

Opinion on a notification for Prior Checking received from the Data Protection Officer (DPO) of the European Central Bank (ECB) on "medical files kept by the ECB's medical adviser" and "recording of medical information in the personal file"

Brussels, 20 October 2006 (Cases 2006-240/241)

1. Proceedings

Following a consultation by the ECB, the European Data Protection Supervisor (EDPS) sent a letter on 6 January 2006 to the ECB stating that he considers the ECB to be the controller of the following processing operations: "medical files processed and stored by the medical adviser in the premises of the ECB" and "medical data received from the medical adviser in the form of medical certificates". As data processing related to health is a priority established by the EDPS for ex post prior checking, the EDPS asked the ECB to submit both processing operations for ex post prior checking.

By letter of 22 May 2006, the ECB sent two notifications: "medical files kept by the ECB's medical adviser" and "recording of medical information in the personal file". Since both processing operations are linked, the EDPS considered it practical to treat the two notifications in one opinion.

A request for further information was made on 16 June 2006. The DPO replied to this request on 21 July 2006. A further request for information was made on 27 July 2006. The DPO replied to this request on 18 August 2006. Another request for information was made on 28 August to which the DPO replied on 22 September. To allow comments and final information from the DPO, a suspension for seven days was accorded on 11 October 2006.

2. Examination of the matter

2.1. The facts

The Medical Adviser of the ECB is an external provider of data (independently contracted by the ECB) who acts on behalf of the Controller (the ECB). The Medical Adviser keeps the medical files of all ECB staff members as well as the medical files of the candidates selected to fill permanent or fixed-term positions (including those of selected candidates having been declared non fit to fill the position due to health reasons). This, in order to implement the relevant legal provisions as they are laid down in the Conditions of Employment, the Staff Rules and the Rules for Recruitment of the ECB.

Indeed, Article 31 of the Conditions of Employment (Article 28 of the Conditions of Short-Term Employment) provides for paid sick leave in case members of staff are unable to perform their duties because of illness or accident. Provisions of Articles 31 and 28 can be found in the part 5.13 of the ECB Staff Rules and in the part 5.10 of Rules for Short-Term Employment. In case of disability (confirmed by medical advice) Article 32 of the Conditions of Employment provides for a disability pension. The Administrative Circular 05/2004 on "Rules For Recruitment" stipulates that a candidate may be recruited only on condition that he/she is physically fit to perform his/her duties. This has to be certified by the ECB's Medical Adviser after a medical examination.

The Medical Adviser may send the relevant medical information - the communication of the conclusion of a medical assessment - to the Human Resource unit in charge of it. These "confirmation letters" are stored in the personal file of the data subject. The medical certificates which are currently kept in the personal file will soon be stored in a separate file (following the recommendation of the EDPS in the opinion 2004-277).

All members of staff as well as the following persons are subjects for the processing operations. :

- Selected candidates having failed the pre-appointment "medical clearance procedure" due to health reasons.
- Successful candidates who undergo the "medical clearance procedure" but finally do not take up the appointment for personal reasons other than health.
- Children or other dependents of members of staff whenever medical information concerning them is regarded as necessary to benefit from a specific ECB policy (e.g. claims of higher child allowance, pension scheme).

Categories of data

In the medical file:

Basic personal data of staff members and medical data related to the fulfilment of their professional duties are stored. Basic personal data and medical data of candidates who did not take up the appointment after the "medical clearance procedure" (for the latter only No.6 below applies) are also kept. Those data can be divided in the following two categories:

Category A. Data requested by the ECB from the Medical Adviser (in form of a "high-level" confirmation letter) and which are related to the following activities:

1. Assessment by the Medical Adviser of staff members' fitness to return to work after long term sick leave.
2. Assessment by the Medical Adviser of staff members' health situation related to work accidents or to health and safety conditions.
3. Assessment of medical certificates and referrals for second opinions requested by the Medical Adviser where the Medical Adviser is not satisfied with the prescribing private doctor's prognosis or where the Medical Adviser does not have the ability to judge or where it is necessary for the fulfilment of requirement imposed by specific ECB policies (e.g. disability pension).
4. Contact by the Medical Adviser with staff members who are on long term sick leave or disability.
5. Notices of reduced working hours due to medical circumstances.
6. Assessment as to whether a selected external candidate can take up the appointment ("medical clearance procedure"). In the case of confirmation, the standard letter sent to

Human Resources states that “there is no objection from a medical point of view to fulfil the position offered”.

