Opinion on the notification of a prior check received from Data Protection Officer of the European Commission in relation to the file *'persons with reduced mobility – emergency plan'*.

Brussels, 11 November 2009 (File 2009-0014)

1. Procedure

On 6 January 2009, the Data Protection Officer ('the DPO') of the European Commission ('the Commission') submitted a notification pursuant to Article 27(3) of Regulation (EC) No 45/2001 regarding the file ***'persons with reduced mobility – emergency plan'*.**

On 9 February 2009, the Commission DPO was sent some questions by email. Answers and clarifications were returned on 9 July 2009. The draft opinion was sent to the Commission DPO on 4 September for comments. Comments were received on 11 November 2009.

2. Facts

The processing of personal data relating to ***'persons with reduced mobility – emergency plan'*** is carried out by department DG-ADMIN.DS.6 of the Commission.

Data subjects
The data subjects are all Commission staff and all visitors who have reduced mobility ('persons with reduced mobility' or 'PRM').

Purpose
The purpose of the data processing is to provide more effective assistance for persons with reduced mobility during evacuation drills and in the event of a genuine emergency evacuation of the Commission buildings.

Legal basis
The legal basis for the processing operation arises from Article 1(6) of the Staff Regulations of Officials of the European Communities ('the Regulations') and Commission Decision C(2006)1623 of 26 April 2006 establishing a harmonised policy for health and safety at work for all Commission staff.

An agreement was signed between the Commission and the security company that employs the security agents collecting the data for the data processing operation in question. The agreement is governed by Belgian law. Clause I.9 of this agreement makes reference to the principle of data protection and stipulates, inter alia, that, *'the contracting party may only act on the instructions of the data controller…'*. Furthermore, Clause I.9 of the agreement lists all the security measures provided in Article 22(2)(a-i) of Regulation (EC) No 45/2001. Clause II.9 of the agreement emphasises the principle of confidentiality, stipulating that, *'the contracting party shall obtain an undertaking from all members of its staff and its administrative and management*

bodies to respect the confidentiality of all information directly or indirectly connected with the performance of their duties and not to disclose this information to third parties...'.

Procedure and processing operation

According to the procedure established by DG-ADMIN.DS.6, upon arrival in the Commission building or when transferring to a different building, data subjects are invited by the security agent to record their details, on a purely voluntary basis, in the register book entitled 'Assistance in the event of an evacuation', which is kept at the building's reception desk. The main details they have to record are the times of their arrival and departure, the location they will be in and the telephone number of that location.

The register consists of individual forms and is in two sections: one for staff and one for visitors. The security agent who collects the data from the data subject also fills in their own name on each form.

For the staff form, the data subject provides the following data:

- start date,
- end date (optional),
- surname and first name,
- building/office,
- telephone number,
- type of assistance (optional), and
- signature of consent.

For the visitor form, the data subject provides the following data:

- date,
- surname and first name,
- building/office,
- telephone number,
- type of assistance (optional)
- signature of consent, and
- time of entry and time of departure.

On both forms (for staff and visitors) if the 'signature of consent' is required, it is explicitly stated that by signing the form the person acknowledges that they have received the regulatory information about the processing of the data, in particular the information notice, as well as the instructions to be followed in the event of an evacuation.

A consultation record is also kept, which lists the date, name and capacity of the person who has consulted the form, together with the reason and their signature. Persons organising evacuation exercises may ask to see the list of PRMs, so that they can provide more effective assistance. The security agents must then indicate the reason for the request and enter their name on the form.

Recipients

The recipients of the collected data forms are:

- the security guards on duty at the reception desks,
- first response fire officers,
- fire chiefs, and
- persons responsible for evacuation, namely the emergency fire teams.

All these persons only have access to the forms in the event of an emergency.

The security agents on duty in the reception areas belong to an outside security company and are managed by the Commission's Security Department.

The other recipients are either officials or employees with a different status and are employed by the Commission.

