Opinion on the notification for prior checking from the Data Protection Officer of the Office for Harmonisation in the Internal Market (OHIM) on medical records

Brussels, 28 April 2006 (Case 2005-168)

1. Procedure

1.1. On 20 July 2004 the European Data Protection Supervisor (EDPS) sent a letter to all Data Protection Officers asking them to make an inventory of the cases likely to be subject to prior checking by the EDPS as provided for by Article 27 of Regulation (EC) No 45/2001 (hereafter the "Regulation"). The EDPS asked for an inventory of all processing operations subject to prior checking, including those commenced before his appointment, for which, the checking could not be regarded as "prior" but which would undergo "*ex post" checking*.

1.2. The EDPS identified certain priority themes and chose a number of processing operations subject to ex-post prior checking to be addressed. These include medical records.

1.3. On 4 July 2005 the EDPS received notifications from the Office for Harmonisation in the Internal Market (hereafter "OHIM") regarding the processing of personal data in the context of the following procedures:

- medical check-ups
- the Invalidity Committee
- the processing of medical leave
- the transfer of medical records
- visits checking up on absentees.

1.4. On 11 July 2005 the EDPS asked the Data Protection Officer (DPO) for information.
An initial reply was received on 10 October 2005 (90-day suspension).
Further information was requested on 12 October 2005.
A further reply was given on 22 November 2005 (41-day suspension).

1.5. On 21 November 2005 the EDPS was visiting the OHIM and took the opportunity of meeting the medical department.

1.6. On 29 November 2005 the EDPS requested further information. This request was addressed to the Director of the Human Resources Department, Mr Juan Ramón Rubio, as the DPO was about to leave his position. A reply was given on 13 March 2006 (105-day suspension).

2. Examination of the case

2.1. Facts

The OHIM medical department manages the medical records of officials and agents. The information contained in these records is used for different purposes: medical check-ups, the annual medical check-up, management of medical leave and medical examinations in the event of illness or sick leave.

Pre-recruitment medical check-up

The OHIM requires anyone eligible for recruitment to undergo a medical examination. This medical examination is either carried out by the Medical Department itself, or it is contracted out to a hospital. In the latter case, the hospital carries out only those examinations requested in the agreement drawn up by the OHIM's medical department, and all the results are sent to the OHIM.

Candidates must also fill out a medical questionnaire as part of the medical examination in order to assess their medical fitness.

All the data relating to this medical check-up is entered in the PREVEN CS32 programme (see description of PREVEN CS32 below). Any data in hard copy (medical certificates, for example) is put into the medical records.

Annual medical check-up

During his/her career, officials must undergo a medical check-up every year either by the institution's medical officer or by a medical practitioner chosen by them (Article 59(6) of the Staff Regulations).

The medical practitioner enters the results of medical tests and analyses carried out as a result of the check-up into the PREVEN CS32 system (see description of PREVEN CS32 below). Any data in hard copy (medical certificates) is put into the medical records.

If officials choose to have this medical check-up at an independent medical practitioner's, and would like reimbursement for this from the medical department afterwards, they must send the medical department all the results of their examinations.

Management of medical leave

An official who provides evidence of being unable to carry out his/her duties by reason of illness or accident shall be entitled to sick leave. He shall produce a medical certificate if he is absent for more than three days, and this certificate is valid only if it is signed by the examining doctor. The certificate is kept in the official's medical records.
The doctor enters the official's leave in the PREVEN CS32 medical management system. A document bearing the person's name and the number of days of absence is then sent to the administration.

Medical examination in the event of illness or sick leave

In certain cases, the examining doctor, a Department Director or Head of Service may consider that a medical examination is necessary. After the examination, the examining doctor draws up a report which contains administrative and medical information. The medical report is stored in the medical records and the administrative part is sent to the administration. Medical records are kept under lock and key in an area accessible only to medical staff.
If the data subject considers the conclusions of the examining doctor to be unjustified on medical grounds he/she may request that an independent doctor be involved. The independent doctor's opinion is binding.

