded as actual leave in the flexitime system. Another example is the case when staff manually has to enter an absence without medical certificate into the flexitime system when he/she returns to the office. This entry needs to be validated not only by the

immediate superior, but also by the Leave Office which checks the conformity to the rules (maximum 3 days in a row and maximum 12 days per calendar year). If the absence is not in conformity with the rules, the Leave Office will contact the staff member to regularize the situation.

Manual entries and corrections on the GSC intranet will be possible (subject to validation by local managers). Manual recordings into the system may take place in various instances, which require validation by the immediate superior: if a badge is broken or has been lost, the staff member enters a manual recording of working hours in the flexitime system; or in case training takes place outside of the Council's buildings; staff member on mission should submit manual recording for travelling and working hours on a mission; in case of an absence without a medical certificate the staff member has to enter a manual recording of the absence into the flexitime system when he or she returns to the office.

System maintenance information and data processing:
The responsibility for the maintenance of master data in the flexitime system will be assigned to the office that will be responsible for the administration of flexitime within the GSC. The following master data will be maintained: Users, Security settings, Public holidays and office closure, Flexitime rules.

Data processing will take place on two levels: 1) on central level, the Leave Department will cooperate with the informatics service; and 2) on local level, the superior in charge (head of unit) or, in certain cases, the manager of the unit to whom that power is delegated.

The Flexitime information system will be managed by hardware installed in the premises of the Council of the EU and a software package designed for the purposes of Flexitime. An external company has been carrying out the development, delivery and installation of software and hardware for the Flexitime Information System, and will provide the support, maintenance and additional development service (as a result of a procurement procedure). A possibility of remote interventions [...] by the authorised staff of the external company to the Council's premises is granted. The scope of remote access/intervention is related to maintenance and operations of the installed system, for which the contractor has full operational responsibility. The option of remote intervention is aimed to allow for urgent and 24 hours x 7 days intervention on the system in case of operational malfunction.

Pilot project:
At the time of writing the prior checking opinion preparatory measures related to the Flexitime Information System are under way. As foreseeable from spring 2006 a pilot project will be launched by the GSC for a limited time period with the aim of testing the system in actual situations. Volunteering officials from various units covering around 350 persons will participate in the pilot project. The pilot test will include the use and recordings by the badge readers, and leave administration and leave request made via Intranet. The pilot test involves the Organigramme and the ARPEGE system. The same security measures designed for the Flexitime system will be applied during the pilot testing. The test phase will be preceded by an information phase where officials will be informed about the respective staff notes (CP 41/03 and 19/04), information sessions will be organised, the 45/2001 (EC) Regulation will be distributed, and they will be informed about their rights under section 5 of the 45/2001 Regulation. It is to be noted that during the pilot project the traditional paper registration of working hours and leaves and the use of Flexitime IT system will take place in parallel, meaning that the same information will be recorded twice, on paper and in addition in the IT system. The administrative decision has not been passed whether data related to working hours and leaves

originating from the pilot project will be kept once the Flexitime system will be in operation and, if it is retained, for what purpose.

The exact timing of launching the full-scale operation of Flexitime Information System depends on the results and assessment of the pilot phase.

It is to be noted that even after launching the operation of Flexitime system, the data from the traditional administration of leaves and absences will continue to be kept for an undefined period, until it is seen necessary.

Purposes of processing personal data:

The purposes of data processing are: registration and management of working time and presence; calculating rights to leave and controlling the takings of leave; placing and following the leave request by intranet; calculating automatically the overtime and exceptional working hours. Although not mentioned in the prior checking notification, capacity planning is also a purpose. The "Tendering specifications" state: "Each department manages the attendance of its workforce in accordance with its responsibilities, taking account of its main operational connections. The flexitime system will support the heads of department and the immediate superiors by offering the possibility of creating an overview of the planned and actual attendance of staff members based on the individual timetables and the recordings of leave." (Point 4.5.2. of Tendering specifications).

Aside form management purposes, evaluation purposes are also present. This view is supported by Point 5 of Staff Note 41/03 (26.03.2003) explaining that: "Recording is no more than a necessary instrument for managing flexitime in an appropriate way. *It should not be seen as a sign that the Administration mistrusts officials or wishes to check on their activities and attendance. The introduction of the system could indeed bring to light any irregularities or abuses in performance. That is normal and beneficial.* For all that, however, recording is not designed to function as a repressive system". Furthermore, absence records will eventually also be used when every two years a special committee proposes promotion. In this context absence records will constitute part of the evaluation process. The prior checking notification mentions "qualification" among the data to be processed. A working document[1] mentions an import of persons who can be promoted ("import des personnes pouvant être promues") from the ARPEGE system and to store that list. The list will not be visible in the application.

Types of data involved:

It is to be noted that at the time of writing the prior checking opinion, no final decision has been made on the exhaustive list of personal data that will be processed.

According to the prior checking notification, the central information system processes the following types of data:

- Information on staff member: name; first name; personal number; address; e-mail address; link to organisational part of GSC; part-time/full-time (taux d'activité); entry date; exit date; category; grade; qualification; statute; birth date; right to overtime.
- Information relating to badging: date, hour, arrival/departure and place of origin of badging (sens et origine du pointage).
- Working hours.

[1] Page 19 of "Spécifications Fonctionnelles Détaillées des Interfaces".

- Information relating to absences, training, missions: date/time of start; date/time of end; total duration; motive.
- Results of calculation: working hours, breaks, remaining days of leave.

In the course of the further inquiries made by the EDPS during the prior checking procedure, the EDPS received the information that the following data will also be processed:

- Sex, seniority rate (date d'ancienneté), NUP identification, badge identification, place of origin, telephone number (work).
- Absences due to health reason will be recorded by three types of code: absence with/without medical certificate, and special absence (e.g.: illness of family member).