Right of access, rectification, blocking and erasure
It is stated in the notice that data subjects are free at all times to consult their data and to have them rectified by the security officers.

Requests to block or erase data are implemented within 48 hours, provided that the request is justified.

Right to information
As regards the right to information, the notification states that an information notice entitled 'Information for Persons with Reduced Mobility' is available at the reception desks when data subjects voluntarily register their details, as well as on the IntraComm website. The following information is provided in this notice: the identity of the processor, the purpose of the processing operation, the recipients, the fact that it is optional to answer the questions, the right of access and rectification, the legal basis of the processing operation, the time limit for keeping the forms and the right to call upon the EDPS at any time.

Storage of data
Outdated forms pertaining to Commission staff are checked and disposed of at the end of each month. Visitor forms are checked and disposed of at the end of each month. DG-ADMIN.DS.4 is responsible for destroying the forms.

Before the forms are disposed of, an anonymous statistics form is compiled, listing the month and/or year, the number of persons with reduced mobility and the name of the security agent.

How the data is kept and security measures
The only information in the notice is that the data are collected in paper format and that the register is kept at reception under the watch of the guards in the various buildings.

3. Legal aspects

3.1. Prior Check

Regulation (EC) No 45/2001 applies to the processing of personal data by all Community institutions and bodies insofar as such processing is carried out in the exercise of activities all or part of which fall within the scope of Community law (Article 3(1)). The data processing in question here is carried out by the Commission and the processing is carried out in the context of activities that fall within the scope of the first pillar and hence within the scope of Community law.

Data on persons with reduced mobility are processed in paper format which is intended to form part of a filing system. Article 3(2) of the regulation therefore applies.

This processing operation therefore falls within the scope of Regulation (EC) No 45/2001.

Article 27(1) of Regulation (EC) No 45/2001 states that 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 shall be subject to prior checking by the EDPS. Article 27(2)(a) mentions 'processing of data relating to health and to suspected offences, offences, criminal convictions or security measures' as being operations likely to present such risks. The processing operation in question is aimed at a special category of people, namely people with reduced mobility, with a view to providing them with assistance during evacuation drills and in the event of an emergency evacuation of the building. There is clearly a medical aspect to reduced mobility. In particular, the information that data subjects may be requested to volunteer about the type of assistance they may need, in case of an emergency, could reveal information about their health. This is why this processing operation comes under the scope of the prior checking procedure on the basis of Article 27(2)(a) of Regulation (EC) No 45/2001.

In principle, the check by the EDPS should be carried out prior to the processing operation being put in place. In this case, because the EDPS was appointed after the operation had already been put in place, the check is necessarily an ex post check. This in no way affects the implementation of the recommendations made by the EDPS.

The official notification was received by post on 6 January 2009. Under the terms of Article 27(4) of Regulation (EC) No 45/2001, the two-month period within which the EDPS must deliver his opinion was suspended. Due to the 218-day suspension, the EDPS will therefore deliver his opinion by 11 November 2009 at the latest (150 days of the suspension + 68 days for comments).

3.2. Lawfulness of the processing operation

According to Article 5 of Regulation (EC) No 45/2001, personal data may only be processed when at least one of the five conditions stipulated in this Article is met.

Among the five conditions stipulated in Article 5, Article 5(a) specifically provides that the data processing may be carried out 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 in the legitimate exercise of official authority vested in the Community institution or body'*.

In the light of this condition, two factors need to be analysed, the first being whether or not the processing operation is required under the Treaties establishing the European Communities or other legal instruments and the second being whether the processing operation is necessary in the public interest (necessity test).

In the case in point, the **legal basis** for the processing operation is Article 1(6) of the Regulations and Commission Decision C(2006)1623 of 26 April 2006 establishing a harmonised policy for health and safety at work for all Commission staff.

