Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Training Foundation regarding ETF - Flexitime Procedure

Brussels, 26 February 2009 (Case 2008-697)

1. Proceedings

On 18 November 2008, the European Data Protection Supervisor (EDPS) received from the Data Protection Officer (DPO) of the European Training Foundation (ETF) a notification for prior checking relating to the processing of personal data in the processing operation of Flexitime (recording of the leave and Flexitime) of staff members.

The ETF Draft "Guide to Flexitime" was attached to the notification.

The case was suspended while further information was sought on 5 December 2008 and this information was provided on 17 December 2008. The case was suspended again pending comments on the facts of the case on 7 January 2009 and these comments were provided on 12 January 2009. The case was suspended again pending comments on the draft opinion from the DPO on 3 February 2009 and these comments were provided on 11 February 2009.

2. The facts

According to the notification, the **purpose** of the processing operations is to ensure equal and fair treatment on a flexible working approach with a view to supporting staff to better conciliate work and private life. The ETF believes that Flexitime can be a very effective tool in allowing staff to balance their professional and private commitments. The ETF's interest in the use of Flexitime is the higher motivation of its staff resulting from their greater responsibility for the organisation of their time. Furthermore, the main objective of the scheme is daily flexibility, not recuperation. Work should be organised in such a way that it can be accomplished in a normal 7½ hour working day; time in excess of this should be worked only where justified by the workload and/or where agreed with the superior. The accumulation of time credits must thus be in direct relation with the work to be accomplished; prolongation of daily working schedules with the simple aim of accumulating time credits has to be avoided. As explained in the ETF guide to Flexitime, the period during which flexi workers are free to choose their arrival, lunch break and departure times, runs from 7.30 to 09:30, from 12:00 to 14:00 and from 16.00 to 20.30.

The **data subjects** concerned are all ETF staff covered by the Staff Regulations and by the Conditions of Employment of Other Servants (Contract Agents, Local Agents, Temporary Agents) regardless of function group or grade, and Seconded National Experts. The current

provisions shall apply by analogy to persons authorised to work part-time. In that case the standard working hours and core time, the time counted for absences and the maximum time credited or debited shall be reduced in proportion to the reduced working time.

The **data collected** are: card number (RFID tag Mifare type) linked to a login (meaning linked to the name of the person in a second stage), daily events such as arrival and departure, duration of lunch break, leaves, holidays, missions of all staff concerned. On the basis of this data, the system calculates, for each person, a balance (positive or negative) compared to the expected amount of hours per month. The localisation data of the Flexitime readers are only collected for technical troubleshooting purpose; and can only be accessed by the IT system administrator with specific access control rights. The system only processes the data related to the person, the time and the direction (entry or exit).

According to the notification, besides the data subjects, the **recipients** of the data are the Human Resources Unit (Head of HR, Leave Managers) and the respective Line Managers. Due to the technical functions in accessing personal data of the system, infrastructure and technology management (ITM) Unit (software developers) may also access the data. They are not considered as data recipients but they have to be informed and made aware of the data protection aspects (especially, confidentiality and security). No transfer of data will be done to third countries, or international organisation. The Flexitime is only for internal use to the benefit of staff members for better reconciling their private and professional life.

Procedure to use Flexitime:
For the introduction of the Flexitime, the HR Unit will ask all staff interested in benefitting from a flexible working pattern to discuss this with their line manager who shall validate the request after having assessed that continuity of service is not at risk and inform HR Unit on his/her decision. The draft Guide to Flexitime sent to the EDPS explicitly refers to the voluntary basis of participation in the use of Flexitime.

A personal badge is provided upon implementation of the Flexitime. For staff members who initially did not declare their interest but who at a certain point in time would like to benefit from a flexible working pattern, they shall communicate it at the time of their decision to their line manager who as above mentioned shall communicate his/her decision to the HR.

