Guidelines concerning the processing of personal data in the area of leave and flexitime

EDPS 2012-0158

These guidelines ("**Guidelines**") are issued by the European Data Protection Supervisor ("**EDPS**") in the exercise of the powers conferred on him in Articles 41 (2) and 46 (d) of *Regulation (EC) No 45/2001 on the protection of personal data by European institutions and bodies* ("**the Regulation**").

The content of these Guidelines is based on the existing EDPS positions in the area of leave and time management system (Flexitime) consisting of several Opinions on the respective data processing operations by several EU institutions and bodies (See Annex).

The Guidelines cover the processing of personal data in the management of all entitlements for sick leave, annual leave and in general all special leave[1] in the related working conditions of Officials, Temporary Agents (TA), Contract Agents (CA) and Seconded National Experts (SNE). The Guidelines also include an analysis of flexitime processing operations[2]. The Guidelines cover the processing of this data by administrative services in the EU bodies and institutions. Therefore, it does not cover the corresponding processing of data by the medical services; such processing of data is covered by the EDPS Guidelines concerning the processing of health data in the workplace by EU (formerly Community) institutions and bodies[3].

[1] Leave covers annual leave, sick leave and the following special leave (as describe in Annex V to the Staff Regulations): Adoption of a Child, Adoption of a Disabled Child, Change of Residence, Consultation Outside of Work (more than 65 km), Court Summons, Death of Parents in-Law, Death of Relative, Death of Spouse, Death of Spouse during Maternity Leave, Death of a Brother/Sister, Death of a Child, Elections, Exams/Competitions, Health Cures, Irregular Absences (Leave Office use only), Marriage, Marriage of a Child, Maternity, Military Obligations, Other Reason, Outside Activities (art. 12b), Serious Illness Parents in-Law, Serious Illness of Relative in Ascending Line, Serious Illness of Spouse, Serious Illness of a Child, Training, Very Serious Illness of a Child.

[2] The goal of any flexitime policy is to make the working methods more flexible in order to make it easier to reconcile the demands of private life and work. 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 can also be 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.

[3] Guidelines concerning the processing of health data in the workplace by Community institutions and bodies: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/09-09-28_Guidelines_Healthdata_atwork_EN.pdf.

The main objective of the Guidelines is to offer guidance to all EU institutions[4] and bodies in the processing of personal data by their administrative services in the frame of leave and flexitime procedures. In this regards, the Guidelines also serve to assist Data Protection Officers (DPOs) and data controllers in notifying leave and/or flexitime related data processing operations to the EDPS for prior checking where relevant.

The structure of the Guidelines follows closely the one which is used in the notification form for prior checking. The DPO network has been consulted on the draft Guidelines on 29 September 2012.

1. PRIOR CHECKING

Article 27(1) of the Regulation sets forth that 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" are to be **prior checked by the EDPS**. Prior checks serve to determine whether such processing of data is planned by an EU administration in compliance with the Regulation, or whether the system needs to be improved from a data protection point of view.

1.1 Leave

- The processing of data on leave may imply the processing of data relating to health (e.g. medical leave, maternity leave, and some other types of special leave) and therefore falls under **Article 27(2)(a)** of the Regulation which requires prior checking by the EDPS of "processing of data relating to health".

As to the concept of data relating to health, the EDPS defined it in his Guidelines concerning the processing of health data in the workplace by EU institutions and bodies[5]:

> "*Health data generally refers to personal data that have link with the health status of a person This would normally include medical data (e.g. doctor referrals and prescriptions, medical examination reports, laboratory tests, radiographs), as well as administrative and financial data relating to health (e.g. medical appointments scheduling, invoices for healthcare service*

Although links exist between these two Guidelines, it must be noted that the Guidelines on health data relate mainly to the processing of medical data in the context of pre-recruitment and annual check-up and that only references are made to leave when health related data are processed. On the contrary, the Guidelines on leave and flexitime focus on all the categories of leave and do not limit themselves to the processing of health related data. Therefore, they must be considered as complementary but different Guidelines.

[4] It must be noted that some EU institutions and bodies (i.e. the European Central Bank, the European Investment Bank) are not subject to the EU Staff Regulation and the conditions of Employment of Other Servants, as they have their own statutory labour and social security law framework, which are quite similar in terms of civil service law concept but there are also differences. Therefore, elements that differ are underlined in the Guidelines, if necessary.