The Appointing Authority may refer to the Invalidity Committee the case of any official whose sick leave totals more than 12 months in any period of three years. The Invalidity Committee is made up of three doctors: one representing the Office, one representing the person concerned and a third 'neutral' doctor. The Committee prepares a medical report stating that the person is permanently or temporarily incapable of work (or "not incapable"). This report is then given to the person concerned and to the administration for approval by the Director of the Human Resources Department.

An institution or agency appeals request that the medical records (or part thereof) be sent to the institution's or agency's medical department. The records may not be transferred without the consent of the data subject.

The PREVEN CS32 computer application manages the medical data of staff working at the institution. Three applications are used, namely 'membership', 'incidents' and 'medical management'. The 'membership' application is used for recording basic personal data, such as name, personal number, data of birth… The 'incidents' application is used for recording absences owing to illness or accident; the reasons for the absence must be given, as well as the date of the first day of absence. The 'medical management' application is used for the daily management of an individual's medical data and also contains information on the kind of medical examination undergone. This application is also used for producing notes on a check-up and possibly printing them out for the data subject. The tool is also used for producing lists of data according to different criteria (by date, according to the type of check-up…) and for drawing up any statistics.

The OHIM's medical officer and nurse run the Medical Department in their capacity as contractual staff and are answerable to the person in charge of the Human Resources Department.

The documents containing data on the staff recruited are kept in a medical file for 30 years. The same applies to data stored in PREVEN CS32. Data from medical examinations that take place as a result of medical check-ups on staff who are not recruited is kept by the OHIM for an unspecified length of time. A copy of the results can be sent to the data subject on request.

Invitations to go for a medical check-up or to appear before the Invalidity Committee are sent by letter. The letter states that Articles 11 and 12 of Regulation (EC) No 45/2001 ensure that data is kept confidential.

If access to medical records is requested the OHIM sends the sections requested to the data subject. This information may include any medical documents supplied by the official or servant, the results of examinations carried out by the OHIM's medical department or a full copy of the medical records contained in the PREVEN CS32 application.

2.2. Legal aspects

2.2.1. Prior checking

This prior checking relates to several notifications received from the DPO which are being treated together as they concern the processing of personal data contained in medical records. Unless stated otherwise, all the comments apply to all the processing operations as data processing in the medical department must be seen as a whole.

The processing under consideration in this case involves both the manual and automatic processing of data. In practice, the data is put into the data subject's medical records and into the PREVEN CS32 application. It falls within the scope of Regulation (EC) No 45/2001 (hereinafter "the Regulation") since it involves the processing of data on an identified person (Article 3(2)). The processing involves data relating to health, which is a "special" category of data, and is subject to the provisions of Article 10 (see section 2.2.3 below).

The data is processed by a Community body and is carried out in the exercise of activities within the scope of Community law (Article 3(1)).

Article 27(1) of the Regulation 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 the processing of data relating to health. Medical files clearly contain health-related data and are therefore subject to prior checking by the EDPS.

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. This is not a serious problem however in that any recommendations made by the EDPS may still be adopted accordingly.

The EDPS received the DPO's notification on 4 July 2005. According to Article 27(4) of the Regulation the present opinion must be delivered within two months following receipt of notification, and for the case in point this means by 4 September 2005. A request for information extends the deadline by a period of 236 days, thus for the case in hand postponing the date to 28 April 2005.

2.2.2. Legal basis and lawfulness of the processing operation

The processing of data contained in medical files is based on various articles of the Staff Regulations.

Article 33[1] of the Staff Regulations of Officials of the European Communities (hereafter the "Staff Regulations") provides that "before appointment, a successful candidate shall be medically examined by one of the institution's medical officers in order that the institution may be satisfied that he fulfils the requirements of Article 28(e)" i.e. that he is physically fit to perform his duties. This article is the legal basis for the medical examination of successful candidates. It should be emphasised that this article can serve as the legal basis only for

[1] Pursuant to Article 13 of the Conditions of Employment of other servants of the European Communities, Article 33 of the Staff Regulations applies by analogy to other servants.

examinations carried out on successful candidates, and not on potential candidates for a recruitment procedure.

Article 59(6)[2] of the Staff Regulations provides that during his/her career, officials shall undergo a medical check-up every year either by the institution's medical officer or by a medical practitioner chosen by them.

