Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Center for Disease Prevention and Control (ECDC) concerning "Time and absence management"

Brussels, 22 June 2009 (Case 2009-072)

1. Proceedings

On 26 January 2009, the EDPS received a formal prior checking notification by email from the Data Protection Officer (DPO) of the European Center for Disease Prevention and Control (ECDC) on the data processing operations relating to time and absence management.

On 9 February 2009, the EDPS requested additional information. On 20 April 2009, the ECDC sent to the EDPS a second notification form replacing the former one as well as additional information.

On 18 June 2009, the EDPS sent the draft opinion for comments to the DPO. These comments were received on 22 June 2009.

2. Facts

In the frame of the Staff Regulations and Conditions of Employment of Other Staff, the Commission decision C(2004)1597 introducing implementing provisions on leave, and ECDC internal procedure on working hours (ECDC/ADM/021) of 5 December 2007, the Human Resources section of ECDC (the "data controller") has introduced both a manual and an automatic data processing for purpose of managing working times and absences of the staff working at ECDC.

Since 21 January 2008, the data controller has implemented an automatic data processing (SAP) to facilitate the recording and management of time of staff working at ECDC.

The SAP system is composed of two main applications: one is an employee self-service portal, which allows employees to feed the database with their own data; the other one is a manager self-service portal, accessible by authorized persons within ECDC for purpose of management and approval of time and absence of the staff.

The Employee Self-Service application is composed of the three following modules:

- *Employee search*: it enables the staff to search through the staff directory, which provides basic information about staff and their position within ECDC;
- *Personal information*: staff directly fill in and modify their own personal information such as contact details and emergency address;

- *Working time*: staff members directly record in the database their working times and their absences (pre-defined absence type), consult their leave entitlements, and file requests regarding leaves and working time.

The Manager Self-Service application allows authorized persons (in HR, Unit, line of management) to consult the working times and presence/absences of the staff, and to approve/reject the following requests from staff: annual leave, flexi day, special leave, requested work, and compensation. Furthermore, the SAP database allows authorized persons to generate regular reports, per person and per unit, regarding: (i) sick leave, (ii) working time and absences, (iii) leave entitlements, and (iv) special leave, maternity leave, leave on personal grounds and all other forms of leave provided in applicable regulations. Such information is also transferred in electronic form to the HR responsible for the "Attendance" email inbox.

Reports are generated on an individual basis to ensure that the employee doesn't exceed the number of days of absence for sickness without providing medical certificates, to monitor anomalous situations and to monitor the working hours of the employees and units with the aim to avoid a work overload of the staff. ECDC informed the EDPS that reports are not used to conduct an evaluation of the person.

While the **data processing** performed by HR in respect of time and absence management is to a large extent automatic through the use of SAP, some parts of the processing remain manual. In particular, supporting documents for absences and leave are usually processed manually. Certain specific types of leave, for which additional information must be provided by staff, are processed manually by HR: working time, mission, parental/maternity leave, family leave, sick leave, other leave.

The **data subjects** in respect of the data processing performed in the SAP database are the members of the statutory staff of the ECDC, i.e. temporary agents, contractual agents, and SNEs. In addition, trainees' data concerning absences and leave are processed by the HR section on a manual basis. Certain data relating to the staff family members may also be collected and processed.

The data processing operations, both automatic and manual, are intended for the following **purposes**: (i) to allow staff members to manage their working time in the frame of the flexitime policy, (ii) to allow management to approve working time, leave and absences, and (iii) to ensure that supporting documents are provided.

The following **types of data** are processed:

- on SAP: (i) personal details, such as surname, first name, date of birth, gender, nationality, e-mail address, address, emergency address, country, telephone, fax, personal number (staff number), relatives data, dependents data; (ii) working time data, holiday and flexitime entitlements, absences, leaves and reasons for the leave.

- in "attendance file" (paper file): surname, first name, date of birth, gender, nationality, e-mail address, address, emergency address, country, telephone, fax, personal number (staff number), relatives data, dependents data, absence justifications (e.g. medical certificates), expenses and medical benefits, special

leave justifications (e.g. rental or purchase contracts of property, death certificates of relatives, birth certificates of children, marriage certificates), requests for change of holiday (due to private or religious reasons), information about stand-by duty working time (to ensure financial compensation). Occasionally data concerning the data subject's private sphere (e.g. sexual orientation), concerning pay and allowances, concerning the data subject's family and/or concerning missions and journeys may emerge in the documents provided in support of leave and absence justifications.