One common badge is used both for the entry to the building and for Flexitime but the Flexitime readers and the access control readers are separate machines. Moreover, the access to the building and the Flexitime systems are not interlinked and consequently, staff using Flexitime has to badge both machines: one for the entry to the building and one for Flexitime. Staff not using Flexitime only badge for entrance.

The **information** which is provided to the data subjects is described as follows:
Complete information on privacy statement and treatment of data will be included in the relevant policy and will be posted on the ETF Intranet, accessible to all ETF staff at any time.

In particular, the following information will be provided electronically to each "flexi worker":
- the identity of the controller
- the purpose of the processing for which data are intended and the legal basis,
- the recipients of personal data,
- the origin of data,
- the right of the data subject to access and to rectify data concerning him or her,
- the retention period of the data at ETF,
- the right of recourse to the EDPS at any time.

As regards the **rights of the data subjects**, according to the notification, Flexitime is managed via a Lotus Notes database and accessible via the ETF Intranet. This database is accessible by each data subject with her/his login and password. Therefore, the data subjects (users of the application) could verify and, if necessary, ask for correction/deletion of the data via electronic request. Requests for corrections after more than 5 days of presence in the office will not be accepted unless in case of force majeure. In addition, data subjects can exercise their rights under Regulation (EC) No 45/2001 at any time upon request addressed to the data controller.

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

The automated processing operations are the following:
- Time registration (data and time) of the swipes for each person (the unique identifier and the time registration);

- Transfer of the time registrations to the rest of the application where the link is made between the unique identifier of the chip and a person the personal number of the data subject. The time registrations of a person will be grouped over one day and the next morning will appear on the personal Intranet Flexitime of each person. In case of unreadable data by the system (incorrect badging or else) a red cross will appear on the day when a "problem" has occurred and no working time will be accounted. This allows a quick and clear notification to each staff member to ask for correction;

- Concerning the calculation of working time and the corresponding time credits/debits, the Flexitime system is linked to other applications such as SIC Leave and SIC Mission[1]. This interconnection allows to the system to count automatically working time and any time registered as out of the office via these two databases. Consequently, the data contained in the Flexitime system comprises not only the number of hours worked of each person in a month but also has a reference to the ETF closing days, week ends, and part time patterns. According to the additional information provided, there is no processing of medical data when validated requests are sent from Sic Leave and Sic mission to Flexitime. Moreover, the same symbol is used in the Lotus database to indicate illness, special leave and annual leave.

- Reporting linked to the interest of the service and statistical purpose (and therefore anonymous aggregated data are used);

[1] SIC Leave and SIC Mission validated requests are automatically transferred into the Flexitime system. In particular, the automated processing operations are as follows:
- calculation of working time via clock in and out registered time;
- calculation of working time while staff members have an "out of office" period validated by their manager via SIC (leave or mission);
- the expected number of hours to be worked in a month taking into consideration ETF closing days, week ends, etc;
- time credits/debits.

- Requests for correction of working time will be asked via electronic system, to be validated by respective line manager and once validated, the corrected data will be automatically imported in the Flexitime system, erasing and replacing the incorrect registered one.

The manual processing operations relate to allocating part time workers to their respective part time approved conditions (50%, 60%, 70%, 75%, 80%, 90%). Technically this processing means that for each staff in part time, the approved percentage of their working pattern shall be introduced manually in order to get the expected working time in a given period and the maximum pro-rata credit/debit balance a part time worker can generate. Therefore partial manual processing is only applicable to the specific cases of part time workers.

With regards to **blocking and erasure** of data, the notification foresees an opt out procedure with possibility to erasure of data. In the case of request to opt out of Flexitime, staff members are requested to do so at the end of a calendar month.

Staff member will therefore be requested to continue to register daily working hours, until the end of a calendar month. Opting out of Flexitime is possible only if the time balance is at least zero, or positive.

Although this opt-out procedure is not similar to a blocking or erasure procedure, once the person has opted out (with a balance at zero), the data can be completely erased within 2 weeks of the request. Only anonymous data will be kept longer for statistical purpose.