[5] See point on "concepts" of the Guidelines concerning the processing of health data in the workplace by EU institutions and bodies adopted on September 2009, available on the EDPS website.

provision, indication of the number of days of sick leave, sick leave management)".

Therefore, even if medical information is kept separate from administrative information, in the case of recording of leave, the EDPS' position has been to consider that processing of personal data relating to health occurs nonetheless. Thus the respective processing operations have to be prior checked by the EDPS.

- In some other cases, when data concerning attendance and leave in the workplace are processed to assess the conduct of the official, prior checking would be required under **Article 27(2)(b)** of the Regulation. This is especially true when the processing of data concerning leave allows the evaluation of the conduct of the staff members, including the use in the annual evaluation and/or promotion procedure. In such case, the EDPS would need to analyse the processing operations not only if the evaluation that takes place is explicitly foreseen in the procedure, but also if taking into account of all the elements, the processing is "intended" to evaluate.

For instance, the EDPS would also assess a procedure on leave which does not foresee any form of evaluation but which evaluation can be deducted from the other elements of the procedure (reporting having consequences on the annual evaluation report, promotion procedure, etc...).

- Finally, the processing may be covered by **Article 27(2)(d)** of the Regulation for those processing operations where there is administrative follow-up of unjustified absences owing to illness and which leads to a reduction in leave entitlements and/or withholding of pay, which constitute '*processing operations for the purpose of excluding individuals from a right, benefit or contract*'.

1.2 Flexitime

The initial purpose of Flexitime is to facilitate the conciliation of the obligations of the private life and the professional life of the staff of EU institutions/bodies. For this purpose, EU Institutions/bodies may allow their personnel to distribute unevenly the 37½ hours per week over the five working days, while fully respecting the provisions of the Staff Regulations and the interest of the service. Moreover, and within certain limits, previously accumulated time-credits maybe recuperated in various forms (per hour, half or full days).

By doing this, the EU institutions/bodies intend to increase the motivation of their personnel while making them more responsible for the organisation of their working time.

In principle a flexitime system is not subject to prior-checking[6] if:

[6] The EDPS also took the view in case 2007-0063 that Commission's DGs as well as agencies that follow DG HR (previously ADMIN) directions on Flexitime are covered by its general notification, whilst still retaining local responsibility. Only if a DG or agency were to use a system that differed from the general Commission notification, would it have to notify separately the aspects of its system which are different from the one established by DG HR and would have an impact on data protection.

- the purpose is an efficient use of human resources (planning and resource allocation) / budgetary resources and does not explicitly include the evaluation of staff, their conduct, efficiency or
- flexitime data is not processed in the staff appraisal procedure and the structure of the system does not imply a clear *risk* of use for the purpose of evaluation.

Furthermore, if Human Resources services would like to use flexitime data for further purposes (identification of excessive workload, evaluation) this must be clearly stated as a specific purpose of the processing operations. Besides, given the initial purpose of a flexitime system, the EDPS also considers that in view of the data that would normally be processed through a flexitime processing operation (i.e. individual report on time spent at work), HR services can not use this data as sole basis for evaluation/indicators of excessive workload of a staff member.

The following paragraphs examine the cases for which article 27 of the Regulation would apply and require prior-checking:

-**Article 27 (1)**: In principle, when RFID is used in HR related matters (like in a badge for a flexitime application), such application involves the processing of personal data. Even if the chip contains only an ID number, this number and all other data connected to it are personal data within the meaning of the Directive 95/46 and Regulation 45/2001, as this number is uniquely related to the data subject, i.e. the employee holding the badge[7].

When implementing a flexitime application making use of RFID technology, the data controller should take into account existing best practices[8], including the conduct of a data protection impact assessment[9] in order to assess privacy risks related to the application and should take appropriate technical and organisational measures to mitigate identified risks, by applying the principle of privacy by design. Where the impact assessment concludes that there are specific risks for the data subjects, the processing should be notified for prior checking to the EDPS.

[7] See PC 2007-0218 on "implementation of Flexitime - specific to DG INFSO" and 2008-697 on "implementation of Flexitime at the ETF".

[8] Guidance on data protection issues related to RFID has been given in several opinions of the EDPS and the Article 29 Working Party, such as Article 29 "Working document on data protection issues related to RFID technology", 19/01/2005 available on the Europa website, EDPS Opinion on the Commission RFID Communication 2007; EDPS Opinion on privacy in the Digital Age.