The "working documents" (not final versions) that the EDPS has received describe a broader scope of personal data to be processed by the Flexitime system. During the Flexitime meeting it was clarified that those "working documents" are samples and some of the categories of data described there will not apply to the Flexitime project (like *zone scolaire*, civil status, nationality, children's personal data including their handicap). The EDPS will make a point on that in the data quality part of the opinion. (See part 2.2.3)

Linking databases

Flexitime system consists principally of 1.) the badge readers which records the entries and departures of the staff members on the basis of the badge number, and 2.) IT application which make possible the management of working hours.

The creation of Flexitime system involves a number of databases: ARPEGE (Human resource management), Congé (Registration and management of leave and registration of overtime), Organigramme (Organisational database), Paie (NAP- New Payroll System), Babylon database (the entries to the building are here recorded with the access control) and IDE Carte system (responsible for making the badges).

The system imports administrative data from the "ARPEGE" system. The aim of the interface is to create a "personal file" of the individuals in the central information system. ARPEGE contains information related to the staff necessary for handling personnel affairs. Flexitime will import from ARPEGE the following data: personal data: surname, first name, date of birth, place of origin; professional data: personal number, seniority rate (date d'ancienneté), status, category. The ARPEGE system will communicate on a daily basis with Flexitime to create/amend the personal files as soon as possible according to the modifications carried out in ARPEGE. It does not provide sensitive information (like health data).

Leave balance (soldes des congés) and supplementary hours will be a unique importation of data from the Congé system at the time of launching Flexitime.

The Flexitime information system will interface with Organigramme, and will import data on the organisational structure ("libellé de l'entité", level in the structure), the attachment of the person within the organisation (personal number, entity of attachment) and the attachment of every person to a superior for the purpose of validating the leaves (personal number of the staff and the superior, entry date into service). These data will be imported daily. The aim of the interface is to attach the individual to the organisational structure in the flexitime application and also to update it in case an individual's attachment changes or to re-attach group of people if the structure of the organisation changes.

An interface with Active Directory will be put in place. The GSC uses Active Directory for the management of the access to the IT resources by the user. The personal data involved are: login, password, telephone number, email. For the purposes of Flexitime system it is proposed by the GSC to add the personal number to the data which feeds Active Directory. (See in part 2.2.8. Processing of personal number or unique identifier for more details) From the beginning of the project, the GSC urges the integration of Flexitime application with the annual Active Directory, in order to 1) allow flexitime users to use the same "login and password" that they use at the opening of the Windows session, so as to simplify the work of the users; and 2) solve certain security weaknesses of the "password and login" system. And, there are around 3000 users for that application, it is important 3) to rely on an automatic integration of the new officials' data (login, password, email, telephone number, office number and *personal number*) because the system works with multiple interfaces and, as a consequence, there is a risk of having inconsistencies -that work was already done in Active Directory-; and 4) to have an automatic and integrated update of the data mentioned, taking into account the existing flow of personnel in the GSC and the variable character of certain data (new personnel, staff on pension, temporary staff, modifications in the telephone number, modifications in the mailing address, etc).

The interface from the Flexitime to the "Paie" system concerns principally the transfer of data related to the supplementary hours to be paid. The interface concerns: the NUP code, period, *taux* and the name. The Flexitime system automatically calculates hours which may give rise to compensation. If those hours are duly validated by the immediate superior, the system exports them to the Leave Office. The Leave Office enters the acquired compensatory hours in the Congés system. Data exportation will take place on a monthly basis.

Information systems related to the badges are involved by the creation of the central information system of Flexitime: Babylon database which registers the arrivals into the building and controls thus the access, and IDE Carte system which is responsible for making the badges. In the IDE Carte system the bagde number, the personal number and the abbreviated name are introduced manually, and without any validation mechanism. This system keeps the pictures that are shown on the badges. There is no connection, no verification whatsoever between Babylon and IDE Carte.

Personal badge related databanks are involved because the personal badge will serve as Flexitime badge. The badge readers will identify the staff member, at the time of clocking in/out. Therefore the badge numbers are fed in advance in the Flexitime system. A unique connection is created between the badge number and personal number in the Flexitime system.

Inaccurate and unreliable personal data should be corrected in the databases responsible for the personal badge. See also description in "Accuracy of data" part for more details.

Data transfer automatically takes place between the various databanks (ARPEGE, Paie, Flexitime), and can not be influenced by the users.

Accuracy of data

Ensuring data accuracy (consistency of badge number and personal number) before the launching of the system and once it is in operation:
The establishment of flexitime system will require the accuracy of personal data registered in all databases. Actually, in the IDE Carte system the badge number may not be accurate (badge number recording is reliable only in the Babylon system) and, as in the IDE Carte database the recording of the personal number takes place only manually and without validation by the

ARPEGE system, various administrative alternatives are considered to ensure accuracy of personal data and to exclude errors or omissions**.**

The proposed solutions by the Unité Solutions Administratives are the following:
- Before the system will be operational, a massive load of badge numbers and personal numbers of civil servants who are already in service is mandatory. To that end, the errors of the current IDE carte system will be corrected. For that aim, many reports identifying errors and missing information will be provided to the accreditation service.
- For the subsequent and daily incorporation of badges of the new civil servants as well as for the replacement of defective badges, it is suggested to use a specific option of Flexitime application; this option is exclusively reserved for authorized accreditation personnel.

