**Opinion on the notification for prior checking from the DPO (Data Protection Officer) of the Council of the European Union in relation to the "Vaccination Programme" dossier**

Brussels, 5 May 2006 (Case 2004-262)

## 1. Procedure

1.1. On 20 July 2004 the European Data Protection Supervisor (EDPS) sent a letter to the Data Protection Officers (DPOs) asking them to prepare an inventory of data processing operations that might be subject to prior checking by the EDPS as provided for by Article 27 of Regulation (EC) No 45/2001 (hereinafter referred to as "the Regulation"). The EDPS requested notification of all processing operations subject to prior checking, including those that commenced before the Supervisor was appointed and for which checking could never be regarded as prior, but which would be subject to "ex post" checking.

1.2. On the basis of the inventories received from the Data Protection Officers, the EDPS identified priority issues, including the medical files. On 10 November 2005, the EDPS asked all the DPOs to update their inventories.

1.3. On 30 November 2005, the EDPS received postal notification regarding prior checking of data processing in the context of the "Vaccination Programme" dossier.

1.4. Additional questions were sent on 5 December 2005, 24 March 2006 and 24 April 2006. The replies were received on 10 March 2006, 24 March 2006 and 25 April 2006, respectively.

## 2. Examination of the case

### 2.1. The facts

The purpose of the data processing operation is to ensure that personalised vaccination programmes and the various booster vaccinations are updated and monitored, at the request of the data subject for personal reasons or in the interests of the service.

The data subjects are the officials, temporary staff and auxiliary staff.

The categories of data are as follows:

A) Periodic list (2-3 weeks) of persons selected and the vaccines to be administered to them as of that date. Data contained in that periodic list: identification (personnel number); full name and date of birth; date of last vaccination; type of vaccine and new date of vaccination.

B) Patient file (personal data). Data contained in the patient file: identification; full name; date of birth; office; address. There follows a list of all the vaccines, setting out their status, dates of previous injections and the date of the next injection.

C) Standard booster reminder letters. Data contained in the standard letter: full name; office address; the booster in question; the vaccines already administered and the date of the next booster.

As regards the information, the dispensary staff inform the data subjects in writing (printout of computer file) of their forthcoming vaccinations and inform them orally that they may request a copy of their personal file under the responsibility of the controller. A copy is also filed in the personal medical file. This information is provided when vaccines are updated or at any other time at the request of the data subject. Most of the data entered in the vaccination programme are provided by the data subjects themselves and are supplemented in the course of periodic updates.

At the request of the data subject, the medical service will print out the personalised "patient" file. Rectifications may be made by the data subject. Data can be deleted only at the express request of the data subject; the reasons for deletion are specific to the data subject in question. The controller pointed out that it was not in the interest of the data subject to request deletion, since it was he or she who had provided the information for monitoring purposes. After deletion at the request of the data subject, the medical service would no longer have a written record on the basis of which to continue to update the data.

The processing operations are carried out automatically (updatable programme installed on a PC with a back-up made by the ITD) and manually (hard copy, file for patients who request a copy).

The persons to whom the data are likely to be communicated are GSC doctors and nursing staff.

With regard to the personal data storage policy, the controller pointed out that the data remained useful even for people no longer in active service. A printout of their file is supplied to them. A copy is placed in the medical file and the electronic version is then deleted.

The vaccination programme is not "obligatory". It is an aspect of preventive medicine, and takes account of the protection which the employer is supposed to offer workers in the context of missions. Before departing on mission, officials are informed of medical factors, particularly in relation to the vaccine against yellow fever (the only obligatory vaccine for access to certain countries), malaria prevention and recommendations regarding other vaccines considered to be useful, particularly in countries in which, owing to hygiene conditions, certain preventable contagious diseases are more frequent. In view of the seriousness of yellow fever and malaria, the employer could not contemplate exposing employees to a known and avoidable risk before sending them on mission. For all other non-obligatory vaccines, the employer facilitates its employees in every way, taking account of the medical basis for this practice.