[9] For instance, Commission Recommendation C(2009) 3200 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification states under point 5 that operators of RFID applications should:

a) conduct an assessment of the implications of the application implementation for the protection of personal data and privacy;
b) take appropriate technical and organisational measures to ensure the protection of personal data and privacy;
c) designate a person or group of persons responsible for reviewing the assessments and the continued appropriateness of the technical and organisational measures to ensure the protection of personal data and privacy;
d) make available the assessment to the competent authority at least six weeks before the deployment of the application.

- **Article 27 (2) (a)**. If the flexitime system as a whole also covers the recording of sick leave, Article 27(2) (a) applies, as sick leave may reveal the health status of a data subject. However, it is only if the data processing at stake involves the processing of data relating to health on a regular basis, and not just on a purely occasional or incidental basis, that the need for prior checking under Article 27(2)(a) of the Regulation would be justified. If the processing only leads, for instance to the presence of the word "leave" on the timesheet, this would not be considered sufficient for the need of a prior-checking procedure.

- **Article 27 (2) (b).** In some cases, personal data processed by the flexitime system can fall under the scope of Article 27 (2) (b) when attendance in the workplace are used to assess the conduct of the official. This is especially true when 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, including its use in the annual evaluation and/or promotion procedure or if it is anticipated that the data gathered may also be used for purpose of evaluating a person in case there is suspicion of misconduct of the staff member. The EDPS stresses that this should apply whether the purpose of evaluating staff is *explicit* or *implicit* (the existence of an implicit purpose can be deduced from the objective characteristics of the system, e.g. existence of individual reports, conservation periods etc.).

- **Article 27 (2) (c).** It is possible that processing operations on flexitime also fall under Article 27(2)(c). This article provides for prior checking of *"processing operations allowing linkages not provided for pursuant to national or Community legislation between data processed for different purposes"*. This provision is intended above all to prevent data collected for separate purposes from being linked for a different purpose. By linking flexitime data with another system (for instance an access control system), linkages may be created and these linkages may not be provided for by national or EU legislation. In such case Article 27(2)(c) applies. It is the linkage of the processing operations which would be analysed in such situation, and not simply the flexitime processing operations.

In the event that such linkage is made for the purpose of the verification of flexitime clocking operations with respect to data on physical access checks, the EDPS has already considered that the necessity and proportionality of such processing operations were debatable and considered such linkage excessive. The EDPS is generally not in favour of systems that would have the purpose to combine the processing of personal data in the context of flexitime with the processing of personal data in the context of access controls for compliance/verification purpose. The EDPS considers that the institutions and bodies have other means at their disposal in order to identify members of staff who are failing to comply with the existing rules.

Finally, the EDPS draws the attention of the EU institutions and bodies to the fact that he is not in favour either of systems that would allow the processing of personal data for both purposes of flexitime and access control. Indeed, these processing operations are set by EU institutions and bodies for two distinct purposes (flexitime on one side and access control on the other side), the access to the data is limited to the relevant persons of the institution/body (most of the time HR staff for the Flexitime and the local security officer for the access control data) and the retention periods applicable to each processing operations are different.

2. LAWFULNESS OF PROCESSING

In the context of leave and flexitime, the lawfulness of the processing must be considered, in most of the cases, in the light of Article 5(a) of the Regulation which reads: "*personal data may be processed only if processing is necessary for the performance of a task carried out in the public interest on the basis of the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof or in the legitimate exercise of official authority vested in the Community institutions or body or in a third party to whom the data are disclosed*". In this regard, Recital 27 of the Regulation also states that "*Processing of personal data for the performance of tasks carried out in the public interest by the Community institutions and bodies includes the processing of personal data necessary for the management and functioning of those institutions and bodies*".

The legal base for the processing of personal data operations can be found in the Staff Regulations (SR):

Leave in general is covered under Chapter 2 of Title IV: Working conditions of officials of the Staff Regulations (Articles 57-60), applied by analogy to other servants of the European Communities, which are defined in Titles III & IV of the Staff Regulations:

- Annual leave (Article 57 SR), Special leave (Annex V SR), Maternity leave (Article 58 SR), Sick leave/family leave (Article 59 SR), Leave on personal grounds and unpaid leave (Articles 15, 37 and 40 SR) form the legal basis of these processing operations.

