Opinion on the notification for prior checking from the Data Protection Officer of the European Parliament regarding the "individual workplace" dossier

Brussels, 17 December 2009 (Case 2009-650)

1. Procedure

On 20 July 2009 a consultation within the meaning of Article 27(3) of Regulation (EC) No 45/2001 ("the Regulation") was sent to the European Data Protection Supervisor (EDPS) by the Data Protection Officer of the European Parliament concerning the need for prior checking in connection with the "individual workplace" dossier. The EDPS gave a favourable reply on 12 October 2009, which counts as the official date on which note was taken of the notification of the said processing operation.

The draft opinion was sent for comments on 8 December; these were received on 16 December 2009.

2. The facts

The purpose of the processing operation is to use data in following up requests for an analysis and in recommendations made in the course of work-related ergonomic assessments.

The data subjects are all officials and other staff and, in future, will also include Members of Parliament and accredited assistants.

Description of the processing operation: the Prevention and Protection at Work Service may receive a request directly from the data subject or following a campaign by that unit, or upon a request from the Medical Service to furnish the data subject's office. The unit then conducts an inquiry and draws up a file note addressed to both the data subject and the Medical Service. It contains more references to the environment than to the data subject's personal traits. Recommendations are forwarded to the departments concerned (IT, telecommunications, furniture supplies). The latter sometimes receive a separate note instead of the file note.

The following data are processed: administrative addresses, telephone and health-related information.

Data subjects receive the following information: a copy of the report. General information in the form of a confidentiality statement is non-existent.

Exercise of the right of access and the right of rectification is ensured by the Bureau's Decision of 22 June 2005.

The processing operation consists of manual processing of personal data contained in a file.

The information is forwarded to the medical officer and the departments concerned by the issue of recommendations. The data are transmitted on paper only.

The data are kept indefinitely (as long as the data subjects are employed by the European Parliament), which is justified by the fact that the health condition at issue may persist or reappear. They are also kept for historical, statistical or scientific purposes but would not seem to be rendered anonymous when the controller notifies the DPO.

In view of the security measures [...].

3. Legal aspects

3.1. Prior checking

The management of data in inquiries and reports relating to the ergonomic conditions of individual workplaces constitutes processing of personal data ("any information relating to an identified or identifiable natural person" - Article 2(a) of the Regulation). The data processing is carried out by an institution in the exercise of activities which fall within the scope of Community law.

The processing is carried out manually and the data are intended to form part of a structured system of data which are accessible via specific criteria (Article 3(2) of the Regulation).

The processing therefore falls within the scope of the Regulation.

Article 27(1) of the Regulation requires prior checking by the EDPS of processing operations likely to present specific risks to the rights and freedoms of data subjects. Article 27(2) lists the processing operations likely to present such risks. In Article 27(2)(a) processing operations likely to present such risks are described as "*processing of data relating to health and (…)*". Inquiries and recommendations relating to workplace ergonomics constitute processing of personal data coming within the scope of Article 27(2) and as such subject to prior checking by the EDPS. Article 27(2)(a) is applicable because the processing specifically concerns data relating to health.

In principle, the EDPS carries out his checks before the processing is set up. In this case, the EDPS was appointed after the system had been set up, and therefore checking necessarily has to be performed *ex post.* That in no way prevents suitable application of recommendations made by the EDPS.

On 20 July 2009 the European Parliament's DPO consulted the EDPS under Article 27(3), in connection with the "individual workplaces" dossier on whether the processing involved had to undergo prior checking. The EDPS responded favourably on 12 October 2009, which therefore counts as the official date on which note was taken of the notification of the processing at issue. Work on the case was suspended for 8 days in order to allow the DPO and the controller to comment on the decision. The EDS will therefore deliver an opinion by 21 December 2009 (13 December 2009 plus 8 days of suspension).

3.2. Lawfulness of the processing operation

The lawfulness of the processing operation must be examined in the light of Article 5(a) of the Regulation, which provides that *"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".

In this case, the Prevention and Protection at Work Service acts in the context of a task carried out in the public interest. The processing operation set up contributes significantly to the sound functioning of the institution by ensuring the health and safety of staff at work. Assessment of ergonomic needs and the occasional processing of health-related data are necessary to fulfil this task. The lawfulness of the proposed processing operation has, therefore, been observed.

The legal basis for the processing operation derives from the implementation of Directives 89/391 (of 12 June 1989 on the introduction of measures to encourage improvements in the safety and health of workers at work) and 90/270 (of 29 May 1990 on the minimum safety and health requirements for work with display screen equipment) as well as Article 1e(2) of the Staff Regulations of officials of the European Communities ("*Officials in active employment shall be accorded working conditions complying with appropriate health and safety standards at least equivalent to the minimum requirements applicable under measures adopted in these areas pursuant to the Treaties.*").

The legal basis therefore complies with and supports the lawfulness of the processing operation.

Furthermore, health-related data are described in Article 10 of the Regulation as "special categories of data".

3.3. Processing of special categories of data

Files compiled during the processing of inquiries and recommendations relating to ergonomics may occasionally include data on the health of officials or other staff.