7. Data related to children or other dependants of ECB staff members whenever medical information concerning them is regarded as necessary to benefit from a specific ECB policy (e.g. claims for higher child allowance on account of a physically challenged child, pension scheme).

Category B. The medical data as such deriving from the medical examinations which form the main part of the medical files kept by the ECB’s Medical Adviser (the medical file contains all relevant information that serves as basis for the communication of the “conclusion”- confirmation letter - to the Controller). Data contained in part 1 of the medical questionnaire which are filled in by the selected candidates, if need be, with the help of his/her private doctor also belong to this category. The Medical Adviser documents the results of his/her examination in the second part of the questionnaire. It is also possible that the candidate’s private doctor examines the candidate and documents the results in part 2 of the questionnaire. The filled in questionnaire forms the basis of the Medical Adviser’s assessment regarding the ability of candidates to fulfil their professional duties.

Data derived from ECB - wide medical prevention measures like flu vaccinations campaigns, etc. - where staff members voluntarily take part, are filed outside the medical files (separate folders).

In the personal file:

Basic personal data of staff members and the ECB’s Medical Adviser confirmatory letters with regard to medical data related to the staff’s capability to fulfil their professional duties are stored. Basic personal data and the ECB’s Medical Adviser confirmatory letters with regard to medical data of dependents of members of staff (children) are also kept. The data are the same as the category A of the medical file. No medical data as such is stored in the personal file.

The following medical information is stored outside the personal file:

In cases where selected candidates, who, due to health reasons, are not recognised by the ECB’s Medical Adviser as being able to perform the tasks, no personal file is opened; medical information is stored by the Medical Adviser. Only the Medical Adviser’s standard letter which in this case would not support the appointment would be attached to the recruitment file. In cases where selected candidates did not take up the appointment for other reasons than medical ones, the standard letter supporting the appointment is kept in the special folder "Rejected offers/withdrawn". The actual medical information is stored by the Medical Adviser.

Medical certificates relating to third parties are submitted and processed manually in cases where a member of staff requests special leave to take care of a sick relative. Such medical data is not filed in the personal file but with the request for special leave.

The processing operation

Personal data contained in the medical files undergo both automated and manual processing operations. Manual processing operations take place: hard copies of the relevant certificates or/and relevant forms etc. are stored in the medical file. Documents related to medical examinations, medical questionnaires etc. are stored in the medical file in the custody of the

Medical Adviser. Automated processing operations take place for the category A (basic personal data of the data subject, production of the standard and confirmation letter and their electronic saving).

Personal data related to health contained in the personal files undergo only manual processing operations. Manual processing operations take place with respect to the personal file of staff members where the confirmations/recommendations signed by the ECB's Medical Adviser are filed as original.

Conservation of data

Data contained in the personal files and in the medical files are destroyed 10 years after staff members have left the ECB if there are no pending claims or any other open issues concerning their ECB employment relationship. The personal file of pensioners will be destroyed 10 years after the end of the year in which the last ECB pension payment was made to either the pensioner or one of his entitled dependants, respectively, provided that there are no pending claims or other issues still open.

In cases where selected candidates do not take up the appointment - regardless of the reason - the Medical Adviser keeps their medical data for a period of ten years. The medical certification produced by the Medical Adviser is also kept, together with all the other documents related to the candidate's application, in the special folder "Rejected offers/withdrawn" for three years.

Recipients

As concerns data belonging to category A contained in the medical file, there is no disclosure vis-à-vis third parties with the following exceptions: the Controller receives from the Medical Adviser in writing a "high-level" assessment from a medical point of view, if requested, the Medical Adviser may send medical certificates received from the staff member's private doctor to an external medical referee in order to obtain a second medical opinion in the extended sick leave cases or in the disability pension procedure.