When the making of a new badge is necessary, the complete name of the person and his personal number would be already available, at Flexitime level, through the ARPEGE database. Before delivering the new badge, the accreditation personnel will encode the personal number or the name in order to conduct a search of the civil servant in question and, if everything is correct, the accreditation personnel will insert the badge number that is associated to him.

This procedure aims to ensure a better data quality because the introduction of incorrect personal numbers is avoided and, as a consequence, this guarantees that civil servants are always identified by Flexitime and there is an immediate recognition of entries and departures associated to a new badge from the moment it is made. (Information as of 23.08.2005 from the document: Projet Flexitime. Interface Accréditation -Flexitime. Analyse de situation et Proposition de solution.)

In practical terms, this means that in the preparatory phase the following measures take place: loading the personal number and the badge number in the IDE carte system; verifying the personal numbers with the Congé service; correcting the anomalies in the IDE carte system; verifying the badge numbers with the Babylon system; correcting the anomalies in the IDE carte system; final loading of the data. Once the Flexitime system is in operation, there will be direct connection to the system and all information will immediately be put in the Flexitime system. Both the uploading and correction of data will take place via a special screen.

Access to information in the system

General description:

The access to and the usage of a specific elementary functionality of the system will be assigned to a specific user by the means of a specific elementary right. These elementary rights can be grouped within a profile. Based on the function/role of a specific user the flexitime administrator assigns one or more user profiles to that user. Access rights will be assigned to the various user profiles during system setup.

The access authorisation to the system will be implicit by the assignment of different user/manager profile in order that a user can not access data other than his/her own data, a manager can not access data other than that of the staff in his/her unit. Only the Leave office (Service congés, which will be renamed in the future as "Service Gestion du temps") will have access to all data of the entire staff, which is actually the case.

At least the following user profiles can be distinguished: flexitime administrators, normal staff members, staff members in the Leave Office, Staff members in the secretariat of the Medical Service and immediate superiors or heads of departments. Access to information in the system is restricted and provided according to operational requirements.

Access by officials:
Each official can have access to his "personal" balance at any time. As a rule, regular staff members can only see, change or update their own recordings. Each official has access to an on-screen programme through Intranet where he can view his updated "balances": hours worked, flexibility credits/debits, holyday allowance, overtime, etc. The official will also be able to have a computer "dialogue" with his immediate superior, for example to confirm a request for leave or to correct recorded information.

Access by managers/superiors:
Access to information in the system is restricted and provided according to operational requirements. Departmental heads, for example, will be able to access the necessary information on the working hours and attendance of their staff.

The information that managers will receive concerns: planning, badging, absences, anomalies, regularisation.

Superiors will be able to search for the employees under their responsibility by their name or personal number, but they will not be able to search for a group of individuals based upon search criteria, for example officials working certain hours in excess.

Managers will not be able to access personal data contained in the "personal file" of the staff member created in the central flexitime system.

Every manager (as a main rule, the head of unit) will have access to the data of the personnel under his responsibility. Managers will use a secret code.

Managers will have their access rights only until they serve in their post.

Beside using the broad term of "managers" the background documentation mentions various particular categories of "managers" with access rights to the information of staff processed by the Flexitime system. Examples: *immediate superiors* will validate recording of travelling and working hours on mission, manual recording of absences without a medical certificate, individual timetables.[2] Flexitime system supports the *heads of departments and the immediate superiors* by offering the possibility of creating an overview of the planned and actual attendance of the staff members based on the individual timetables and the recordings of leave.[3]

The manager can delegate the execution of a task (but not the responsibility) in case of his/her absence for the good pursuit of the system. The mechanism to ensure a good functioning of that procedure is under examination. The managers of the system will be designated by decision of the Deputy Secretariat General. The list of managers has not been determined yet.

Access by the Leave administration service:
Only one unit, *Service Congés de l'Unité "Gestion des doits" (*Leave Department) will have access to all personal data of all staff members within the central Flexitime system to manage leave administration. The information that the *Service Congés* will receive is the name of new agents introduced in the system, supplementary hours and the follow-up of absences, in certain cases. This Leave Department will also assist the evaluation process of flexitime rules after a year has passed since the start of the operation of Flexitime system.

[2] Tendering Specification, Section 4.3.1. and 4.3.4 and 4.5.1.
[3] Tendering Specification, Section 4.5.2. Capacity planning.

Reporting mechanism, monitoring:
It is planned that anomalies statistics and trends can be monitored via a reporting mechanism. Depending on privileges (elementary rights and profiles) assigned to the specific user, that user will have access to a certain number of reports. The extent of the report will vary according to these privileges (individual information, information for a group or a team). As the controller specified in more detail (as response to the request for supplementary information), every manager (as a main rule, the head of unit or the one having delegated power due to e.g. absence of the head of unit) will have access to the data of the personnel under his responsibility by the use of a secret code. Only one unit of the "Congés" service *(Service "Congés" de l'Unité "Gestion des doits")* will have access to all personal data of the staff members.

The information should *interalia* help the Appointing Authority to review the flexitime system after one year of operation and to re-examine some of the details. Examples of these reports are:

- Average flexitime credit or debit per staff member;
- Number of times recording lunches has been forgotten;
- Number of times requests for flexi-leave are entered afterwards;
- Range of starting times and finish times;
- Developments in the starting and finish times;
- Developments in number of working hours per staff member per day;
- Recordings outside the individual timetable with a margin of 15 minutes;
- Recordings outside the normal working hours;
- Recordings outside the framework timetable;
- Recordings outside the maximum flexitime day;
- Recordings outside the maximum working days;
- Recordings of working hours on weekends and public holydays;
- Individuals that forgot to clock out;
- Individuals that forgot to clock out for lunch in a given period;
- Number of days absence through uncertified illness;
- Hours worked over and above the maximum credit which did not give rise to compensation.