- Furthermore, Articles 11, 16 to 18, 58, 81 and 91 of the *Rules applicable to other servants of the European Communities* provide rights to leave for those individuals who are not covered by the Staff Regulations, but are nonetheless employed as temporary and contract agents.

- Finally, it may be possible that implementing rules of institutions and bodies adopted on the basis of Article 110 of the Staff Regulations provide for a further legal basis in the light of Article 5(a) of the Regulation.

The EDPS notes that the processing of personal data in relation to leave is considered as necessary for the performance of the institutions and bodies' obligations towards staff as provided by the above-mentioned rules. Therefore the processing of personal data carried out in this context would be considered as lawful in accordance with Article 5(a) of the Regulation.

- Article 55 SR forms the legal basis for flexitime processing operations, understood as working arrangements allowing staff to balance their professional and private life. Such working arrangement should also be reflected in a decision adopted by the institution/body on flexitime. In the case where an EU institution or body would like to adopt a procedure that would serve another purpose or other purposes, the EDPS considers that Article 55 would not be a sufficient legal basis and another legal basis would need to be adopted to reflect this different purpose.

3. PROCESSING OF SPECIAL CATEGORIES OF DATA

According to Article 10 of the Regulation, processing of certain sensitive data is prohibited except in certain predefined circumstances.

Article 10(1) of the Regulation states that *"the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and of data concerning health, or sex life are prohibited"*.

Article 10(2) of the Regulation provides a list of exceptions lifting the general prohibition of the processing of such data:

- In particular, Article 10(2)(b) states that *"processing is necessary for the purposes of complying with the specific rights and obligations of the data 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, or, if necessary, insofar as it is agreed upon by the European Data Protection Supervisor, subject to adequate safeguards"*.

In most cases, in the context of leave, the processing of certain health related data is considered as necessary in order to comply with legal obligations as laid down in Article 59, 60 and Annex V of the Staff Regulations and Articles 16, 58 and 91 of the Rules applicable to other servants of the European Communities. Therefore it is deemed necessary to comply with the rights and obligations of the controller in this matter.

This justification may apply in the following cases:

- processing of personal data related to health in the context of the sick leave may reveal elements relating to the health status of the data subject. Moreover, when a medical certificate is provided, the medical specialization of the doctor may potentially provide additional information on the health of the data subject.

Normally, data on the specialization of the doctor should only be sent to the medical service. However, in the context of a medical appointment during working hours, the data subject must usually provide to the person in charge of leave of his/her institution/body a certificate of presence and the specialization of the doctor may appear on this certificate. This situation would be covered under article 10(2)(b).

- processing of personal data related to health in the case of leave in connection, for instance, with the adoption of a disabled child, health cures, serious illness of spouse, and other types of special leave. Additionally, in case of parental and family leave, further processing of health related data takes place. Data which could reveal the sexual orientation of a staff member and his/her partner where he/she applies for leave to care for them or in the case of same-sex marriage are also processed.

- processing of personal data related to health in the framework of medical check for the purpose of sick leave control and management in case of absences. Staff Regulations, Conditions of Employment, as well as the respective Implementing Rules require processing of health related data in such case and are covered under article 10(2)(b).

4. DATA QUALITY

Pursuant to Article 4(1)(a), (c) and (d) of the Regulation, personal data must be processed fairly and lawfully, be adequate, relevant and not excessive in relation to the purpose for which they are collected and further processed, as well as accurate.

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

The EDPS considers it appropriate that no medical data should be contained in the attestation that may be sent to Human Resources by the Medical Service. It should only contain administrative data.

As he already underlined in the Guidelines on health data, the EDPS is aware that in some agencies no medical service has been set up and the agencies outsource the processing of all medical data to the Commission medical service or to an external service provider (i.e. external doctor). In such case, the EDPS refers to his recommendations made in the Guidelines on health data (paragraph 8).

Moreover, as a general rule, only necessary information should be processed.

For instance, if someone is asking for a special leave in view of taking part in a competition, many documents are required: the application form, the invitation to the examination and proof of presence the day of the competition. The EDPS considers that in the light of the Data Quality principle only the invitation and attestation of presence should be sufficient for such type of leave. This position is in line, for instance, with the European Commission Decision of 5 November 2010 on implementing provision on leave.

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 working-hours regime (part time). As a general guideline, the EDPS underlines that only specific legal obligations can result in the processing of relatives' personal and sensitive data in the leave/flexitime systems and only for the purposes of administering working hours/ leaves to the extent it is necessary for that purpose.