- in "personal file" (electronic and paper files): surname, first name, date of birth, gender, nationality, e-mail address, address, emergency address, country, telephone, fax, personal number (staff number), relatives data, dependents data, rental or purchase contracts of property, birth certificates of children, marriage certificates (to fix rights and allowances).

The data are accessible to the following internal **recipients** within ECDC:

- For all data processing (SAP, attendance file and personal file): Head of HR, one HR assistant, one back-up assistant, and HR secretary have access to all time and absence information of all staff. Justifications for leave and absence (such as medical certificates, birth certificates, marriage certificates, other reasons for the leave) are only processed by the HR section and are not disclosed to any other recipient than HR.
- In addition, for data processed on SAP only:
  - Head of Unit and one secretary per Unit appointed by HR upon request of the Line manager have access to data processed on SAP for all staff in their Unit.
  - Each line manager has time and absence information processed on SAP for all its team members.
  - In addition, secretaries with special access role to the SAP system can :
    • Access to information on attendance/ absence of their Unit members
    • Generate reports on:
    – Mission/Sick leave/ Special leave etc. per person/per Unit
    – Times entered by staff members
    • Assist staff as a first point of contact when experiencing problems with Time recording
    • Assist Head of Unit and Line Managers regarding leave approval.

The Controller, one HR assistant, one back-up assistant and HR secretary may be contacted at any time by the data subjects to exercise **the right of access, to rectify, to block, to erase, and to object** basic identity information. Moreover, each staff member has direct personal access to his/her own personal information contained in the SAP database, and may correct himself/herself personal contact information and most of his/her data on time and absence. However, data subjects must file a request to obtain correction of the following data: (i) change of holidays due to private or religious reasons, (ii) stand-by-duty (HR gathers information about stand-by-duty working times and ensures that financial compensation is paid accordingly).

As concerns **information about the data processing**, ECDC has adopted a data protection policy concerning the protection of personal data in relation to time and absence management. In addition, a data protection clause has been included in the

SAP self-service application. Moreover, during the newcomers' presentation staff are informed about their rights and the procedure to access and rectify data relating to them.

As concerns the **retention of data**, the notification indicates that ECDC is currently drafting a Data Retention Time-Limit policy, which is expected to be adopted by the Director of the Centre in 2009. In his request for additional information, the EDPS asked that a draft be provided to the EDPS. This request was however not satisfied.

As regards **security measures**, the notification indicates that hard copies of documents and/or data are transferred from the data subject to HR in a closed envelop, via e-mail or handed in person to HR, and they are filed in a protected cupboard in the HR premises. All electronic data are stored in SAP. Access is restricted to HR team members dealing with time management and to Head of Administrative Unit and Head of HR Section. Only HR staff members can have physical and digital access to the personal files via ECDC network credentials. Restricted access code to IT systems is provided. Access to SAP is customized according to the profile of the user.

3. Legal aspects

3.1. Prior checking

The management of time and absence by ECDC constitutes a processing operation falling under the scope of Regulation (EC) No 45/2001 since it involves the collection, recording, consultation and organisation of personal data (Article 2(a) of the Regulation) by a Community body. Some parts of the processing are automatic in SAP, while other parts of the processing are manual; in the latter case the data form part of a filing system (Article 3(1) of the Regulation). The processing involves data relating to health and qualified as a "special" category of data, subject to the provisions of Article 10 (see below 3.3).

Article 27 (1) of Regulation (EC) No 45/2001 subjects to prior checking by the EDPS all "*processing operations likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes*". Article 27(2) of the Regulation contains a list of processing operations that are likely to present such risks such as processing of data relating to health (Article 27(2)(a)) and processing of data intended to evaluate personal aspects relating to the data subject (Article 27(2)(b)).

The processing operations carried out in the context of time and absence management present specific risks as they involve processing data revealing the state of health of the data subject (e.g. processing data on sick leave, medical certificates). Because the data processing at stake involves processing data relating to health on a regular basis, and not just on a purely occasional or incidental basis, this justifies the need for prior checking under Article 27(2)(a) of the Regulation.