As a consequence, for **statistical** and **historical** data, only anonymous data will be kept and therefore no association between the name and the data will be possible. Only aggregated data will be kept.

As regards the **storage**, the data are stored in a Lotus Notes database. It is transferred from the RFID tag (where there is no knowledge of the person, only a code number) to Lotus Notes, where it is then associated to each person.

There are 3 clock in/out swipe machines (at the 3 main entrances of the ETF building). The badging can not be accidental as people need to put the card voluntarily on the swipe machines.

The **retention** period is set as follows: Flexitime individual data will be stored for the ongoing calendar year. They will be deleted once the transfer of unused days of annual leave to the following year has been closed and at the maximum by end of March of the following year. Furthermore, ETF foresees that the retention period for both type of data, administrative and technical (audit trail) of the Flexitime system will be kept for the same time period (maximum up to 15 months). In the information provided, ETF ensures that all necessary technical measures will be implemented in order to guarantee the respect of this security aspect.

As explained above, aggregated data rendered anonymous will be kept for longer time only for historical trend statistics.

The **security measures** of the system
(...)

3. Legal analysis

3.1. Prior checking

Regulation (EC) No 45/2001 of the European Parliament and of the Council on the protection of personal data by Community institutions and bodies and on the free movement of such data (hereinafter Regulation (EC) No 45/2001) applies to the processing of personal data by Community institutions and bodies.

Personal data are defined as any information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity.

The Flexitime application of the ETF processes personal data because the data relate to natural persons who are identifiable, for instance by the use of names or personal numbers. Even the serial number of the badge, which in itself is non personal data, becomes, in the system, a personal number from the moment it is linked or is linkable to identification data and is used to record that a badge issued to a particular staff member has passed the reader. The natural person can be identified, directly or indirectly by reference to an identification number. The data processed in connection with recording of the leave and Flexitime of ETF staff members therefore qualify as personal data according to Article 2(a) of Regulation (EC) No 45/2001.

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

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*". The Flexitime system of the ETF uses a badging system based on RFID technology. The EDPS considers that the inclusion of such a technology (the RFID chip embedded in the badge) into a Flexitime system constitutes an important innovation in a Flexitime system and represents a specific risk.[2] Therefore, the current prior checking falls under Article 27(1) of the Regulation.

The Flexitime at the ETF concerns both automatic and manual processing. This is partly automated processing. Therefore Article 3(2) of the Regulation applies.

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

The notification was received on 18 November 2008. Pursuant to Article 27(4) of Regulation (EC) No 45/2001, the two-month period within which the EDPS must deliver an opinion was suspended for a total of 17 days to obtain additional information. It was also suspended for 7 days to allow comments on the draft Opinion. In the light of further elements which were provided by the DPO in her comments, the EDPS decided to extend by 2 weeks, the deadline to adopt his opinion. The Opinion must therefore be adopted no later than 27 February 2009.

[2] See: Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Commission on "the implementation of Flexitime - specific to DG INFSO", issued on 19 October 2007 (case 2007-0218).

3.2. Lawfulness of the processing

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

Of the various grounds listed under Article 5 of Regulation (EC) No 45/2001, the processing operation notified for prior checking falls under Article 5 a), pursuant to which data may be processed if the processing is "*necessary for performance of a task carried out in the public interest on the basis of the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof or in the legitimate exercise of official authority vested in the Community institution or body or in a third party to whom the data are disclosed*".

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

Relevant legal grounds in the Treaty or other legal instruments
The legal basis for the processing is to be found in:
- the Staff Regulations of officials and Conditions of employment of other servants (especially Article 55);
- the ETF guide to Flexitime that will be adopted, following the EDPS' opinion.