Security measures have been adopted. [...]

## 2.2. Legal aspects

### 2.2.1. Prior checking

The management of data concerning the vaccination programme constitutes processing of personal data ("*any information relating to an identified or identifiable natural person*" – Article 2(a)). The data processing in question is carried out by an institution in the exercise of activities which fall within the scope of Community law (Article 3(1)), and is carried out wholly or partly by automatic means, or intended to form part of a filing system (Article 3(2)). Accordingly, it falls within the scope of Regulation (EC) No 45/2001.

Article 27(1) of Regulation (EC) No 45/2001 requires prior checking by the EDPS of 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 likely to present such risks.

The present case qualifies for prior checking given that it concerns "*processing of data relating to health"* (Article 27(2)(a)). The processing operations performed in the context of the vaccination programme fall into this category.

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

The DPO's notification was received on 30 November 2005. Under Article 27(4) the present opinion must be delivered within the following two months. The deadline was suspended for 99 days; the Supervisor therefore had to deliver his opinion by 5 May 2006.

### 2.2.2. Legal basis and lawfulness of the processing operation

The general legal basis for processing is Article 207 of the EC Treaty, under which the Council adopts its own rules of procedure. Article 23 of the Council Decision of 22 March 2004 adopting the Council's Rules of Procedure stipulates that the Council shall decide on the organisation of the General Secretariat.

More specifically, the legal basis for processing is Article 59(6) of the Staff Regulations: "Officials shall undergo a medical check-up every year either by the institution's medical officer or by a medical practitioner chosen by them. (…)".

In practice, Article 59(6) of the Staff Regulations provides for preventive medical action. It implements an obligation which does not concern the vaccination of officials going on mission, but introduces an annual check-up. Vaccination, which also constitutes preventive medical action, is not covered by a specific provision. Nonetheless, the employer has a duty

of care towards its employees under the general principle of responsibility. The vaccination programme is not obligatory, but it enables the employer to apply the above principle to the officials it sends on mission to countries in which there are "obligatory" vaccinations. The programme also offers officials a follow-up service for non-obligatory vaccinations.

In short, there is no specific legal basis laying down an obligation for this programme. Nonetheless, the employer has a duty of care towards its employees under the general principle of responsibility, particularly when they are exposed to specific risks in certain areas of the world.

As well as the legal basis, the lawfulness of the processing operation must also be considered in relation to the Regulation. Article 5(a) provides that "*Personal data may be processed only if processing is necessary for the performance of a task carried out in the public interest on the basis of the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof or in the legitimate exercise of official authority vested in the Community institution or body or in a third party to whom the data are disclosed,* (…)".

In the present case, the medical service acts in the context of a task carried out in the public interest, on the basis of Article 59(6) of the Staff Regulations and of its duty of care to its employees, and also in accordance with a general principle of responsibility.

That being so, the processing operation proposed is therefore lawful.

Moreover, data relating to health are among the data which Article 10 of Regulation (EC) No 45/2001 classes as "special categories of data".

### 2.2.3. Processing of special categories of data

The vaccination programme files include data relating to the health of officials, as mentioned in section 2.1.

Article 10(1) states that *"[t]he processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and of data concerning health or sex life, are prohibited.*"
Article 10(3) states as follows: "*Paragraph 1 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*." Accordingly, this rule applies to the present case.

Moreover, the exception provided for in Article 10(2)(b) also applies: "*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* (…)". The Staff Regulations and the obligations referred to in section 2.2.2 fulfil these conditions.

### 2.2.4. 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 the context of the "Vaccination Programme", described in section 2.1 of this opinion, do not seem excessive in relation to the intended purpose.

Moreover, the data must be "*processed fairly and lawfully*" (Article 4(1)(a) of the Regulation). Lawfulness has already been considered in section 2.2.2 of this opinion. As for fairness, this relates to the information which must be transmitted to the data subject (see section 2.2.7 below).