Article 59 of the Staff Regulations provides that: officials must produce a medical certificate if they are absent for more than three days; the institution can require the person concerned to undergo a medical examination arranged by the institution; the institution may refer the matter to the Invalidity Committee under certain circumstances; and that the official is obliged to undergo a medical check-up every year. The institution manages leave in accordance with this regime.
Article 59(1) of the Staff Regulations also provides that, under certain circumstances, the examining doctor, a Director or Head of Service may deem a medical examination to be necessary.

Lastly, Article 59(4) of the Staff Regulations provides that the Appointing Authority may refer to the Invalidity Committee the case of any official whose sick leave totals more than 12 months in any period of three years.

According to the Regulation, the lawfulness of the processing is therefore based on the performance of a task carried out in the public interest on the basis of legal instruments adopted on the basis of the Treaties establishing the European Communities and in the legitimate exercise of an official authority vested in the Community institution (Article 5(a)). However the need for the data to be collected and processed for the performance of a task provided for in the Staff Regulations must be demonstrated (see below on special categories of data).

2.2.3. Processing of special categories of data

According to Article 10 of the Regulation, the processing of personal data concerning health is prohibited unless grounds can be found in Article 10(2) and 10(3).

The case in hand clearly relates to the processing of personal data on health.

As has been explained above concerning the legal basis, the justification for processing such data can be found in the Staff Regulations and therefore complies with Article 10(2)(b) of the Regulation, according to which the prohibition shall not apply where 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 it is authorised by the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof".

Insofar as it is an exception to the general prohibition, Article 10(2)(b) must be interpreted strictly. On the one hand, the rights and obligations of the controller are qualified as specific. Thus, according to Article 33 of the Staff Regulations, before appointment, a successful candidate must be medically examined by one of the institution's medical officers in order that the institution may be satisfied that he fulfils the requirements of Article 28(e), namely that he

[2] Pursuant to Article 16 of the Conditions of Employment of other servants of the European Communities, Article 59 of the Staff Regulations applies by analogy to other servants.

is physically fit to perform his duties. This provision therefore justifies the processing of sensitive data considered as relevant in order to determine whether a person is fit to perform his duties. On the other hand, if the data processing is 'necessary' it is indispensable, which creates additional constraints when applying Article 4(1)(d) of the Regulation, as will be explained under "data quality".
Lastly, the scope of Article 33 of the Staff Regulations should also be examined. As the scope covers "successful candidates", medical examinations for staff who have not yet been recruited are beyond what is permitted under Article 33 of the Staff Regulations. It should be ensured that the data of successful candidates only is processed.

The ban on processing health-related data can also be lifted where the processing is "necessary for the purpose 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" (Article 10(3) of the Regulation). By reason of their function, the medical officers and nurses are health professionals subject to the obligation of professional secrecy. Article 10(3) of the Regulation may therefore serve to justify data processing in the context of medical examinations or processing by the Invalidity Committee.

If health-related data is transferred to third parties other than the Medical Department, it must also be ensured that Article 10 is complied with. As will be seen below (under 2.2.6), depending on the circumstances, medical records may be transferred to an independent doctor, to the Invalidity Committee or to other institutions or agencies. The administrative data relating to a medical check-up or absence for medical reasons, such as the date and length of absence, are sent to the administration. This data is transferred to comply with labour-law obligations arising from the Staff Regulations or with the explicit consent of the data subject. Article 10(2) of the Regulation is fully respected.

It should also be pointed out that Article 1 of Annex VIII to the Staff Regulations and article 32 of the Conditions of employment of other servants (CEOS) also provide that if the medical examination prior to recruitment shows the data subject to be suffering from sickness or invalidity, the Appointing Authority may decide that expenses arising from such sickness or invalidity are to be excluded from the reimbursement of expenditure provided for in Article 72 of the Staff Regulations. If the data collected during the pre-recruitment medical examination also serves this purpose, Article 72 of the Staff Regulations would justify the processing of sensitive data pursuant to Article 10(2)(b) of the Regulation.

2.2.4. Data Quality

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.".