Necessary to perform a task carried out in the public interest
In considering whether the processing operation fulfils the second condition under Article 5 (a), the issue is not whether there is a *specific need* to develop "a badging system using RFID" to implement a Flexitime system, but whether the processing in such a system is necessary for the performance of a task carried out in the public interest.

Moreover, as already underlined in previous prior-checks[3], the required "need" does not mean that it should be *unavoidable* but that it can be considered reasonably necessary in the specific context for fulfilling the purpose aimed at. Therefore, there is a margin of appreciation left at the discretion of the administration in deciding whether to implement this system using RFID. If the necessary safeguards and proportionality are present, it can be considered that such a system fulfils the conditions of need.

The EDPS notes that the ETF carries out the processing activities for a task in the public interest. Indeed, the processing operations are taking place in the framework of a mission carried out in the public interest on the basis of Staff Regulations of the officials of the European Communities and the conditions of employment of other servants of the European Communities.

[3] See for instance PC 2007-0218 mentioned in footnote 2.

Finally, as described in the facts, the participation in the Flexitime system itself is made on a voluntary basis.

The EDPS is satisfied that the processing operation as such meets the conditions of lawfulness. This opinion shall further concentrate at the safeguards to address the specific risks presented by this processing operation.

3.3. Data Quality

Data must be "*adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed*" (Article 4(1)(c) of Regulation (EC) No 45/2001).

The data collected are a card number (serial ID number) and daily events such as arrival and departure. There are 3 clock in/out swipe machines at the 3 main entrances of the ETF.

The precise data collected are: card number linked to a login, daily events such as arrival and departure, duration of lunch break, leaves, holidays, missions of all staff concerned. On the basis of this data, the system calculates, for each person, a balance (positive or negative) compared to the expected amount of hours per month. There is then a transfer of the time registrations to the rest of the application where the link is made between the unique identifier of the RFID chip and a person.

Moreover, the data are stored in a Lotus Notes database. The card number is transferred from the chip to Lotus Notes, where it is then associated to each person. In terms of data quality, the EDPS considers that the personal data of staff members of ETF who do not wish to use Flexitime should not be imported into the Lotus Note database.

Apart from that, the EDPS considers the data adequate and relevant. Those data are not considered excessive.

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

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

Data must be accurate, and where necessary, kept up to date" (Article 4 (1) (d). The system in general must ensure data accuracy and the updating of the data. In the analyzed processing operation, the Lotus database is accessible by each data subject with her/his login and password. Therefore, the data subjects (users of the application) could verify and, if necessary, ask for correction/deletion of the data via electronic request. Requests for corrections after more than 5 days of presence in the office will not be accepted unless in case of force majeure. In addition, data subjects can exercise their rights under Regulation (EC) No 45/2001 at any time upon request addressed to the controller.

As explained in the facts, in case of unreadable data by the system (incorrect badging or else) a red cross will appear on the day when a "problem" has occurred and no working time will be accounted. This allows a quick and clear notification to each staff member to ask for

correction. The EDPS considers however that this practice is not sufficient in order to ensure the quality of data. The EPDS proposes that when an error occurs in the time registration or in the transfer of data to the Lotus database, an email should be sent to the person with all his time registrations that would inform him/her that an error occurred.

The data subject has the right to access and the right to rectify data, so that the file can be as complete as possible. Further, on the right of access and rectification, see point 3.8 below.

3.4. Conservation of data/ Data retention

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

According to the information provided by the ETF, the retention period for both types of data, administrative and technical (audit trail) of the Flexitime system will be the same (maximum up to 15 months). The EDPS agrees with the proposal that administrative data of the Flexitime are stored for the ongoing calendar year and that they will be deleted once the transfer of unused days of annual leave to the following year has been closed and at the maximum by end of March of the following year.

However, the EDPS can not accept a similar retention period for the conservation of technical data in the application of the ETF (audit trail related data). Indeed, the Flexitime application works as a buffer of time registrations before these are sent to the Lotus Note Database. Therefore there is no need to keep these data for a long period of time. In the case of the ETF and given the necessity to keep an audit trail of the Flexitime application, the EDPS advises to implement a storage period of data for a maximum of one month.