Lastly, 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 system described applies all reasonable measures to ensure the accuracy of the data. Moreover, the data subject is made aware of his or her right of access to and right to rectify data, in order to ensure that the file remains as comprehensive as possible. With regard to these two rights, see section 2.2.6 below.

### 2.2.5. Conservation 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).

In the present case, the time limit for storing the data was not determined.

In the context of interinstitutional discussions on the time-limits for storing medical data, the EDPS welcomed the possibility of reaching agreement on this matter in the light of Regulation 45/2001. Consequently, the institution concerned needs to implement the deadlines for the storage of data established on an interinstitutional basis after approval by the EDPS.

It is therefore important for the GSC's medical service to consider the decision to be taken in this regard, and to make the relevant changes at the appropriate time.

In any event, the data are not stored for historical, statistical or scientific purposes (Article 4(1)(b)).

### 2.2.6. Right of access and rectification

Article 13 of the Regulation makes provision, and sets out the rules, for right of access at the request of the data subject. Article 14 of the Regulation allows the data subject a right to rectification. In the present case, the medical service prints out the personalised patient file. However, the right of access must also be granted in relation to the periodic list, if so requested by the data subject in respect of data relating to him or her. The right of rectification is respected. With respect to deletion, although the controller considers that it is not in the interest of the data subject to request deletion, since it is he or she who has provided the

information for monitoring purposes, provision should be made for this possibility in cases in which the data subject does indeed have a reason to request deletion.

### 2.2.7. Information to be given to the data subject

The Regulation provides that the data subject must be informed where his or her personal data are processed and lists a series of specific items of information that must be provided. In the present case, the data are collected directly from the data subject and indirectly through the preparation of the periodic lists and the standard booster reminder letters.

The provisions of Article 11 (*Information to be supplied where the data have been obtained from the data subject*) and Article 12 (*Information to be supplied where the data have not been obtained from the data subject*) on information to be given to the data subject apply in this case.

As mentioned in section 2.1, the controller provides certain information. However, this information does not comply in full with the requirements of Article 11 and/or Article 12 of the Regulation.

The data subject must be notified of the information specified in Article 11(a) (identity of the controller), (b) (purposes of the processing operation), (c) (recipients or categories of recipients of the data), (d) (whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply) and (e) (existence of a right of access to, and the right to rectify, the data concerning him or her). The same goes for point (f), which stipulates the following: legal basis of the processing operation, time-limits for storing the data, the right to have recourse at any time to the European Data Protection Supervisor. It guarantees that processing is carried out completely fairly. The same reasoning applies in relation to Article 12 of the Regulation.

The EDPS therefore recommends that all the information specified in Articles 11 and 12 be notified to data subjects.

### 2.2.8. Transfer of data

The processing operation should also be scrutinised in the light of Article 7(1) of the Regulation. The processing covered by Article 7(1) is the transfer of personal data 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*".

Article 7(1) of the Regulation is complied with because the only transfers of data carried out are within the institution to persons involved in the vaccination programme.

### 2.2.9. Security

In accordance with Article 22 of Regulation (EC) No 45/2001 on 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*".

[...]

**Conclusion**

The processing proposed does not appear to involve any infringement of the provisions of Regulation (EC) No 45/2001 provided that the comments made above are taken into account. This implies in particular that:

- the GSC's medical service should consider the decision that needs to be taken, at interinstitutional level, in relation to the conservation of medical data and, consequently, make the relevant changes at the appropriate time;
- right of access should also be granted in relation to the periodic list, if so requested by the data subject, in respect of data relating to him or her;
- with regard to deletion, this possibility should be provided for if the data subject has reasons for requesting it;
- all the information specified in Articles 11 and 12 should be notified to data subjects;
- security measures should be adopted to eliminate the risks highlighted.

Done at Brussels, 5 May 2006

Peter HUSTINX
European Data Protection Supervisor