Even though certain standard data will always be present in medical files such as the name, date of birth and personal number, the precise content of a medical file will of course vary according to the case. However, there must be some guarantee that the principle of data quality is complied with. This could take the form of a general recommendation to the persons handling the files asking them to ensure that this rule is observed.

Data quality must also be ensured in the medical questionnaire filled in by successful candidates or staff already employed. Any information requested must be relevant to the

purpose for which the data is collected. The questionnaire on medical fitness may only serve the purpose of determining whether or not a person is physically fit to perform his/her duties (Article 28(e) of the Staff Regulations).

This therefore raises the issue as to what can be considered as medical data which is likely to have an impact on the performance of the data subject's duties. The type of data will vary according to the type of function (office work or other, for example). The EDPS would like to draw attention to the fact that the relevance of some of the data collected via the form for assessing the fitness of the data subject to perform his/her duties needs to be proven; the EDPS questions the relevance of certain information, such as that on the medical history and current state of health of the spouse and children. The EDPS recommends that the data in the questionnaire on medical fitness be assessed in the light of data protection principles.

In cases T-121/89 and T-13/90 the Court of First Instance found that "the medical officer of the institution may base his finding of unfitness not only on the existence of present physical or psychological disorders but also on a medically justified prognosis of potential disorders capable of jeopardizing the normal performance of the duties in question in the foreseeable future". Even though the ruling was subsequently annulled by the Court (C-404/92), this interpretation of the concept of "fitness" was not challenged. Even though terms such as "potential disorders" and "foreseeable future" are vague in terms of data protection, the relevance of the data in respect to the normal performance of duties must be proven. The link between a potential disorder and fitness to carry out one's duties will need to be demonstrated.

In the context of annual medical check-ups carried out by a medical practitioner chosen by the official (Article 59(6) of the Staff Regulations), it must be established to what extent the medical department needs to receive the medical report and copies of complementary examinations carried out should the data subject request reimbursement. It must be examined whether the main objective of the medical check-up cannot be attained by means of a statement from the medical practitioner attesting the official's state of health and establishing whether or not certain examinations have been carried out, but without communicating the documents themselves.

According to Article 4(1)(d) of the Regulation, personal data must be “accurate and, where necessary, kept up to date", and “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.” For the case in point, the data takes the form of, for instance, results of medical examinations or notes taken by the doctor; it is not easy to ensure or assess the accuracy of this data. However, the EDPS emphasises that the institution must take every reasonable step to ensure that data is up to date and relevant. For example, to ensure that medical records are complete, any other medical opinions submitted by the data subject must also be kept in the file.

Lastly, it is not out of the question that, in the light of Article 72 of the Staff Regulations, the medical questionnaire issued at the pre-recruitment medical examination might also be used to establish the insurability of the person concerned. If this were the case, the EDPS recommends splitting the questionnaire in two so that the relevance of the data in relation to the two possible purposes (namely physical fitness for duty and insurability of the data subject) can be assessed appropriately. Obviously, only the data necessary for determining fitness for duty can be required in the part on fitness. The relevance of data for insurance cover must be examined separately.

2.2.5. Conservation of data

The general principle in the Regulation is that personal data may be kept in a form which permits identification of data 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).
According to this provision, if personal data has to be kept for historical, statistical or scientific purposes, the Community institution or body must ensure that it will be stored either in an anonymous form or that it will be stored only if it is encrypted.

Depending on the information obtained, data on medical history is stored for thirty years. The same applies to data stored in PREVEN CS32.

A question on the length of time for which medical records could be kept was raised at the *Collège des Chefs d'administration* (CA6D 1975/00). At its meeting on 6 October 2005 the *Collège des Chefs d'administration* discussed the possibility of storing data for 30 years. The discussion was based on a survey held in the Member States which reveals that because of the medical consequences of prolonged exposure to certain substances (such as asbestos) data needs to be kept for up to thirty years so as to be able to measure the effects of exposure. As the length of time for which data may be stored is still under discussion the OHIM will have to take account of the outcome of these inter-institutional discussions; the EDPS would like to be consulted in these discussions.

Pursuant to Article 59(4) of the Staff Regulations data on sick leave can justifiably be stored for at least three years. At the end of those three years one might question the justification for storing such data any longer. The data must in any case be deleted when the deadline for contesting or reviewing the data expires.