Article 10(1) provides that "*the processing of (…) data concerning health (…) are prohibited.*"

Article 10(2)(b) applies to this case: *"paragraph 1* (prohibiting the processing of data concerning health) *shall not apply where 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…".* Here the Parliament, in its capacity as employer, is actually complying with Article 10(2)(b) by processing the data submitted (see "legal basis" above).

Lastly, in this case, certain health-related data are provided by the Medical Service (request made by the Medical Service. Given the nature of such data (concerning health), Article 10(3) (special categories of data) of the Regulation is applicable here. That provision stipulates that "*paragraph 1* [prohibition on the processing of data concerning health] *shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy*". By dint of their posts, the doctors and staff of the services concerned are bound by professional secrecy. In this context Article 10(3) is duly complied with.

However, all persons (other than Medical Service staff) processing these data must be informed that they are bound by professional secrecy, in order to ensure the processing of special categories of data, as recommended by the EDPS.

3.4. Data quality

"Personal 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 the Regulation).

The data processed in connection with the Prevention and Protection at Work Service's files may be health-related. It is important that persons processing the data relating to the various files should be properly informed of their obligation to respect the principle established by Article 4(1)(c), and that they should take that principle into account when processing the data. The EDPS recommends that everyone processing such data should be informed of the obligation to observe the principle set out in Article 4(1)(c) of the Regulation.

The data must also be "processed fairly and lawfully" (Article 4(1)(a) of the Regulation). Lawfulness of the processing operation has already been considered in section 3.2 of this opinion. Fairness relates to the information which has to be given to the data subject (see section 3.8 below).

Finally, the 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 data subject has right of access to data and right to rectify data, in order to ensure that the file is as complete as possible. See point 3.7 below on these two rights (access and rectification).

3.5. Storage of data

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) of the Regulation).

The data are kept indefinitely. Provision has also been made to keep them for historical, statistical or scientific purposes, but they are not rendered anonymous.

The EDPS finds this storage period unacceptable. The fact that health problems may reappear is no justification in itself. The EDPS recommends that a proportionate time-limit be set, and that data kept for statistical purposes be rendered anonymous.

3.6. Transfer of data

The processing operation should also be examined in the light of Article 7(1) of the Regulation. The processing alluded to in Article 7(1) is the transfer of personal data within or between Community institutions or bodies "if the data are necessary for the legitimate performance of tasks covered by the competence of the recipient".

The EDPS wonders about the need to transfer medical data to the departments affected by the implementation of recommendations made. The EDPS recommends that health-related data only be supplied to the Medical Service and that they be deleted upon drafting the note addressed to the various departments which sets forth the recommendations to be implemented.

3.7. Right of access and right of rectification

Article 13 of the Regulation makes provision, and sets out the rules, for exercising a right of access at the data subject's request. Article 14 affords the data subject a right of rectification. The notification states that both rights are guaranteed by the Bureau's Decision of 22 June 2005 (implementing rules relating to Regulation (EC) No 45/2001 - Articles 8 et seq.)

The EDPS welcomes the possibility afforded to data subjects to exercise their rights, but underlines the need to inform them thereof (see below).

3.8. Information to be given to data subjects

The Regulation stipulates that the data subject must be informed if his or her personal data are processed and specifies a series of compulsory items - for some of which the obligation depends on circumstances - to be provided to the data subject unless he or she already has such information. In the present case, some of the data are collected directly from the data subject: here, Article 11 *(Information to be supplied where the data have been obtained from the data subject)* is applicable. Other data are collected from the Medical Service: in that case, Article 12 *(Information to be supplied where the data have not been obtained from the data subject*) concerning information to be supplied to the data subject is applicable.

The only information supplied to the data subject is the report drawn up by the unit. The fact that there is no confidentiality declaration prevents the data subject from exercising his or her rights fully. Providing information to the data subject also contributes to fair processing of the data relating to him or her (see 3.4 above). Consequently, the EDPS recommends that, for the type of processing at issue here, all the provisions of Articles 11 and 12 be communicated to the data subjects, so that these Articles of the Regulation can be complied with in full. This could take the form of a posting on the said unit's website or the circulation of the outcome, by the unit, each time an inquiry has been conducted and a report transmitted.

3.9. Security

Article 22 of Regulation (EC) No 45/2001 provides that the controller must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks presented by the processing and the nature of the personal data to be protected. These security measures must, among other things, prevent any unauthorised disclosure or access.

Both the technical and organisational measures taken in relation to this processing are described in detail.

On the basis of the information available, the EDPS has no reason to believe that the Parliament has not complied with the security measures required by Article 22 of the Regulation.

Conclusion

In order to comply with Regulation (EC) No 45/2001, the proposed processing operation must take the above comments into account. This means, in particular, that:

- all persons processing the data in question should be informed that they are bound by professional secrecy, in order to ensure the processing of special categories of data;
- everyone processing such data should be informed of the obligation to observe the principle set out in Article 4(1)(c) of the Regulation;

- a proportionate time-limit should be set, and data kept for statistical purposes rendered anonymous;
- health-related data should be deleted upon drafting the note addressed to the various departments which sets forth the recommendations to be implemented;
- all the provisions of Articles 11 and 12 should be communicated to the data subjects, so that these Articles of the Regulation can be complied with in full.

Done at Brussels, 17 December 2009.

[Signed]

Giovanni BUTTARELLI
Assistant European Data Protection Supervisor