In the Flexitime meeting, it was explained, that these reports are not intended to evaluate individual conduct of the staff member, rather to assess flexitime rules in the form of general reports and eventually to adapt the flexitime rules according to the findings. That evaluation will be done through anonymous statistics.

Corrections/rectifications

Staff will be able to request a correction of working hours recorded, if duly justified. All requests for correction are sent to the immediate superior for validation. Once the immediate superior has validated the request, the working hours and personal balances are updated accordingly. Corrections of working hours can also be made by the superior, the Leave Office or the secretariat of the Medical Service. These corrections are then automatically validated by the system.

In some cases correction of data will occur in cooperation between various competent units: Requests should be submitted for annual leave, special leave or compensatory leave in the flexitime system for approval by the immediate supervisor. After validation by the immediate supervisor, the request for leave are automatically sent to the Leave Office. The Leave Office performs a number of checks and validates the requests for leave in the flexitime system. If the Leave Office finds any errors, they will inform the staff member and agree on corrective actions.

After this second validation the requests are entered in the Congé system where the annual leave entitlement or the personal balance of compensatory hours are updated.

The arrival and departure data recorded by the badges can neither be modified nor deleted. The system does not have a correction mechanism which could detect such abuses like a recording by someone else's badge. Beyond the possible disciplinary measures in case of manifest abuse, the manager always has the possibility to make certain corrections at the justified request of the user. Examples where the manager can make corrections: forgotten badge, or validation of certain anomalies which are justified (for example: in case of surpassing the framework hours for reasons of the service).

Data concerning the individual timetables can be modified by the person concerned or by his/her manager. Manual recording of arrivals and departures are different, because there is no badge-identification**.** When an exceptional arrival or departure requires a correction, the information sent via the badge reader (badgeuse) will remain marked in the database.

Personal data coming from the ARPEGE (GRH) is not modifiable. The users can not influence the automatic data processing from ARPEGE to Flexitime and from Flexitime to Paie system. In case an error occurs or some data are missing, the person concerned should contact the "Congés" service, which is responsible for taking the necessary measures to correct the data in the ARPEGE or Paie system and to send the corrected information to Flexitime.

In certain instances, "correction" takes the form of re-submitting and re-calculating data. For example: compensatory allowances for working overtime are calculated on a monthly basis. Staff members in certain categories and grades (the ones that are entitled to compensation or remuneration for working overtime) need each month to submit their overtime for validation by their immediate superior and processing by the leave office. Upon submitting the recorded overtime, the staff members can indicate whether they want these hours to be compensated (time for time) or whether they want remuneration (money for time) for the hours overtime. After submission the recorded overtime is sent to the immediate superior for validation and then to the Leave Office for processing. A staff member whose compensatory allowances have been processed should no longer make any corrections or recordings for previous periods. If corrections are necessary, compensatory allowances must be resubmitted and recalculated.

Information to be supplied to data subjects:

Providing information about the operation of flexitime is envisaged by various means to the staff and agents, including communications to the personnel and training sessions.

An internal regulation is under elaboration. This internal regulation will explain in more detail how staff can access or rectify their data, the remedy mechanism, etc.

Participants in the pilot will receive information about their rights as data subject, Regulation (EC) 45/2001 will be distributed and training sessions will take place.

Conservation

Data concerning the recording of working hours and absences will be kept for 5 years from the date of badge recording in the system and for longer period if required in case of litigation.

Conservation period for personal data in the central system other than working hours and absences, like category, grade, attachment, address, is not defined.

No data storage period is provided for personal data relating to absences and leaves recorded and kept in the traditional leave administration system (which will exist parallel with the Flexitime system for an undefined period of time).

There is no decision yet whether to conserve and for how long data recorded and processed during the pilot project.

Security

A username and password will be required from users to log on to Flexitime information system. Access to the system is restricted, depending on the role of the individual concerned. Managers will have a special code to enter data of staff under their responsibility. As it was confirmed during the clarification meeting, this action can only take place inside the GSC domain and not remotely. Various security measures are envisaged to guarantee the integrity, confidentiality and availability of Flexitime system.

2.2. Legal aspects

2.2.1. Prior checking

The prior checking notification implies the processing of personal data as defined in Article 2 (a) of Regulation (EC) No 45/2001 ("any information related to an identified or identifiable natural person").

Flexitime system processes personal data of staff of the GSC in the employment context under Community law; therefore it clearly falls under the scope of Article 3 (1) of Regulation (EC) 45/2001.

Moreover, the processing of personal data wholly or partly by automatic means is subject to Regulation (EC) 45/2001 according to Article 3 (2), which is the present case, because the creation and operation of the information system of flexitime involves automatic processing, but at some instances manual recording into Flexitime system may also take place. As those manual data form part of a filing system, they fall equally under Article 3 (2) of the Regulation.

Article 27 (1) of Regulation (EC) No 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". Article 27 (2) of the Regulation contains a list of processing operations that are likely to present such risks. Among those are processing operations intended to evaluate personal aspects relating to data subject, including his/her ability, efficiency and conduct (Art. 27. (2) (b)); processing of data relating to health (Art. 27(2) (a)); and processing operations allowing linkages not provided for pursuant to national or Community legislation between data processed for different purposes (Art. 27.2 (c)).

Personal data processed by the Flexitime system falls under the scope of Art. 27 (2) b). Attendance and leaves in the workplace constitute conduct of the official. The processing of data concerning working hours and absences by the flexitime system is meant to make possible the evaluation of the conduct of the staff members in the context of employment, including its use in the promotion procedure.