There is also the question of the storage of results of medical examinations on candidates who, after having undergone the medical examination, have not been recruited, be it for medical or other reasons. Data on these candidates obtained in the context of the medical examination provided for under Article 33 of the Staff Regulations should not be kept for thirty years. The EDPS considers that such data should be kept for only a certain period of time; this could be the same length of time as that during which the data, or a decision taken on the basis of such data, can be contested.

2.2.6. Transfer of data

The notification sent by the Data Protection Officer states that information contained in medical records can be disclosed to doctors and nursing staff, the Invalidity Committee and to other institutions and agencies. The administrative information (name of the person + days absent) is sent to the administration.

Article 7 of the Regulation provides that personal data may only be transferred within or to other Community institutions or bodies if the data is necessary for the legitimate performance of the tasks covered by the competence of the recipient. When a request is made for transfer of information contained in a medical file, the person responsible for the medical file is required to verify the competence of the recipient and to make a provisional evaluation of the need for the data transfer. The recipient shall process the data only for the purposes for which it was transmitted.

The Staff Regulations provide for data to be transferred to the Invalidity Committee, and such transfers are therefore within the competence of the recipient. Data on sick leave may also be communicated, as this data is required for the recipients to carry out tasks within their competence. Data may also be communicated to another institution or agency when a person is transferred.

2.2.7. Processing including the staff or identifying number

Under Article 10(6), the European Data Protection Supervisor "shall determine the conditions under which a personal number or other identifier of general application may be processed by a Community institution or body." The present decision does not aim to establish the general conditions for using the personal identifying number, but only its use in the context of the PREVEN CS32 application. For the case in hand, use of the personal number for the purpose of recording data in the system is reasonable in that this number is used to identify the person in the system and thus helps ensure that the data is accurate.

2.2.8. Right of access and rectification

According to Article 13 of the Regulation, the data subject shall have the right to obtain, without constraint, from the controller, communication in an intelligible form of the data undergoing processing and any available information as to its source.

Article 20 of the Regulation provides for certain restrictions on this right, notably where such a restriction constitutes a necessary measure to safeguard the protection of the data subject or of the rights and freedoms of others.

By virtue of Article 26a of the Staff Regulations, officials have the right to acquaint themselves with their medical files, in accordance with arrangements laid down by the institutions. These arrangements make it possible to reconcile the data subject's right of access with the possible precautions to be taken as regards the transmission of data which is particularly sensitive for the data subject. In practice, in certain cases, if direct access to the data by the data subject might be detrimental, access can be given via the intermediary of a doctor. However, the EDPS is not acquainted with the arrangements adopted by the OHIM. In order to be able to judge whether such measures are compatible with the Regulation, the EDPS would have to be duly informed of the adoption of such implementing measures.

Article 14 of the Regulation gives the data subject the right to rectify inaccurate or incomplete data. This right is somewhat limited as regards medical data, to the extent that the accuracy or completeness of medical data is difficult to guarantee. It may however apply as concerns other types of data contained in medical files (administrative data, for example). Furthermore, as mentioned above (under "quality of data") the data subject may request that his medical file be complete in the sense that he may request that information such as counter opinions by another doctor or a Court decision on an element of the medical file be placed in his file so as to ensure it contains up-to-date information.

2.2.9. Information for data subjects

Articles 11 and 12 are on the information to be given to data subjects in order to ensure transparency in the processing of personal data. Article 11 provides that when the data is obtained from the data subject, information must be given at the time of collection. When the data is not obtained from the data subject, the information must be given when the data is first recorded or disclosed, unless the data subject already has the information. Since in this case

information is first obtained from the data subject as part of the medical examination prior to entry into service, this questionnaire could be taken as an opportunity to provide the data subject with appropriate information, at least as far as the processing of medical data in the context of the pre-recruitment medical examination is concerned.

The letter inviting the data subject to undergo a medical check-up or Invalidity Committee examination states that pursuant to Articles 11 and 12 of the Regulation the data will be kept confidential. This information is also stated on the medical questionnaire given to the data subject at the medical check-up.