The draft guide to Flexitime foresees that data subjects who opt out of Flexitime (provided that their balance of time credits/debits is at zero) have the right to ask for deletion of individual data. Once the person has opted out (with a balance at zero) the data can be completely erased within 2 weeks of the request. The EDPS would like this 2 week-period to be explicitly added in the privacy statement of the ETF Flexitime.

In a similar way, ETF should foresee a procedure to delete Flexitime data (administrative and audit data) of people who have left the Agency. In such cases, the EDPS already considered that a period of 2 weeks was proportionate to the purpose of the processing.

As regards statistical data, aggregated data rendered anonymous will be kept for longer time only for historical trend statistics. The EPDS considers that such retention is proportionate and complies with Article 4(1)(e).

3.5. Compatible use / Change of purpose

Article 4(1)(b) of the Regulation provides that personal data must be "*collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes*". The purpose of the processing is that, based on the principle of time-keeping of worked hours, the main objective of the scheme is daily flexibility, not recuperation. In fact the purpose of Flexitime is to allow staff to decide when they wish to start work, take lunch

and go home in the general context of a 37½-hour week[4] while respecting the core time and interest of the service.

It is the understanding of the EDPS that there is no change of purpose to the processing and no secondary purpose sought. Therefore, the EDPS would suggest adding in the ETF draft guide Flexitime that ETF does not use the data processed in the analysed context for any purpose other than for the purpose it sought to fulfil, and that the "card number" is not used for any other purpose than the Flexitime framework and that it is only stored in the ETF Flexitime application for linking the card to the person.

Article 6.1 of Regulation (EC) No 45/2001 is not applicable to the case and Article 4.1.b of the Regulation is respected, provided that the above recommendations are implemented.

3.6. Transfer of data

Article 7 of the Regulation provides that *"personal data shall only be transferred within or to other Community institutions or bodies if the data are necessary for the legitimate performance of tasks covered by the competence of the recipient"*.

The notification explains the categories of persons who could have access to the registered data via the IT registering application of ETF. As already explained in the facts, due to the technical functions in accessing personal data of the system, infrastructure and technology management (ITM) Unit (software developers) may also access the data, although they are not intended as recipients who would process the data. The EDPS does not consider them as data recipients. Nevertheless, the ETF has to ensure that they are informed and made aware of the data protection aspects (especially, confidentiality and security).

Moreover, the EDPS does not consider the data subjects as recipients of the data. In fact, they are the data subjects of the processing but not the recipients of these data.

Therefore, the categories of recipients are the data controller (Head of HR Unit staff responsible for leave/absences management) and respective line managers. Transfers to these recipients are legitimate since they are necessary for the legitimate performance of the tasks covered by the competence of the recipient.

The EDPS also understands that there will be no data transfer outside of the ETF. The data collected in the Flexitime application are not accessible for anyone outside the ETF.

No transfer of data will be done to third countries, or international organisation. The Flexitime is only for internal use to the benefit of staff members for better reconciling their private and professional life.

3.7. Processing of personal number or unique identifier

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

[4] As per Article 55 of the Staff Regulations.

The badge number and the personal number co-exist in the Flexitime system for practical reasons. The badge number will be necessary because the personal badge will be used to clock in/out via the use of the badge readers. For the case at hand, the use of the staff personnel number for the purpose of recording data in the system is reasonable considering that this number is used to identify the person in the system and thus helps ensure that the data are accurate. Therefore, Article 10(6) is complied with.