The necessity of processing operations is also referred to in Paragraph 27 of the preamble to Regulation (EC) No 45/2001, which 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*'. In the case in point, the processing is necessary for the management and smooth running of the Commission in the context of 'a harmonised policy for health and safety at work for all Commission staff'. The EDPS considers in particular that the work done by DG-ADMIN.DS.6 is part of a 'task carried out in the public interest', since the collection of particular data by the security guards is necessary in terms of safeguarding the wellbeing and

safety of persons with reduced mobility in the event of an emergency evacuation of the Commission buildings.

Furthermore, the processing operation also fulfils the condition stipulated in Article 5(d), requiring that *'the data subject has unambiguously given his or her consent'*. In this instance, the data subjects register their names in the book and fill in the form on a voluntary basis if they require assistance in the event of an emergency evacuation. The EDPS is completely satisfied that the information regarding the type of assistance is stated as being optional and that data subjects are only required to sign the form if they have received the regulatory information regarding the data processing.

The proposed processing operation therefore complies with the requirement of lawfulness.
Moreover, in Article 10 of Regulation (EC) No 45/2001, data concerning health are classed under *'Special categories of data'*.

3.3. The processing of special categories of data

Article 10(1) of Regulation (EC) No 45/2001 stipulates that the processing of health-related personal data is prohibited unless it is justified on the grounds stated in Article 10(2) or Article 10(3).

Article 10(2)(b) states that the prohibition on processing health-related data does not apply when, *'processing is necessary for the purposes of complying with the specific rights and obligations of the controller in the field of employment law insofar as it is authorised by the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof'*. In this case, the processing of health-related data, namely the question about the type of assistance required by data subjects who are staff members is justified as it is necessary in order for the Commission to abide by its specific obligations and duties as an employer, in accordance with Article 10(2)(b).

Moreover, the prohibition on processing health-related data does not apply *'when the data subject has given his or her express consent'*, as stipulated in Article 10(1). In this instance, the data subjects, including visitors, provide the data in question voluntarily to the security agents (see point 3.1 above).

No information about the nature of the subject's disability is disclosed in the register. However, the nature of the register itself, which records the surname and first name of the person with reduced mobility and the type of assistance they will need, allows data relating to the data subjects' health to be deduced even though the nature of their disability is not specified. In view of this, the EDPS recommends that the whole security agent team be reminded that data relating to health must be handled in accordance with the principles of medical secrecy and that the agents should be required to abide by a duty of professional secrecy equivalent to that of healthcare professionals, in order to ensure compliance with Article 10(3) of Regulation (EC) No 45/2001.

3.4. Controller and processor

According to Article 2(d) of Regulation (EC) No 45/2001, the data controller is *'the Community institution or body, the Directorate-General, the unit or any other organisational entity which alone or jointly with others determines the purposes and means of the processing of personal data'*. The controller is responsible for ensuring that the obligations laid down by the regulation are fulfilled (duty of information towards the data subject, safeguarding the data subject's rights,

choice of data processor, notifying the Data Protection Officer, etc). The processor is the *'natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller'* (Article 2(e)).

In this case, the security agents are managed by a security company with which the Commission has signed an agreement.

The Commission can be defined as the controller as it is the Commission that determines the purpose and means of collecting the data subjects' data, namely by creating a register of staff and visitors with reduced mobility in order to provide them with more effective assistance and safety. The security company can be defined as the processor as it processes the data on the Commission's behalf. In particular, the security agents, who are employed by the security company, collect the data concerning the staff and visitors with reduced mobility in accordance with the instructions of the Commission's Security department. The roles of the controller and the processor are therefore in compliance with Articles 2(d) and 2(e) respectively of Regulation (EC) No 45/2001.

3.5. Data quality

According to Article 4(1)(c) of Regulation (EC) No 45/2001, personal data must be *'adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed'*. The processed data described above under the heading 'Facts' are necessary and relevant in relation to the purpose of the processing operation. The EDPS is therefore satisfied that there is compliance with the principle of proportionality expressed in Article 4(1)(c).