As concerns the data belonging to category B contained in the medical file there are no recipients other than those defined by the Medical Adviser in accordance with the rules governing the patient-physician relationship.

As concerns data belonging to category A contained in the personal file according to the Staff Rules/Rules for Short-term Employment, the only recipients of the documents in the personal file can be: the members of the Executive Board; the members of staff who, for professional reasons, need to have access to the information contained in the file and whose access is authorised by the Director General Human Resources, Budget and Organisation or his/her Deputy Director General. These parties will be subject to the legal obligation of professional secrecy; a member of staff may authorise the Director General Human Resources, Budget and Organisation or his/her Deputy Director General - subject to the approval of the Executive Board - to make his/her personal file available to third parties.

Right of the data subject

In order to access data contained in the medical files kept by the Medical Adviser, the data subjects have to contact the Medical Adviser who can grant them access in accordance with the rules and the limitations governing the patient-physician relation.

In case a selected candidate fails the pre-appointment medical clearance procedure because of health reasons, he/she should address a request to access his/her medical data to the Medical Adviser in the first instance and the Medical Adviser informs then Human Resource of the contact. The rules and the limitations governing the patient-physician relation apply.

Once the high level medical information contained in certificates, or the Medical Adviser's confirmations and recommendations are sent to the Controller and are incorporated in the personal file the general rules set out in Article 7 of the Conditions of Employment (Article 12 Conditions for Short-term Employment) and Article 1.3 of the ECB Staff Rules (Article 1.3 Rules for Short-term Employment) apply. According to these articles each member of staff has the right at any time, even after leaving the ECB, to access his/her personal file and consequently the relevant medical information.

As to the exercise of all other rights laid down in Section 5 of the Regulation (rights of the data subject), the data subject shall contact the Medical Adviser. The rules and the limitations governing the patient-physician relation apply.

Information to the data subject:

Staff members are informed about the most important provisions laid down in the Conditions of Employment for staff of the ECB and the ECB Staff Rules or Conditions of Short-term Employment and the Rules for Short-term Employment, which describe the rules and procedures related to the medical files, when they start working at the ECB in specifically organized "induction seminars". The relevant documents are also published on the ECB's intranet site. The same documents plus the relevant Administrative Circular 05/2004 on the "Rules for Recruitment" are also published on the specific pages of ECB's website in order to be available for candidates.

Staff members can contact the Controller for any additional information falling under the scope of Articles 11 and 12 of the Regulation. The Controller may refer the data subject to the Medical Adviser who is acting on behalf of the Controller, as appropriate.

Security measures

The medical file

As concerns medical files, they are stored in a separate archiving room (in fireproof cupboards) at the ECB Medical Centre with secured limited access. Access to the files is granted only to the Medical Adviser and the staff acting under his/her guidance.

As concerns data related to the medical files, which undergo automatic processing operations, access is granted only to persons authorized by the Medical Adviser who, for professional reasons, need to have access to the information (individual passwords have been attributed) in accordance with the rules governing the physician-patient relationship. Currently, this is only the Medical Adviser's staff.

The general ECB security measures relevant to all ECB IT systems also apply.

The personal file:

As concerns personal files, they are stored in a separate archiving room (in fireproof cupboards) with secured limited access. Access to the files is granted only to a limited group of staff members working in the field of "Human Resources" via an automatic access control system.

2.2. Legal aspects

2.2.1. Prior checking

The two notifications received on 22 May 2006 relate to the processing of personal data ("any information relating to an identified or identifiable natural person" – Article 2.a) by a Community body in the exercise of activities within the scope of Community law. The notifications are treated together as they both relate to the processing of medical data coming from the medical file. The medical files' management and the recording of medical information in the personal file by the ECB involve the collection, recording, organisation, storage, retrieval, consultation, etc. of personal data (Article 2.b) of the Regulation).