3.8. Right of access and rectification

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

The prior checking notification and the supplementary information submitted by the controller describe the possibility of access to and mention the possibility of rectification of personal data by a staff member: In the ETF Flexitime system, a data subjects has the *right to access and to ask for rectification* of data concerning him or her via electronic request

According to the notification, Flexitime is managed via a Lotus Notes database and accessible via the ETF Intranet. This database is accessible for each data subject with her/his login and password. Flexi workers may consult their own time account at any time. Therefore, the data subjects (users of the application) could verify and, if necessary, ask for correction/deletion of the data via electronic request. Flexi workers are responsible for checking the recorded time by the electronic system in place and inform in due course HR via eRequest (Flexitime) about corrections to be done. Requests for corrections after more than 5 days of presence in the office will not be accepted unless in case of force majeure. In addition, data subjects can exercise their rights under Regulation (EC) No 45/2001 at any time upon request addressed to the data controller.

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

Therefore, in the case of a true prior-check analysis as it is the case here, the EDPS considers that ETF should introduce a procedure by which a data subject could request the blocking of data relating to him/her. This solution should not lead to the disruption of the system.

However, if ETF considers that such system may prove impossible to implement and that he can bring to the EDPS legitimate objections, the EDPS can propose an alternative to blocking. In his opinion of 29 March 2007 in the case of the TIM module integrated in SYSPER 2 of the European Commission, the EDPS agreed with a solution which could also be applicable. Similar to the TIM module integrated in SYSPER 2, the data blocking inside the ETF Flexitime application could only be applied in a selective way as a complete blocking would obstruct the totality of the data processing. The solution could consist, each time a blocking is requested to prove the facts, in taking a "snapshot" of the data by means of a printout, a backup or a CD Rom the same way as in SYSPER2 - TIM. With this solution, three copies should be made available, one for the requesting person (complainant), one for the data controller and a final one for the DPO of the ETF. Indeed, in the case of a complaint, it would

facilitate his/her intervention. This solution would be acceptable because it is for evidence purposes (Article 15.1.b and 15.1.c of the Regulation).

The EDPS notes that, according to the notification Article 20 of Regulation (EC) No 45/2001 is not to be applied, in principle, in the context of this data processing operation.

In conclusion, the EDPS considers that the conditions of Articles 13 and 14 of the Regulation are met, with due respect to the modification of the retention period (see point 3.4 Conservation of data).

3.9. Information to the data subject

Articles 11 and 12 of Regulation (EC) No 45/2001 list information that must be provided to the data subjects. These articles list a series of compulsory items and another set of information. The latter are applicable insofar as, taking into account the particular circumstances of the treatment in question, they are necessary in order to ensure a fair data processing with regard to the data subject. In this case, part of the data is collected directly from the data subject and another part from other sources.

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

Article 12 (*Information to be supplied where the data have not been obtained from the data subject)* should also be observed as the list of identification information is retrieved from ETF Human Resources' department.

As described in the notification, complete information on privacy statement and treatment of data will be included in the relevant policy and will be posted on the ETF Intranet, accessible to all ETF staff at any time. Moreover, the privacy statement will be handed out to each flexiworker together with their personal badge.

At the moment, the privacy statement is part of the ETF guide to Flexitime (point 6 data protection issues). The EDPS suggests that the ETF considers giving this information a more prominent place in the guide or perhaps even adopting a specific privacy statement, which would be materially distinct from the guide but handed over together with the guide. In any case, it should be provided to staff before they start participating in the Flexitime. The reason is to clearly draw the attention of the data subjects to their rights by informing them via a specific privacy statement.

The draft of the specific privacy statement contains most of the elements of Articles 11 and 12 of Regulation No 45/2001. However, this needs to be completed so that it fully complies with Articles 11 and 12 of Regulation No 45/2001. For instance, the privacy statement should also contain the purpose of the processing. Further clarifications are also needed as regards the retention of data (see point 3.4 above) and the blocking of data (see point 3.8 above).

3.10. Security measures

According to Article 22, the controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected.

(...)