In the context of a flexitime system used with a badging system, besides the identification data, the EDPS considered it relevant to collect the ID numbers of staff members as well as their clock-in and clock-out time. Moreover, in any voluntary flexitime system, the EDPS emphasizes that the clock-in and clock-out data of staff

members who do not wish to participate in the flexitime scheme should not be processed.

Moreover, in terms of accuracy of the data, as already explained above, a flexitime system's initial purpose is set to balance professional and private life of staff members and it normally does not have as a specific purpose the detection of fraud. While the EDPS recognises the existence of a normal control by the superior of the accuracy of flexitime declarations introduced by staff, this should not lead to situations where staff members should need for instance to sign a presence register when the flexitime system that is used by the EU institution and body already allows the verification of the accuracy of the data by giving access to the immediate superior and the data subject to the flexitime data (Sysper2, for instance). Such procedure should be sufficient in order to ensure accuracy.

Accuracy: Article 4(1)(d) of the Regulation provides that data must be *"accurate and, where necessary, kept up to date"*. Moreover, this Article also states that *"every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified"*.

The EDPS also emphasizes that if request upon accuracy of the data is made by the data subject, this request should be recorded. Additionally, the data subject should have the right to access and the right to rectify (administrative) data so as to render them as accurate and complete as possible.

As to flexitime systems, the EDPS underlines that in order for the data to be accurate and up-to-date, the system in general must be designed in such a way as to ensure data accuracy and the updating of the data. In addition, to guarantee accuracy, the right to access to one's data for the purposes of verification by the data subject and the right to rectification must be respected.

Fairness and lawfulness: the data must be *"processed fairly and lawfully"* (Article 4(1)(a) of the Regulation). The lawful character of the processing must be ensured according to the lawfulness examined on point 2 above. Fair process means that relevant and complete information is forwarded to the data subjects (this point is examined below under Information).

5. DATA RETENTION

According to Article 4(1)(e) of the Regulation, personal data may be kept in a form enabling the identification of data subjects for no longer than **necessary** for the **purposes** for which they were collected or further processed. Further storage of data for historical, statistical or scientific purpose is possible in anonymous form only. As a consequence, the EDPS takes the view that there is no justification for keeping the data indefinitely, given the initial purpose of collecting it.

Moreover, as a general rule applicable to the disposal of records with financial link, on the basis of Article 49 of the Implementing Rules to the Financial Regulation "*Personal data contained in supporting documents shall be deleted where possible*

when those data are not necessary for budgetary discharge, control and audit purposes".

The EDPS insists that clear retention periods must be set forth for different types of absences and that these apply to both, on-line data and hard-copies or supporting documents.

The retention periods depend on the type of leave and vary in accordance with the purposes for which the data were collected and processed. Due to the specificities pertaining to the different types of leave, the following sections will examine the different types of data collected and processed for the respective type of leave in the light of guidance issued by the EDPS in his Opinions.

5.1. SICK LEAVE

The purpose of checks on absences due to illness is to ensure that the absence is justified.

In general, the EDPS has considered that a conservation period of at least three years for administrative data relating to sick leave can be justified for the HR by the implementation of Article 59 (4) of the Staff Regulations. This Article sets the rule that the Appointing Authority may refer to the Invalidity Committee the case of any official whose sick leave totals more than 12 months in any period of three years. However, the EDPS accepts the proportionality of a retention period exceeding the three years that would be strictly required[10]. Therefore, a longer conservation period by the HR could apply in order to cover periods when a dispute or an appeal is underway.[11]

5.2. ANNUAL LEAVE

Keeping data on days of annual leave can be justified if leave is carried over from one year to the next. Moreover, it is possible that an institution/body gives consideration to other leaves taken by a person in the immediately preceding years in view of better management and coordination. Therefore, as a reasonable conservation period and in view of aligning retention periods, the EDPS accepts a retention period that would not exceed three years for annual leave.

5.3. OTHER LEAVE

It is appropriate to retain data on part-time, parental and family leave until termination of employment with the respective institution and even beyond this period in cases in which any right of the data subject still persists or there is an ongoing appeal.

---

[10] See, for example, the EDPS Guidelines concerning the processing of health data in the workplace, page 12: "Article 59 (4) of the Staff Regulations could justify a conservation period of 3 years for data necessary to justify an absence due to sick leave. The only justification for keeping them any longer would be if a dispute or appeal were under way".