Flexitime information system concerns the recording of sick leave, as well. As sick leave may reveal elements about the health status of the data subject,[4] Article 27(2) (a) applies.

Article 27(2) (c) provides for prior checking of processing operations allowing linkages not provided in national or Community legislation between data processed for different purposes. "This provision is intended above all to avoid data collected for different purposes being linked. The risk of linking data is that quite different information may be deduced by means of the link, or the original purpose be distorted. Linkages not provided for under national or Community legislation thus entail certain risks with regard to data protection where the end purposes differ."[5] In the present case links between databases are created: ARPEGE, Organigramme, and Active Directory will feed the central information system of Flexitime, and Flexitime will send personal data to the Paie system. These linkages are not a priori provided for under national or Community legislation.

ARPEGE is the human resource management databank, and necessary administrative data are imported from there on a daily basis. The linkage with Organigramme implies importing data about the organisational structure, attachment of the person in the organisation and attachment to the superior. The link with Active Directory will concern connection identifiers (see below, 2.2.8.).

The recording of working hours, leaves and absences constitutes a narrower purpose within the broader sense of human resource management by the ARPEGE system or data processing for administrative purposes by Organigramme or Active Directory. This overlapping means that no specific risks due to linkage are at stake in this case and, therefore, the linkage in itself, although subject to analysis, is not specific ground for prior checking.

The EDPS has received the notification sent by regular post by the DPO on 13.09.2005. On 10 October 2005, request for additional information was made. The period of two months for prior checking was suspended from that date. The final date when the EDPS has received all information requested previously was 2 December 2005. However the fixing of the date of the Flexitime meeting on 30 November 2005 maintained the suspension until the Flexitime meeting took place on 15 December 2005.

According to Article 27(4) the present opinion must be delivered within a period of two months, which would lead to 14 November 2005. The period was suspended for 66 days (between 10 October- 15 December) and thus postponed the date to deliver the opinion not later than 19 January 2006.

The prior checking opinion of the EDPS will be limited to the examination of the Flexitime information system, and will not take position regarding the content or fairness of Flexitime rules or their applicability to the officials of the GSC.

2.2.2. Legal basis for and lawfulness of the processing

The legal basis for the data processing regarding working hours may be found in Article 55 of the Staff Regulations of officials of the European Communities, which specifies the general conditions related to the duty of the officials in active employment to be at the disposal of their institutions (normal working week: max. 42 hours) and gives the institutions the power to decide

[4] See Case 2004-277. "Recording of absences of ECB staff members unable to work because of illness or accident" (Point 2.2.1.); and Case 2004-278 on the "SIC Congés" system- ECJ (Point 2.2.1. and 2.2.3.)
[5] See Case 2004- 319, Skills Inventory- Council (Point 2.2.1)

on the hours of the working days and to lay down rules for the detailed application of the paragraph. Staff Note 2/82 regulates working hours applicable as from 4 January 1982 and Staff Note 41/03 provides information on the position of the Appointing Authority's representatives on the aims and details of flexitime system. Staff Note 88/05 constitutes a reminder of the key points of the new system. At the time of writing this opinion, an internal regulation is under drafting procedure concerning flexitime. It will lay down flexitime rules in the form of a binding legal instrument.

The scope of Flexitime system, as it is created by the Council, will not solely relate to working hours, but will concern administration of absences and leaves as well, and will count and transfer data on supplementary hours to be paid or compensated. Thus, provisions of the Staff Regulation concerning overtime (Art. 56), special allowances (Art. 56.a-56.c), annual leave (art. 57), sick/pregnancy leave (Art. 58& 59), and absences (Art. 60) also constitute legal basis of the processing operation. As Flexitime also includes the use of data for promotion evaluation, Article 45 of the Staff Regulation is also to be considered the legal base for that purpose. Therefore, the EDPS recommends including in the internal regulation under elaboration references to the relevant sections of the Staff Regulation.

Analysis of the legal basis and analysis of lawfulness of processing go together. Article 5 (a) of Regulation (EC) 45/2001 says that processing is lawful, among other grounds, if it is the "*legitimate exercise of official authority vested in the Community institution."* The GSC, as Appointing Authority, exercises the power to fix the framework for working hours, to develop a system for recording working hours, absences and leaves of its staff members. The processing of personal data of GSC staff members by Flexitime information system constitutes legitimate exercise of the official authority vested in the Council of the EU. The legal basis provided by Article 55 and the respective provisions of the "Working conditions of officials" of the Staff regulation confirms that the processing is lawful.

2.2.3. Processing of special categories of data

According to Article 10 of Regulation 45/2001, processing personal data concerning health is prohibited unless grounds can be found in Article 10 (2) or 10 (3).

Although sick leave records in the Flexitime information system are coded as leave "with/without medical certificates", they are data concerning health as they reveal information about the data subject's state of health.

Article 10 (2) (b) stipulates that the ban on processing sensitive data does not apply if " processing is necessary for the purposes of complying with the specific rights and obligations of the controller in the field of employment law insofar as it is authorised by the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof." Since the ground for processing sick leave data in the Flexitime database can be found in Article 59 of the Staff Regulation, they may be deemed necessary to comply with the rights and obligations of the controller.

2.2.4 Data Quality

Data must be *adequate, relevant and non excessive* in relation to the purposes for which they were collected and/or further processed (Article 4.1.c).

The data processed by the Flexitime system, as they were presented in the meeting with the Council, in general, seem to be relevant and adequate.

The EDPS however would like to point out that the exact place of badging (appearance of the badge reader number in the central system, accessible by the superior) may be excessive for the purpose. Providing evidence about attendance in certain buildings (because of being on training, for example) is not within the purpose of the system and, if the data are accessible by the superior, it may lead to location "surveillance" by the employer over the employees. Therefore, the EDPS recommends the GSC to reconsider whether processing information about the origin of badging (*sens et origine du pointage*) is strictly necessary for administering working hours and absences.