Furthermore, the data processing largely contributes to evaluating personal aspects of the staff in relation to taking a decision on whether or not to grant a leave/special leave. Moreover, it is anticipated that the data gathered in SAP may also be used for purpose of evaluating a person in case there is suspicion of misconduct of the staff member. Despite the fact that the processing is not in itself intended to evaluate

personal aspects of the data subject such as his/her ability, efficiency or conduct it largely contributes to such a purpose, so that Article 27(2)(b) of Regulation (EC) No 45/2001 must also be taken into account as a possible additional ground for prior checking.

Since prior checking is designed to address situations that are likely to present specific risks, the opinion of the EDPS should be given prior to the start of the processing operations. In this case however the processing operations have already been established. This is not a serious problem however as far as any recommendations made by the EDPS may still be adopted accordingly.

The notification of the DPO was received on 26 January 2009. A request for information suspended the two months time frame within which the EDPS must render his opinion. A second notification, replacing the original notification, was then sent to the EDPS on 20 April 2009. The delay for rendering the opinion is therefore of two months as of the date of the new notification + 3 days of suspension for comments, and shall be rendered on 24 June 2009 at the latest.

3.2. Lawfulness of the processing

Personal data may only be processed if legal grounds can be found in Article 5 of the Regulation. In particular, Article 5(a) of the Regulation provides that personal 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*".

In order to determine whether the processing operations comply with Article 5(a) of the Regulation, two elements must be taken into account: first, whether either the Treaty or other legal instruments foresee a public interest's task, and second, whether the processing operations carried out by the data controller are indeed necessary for the performance of that task.

Legal Basis. The Staff Regulations of the European Community (in particular Articles 55 to 61) and the Conditions of Employment of Other Servants of the European Community (CEOS) (in particular Articles 16, 17, 57-60, and 91) lay down the rules concerning working time as well as leave and absence of civil servants and other servants. In the framework of these rules and the Commission decision C(2004)1597 introducing implementing rules on leave, the ECDC adopted an internal procedure on working hours (ECDC/ADM/021) which introduces and defines the modalities of the flexitime system and which specifies the rules on working time as well as on leave and absences applicable at ECDC. In addition, stand-by-duty rules applicable at ECDC are defined in a decision of the Director of ECDC No 12/2007. The Staff Regulations, CEOS, implementing rules on leave and ECDC's internal decisions provide the legal bases that justify the processing of data of the staff working at ECDC for purpose of managing time and absences.

The EDPS however underlines that if the processing is intended to monitor on a regular basis the staff in order to evaluate certain personal aspects of the data subject, such as his/her ability, efficiency or conduct, a specific legal basis should be adopted by ECDC in order to carry out the processing for such purposes. In this view, the

EDPS notes that while the legal basis justifies that reports are generated in SAP on an individual basis for purpose of time and absence management, it does not provide a sufficient legal basis to use such individual reports to monitor the staff for purpose of evaluation of their ability, efficiency or conduct.

Necessity Test. According to Article 5(a) of the Regulation, the data processing must be *"necessary for performance of a task"* as referred to above. The data processing implemented by ECDC is necessary in order to ensure that ECDC complies with its legal obligations as an employer and that it provides its staff with all its rights and benefits in the field of employment. Thus, the EDPS considers that the data processing complies with the necessity test and can be considered as lawful under Article 5(a) of Regulation (EC) No 45/2001 provided that it is not used for other purposes than time and absence management.

3.3. Processing of special categories of data

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life is prohibited unless grounds can be found in Article 10(2) and/or Article 10(3) of the Regulation.

The processing at stake may involve medical data in the strict sense and/or data relating to health of the data subject to the effect that the data reveal information concerning the health status of the person (absence for sick leave). In addition, justifications of leave or absence may also contain information revealing the religious beliefs or the sex life of the person. Grounds must therefore be found in Article 10(2) in order to justify the processing of the data.

Article 10(2)(b) provides that sensitive data may be processed if the processing is necessary for the purposes of complying with the specific rights and obligations of the controller in the field of employment law insofar as authorised by the Treaties establishing the Communities or other legal acts adopted on the basis thereof. In this view, the EDPS points out that sensitive data which processing by ECDC falls within the scope of Article 10(2)(b) may only be processed for the lawful purposes for which the processing takes place.

Moreover, the EDPS would like to underline the need for specific guarantees. In the context of the processing performed by ECDC, the processing of data relating to health shall be strictly limited to data indicating the sickness status but shall not extend to obtaining confidential information providing a medical diagnosis about the health of the data subjects. The EDPS further stresses out that, in accordance with Article 10(3) of the Regulation, the processing of medical data in the strict sense shall be restricted to health professionals subject to the obligation of professional secrecy or to persons subject to an equivalent obligation of secrecy.