It has to be noted that the EDPS concluded following the consultation case 2005-292 that the ECB is the controller of the processing operation and the medical advisor is the processor who acts on behalf of the ECB and therefore the ECB is the Community body in the sense of Article 3.1. of the Regulation.

The management of medical certificates by the ECB has already been prior checked by the EDPS (see the case 2004-277 "recording of the absences of ECB staff members unable to work because of illness or accident").

The data are processed both automatically and manually. The personal data which are processed manually are stored in the medical file and in the personal file. Therefore, this processing of personal data falls within the scope of Regulation (EC) 45/2001 as the processing is partly automated and when it is manual the data form part of a filing system (Article 3.2. of the Regulation).

Article 27.1. of Regulation (EC) 45/2001 subjects to prior checking by the EDPS all "processing operations likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes". Article 27.2. of the Regulation contains a list of processing operations that are likely to present such risks.

The processing operations "medical files kept by the ECB's Medical Adviser" and "recording of medical information in the personal file" qualify for prior checking as they contain data relating to health as foreseen in Article 27.2.a).

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 before the EDPS as supervisory authority was set up. In any case, this is not a serious problem in that any recommendations made by the EDPS may still be adopted accordingly.

The notifications of the DPO were received on 22 May 2006. According to Article 27.4 the present opinion must be delivered within a period of two months that is no later than 23 July

2006. Further requests for information suspend the deadline for 89 days. Therefore the present opinion must be delivered no later than 20 October 2006.

2.2.2. Lawfulness of the processing

The lawfulness of the processing operation must be considered. Article 5.a) of the Regulation stipulates 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 instrument adopted on the basis thereof or in the legitimate exercise of the public authority vested in the Community institution or body (...)". As the medical health management and the human resources management it triggers (long term sick leave, work accident, disability, etc.) are necessary for the legitimate exercise of official authority vested in the institution, the processing operation is lawful.

The specific legal basis of the processing operation can be found in the following: Article 31 of the Conditions of Employment (Article 28 of the Conditions of Short-Term Employment) provides for paid sick leave in case members of staff are unable to perform their duties because of illness or accident, provisions of Articles 31 and 28 can be found in the part 5.13 of the ECB Staff Rules and in the part 5.10 of Rules for Short-Term Employment. In case of disability (confirmed by medical advice) Article 32 of the Conditions of Employment provides for a disability pension. The Administrative Circular 05/2004 on "Rules For Recruitment" (part 8.1) stipulates that candidate may be recruited only on condition that he/she is physically fit to perform his/her duties. This has to be certified by the ECB's Medical Adviser after a medical examination.

2.2.3. Processing of special categories of data

Processing of personal data concerning health is prohibited unless grounds can be found in Article 10.2. and 10.3. of the Regulation.

As has been explained above concerning the legal basis, the justification for processing such data can be found in the Conditions of Employment, the Staff Rules and the Rules for Recruitment of the ECB 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 8.1 of the Administrative Circular 05/2004, before appointment, a successful candidate must be medically examined by the ECB's Medical Adviser in order that the ECB may be satisfied that he/she fulfils the requirements of Article 8.1. of the Administrative Circular 05/2004, namely that he/she is physically fit to perform his/her duties. This provision therefore justifies the processing of sensitive data considered as relevant in order to determine whether a selected candidate or a member of staff is fit to perform his/her duties. On the other hand, as the data processing has to be 'necessary', there are additional constraints when applying Article 4.1.d) of the Regulation, as will be explained under "data quality".

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 Advisers 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. This provision entails that there must be a functional separation between health professionals (this is the case as the Medical Adviser is contracted by the ECB) and ECB employees that need to know health related data. The confirmation letters (medical assessment) are transmitted to the Head of the Compensation and Staff Relations Division who forwards it to the relevant Human Resources Expert. In that context, the EDPS would like them to be reminded that they are subject to an obligation of secrecy equivalent to that of the medical professionals.

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 and the date of birth, the precise content of a medical file and of a personal 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. Any information requested must be relevant to the purpose for which the data are 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 (part 8.1. of the Administrative Circular 05/2004 on "Rules for Recruitment").