The EDPS would like to draw the attention to the fact that some of the personal data contained in the "working documents" would be far too excessive for the purposes of recording working hours, leaves and absences. Although it was clarified on the Flexitime meeting that those data do not apply to the Flexitime project, the EDPS makes the point that recording and processing of "*zone scolaire*"[6], or nationality[7] would be excessive for the purposes of administering working hours, leaves and absences, because those data would fall under the broader context of human resource management. Those data can not even be regarded as strictly necessary administrative data serving the purpose of identification.

Personal data of dependents or relatives (like handicap of the child or sickness of the child, for example) may give ground for leave or allow different work-hours regime (part time). As a general guideline, the EDPS would like to note that only particular situations of medical reason can result in the processing of relatives' personal and sensitive data in the Flexitime system and only for the purposes of administering working hours/ leaves to the extent it is necessary for that purpose. Article 10 allows processing those data, only with those limitations.

Data must be *processed fairly and lawfully* (article 4 (1) (a) of Regulation (EC) No 45/2001). The lawfulness has already been examined and fairness is related to the information to be given to data subjects (see below, 2.2.10.)

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 were further processed, are erased or rectified"* (Article 4 (1)(d) of the Regulation).

The use of personal number, which will facilitate the linking of different databases, serves the aim to eliminate data inaccuracies which could occur in the central information system, if the other databases feeding the central system 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.

Correction of anomalies and inconsistencies in the IDE carte database is designed to ensure data quality by the time of launching the Flexitime system.

The EDPS recommends that personal data originating from the pilot project will be kept and further processed in the Flexitime system only if data accuracy and quality is ensured. The parallel recording of working hours and absence in a traditional paper form is an appropriate way to ensure data accuracy and quality. It is especially important because the pilot project will test the functionality of the system and data inconsistencies and inaccuracies may occur.

[6] "Ecrans d'informations sur l'agent."
[7] Page 11 of "Specifications Fonctionnelles Detaillees des Interfaces".

The rights of access and rectification of the data subject to his/her own data are means of guaranteeing the accuracy and ensuring that his/her data are kept up to date. (See also "right of access and rectification"- 2.2.9.)

Data integrity is safeguarded by backup policies and also by the various measures being put in place in case an error occurs in the software, materials or servers.

2.2.5. Conservation of data/ Data retention

Personal data must be kept in a form which permits identification of data subjects for not longer than is necessary for which the data are collected and/or further processed. (Article 4(1)(e)). Article 4 (1) requires that when data are stored for longer periods for historical, statistical or scientific use, personal data should be kept either in anonymous form or the identity of the data subjects should be encrypted.

As a main rule, conservation of the data on working hours and absences in the Flexitime system would last for 5 years, save the case of litigation, where there is no specified time-limit for data retention.

Data conservation as a general rule for 5 years can be appropriate if it meets the time limit within which recordings on working hours and absences can be contested or revised and if it takes into account rights of data subjects which originate from those recordings. Therefore, 5 years of data conservation period may be appropriate provided that this time frame is set up in the light of the deadlines regarding available correction, complaints and remedy mechanism.

The EDPS already laid down some guidelines. Keeping data on days of annual leave can be justified if leave is carried over from one year to the next, but not beyond the year after that.[8] "Keeping data on sick leave for at least three years is justified by the implementation of Article 59 (4) of the Staff Regulation. This view is confirmed by the fact that, when a person is transferred to another institution, only data on sick leave in the previous three years are forwarded. After these three years, there is some doubt as to whether keeping the data is justified. In any event, the data should be deleted at the latest at the end of the period during which they can be contested or revised".[9]

A data conservation period should be fixed regarding the traditional records on working hours and absences in the Conges system. It should concern not only the parallel existence of Flexitime system and the former leave administration records, but also the unique importation of leave balance and supplementary hours from the traditional system into Flexitime.

The controller should provide for a period of data retention regarding personal data, other than recording of working hours and absences, processed by Flexitime system, like previous data - when they have changed- on attachment within the organisational structure, grade, category and necessary administrative data coming from the ARPEGE system. The conservation period should not be longer "than is necessary for the purposes for which the data are collected and/or further processed."

In case data originating from the pilot project will be kept, the Controller should provide for a data conservation period taking into account the above mentioned position.

[8] See Case 2004-278 on "SIC Congés" system-ECJ (Point 2.2.5.)
[9] See Case 2004-278 on "SIC Congés" system-ECJ (Point 2.2.5.)

The EDPS draws the attention that in case anomalies, statistics and trends will be monitored in order to help the Appointing Authority to review the flexitime system after one year of operation and to re-examine some of the details (See "Access to information in the system" part), the statistical use of personal data in relation to working hours would require as necessary steps to render data anonymous. In any even, those data shall not be used for any purpose other than for statistical purpose. (Article 4 (1) (e))

2.2.6. Compatible use / Change of purpose

Data are transferred from different databanks to the central information system of flexitime. The aim of data processing is to manage flexitime rules, administer working hours and absences via an automated system. The processing operation under analysis involves no general change of the specified purpose of the various databases affected and is not incompatible with that purpose. Thus Article 4 (1)(b) is fully respected.

2.2.7. 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 the tasks covered by the competence of the recipients."*

The linking of the databanks constitute technical tools to facilitate transfer of personal data between various services (leave department, human resource, immediate supervisor, paie system). This processing is necessary for the legitimate performance of exercising employment related tasks within the competence of those units: granting authorization for overtime hours, monitoring leaves, human resources planning in the narrow sense, and compensating overtime.