As regards other sensitive data that may be collected by ECDC, guarantees shall be put in place to ensure that this information is not held against the data subject. For example, the information provided to the data subject should clearly inform him/her of the presence of these data and the purposes for which they may be used. It must be

ensured that the persons having access to the data do not use it for any other purposes than those for which it is intended.

3.4. Data Quality

Adequacy, Relevance and Proportionality. According to Article 4(1)(c) of the Regulation, "*personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed*". On the basis of the information available, the EDPS considers that the collection by the HR section of medical expenses and benefits in the attendance file is not relevant for purpose of time and absence management.

Fairness and Lawfulness. Data must also be "processed fairly and lawfully" (Article 4(1)(a) of the Regulation). Lawfulness has already been discussed in paragraph 3.2 above. Concerning fairness, this notably relates to the information which is to be communicated to the data subject (see below, paragraph 3.9).

Accuracy. Finally, data must be "*accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified* " (Article 4(1)(d) of the Regulation). The fact that staff members fill in their data in the SAP application themselves contributes to keeping the data accurate and up to date. Furthermore, as will be seen below in section 3.8, the data subject shall also have access and rectification rights in order to ensure that files relating to him/her are as complete as possible.

3.5. Conservation of data

Article 4(1)(e) of Regulation (EC) No 45/2001 provides that personal data may be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are collected and/or further processed. The data may be kept for longer periods for historical, statistical or scientific use, but either in an anonymous form or with the identity of the data subjects encrypted.

No time-limit for the retention of the data has yet been set out by ECDC. The notification received from the DPO indicates that ECDC is in the course of drafting a Data Retention Time-Limit policy that shall be adopted by the end of 2009.

The EDPS would like to insist on the need for ECDC to determine appropriate conservation periods for retention of the data. These conservation periods must be assessed on the basis of the purposes for which the data are collected and processed. In this case, it may be necessary to define separate retention periods according to the means of processing used taking into account for how long it would be necessary to have them stored on each particular means (on SAP, on other electronic files and in paper files) to achieve the purposes for which they were collected. In this respect, the EDPS wishes to be informed of the data retention periods adopted by ECDC.

3.6. Transfer of data

The notification indicates that data will only be transferred within ECDC; such data transfers must therefore be examined in light of Article 7 of the Regulation (EC) No 45/2001.

Article 7 of the Regulation provides that *"personal data can be transferred within or to other Community institutions or bodies if the data are necessary for the legitimate performance of the tasks covered by the competence of the recipient"* (paragraph 1) and that *"the recipient can process the data only for the purposes for which they were transmitted"* (paragraph 3).

On the basis of the information available, the EDPS notes that the transfers fall, in principle, within the legitimate performance of the tasks covered by the competence of the respective recipients. In particular, the EDPS notes that the transfers to data subjects' hierarchy, to secretaries and to the HR staff are necessary for administrative purposes and for purpose of management of absences and leave. Consequently, Article 7(1) of the Regulation is being complied with.

Concerning medical certificates, the notification indicates that these are only processed by the HR staff and not disclosed to any other recipients. However, the EDPS would like to point out that in principle, all certificates containing medical data to be provided in connection with leave requests or absences shall be submitted directly to a medical service and not to the administration. While an exception from this rule could be envisaged for small agencies or bodies with no medical service, the EDPS however strongly recommends that certificates containing medical data are directly transferred by the data subjects to an external medical service preferably within the Community institutions and bodies, which transfer shall be done in accordance with Article 7 of the Regulation. The HR section shall therefore not process nor store any medical data in any of the time and management files. Data subjects shall be clearly directed to send their medical certificates to the designated external medical service.

3.7. Processing of personal number or unique identifier

The SAP database and paper forms include the processing of the personal identification number. In itself, the use of an identifier is simply a means – in this case, a legitimate means – of assisting the work of the data controller, although it can have important consequences. According to Article 10(6) of the Regulation, the EDPS shall determine the conditions under which a personal number or other identifier of general application may be processed by a Community institution or body.

Since the unique identification number is used solely for administrative reasons, the EDPS considers that it does not raise any specific risks justifying the adoption of particular guarantees in this case.