The EDPS nevertheless considers not only that Articles 11 and 12 do not actually address confidentiality, but also that the information provided does not cover the headings mentioned in Articles 11 and 12 of the Regulation. Moreover, there is no provision for the data subject to be informed in the case of medical leave. Under Articles 11 and 12 of the Regulation, provision should be made for general information on the OHIM's processing of medical data.

If the data contained in the medical questionnaire issued at the pre-recruitment medical examination is also used for assessing the insurability of the data subject pursuant to Article 72 of the Staff Regulations, the EDPS recommends that the person concerned should be duly informed of this.

2.2.10. Processors

The medical officer and the nurse running the OHIM's medical department under the responsibility of the head of the Human Resources Department should be considered as "processors" within the meaning of Article 2(e) of the Regulation, namely "a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller." In certain cases medical check-ups relating to recruitment are carried out by medical institutions. These medical institutions should also be considered as "processors".

In these cases not only should the OHIM choose a processor who can give sufficient guarantees in terms of security measures, but also a contract or legal act should be drawn up between the controller and the processor. It should be ensured that such a contract or legal act exists between the OHIM and the medical officer and the nurse and that this contract contains the terms used in Article 23(2) of the Regulation, namely that the processor can act only on instructions from the controller, and that the obligations set out in Articles 21 and 22 on security are also incumbent on the processor.

A contract of this kind already exists between the OHMI and the Centro Médico Estacion. The contract should be checked to make sure that it covers all the above headings.

2.2.11. Security of processing

According to Articles 22 and 23 of the Regulation No 45/2001, the controller and the processor shall implement the 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. These security measures must in particular prevent any unauthorised disclosure or access, accidental or unlawful destruction, accidental loss or alteration, and prevent all other forms of unlawful processing.

The EDPS has carefully analysed the security measures adopted and considers that they are adequate in the light of Article 22 of Regulation (EC) No 45/2001, provided that the

confidentiality of communications is guaranteed when information is transferred to and from the Medical Department.

Conclusion

The proposed processing operation does not appear to infringe the provisions of Regulation (EC) No 45/2001, subject to the comments made above. This implies in particular, that:

- As Article 33 of the Staff Regulations of Officials of the European Communities can serve as a basis for medical examinations undergone by successful candidates only and not for those undergone by potential candidates for a recruitment procedure, another legal basis must be found;

- compliance with the principle of data quality must be guaranteed, for example in the form of a general recommendation addressed to the people handling the files, asking them to ensure that this rule is adhered to;

- the data in the questionnaire on medical fitness should be assessed in the light of data protection principles;

- the need for the medical department to receive the medical report and copies of additional examinations where the data subject submits a request for reimbursement should be assessed, as should the possibility of meeting the same objectives as those of the medical check-up by means of a statement from the examining doctor attesting the official's state of health and establishing whether certain examinations have been conducted or not, yet without sending the actual documents themselves;

- if the data contained in the medical questionnaire issued at the pre-recruitment medical examination is also used for assessing the insurability of the data subject pursuant to Article 72 of the Staff Regulations, the questionnaire should be split into two parts;

- the institution should take all reasonable measures to ensure that data is up to date and relevant;

- account should be taken of the length of time for which data may be stored as determined by the inter-institutional discussions, and after consultation with the EDPS;

- the data on candidates not ultimately recruited should be kept for only a certain period of time; this could be the period during which the data or a decision taken on the basis of such data, can be contested;

- the EDPS should be informed of the implementing measures for Article 26a of the Staff Regulations as regards data subjects' access to their medical records;

- general information should be provided on the subjects addressed in Articles 11 and 12 of Regulation (EC) No 45/2001 in the context of the OHIM's processing of medical data;

- if the data contained in the medical questionnaire issued at the pre-recruitment medical examination is also used for assessing the insurability of the data subject pursuant to Article 72 of the Staff Regulations, the person concerned should be duly informed of this;

- it should be ensured that the contract between the OHIM and medical data processors contains the terms used in Article 23(2) of the Regulation, namely stating that the processor can act only on instructions from the controller and that the obligations set out in Articles 21 and 22 on security are also incumbent on the processor.

Done at Brussels, 28 April 2006

Peter HUSTINX
European Data Protection Supervisor