The EDPS considers that this sharing of information is *necessary for the legitimate performance of tasks covered by the competence of the recipients.*

In the Flexitime system different users will have different access rights (e.g.: hierarchical superiors, leave department). The controller must define precisely the roles and responsibilities of every user in relation to the criterion of necessity to perform their tasks. Users should have access only to data which can be reasonably required to perform their tasks. Only data strictly necessary to perform the tasks defined can be accessible by the users having access to the system.

These guidelines should be taken into account when managers are designated. It should be precisely defined, within the five levels of management in the organisation of the GSC, which superior (e.g. immediate superior, head of unit) can have access to what personal data of the staff members under his/her responsibility. The scope of the access to officials' data should be the strictly necessary and not excessive to perform the legitimate task of a manager covered by his/her competence.

It should be guaranteed that personal data will be accessible only for those authorised to receive the data. Safeguards should be provided for the mechanism through which managers can delegate their rights of access to staff data (e.g. because of the illness of a manager).

Guarantees must be provided that persons accessing data in the central information system may not use them for purposes other than those compatible with the purpose of the Flexitime system..

2.2.8. Processing of personal number or unique identifier

Article 10 (6) of the Regulation stipulate 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 present opinion will not establish the general conditions of such an use of a personal number, but consider the specific measures necessary in the context of Flexitime.

The GSC intends to use three identifiers in the Flexitime system. 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. Since all relevant databases use the personal number as unique identifier, the use of personal number will facilitate the flux of data from the ARPEGE, Organigramme and Active Directory to the central information system. The use of personal number will also provide for consistency and accuracy of data in the databases involved.

The EDPS received a request to give his opinion on adding the personal number to the Active Directory.[10] The request was justified by several reasons, some already expounded above in part "Linking databases". In addition it was noted that the "login" and "password" exist only in Active Directory. This means that once the user connection is authentified in Active Directory, it is necessary to attach to it an identifier, which will make the link with the Flexitime database. The personal number would be that identifier. All databases of the Administrative Solution unit are based on the personal number. The proposal of the unit means that the personal number will be visible and used only in the Flexitime system with a technical restriction, to which solution the EDPS has no objection in the light of the documents presented and in the light of the Flexitime meeting.

As planned the Flexitime system will use the NUP code to transfer data from the central database to the Paie system. Some documents at the disposal of the EDPS indicate that the Paie system is also based on the personal number (Page 2/4 of Projet Flexitime. Interface Accreditation-Flexitime. Analyse de situation et Proposition de solution. Version du 23/08/2005) It seems to be unnecessary to keep all three identifiers of the staff members in the central database, if data transfer can be realised by using the personal number. The EDPS would like the controller to reconsider whether the use and processing of the NUP code is strictly necessary for the data transfer from the central flexitime system to the Paie system. In case, data transfer can take place in a reliable way by the use of the personal number, it might be a preferable solution.

2.2.9. Right of access and rectification

Article 13 of the Regulation (EC) No 45/2001 makes provision -and sets out the rules- for the right of access of the data subject. Article 14 of Regulation (EC) No 45/ 2001 allows the data subject a right to rectification. These rights are guaranteed by Section 5 of the Council Decision of 13 September 2004 "*adopting implementing rules concerning Regulation (EC) No 45/2001 of the European parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data"*, published in Official Journal L 296 of 21 September 2004. Section 5 of the Council Decision on the procedure for data subjects to exercise their rights lays down general

[10] Flexitime. Gestion du temps flexible. Demande d'integration. Numéro de matricule et Active Directory.

conditions as well as data subjects' right of access, rectification, blocking, erasure and right to object. Reference is also made to notification to third parties, automated individual decisions and exceptions and restrictions.

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

The EDPS suggests that the internal regulation under elaboration refers not only to Article 13 and Article 14 of the Regulation (EC) No 45/2001, but also goes in line with Section 5 of the Council Decision of the procedure for data subjects to exercise their rights.

2.2.10. Information to the data subject

Article 11 deals with situations where information has been obtained from the data subject, and Article 12 where information has not been obtained from the data subject. Both situations apply to the present case.

The EDPS welcomes the fact that extensive consultation took place in the GSC to inform staff about the planned introduction of the Flexitime system and several staff notes provided the updates about the project on behalf of the Administration.

At the time of drafting this opinion, there is an internal regulation under elaboration in the GSC regarding the information and procedures as to how staff members can exercise their rights as data subjects.

The EDPS suggests that each staff member concerned receives information on his/her rights as data subject and the respective procedures to exercise those rights on an individual basis (in the form of an email message, for example) and that the instrument is made permanently available on-line (via Intranet) to grant accessibility to the information to the staff members concerned at any given time. Beside the information required obligatorily under Article 11 and 12 of the Regulation, the EDPS recommends especially the following information to be made public in the same source or in any other appropriate mean in order to ensure fair processing:
- the notice that automatic transfer of personal data will take place between various databanks,
- the legal basis of the processing operation for which the data are intended,
- the time-limits for storing the data,
- the right to have recourse at any time to the European Data Protection Supervisor.

The information on the time-frame of the conservation of their data is especially important, so that staff members can foresee the consequences and they are enabled to contest or revise the records.

Information to the data subjects should be provided in an appropriate and comprehensive form.

2.2.11. Security measures

Article 22 and 23 of Regulation 45/2001 requires the controller and the processor to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of personal data protected. These security measures must in particular prevent any unauthorized disclosure or access, accidental or unlawful destruction or accidental loss, or alteration, and to prevent all other forms of unlawful processing.