This therefore raises the issue as to what can be considered as medical data which are 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 parents, brothers/sisters, spouse and children or on the regularity of the periods and the disorders related to pregnancy. 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.

Data quality must also be ensured in the "confirmation letters" stored in the personal file. According to the samples of confirmation letters received from the ECB, the data contained in those standard letters are adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.

Moreover, data must be processed fairly and lawfully, Article 4.1.a). The lawfulness was analysed above (see point 2.2.2.). The fairness is linked to the information transmitted to the data subject (see below 2.2.8, Information to the data subjects).

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 take 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 are up to date and relevant. The system itself must guarantee the quality of the data. For example, to ensure that medical files and personal files are complete, any other medical opinions submitted by the data subject and the conclusion (in a form of a high-level confirmation letter) it triggers must also be kept in the medical file and in the personal file.

The data subject has the right to access and the right to rectify data, so that the files can be as complete as possible. This also makes it possible to ensure the quality of data (see point 2.2.7).

2.2.5. Conservation of data/ Data retention

The general principle in the Regulation is that personal data may be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed (Article 4.1.e) of the Regulation).

Data contained in the personal files and in the medical files are destroyed 10 years after staff members have left the ECB if there are no pending claims or any other open issues concerning their ECB employment relationship. The EDPS welcomes the period established for keeping the medical data. This long period can be justified by, for instance, 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.

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 part 8.1. of the Administrative Circular 05/2004 on "Rules for Recruitment" should not be kept for 10 years. The EDPS considers that to determine the period of conservation of such data, the length of time as that during which the data, or a decision taken on the basis of such data, can be contested should be taken into account. Concerning the candidates who, due to health reasons, are not recognised by the Medical Adviser as being able to perform the tasks, the conservation of the medical certification kept in the "recruitment" file should follow the same rule.

The EDPS is of the opinion that the period of conservation of the medical certification stored in the special folder "Rejected offers/withdrawn" is reasonable.

It has been considered that it seems obvious that electronic files follow the same rules as paper documents.

2.2.6. Transfer of data

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.

In the case in point, two categories of data might be transferred: medical data as such and data deriving from medical data - the confirmation letters - intended for the Compensation and Staff Relations Division.

For the second category, the processing involves transfers of data within the institution (the members of the Executive Board; the members of staff who, for professional reasons, need to have access to the information contained in the file and whose access is authorised by the Director General Human Resources, Budget and Organisation or his/her Deputy Director General). These transfers are necessary for the legitimate performance of the tasks covered by the competence of the recipients: the human resource management.

For the first category, a medical referee may be the recipient of medical certificates in case the medical advisor needs a second medical opinion. The EDPS notes that the data are necessary for the legitimate performance of the tasks covered by the competence of the recipient. The medical referee is external to the ECB, therefore Articles 8 and 9 apply.

It should be remembered that the other recipients are those defined by the Medical Adviser in accordance with the rules governing the patient-physician relationship. The EDPS emphasises that every transfer decided or authorised by the Medical Adviser has to comply with Articles 7, 8, 9 of the Regulation, depending on the recipient.

Article 8 of the Regulation provides that personal data can only be transferred to recipients other than Community institutions and bodies, subject to Directive 95/46, if the recipient establishes that the data are necessary and if there is no reason to assume that the data subject's legitimate interests might be prejudiced. The Medical Adviser may transfer medical data to the referee if the Medical Adviser establishes that the data are necessary and if there is no reason to assume that the data subject's legitimate interests might be prejudiced.

Data transferred to a third country or international organisation must follow the rules of Article 9 of the Regulation. Therefore, "personal data shall only be transferred to recipients, other than Community institutions and bodies, which are not subject to national law adopted pursuant to Directive 95/46/EC, if an adequate level of protection is ensured in the country of the recipient or within the recipient international organisation and the data are transferred solely to allow tasks covered by the competence of the controller to be carried out."