The EDPS has already clarified, in a previous prior-checking opinion[5], the status of an embedded RFID chip number in a card. The identification number associated to the RFID chip is personal data covered by Regulation 45/2001. Indeed, this identification number when used to record a staff member's behaviour and linked to the personnel number (which means linked to the name of a person, as is the case here), makes this a processing of personal data, which requires compliance with the data protection principles.

(...) the EDPS recommends that the ETF reconsiders the decision taken in terms of technological choices through a new assessment, including a viable timetable to implement the change of technology, taking into consideration the choice of the best available techniques[6]. In such a case, the ETF could also take guidance on other Institutions' example.

Moreover, the EDPS recommends that privacy and data protection be better guaranteed against cloning of the badge or tracking of the cardholder. More appropriate technologies, such as contactless smartcard using random UID, could be selected and implemented[7]. Alternatively, the ETF could implement a stronger shielding protection of the card which is only removed when the card is used. These technical measures should be complemented by policy procedures such as: (i) prohibiting sharing or lending of access cards, (ii) requiring immediate reporting of stolen or lost access cards and (iii) recommending that employees hide their access card when outside the ETF premises.

(...) due to the technical functions in accessing personal data of the system, infrastructure and technology management (ITM) Unit (software developers) may also access the data. They have to be informed and made aware of the data protection aspects (especially, confidentiality and security).

After careful analysis by the EDPS of the security measures adopted, the EDPS considers that these measures are adequate in the light of Article 22 of Regulation (EC) No 45/2001".

Conclusion:

There is no reason to believe that there is a breach of the provisions of Regulation (EC) No 45/2001. Also the European Training Foundation has already implemented part of the draft recommendations made by the EDPS during the period which was provided to ETF to comment on the draft opinion. Though, some of these recommendations still have to be implemented. These recommendations mean in particular that the ETF should:

- Ensure that the personal data of its staff members who do not wish to use Flexitime should not be imported into the Lotus Note database;

---

5 See Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Commission on "the implementation of flexitime - specific to DG INFSO", 19 October 2007 (2007-218).

6 This concept of Best Available Techniques has been promoted by the EDPS in his annual report 2006. Moreover, the EDPS remains available to provide guidance on possible alternate technological choices in the future.

7 This issue was highlighted last year by the International Civil Aviation Organisation (ICAO) see page 22: http://www.mrtd.icao.int/component/option,com_remository/Itemid,256/func,startdown/id,26/

- Ensure that in case of error during the insertion of time registration or in the sending of data to the Lotus database an efficient way to inform the person is implemented to ensure the data quality principle;

- Modify the retention period it envisages regarding the retention of audit trail data;

- Foresee a procedure to delete Flexitime data (administrative and audit data) of people who left the Agency. A period of 2 weeks is considered as proportionate to the purpose of the processing;

- Introduce a procedure by which a data subject can request the blocking of data relating to him/her in case of disputes;

- Ensure that the specific privacy statement is made more prominent and perhaps even made separate from the Guide to Flexitime and handed over to flexi workers when they receive their badge;

- Complete the privacy statement, by adding:
    - a paragraph stating that within 2 weeks after which an opt-out has been accepted, the data of the data subject will be deleted from the database;
    - that it does not use the data processed in the analysed context for any purpose other than for the purpose it sought to fulfil, and that the "card number" is not used for any other purpose than the Flexitime framework and that it is only stored in the ETF Flexitime application for linking the card to the person;
    - aside the mention of the retention of administrative data, a paragraph on the retention of audit trail data compliant with the EDPS' recommendation;

- Ensure that the members of the infrastructure and technology management (ITM) Unit are informed on the data protection aspects of the processing;

- Consider introducing a procedure by which the blocking of data could be ensured. To do so, the use of a "snapshot" of the data by means of a printout, a backup or a CD Rom could be envisaged;

- Introduce stronger security measures on the card and reconsider its technological choice in terms of security.

Done at Brussels, 26 February 2009

(signed)

Giovanni BUTTARELLI
Assistant European Data Protection Supervisor