3.8. Rights of access and rectification

Article 13 of the Regulation establishes a right of access upon request by the data subject. Article 14 of the Regulation provides the data subject with a right of rectification.

Statutory staff of ECDC who is required to use SAP has direct access to, and may correct directly most of his/her personal data contained in the SAP database (within the last 3 months), which allows him/her to exercise these rights in an effective manner.

In general, staff working at ECDC can always exercise their rights of access and rectification at any time by contacting the data controller in writing. The EDPS however notes that the data protection notice provided by ECDC in respect of time and absence management limits the exercise of the rights of access and rectification upon request to the data controller to "basic identity information". The EDPS stresses that the right of access and rectification applies to any personal data processed about data subjects, and this whether they are processed on SAP or on any other electronic and/or paper files.

Moreover, trainees should also be guaranteed the right to access and rectify their data processed in paper files.

Furthermore, the EDPS notes that family members whose data are disclosed by a staff member should also be ensured the right to access and rectify their data. This could be done by inserting in the data protection notice a statement asking the staff who discloses information about a third person (family member or other) in the context of time and absence management to inform this person about his/her rights to access and correct data relating to him/her.

The EDPS therefore recommends that the data protection notice is modified to reflect the recommendations made above.

3.9. Information to the data subject

Articles 11 and 12 provide for information to be given to data subjects in order to ensure the transparency of the processing of personal data. Article 11 provides that when the data is obtained from the data subject, the information must be given at the time of collection. When the data have not been obtained from the data subject, the information must be given when the data are first recorded or disclosed, unless the data subject already has it (Article 12).

In the present case, a data protection notice is provided to persons working at ECDC. The EDPS suggests that the following modifications are implemented in the notice to ensure full compliance with Articles 11 and 12 of the Regulation:

- trainees and staff family members should also be informed of the data processing concerning them. As concerns family members, this can be done by requesting staff members to inform the persons whose data they disclose about the content of the data protection notice.

- the notice shall clearly indicate the data retention periods that are applicable.

- in the section "lawfulness of the processing and legal basis", it is not clear how the mention of "*the selection procedures are necessary for the management and functioning of the Center*" is relevant in the context of time and absence management.

3.10. Security measures

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

On the basis of the available information, the EDPS does not see any indication to believe that ECDC has not applied the security measures required in Article 22 of the Regulation.

4. Conclusion:

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

- The processing is lawful to the extent that it is limited to the purpose of time and absence management. If the processing is intended to monitor on a regular basis the staff and to evaluate personal aspects of the data subject, such as his/her ability, efficiency or conduct, a specific legal basis must be adopted by ECDC in order to carry out the processing for such purposes. In this view, there is currently no legal basis allowing for the production of reports on an individual basis for purpose of monitoring the staff with a view to evaluating them;

- Sensitive data which processing by ECDC falls within the scope of Article 10(2)(b) may only be processed for the lawful purposes for which the processing takes place. The processing of data relating to health shall be strictly limited to data indicating the sickness status but shall not extend to obtaining confidential information providing a medical diagnosis about the health of the data subjects. Specific guarantees shall be implemented as regards the processing of other sensitive data to ensure that this information is not held against the data subject, as described in section 3.3;

- The collection by the HR section of medical expenses and benefits in the attendance file is not relevant in the sense of Article 4 (1)(c) for purpose of time and absence management;

- The EDPS would like to insist on the determination of appropriate conservation periods. These conservation periods must be assessed on the basis of the purposes for which the data are collected and processed, with due account of all the means of processing used and in which data are stored;

- Certificates containing medical data shall be directly transferred by the data subjects to an external medical service preferably within the Community institutions and bodies, which transfer shall be done in accordance with Article 7 of the Regulation. The HR section shall therefore not process nor store any medical data in any of the time and management files. Data subjects shall be clearly directed to send their medical certificates to the designated external medical service;

- As regards data quality, every reasonable step must be taken to ensure that data which are inaccurate or incomplete are erased or rectified. The right to access and rectification shall be ensured to any data subjects, including trainees and staff family members whom data are disclosed, and with respect to any personal data processed about that person, whatever the format in which the data is processed;

- The data protection notice shall be amended in accordance with the recommendations made in sections 3.8 and 3.9 above.

Done at Brussels, on 22 June 2009

(signed)

Giovanni BUTTARELLI
Assistant European Data Protection Supervisor