Article 35 of Regulation (EC) No 45/2001 requires from a Community institution to take appropriate technical and organisational measures to safeguard the secure use of telecommunications networks and terminal equipment. These measures should ensure a level of security appropriate to the risk presented.

Given the scope of the planned data processing operation, strict security measures must be put in place in accordance with the Regulation.

The EDPS welcomes that a separate document describes in a written form how the controller meets its obligations.

Remote intervention/access to the Council's network is permitted for the external company with the aim of correcting malfunctioning of the system. The supplier has to pay a compensation in case of unavailability of the operational services for certain number of hours under the condition specified in the contract.[11] The EDPS considers that remote interventions from contractor's premises to the Flexitime system by the external company, for the purposes of acting rapidly in case of malfunctioning of the system, can be justified under strict conditions. Section 4 (1) of the DTI Security Convention for Remote Intervention requires that "all tasks must be carried out in a physically protected environment with logically protected information technology equipment, which the Secretariat of the Council of the EU may inspect on request."[12] [...]

As to the rest of security measures, after careful analysis the EDPS considers that they are adequate in the light of Article 22 and 35 of Regulation (EC) 45/2001.

2.2.12. Processing data on behalf of controller

Article 23 lays down the requirements when processing takes place on behalf of the controller: choosing a processor with sufficient guarantees in respect of technical and organisational security measures; processing operation being governed by a contract or legal act binding on the processor and stipulating that the processor can act only if he/she received instructions from the controller; and Articles 21 and 22 obligations being also incumbent on the processor. For the purposes of keeping proof, the parts of the contract or legal act relating to data protection and the requirements relating to the measures referred to in Article 22 shall be in writing or in another equivalent form.

Processing of data can take place on behalf of controller, either when the authorised staff of the external company has remote access/intervention to the network of the GSC and come across personal data of the staff, or if the external company sub-contracts all or part of the supplies, services or work to third parties.

In the contract between the subcontractor and the Council it seems that there are no provisions relating to the security obligations of the subcontractor (articles 21 and 22 of the regulation (EC) 45/2001), nor any specifications as to the fact that GFI can act only on instructions of the Council. The EDPS recommends that this be included in the core text of the contract.

Conclusion:

[11] Article 13.5 of the Framework contract , p 10.
[12] Page 5/27 of DTI Security Convention for Remote Intervention. Version 1.00- 29/03/2004

The proposed processing operation does not seem to involve any breach of the provisions of Regulation (EC) No 45/2001, as long as account is taken of the observations bellow. This means in particular that:

- References to the relevant sections of the Staff Regulation should be included in the internal regulation under elaboration as legal basis of data processing

- It should be reconsidered whether processing information about the origin of badging (badge reader number, *sens et origine du pointage)* is strictly necessary for administering working hours and absences or to provide evidences in this context.

- Personal data originating from the pilot project can be kept and further processed in the Flexitime system only if data accuracy and quality are ensured.

- Data retention period on working hours, leaves and absences should be set in line with the period within which recordings can be contested or revise or within which period interests and rights of data subjects may be affected.

- A data conservation period should be provided for personal data on leaves, absences and working hours in the traditional leave administration system (Congés system).

- A limit on the length of time that data are kept should be set in the light of the purposes for which the data are processed, both regarding "traditional files" kept the Congés service (parallel to the operation of Flexitime) and regarding the data originating from the pilot project, if they are kept.

- The controller should provide for a period of data retention regarding personal data, other than recording of working hours and absences, like previous data -when they have changed- on attachment within the organisational structure, grade, category and necessary administrative data. The conservation period should not be longer than necessary..

- If data are kept for statistical purposes, they must be rendered anonymous or encrypted.

- The controller must define precisely the roles and responsibilities of every user in relation to the criterion of necessity to perform his/her tasks. Users should have access only to data which can be reasonably required to perform their tasks. Only data strictly necessary to perform the tasks defined can be accessible by the users having access to the system.

- It should be precisely defined that in the organisation of the GSC, which manager can have access to what personal data of the staff members under his/her responsibility. The scope of the access to officials' data should be the strictly necessary and not excessive to perform the legitimate task of a manager covered by his/her competence.

- It should be guaranteed that personal data will be accessible only for those authorised to receive the data.

- Safeguards should be provided for the mechanism through which managers can delegate their rights of access to staff data.

- Guarantees must be provided that persons accessing data in the central information system may not use them for purposes other than those compatible with the purpose of the Flexitime system.

- The NUP code should be used for processing operations from the central flexitime system to the Paie system, if transfer can not be facilitated otherwise by the use of the personal number.

- The internal regulation under elaboration should refer not only to Article 13 and Article 14 of the Regulation (EC) No 45/2001, but also it should provide in line with Section 5 of 2004/644/EC (Council Decision) of the procedures for data subjects exercising their rights.

- Each staff member concerned should receive the information on his/her rights as data subject and the respective procedure to exercise those rights on an individual basis (in the form of an email message, for example) and the legal instrument describing those rights should be made permanently available on-line (via Intranet) to grant accessibility to the information to the staff members concerned at any given time.

- Data subjects should be informed as required by Articles 11 and 12 of the Regulation, including the fact that data transfer will take place between various databases, the legal basis of the processing operation for which the data are intended, the time-limits for storing the data and the right to have recourse to the EDPS.

- Information to the data subjects are provided in an appropriate and comprehensive form.

- [...].

- In the contract between the subcontractor and the Council, provisions should be included relating to the security obligations of the subcontractor (articles 21 and 22 of the regulation (EC) 45/2001), and specifications as to the fact that GFI can act only on instructions of the Council.

Done at Brussels, 19 January 2006

Peter HUSTINX
European Data Protection Supervisor