[11] The conservation of medical data by medical services is covered by the guidelines on health at work. If, however, an institution or body intends to keep for a longer period sick leave records that could relate to medical cases where the medical consequences of prolonged exposure to certain substances occurs after a rather long period (as can be the case for asbestos or radiation exposure), this should be specifically foreseen in the health data procedure submitted.

For instance, regarding family leave, data may be retained for the entire career of the person to keep track when the total time granted reaches the maximum permitted (Article 42(b) of the Staff Regulations).

Another example regarding leave on personal grounds, data are retained for the entire career of the person to keep track when the total time granted reaches the maximum permitted 15 years (Article 40(2) of the Staff Regulations).

Certain special leave, for instance in the context of credit-time have an effect on the calculation of the pension and require the conservation of the data for longer periods.

It is also possible that EU institutions and bodies have rules regarding financial compensation related to leave. In such case, with regards to payments in respect of leave not taken on termination of service or in the case where overtime can be compensated as paid time-off (compensatory payments in lieu of leave), the EDPS deems it appropriate to retain the data for up to 7 years at most. This conservation period is in line with the EU Rules applicable to the disposal of records with financial links. Thus, according to Article 49 of the Implementing Rules to the Financial Regulation, original supporting documents are to be kept for up to 7 years after the budgetary discharge. However, according to the same Article 49, personal data in supporting documents should be deleted as soon as they are not necessary for budgetary discharge, control and audit purposes.

5.4. FLEXITIME

Data on the flexitime schedule of employees may be retained only during the current calendar year. They should 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 of the following year.

However, in case the calculation of daily working hours is done at the level of the head of unit/sector and is based on intermediate statements, the raw data should be destroyed after the validation of the monthly assessment by the head of unit/sector taking into account the period during which staff can lodge a complaint, therefore the conservation should not be longer than three months at the latest.

If a flexitime system is implemented with the purpose to be used as a possible tool for the evaluation of staff or as a tool for obtaining workload indicators, not only will it have to respect the above mentioned conditions of legal basis and purpose limitation, but the conservation period will also have to be adapted to the purpose of the processing operations and be covered by the respective legal basis.

Flexitime data on staff members who leave the institution/body or of those members who wish to opt out of the flexitime scheme should be deleted within one or two months, as there is no justification for retaining them any longer, subject to the rights of the data subjects mentioned in the flexitime rules of the institution/body.

If the flexitime system is conducted via an electronic badging system, most of the time, the readers of the flexitime system will play the role of a buffer of time registrations before they are transferred to the leave application. In such case, considering the necessity to keep an audit trail of the registering of data, the EDPS accepts that all these data are stored for a maximum of two months.

6. DATA TRANSFERS

In his Opinions on the data protection aspects of leave, the EDPS has identified three possible types of transfers: within or between Union institutions or bodies (Article 7 of the Regulation).

6.1. Transfers under Article 7 of the Regulation

Transfers within or between Union institutions and bodies are in compliance with Article 7 (1) of the Regulation only if "*the **data** are **necessary** for the **legitimate performance** of tasks covered by the competence of the recipient*" (emphasis added).

The necessity of the transfer within Article 7 has been interpreted to mean that the recipient institution, body or agency must first "*establish that the transfer was indispensable*" for the performance of its tasks and duties.[12] Moreover, the transfer of personal data must respect Articles 4(1)(b) and 6 of the Regulation. Indeed, Article 7 is without prejudice to Articles 4, 5, 6 and 10. Thus, the transfer may not entail a change of the purposes for which the data were originally collected and processed. If the transfer, however, entails a change of purpose, it must be expressly provided for in law and the data subject should be informed of it. To fully comply with the Regulation, only relevant data may be transferred and once transferred, they may be processed only for the purposes for which they were transmitted.

In the framework of **leave**, data are communicated to other staff management units or supervisors (Director if acting as AIPN for instance). The transfer is necessary for administering the employment-related tasks of these units. Such transfers may be required only in the context of deciding whether the absence is justified or not and to draw any administrative or disciplinary conclusions, but not in all cases, where the intervention of the line manager or Head of Unit should normally be sufficient.

Administrative documents containing data relating to health should only be disclosed to those recipients who have a need to know and are bound by an obligation of professional secrecy equivalent to the medical one. Unnecessary information about the health status should be removed from these documents if this information is not necessary for the purpose for which the data are transmitted.