Moreover, the data must be *'processed fairly and lawfully'* (Article 4(1)(a)). The lawfulness of the treatment has already been dealt with in point 3.2 of this opinion. As regards fairness, this relates to the information that should be communicated to the data subject (see point 3.9 above).

Article 4(1)(d) of Regulation (EC) No 45/2001 provides that the data must be *'accurate, and where necessary, kept up to date'*. Furthermore, according to the same Article, *'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'*. It can be reasonably assumed that the procedure in place ensures that the data are accurate and up to date. Furthermore, the data subject is made aware of their right to access and rectify the data, which will ensure that the register of forms is as complete as possible. These rights also constitute a further means of guaranteeing the quality of the data (see point 3.8 below).

3.6. Storage of the data

The general principle laid down in Regulation (EC) No 45/2001 is that personal data must be *'kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed'* (Article 4(1)(e)).

As already mentioned, outdated forms pertaining to staff are checked and disposed of at the end of each month and visitor forms are checked and disposed of at the end of each month.

The EDPS considers this time limit to be reasonable and for both groups of data subjects is proportionate to the intended purpose of the data processing.

The data are also collected for statistical purposes in an anonymous format and are stored by DG-ADMIN.DS.4. This further processing is in compliance with Article 4(1) of Regulation (EC) No 45/2001.

3.7. Transfer of data

The processing operation must also be examined in relation to Article 7(1) of Regulation (EC) No 45/2001. The processing operation referred to in Article 7(1) is the transfer of personal data within or between Community bodies if '*necessary for the legitimate performance of tasks covered by the competence of the recipient'*.

To ensure compliance with the provisions of Article 7.1, the Commission must ensure both that all recipients are properly qualified and that the transfer is necessary. In this instance, we are dealing with transfer within the Commission to the first response fire teams, fire chiefs and persons responsible for evacuation and to DG-ADMIN.DS.4 (to erase the data and store the anonymous forms). These recipients perform specific duties and the data that are transferred to them are necessary for the legitimate performance of the tasks that fall within the scope of these duties. The EDPS therefore considers these transfer operations acceptable under the terms of Article 7(1) of Regulation (EC) No 45/2001.

In addition, in accordance with Article 7(3) of Regulation (EC) No 45/2001, which stipulates that *'the recipient shall process the personal data only for the purposes for which they were transmitted'*, the EPDS recommends that recipients within the Commission and other institutions be reminded to process the data only for the purposes for which they were sent to them.

The EPDS wishes to emphasise that he may also be considered to be a recipient of the data on the basis of Regulation (EC) No 45/2001. For example, under the terms of Article 33 (*Complaints by Community staff*) and Article 47(2)(a), he has the right to ask the controller or the Community institution or body for access to any personal data and any information needed for his enquiries. According to the provisions of the Annex to Regulation (EC) No 45/2001, the DPO of the institution in question is also considered to be a potential recipient. Other potential recipients may be the Mediator, OLAF and the European Union Civil Service Tribunal. Article 7(3) must also be complied with in this respect.

Furthermore, the data may also be forwarded to the security company, which is an external body governed by Belgian law. In view of this, the data processing must be examined in the light of Article 8 of Regulation (EC) No 45/2001 with respect to these transfers of data. In this instance, the transfer is covered by Article 8(a), which states that the transfer may be carried out *'if the recipient establishes that the data are necessary for the performance of a task carried out in the public interest or subject to the exercise of public authority'*. The transfer of certain data to the security agents employed by the external company is justified since the transfer is necessary for the performance of the task that the Commission has asked this company to perform in the public interest.

3.8. Right of access and rectification

Article 13 of Regulation (EC) No 45/2001 lays down terms regarding the right of access and procedure for access at the data subject's request. The terms of Article 13 stipulates that the data subject has the right to obtain without constraint from the controller *'communication in an*

intelligible form of the data undergoing processing and of any available information as to their source'.