If the recipient country does not ensure an adequate level of protection, exceptions foreseen by Article 9 paragraph 6 must be considered. In the case in point, paragraphs (a) and (e) are particularly relevant: "By way of derogation from paragraphs 1 and 2, the Community institution or body may transfer medical data if: (a) the data subject has given his or her

consent unambiguously to the proposed transfer, (...) (e) the transfer is necessary in order to protect vital interests of the data subject, (...)."

2.2.7. 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.

As for the data contained in the medical file, the Medical Adviser grants the right of access to the data subject according to the rules and the limitations governing the patient-physician relationship. As for the data incorporated in the personal file, each member of staff has the right at any time, even after leaving the ECB, to access his/her personal file and consequently to the relevant medical information. Therefore, Article 13 seems to be respected, the data subject is granted right of access to all his data.

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

The same rules should apply for the medical certification kept in the recruitment file and in the folder "Rejected offers/withdrawn".

2.2.8. Information to the data subject

Articles 11 and 12 are on the information to be given to data subjects in order to ensure transparency and fairness in the processing of personal data. Article 11 provides that when the data are obtained from the data subject, information must be given at the time of collection. When the data are not obtained from the data subject, the information must be given when the data are first recorded or disclosed, unless the data subject already has the information (Article 12). 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. Data are also obtained from persons other than the data subject (the Medical Adviser for instance), therefore both Articles 11 and 12 apply.

Indeed, the information currently given by the ECB to the data subject concerns the procedure and does not cover all the headings mentioned in Articles 11 and 12 of the Regulation. Although there are some exceptions (the right of access to the personal file foreseen in Article 1.3 of the ECB Staff Regulation), the majority of the headings mentioned in Articles 11 and

12 are not given. Therefore, provision should be made for general information on the ECB's processing of medical data. In order to ensure a fair processing, the EDPS is of the opinion that information on every headings mentioned in Articles 11 and 12 should be given to the data subject.

2.2.9. Processing data on behalf of controllers

The Medical Adviser and the nurse running the ECB's medical 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."

The EDPS reminds that the processor can act only on instructions from the controller but the professional discretion of the medical adviser has to be respected in purely medical matters. The obligations set out in Articles 21 and 22 on security are also incumbent on the processor.

2.2.10. Security measures

After careful analysis by the EDPS of the security measures adopted, the EDPS considers that these measures are adequate in the light of Article 22 of Regulation (EC) 45/2001.

Conclusion:

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

- The human resources services in charge of health related data should be reminded that they are subject to an obligation of secrecy equivalent to that of the medical professionals.
- A general recommendation should be made to the persons handling the files asking them to ensure that personal data are adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.
- The data requested in the questionnaire on medical fitness should be assessed in the light of data protection principles.
- The storage of the results of medical examinations of candidates who, after having undergone the medical examination, have not been recruited, be it for medical or other reasons, should not be kept for 10 years. To determine the period of conservation, the length of time during which the data, or a decision taken on the basis of such data, can be contested, should be taken into account. Concerning the candidates who, due to health reasons, are not recognised by the Medical Adviser as being able to perform the tasks, the conservation of the medical certification kept in the "recruitment" file should follow the same rule.
- The transfers decided or authorised by the Medical Adviser have to comply with Articles 7, 8, 9 of the Regulation, depending on the recipient.

- Counter opinions by another physician or a Court decision on an element of the medical file or of the personal file should be placed in the file (medical or personal) of the data subject so as to ensure that it contains up-to-date information.
- Right of access and rectification should be granted for the "recruitment file" and for the folder "Rejected offers/withdrawn".
- Provisions should be made for general information on the ECB's processing of medical data. In order to ensure a fair processing, the EDPS is of the opinion that information on every heading mentioned in Articles 11 and 12 should be given to the data subject.
- The processor should act only on instructions from the controller, who has to respect his/her professional discretion on purely medical matters, and the obligations set out in Articles 21 and 22 on security are also incumbent on the processor.

Done at Brussels, 20 October 2006

Joaquín BAYO DELGADO
Assistant European Data Protection Supervisor