This is even more relevant in the context of processing of sensitive data such as data relating to health. The EDPS confirms that only conclusions on whether the leave is justified or whether a candidate is apt for work may be transferred to the above-mentioned departments.[13]

[12] F - 46/09, V v Parliament, Judgement delivered on July 5, 2011, par. 131.

[13] As to the transfer of medical invoices, the EDPS refers to his Guidelines concerning the processing of health data in the workplace by Community (now, EU) institutions and bodies.

Sometimes transfers to the Legal Service Department, the Civil Service Tribunal, the European Ombudsman or the EDPS may occur. The EDPS considers that such transfers comply with Article 7 of the Regulation if they are necessary for the legitimate performance of the tasks covered by the competence of the recipient.

Finally, as required under Article 7(3) of the Regulation, all recipients of data should be reminded not to process the data received for any purpose other than the one for which they were transmitted to them.

As regards flexitime, data should only be transferred to the relevant service of the data controller (namely HR). The EDPS takes the view that the (local) security officer should not be a recipient of the data stemming from a flexitime system. Indeed, the situation existing in a flexitime application is different from the security purpose attached to, for instance, the 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 the institution/body and the local security officer is not one of them.

7. CHANGE OF PURPOSE/COMPATIBLE USE

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. [...]"*. Any change of purpose would need to be justified.

Article 6(1) provides that, without prejudice to Articles 4, 5 and 10, *"personal data shall only be processed for purposes other than those for which they have been collected if the change of purpose is expressly permitted by the internal rules of the Community institution or body"*.

Leave:

Data is processed for the purposes of management of leave of staff members. These data may also be used for further processing in the context of the invalidity procedure, as foreseen in Article 59 (4) of the Staff Regulations. In this context, the EDPS takes note that the further use could be considered as compatible.

Flexitime:

The purpose of collecting flexitime data is time-keeping of hours worked. Any change of such purpose therefore needs to be assessed in this regard. An example of a possible change of purpose can exist in the case of the interlinking of flexitime data with another database (Article 27(2) (c)).

- For instance, the EDPS refused the possibility to link an access control database with a flexitime database. For the EDPS, the verification of flexitime clocking operations with respect to data on physical access checks might be justified as necessary only in those specific cases in which there are grounds to suspect that a

member of staff is infringing the flexitime rules. Such verification should then be carried out within the framework of an administrative investigation and not on an automatic basis.

- Another possible change of purpose would be the interlinking between a staff management tool facilitating the organisation of work and flexitime. In such case, the EDPS could accept such change of purpose but he would insist that the internal regulations covering both the flexitime and the management tool processing operations should be modified to contain a clause authorising the re-use of clocking in/out records from flexitime into the other system. The same modification should also take place as regards the internal rules on the linked system, which would need to be amended as to state the flexitime system as one of its source of data.

Finally, the EDPS also emphasizes that if the flexitime system is not to be used in the context of an evaluation process, the flexitime data may not be kept by Heads of Unit and their secretariats, as the data might otherwise be used directly or indirectly for evaluation purposes which would be *prima facie* a case of change of purpose. Therefore, when approval for a flexitime is granted by a superior to a staff, the data relating to flexitime should be deleted by the superior.

8. RIGHTS OF THE DATA SUBJECT

Article 13 of the Regulation 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.

Any procedure of leave should describe the possibility of access to and mention the possibility of rectification of personal data by a staff member.

The right of **access**, the right of rectification and the right to object should be granted in the following ways: all personal data (leave/absences/part-time work/parental and family leave/flexitime) should be accessible to the holder (and are actually partly supplied by him or her). The staff member can thus check them and if necessary correct them directly or ask for them to be corrected by a competent manager (data relating to identification) or by his or her immediate superior (often in the case of a flexitime system).

As regards time-related data (supplied in principle by the holder of the post), some must be validated and corrected, if need be, by a leave manager or the appointing authority, especially if they have a bearing on financial entitlements and/or the duration of the entitlements of the person who entered the data (in the case of parental leave the increased allocation and/or single parent status).

When making use of a **flexitime** system based on RFID technologies, the EDPS has already welcomed the distinction between two categories of processed data: the identification data and the data specifically linked to flexitime.

- The identification data are linked to the administration management system and can, when needed, be changed following the procedure relating to this system. This access by the data subjects could be authorised with a login and password, as adopted by the

institution or body. The data subjects (users of the application) could access, verify and, if necessary, correct their data.