Article 14 of Regulation (EC) No 45/2001 lays down terms regarding the data subject's right of rectification. Just as data subjects have the right of access, they also have the right to change their personal data if necessary.

In the case in question, the data subjects have the opportunity to check their data with the security agents and have them rectified at any time.

Therefore, there is compliance with Articles 13 and 14 of Regulation (EC) No 45/2001.

3.9. Information to be given to the data subject

Articles 11 and 12 of Regulation (EC) No 45/2001 refer to the information that should be supplied to data subjects with a view to ensuring that their personal data are processed in a transparent manner. These articles contain a list of compulsory and optional provisions. These provisions are applicable insofar as, taking into account the particular circumstances surrounding the processing operation in question, they are necessary in order to ensure that the data are processed fairly with respect to the data subject.

In this case, the provisions of Article 11 (*Information to be supplied where the data have been obtained from the data subject*) regarding supplying information to the data subject are applicable, since all the data collected are supplied directly by and with the consent of the person with reduced mobility in question.

As mentioned above, an information notice entitled 'Information for Persons with Reduced Mobility' is available at the reception desks when data subjects voluntarily register their details, as well as on the IntraComm website. The following information is provided in this notice: the identity of the processor, the purpose of the processing operation, the recipients, the fact that it is optional to answer the questions, the right of access and rectification, the legal basis of the processing operation, the time limit for keeping the forms and the right to call upon the EDPS at any time.

The EDPS notes that all the information laid down in Article 11 of Regulation (EC) No 45/2001 is stated in the information notice provided for the data subjects before their data are processed. This fulfils the requirements of transparency and fairness set out in Regulation (EC) No 45/2001.

3.10. Processing by a processor

When a processing operation is carried out on behalf of the controller, Article 23 of Regulation (EC) No 45/2001 stipulates that the controller should choose a processor who can supply adequate guarantees as to the technical and organisational security measures required by the above-mentioned regulation. Performance of data processing by a processor must be governed by an agreement or other binding legal instrument between the processor and the controller, which should stipulate in particular that the processor must only act under the instructions of the controller and that the duties of confidentiality and security regarding the processing of personal data also apply to the processor.

As mentioned above, an agreement was signed between the Commission and the security company. Provisions regarding data protection and security measures are set forth in Clause I.9 of the agreement. The confidentiality principle is stipulated in Clause II.9 of the agreement. It is

also expressly stated that the processor may only act under the instructions of the data processing controller.

The EDPS considers that the provision regarding the role of the processor complies with the terms of Article 23(2)(a) of Regulation (EC) No 45/2001. The duties set forth in Articles 21 (Confidentiality of processing) and 22 (Security of processing) are also complied with, in accordance with the provisions of Article 23(2)(b). The EDPS therefore considers that the agreement between the Commission and the security company fulfils the conditions laid down in Article 23 of Regulation (EC) No 45/2001.

3.11. Security

According to Article 22 of Regulation (EC) No 45/2001 on the security of data 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'*.

The EDPS has not been informed of any security measures that might meet this condition. The EDPS therefore recommends that adequate concrete security measures be taken pursuant to Article 22 of Regulation (EC) No 45/2001.

Conclusion

In order for the processing in question to be compliant with the provisions of Regulation (EC) No 45/2001, the observations set out above must be taken on board. This implies in particular that the Commission:

- must ensure that all security agents are reminded to handle health-related data in accordance with the principles of medical confidentiality and that they should be under a duty of professional secrecy equivalent to that of a healthcare professional;

- must ensure that any persons involved in the processing operation who receives and processes the data be informed that the data may only be used for the purposes of the processing operation;

- must adopt adequate concrete security measures for the processed data, in accordance with Article 22 of Regulation (EC) No 45/2001.

Done at Brussels on 11 November 2009

(signed)

Giovanni BUTTARELLI,