- As concerns data linked to the flexitime application, data subjects may use a flexitime module (themselves or via the line manager) to access, verify and, if necessary, correct their personal data. Therefore, if the line manager agrees in individual access, staff members can correct/complete the time registrations themselves within a time period, usually of one week to ten days. 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 manager.

With reference to the rights of **rectification and blocking**, on some occasions, the right to rectify data is associated with the right to block data, for example when the data subject claims they are inaccurate. 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 the time needed for the data controller to check the accuracy of the data, they must be blocked (at the request of the data subject).

Because the exercise of the right to rectification is to be granted "without delay", the right to blocking of the data shall also be granted without delay and shall even precede the right to rectification.

However, in the few cases of the use of a management system (whether for leave or flexitime) that does not include a possibility to block data selectively, the action of blocking of data may create problems to the whole system. In such cases, the EDPS favours a specific procedure: each time blocking of data is requested by the data subject because the accuracy of the data is challenged, three copies of a "snapshot photo" of the state of the data (by printout, saving or burning a CD-ROM) should be made: one for the data subject; another one for the data controller and a third copy of the printout, backup or CD Rom to be made available to the DPO (or DPC) of the institution concerned. Finally, it should be made clear in the system that a procedure aiming at blocking data has been launched.

The EDPS would accept this solution only because it is for checking purposes (Article 15(1)(b) and 15(1)(c) of the Regulation) and because the IT consequences of modifying the existing management system so that it can block data selectively could not be implemented at the moment. In this case blocking would affect the data subject even more. Furthermore, the possibility of rectifying the accuracy of the data is applicable retroactively as are the associated rights.

9. INFORMATION TO DATA SUBJECTS

Articles 11 and 12 of the Regulation list information that must be provided to the data subjects. These articles list a series of compulsory items and another set of information. In the case of leave, both articles apply because not only data subjects provide the data themselves, but data are also retrieved from an internal database (HR systems).

When a new procedure is being implemented in an institution/body, 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. As to existing procedures, the information has normally already been provided to the data subjects, but it should also remain available on the intranet (if there is one) or should be easily accessible to the data subjects.

The information to be provided to the data subject shall, at least, contain:

(a) the identity of the controller;
(b) the purposes of the processing operation for which the data are intended;
(c) the recipients or categories of recipients of the data;
(d) whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply (for instance in the case of flexitime, the consequences of failure to clock in and out);
(e) the existence of the right of access to, and the right to rectify, the data concerning him or her;
(f) any further information such as:
    (i) the legal basis of the processing operation for which the data are intended,
    (ii) the time-limits for storing the data,
    (iii) the right to have recourse at any time to the European Data Protection Supervisor,

insofar as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

10. SECURITY MEASURES

According to Article 22 of the Regulation, *"the controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks presented by the processing and the nature of the personal data to be protected"*. These measures must *"in particular prevent any unauthorised disclosure or access, accidental or unlawful destruction or accidental loss, or alteration, and to prevent all other unlawful forms of processing"*.

This includes, among others, the fact that any institution/body should ensure that data are not accessible by or disclosed to anyone other than those specified as recipients on a need to know basis.

Moreover, given the particular sensitivity of the processing of health related data and considering that data indicating the health status of a person are processed by HR services during a leave request procedure (e.g. reason for the absence, forms concerning sick leave, medical certificates, etc), the EDPS recommends that all persons within HR services who are responsible for processing information related to the staff members' health status are reminded to process them in accordance with the principles of medical confidentiality.

Although staff members are subject to a general confidentiality requirement under Article 17 of the Staff Regulations (or any agency's funding Regulation), the EDPS considers that this confidentiality obligation is not specific enough to cover their processing of health related data. The EDPS therefore recommends that the institutions and bodies should prepare specific declarations of confidentiality to be signed by the HR staff that they are subject to an obligation of professional secrecy equivalent to that of a health professional, in compliance with Article 10(3) of the Regulation. .

On the development of **Flexitime systems using RFID** technology, the EDPS considers that in order to ensure a high level of technological and organizational security of a Flexitime system application, various eventual risks such as software hacking or physical damages to hardware and the system must be taken into consideration. Such risk analysis should always be part of a first assessment in order to propose solutions such as application of specific technical security measures or secure location and restricted access respectively before implementing an RFID system.

_____