

Opinion on the notification for prior checking received from the Data Protection Officer (“DPO”) of the European Food Safety Authority (“EFSA”) on 17 July 2006 regarding EFSA's pre-employment and annual medical check-ups

Brussels, 23 March 2007 (Case 2006-365)

1. Proceedings

On 10 July 2006, EFSA's DPO informed the European Data Protection Supervisor (“**EDPS**”) via e-mail about EFSA's data processing operations related to its pre-employment and annual medical check-ups. On 17 July 2006, the EDPS received the formal prior checking notification (“**Notification**”) by regular mail.

On 9 August 2006 the EDPS requested further information from EFSA. EFSA's DPO replied on 17 November 2006. On 8 December 2006 the EDPS requested further clarifications. EFSA responded to the additional information request on 11 January 2007. The EDPS sent a final request for additional clarifications on 12 January 2007. EFSA responded on 29 January 2007. The information provided by EFSA in January 2007 raised additional issues with respect to the legal basis and lawfulness of the processing. For this reason, due to the complexity of the case, and in accordance with Article 27(4) of Regulation (EC) 45/2001 (“**Regulation**”), the EDPS extended the deadline by one month. Finally, the procedure was suspended for 7 days between 2 March 2007 and 9 March 2007 during which EFSA's DPO was offered the possibility to comment on the draft EDPS Opinion.

2. Examination of the matter

2.1. The facts

The Notification concerns the annual and pre-employment medical check-ups at EFSA.

2.1.1. Medical check-up under the Staff Regulations and Conditions of Employment

As will be discussed in greater detail in Section 2.2.2.B and 2.2.2.C when addressing the legal aspects of the case, both the pre-employment and the annual medical check-ups are mandatory pursuant to the provisions of the Staff Regulations of Officials of the European Communities (“**Staff Regulations**”) and the Conditions of Employment of other servants of the European Communities (“**Conditions of Employment**”)¹. The obligation to undergo the medical check-ups extends to officials, temporary agents, and contractual agents, as well as to candidates to these positions.

2.1.2. Medical check-up at EFSA

¹ For the sake of brevity, these two documents together will sometimes be referred below as “**Staff Regulations**”.

At EFSA, the medical check-ups are carried out by a qualified medical doctor, the so-called medical adviser ("**EFSA MA**"), and a medical centre ("**EFSA MC**"), which offers testing facilities and specialist services. The medical files are kept by the EFSA MA. Both the EFSA MA and the EFSA MC are independent contractors, selected by EFSA in two separate public procurement procedures during the spring and the summer of 2006. Previously, EFSA relied on the Commission's Medical Service to carry out the medical check-ups. The purposes, content, and procedures for the medical check-ups are described below.

2.1.3. Pre-employment medical check-up at EFSA

As required by the Staff Regulations, candidates for temporary or contractual agent positions at EFSA participate in a pre-employment medical check-up before recruitment.²

Purpose of the pre-employment medical check-up. The primary purpose of the pre-employment medical check-up is to ascertain whether the candidates are fit to perform their duties, as provided in the Staff Regulations.

The medical results are not used to assess health insurance risks: in particular, they are not used to determine whether the candidates will be entitled to health insurance benefits, or what will be the amount of health insurance payable. This is with one exception: EFSA may apply to candidates Articles 32 and 100 of the Conditions of Employment, which allow the appointing authority to limit, for a maximum of five years, the benefits in case of death or invalidity due to a pre-existing condition.

EFSA appears to have no policy, for now, to address what happens if the provisions regarding the limitations on benefits need to be invoked. EFSA explained that currently, in sickness and invalidity matters, EFSA relies on the Commission Medical Service and that it is not yet certain how agencies will be expected to deal with invalidity issues.³ In any event, EFSA confirmed that if a situation arises where these provisions may need to be applied, neither the EFSA appointing authority nor the EFSA Human Resources Department ("**EFSA HR**") will have access to the medical file of the candidate, although some disclosure (not including the content of the medical files themselves) may need to be made to the EFSA appointing authority or EFSA HR regarding the state of health of the candidate.

Beyond these two purposes that are both based on the provisions of the Staff Regulations, EFSA also indicated general "occupational health" purposes. The exact scope of EFSA's occupational health services is not yet clearly outlined and is subject to internal analysis within EFSA. With that said, EFSA clarified that the "occupational health purposes", with regard to both the pre-employment and the annual medical check-ups, include the objective that the check-ups should help determine whether the workplace should be adapted to the special needs of the employee. For example, whether the work environment, the ergonomics of the workstation or the equipment used may need to be adjusted, or whether protective equipment may be needed. EFSA further emphasised that EFSA HR as well as EFSA MA are fully taking into account the principle of non-discrimination referred to in Section 2.2.2.B and D of this Opinion.

Content of the pre-employment medical-check up. As part of the pre-employment medical check-up, the EFSA MA first discusses with the candidates their medical history based on the medical history questionnaires that the candidates themselves complete and sign. A false declaration will render the results of the recruitment medical check-up invalid. In addition to identification data, the questionnaire requests information about past diseases, conditions,

² EFSA has no permanent staff, and the two other staff categories (auxiliary and interim) are not subject to the mandatory medical check-ups.

³ EFSA also noted that sickness and invalidity matters will be subject to a separate notification to EDPS if and when EFSA establishes its own policies and procedures in this respect.

accidents, and surgical and other medical interventions, as well as medications that the candidates regularly take. Candidates are also required to provide information about invalidity, disability, vaccinations, contraception, pregnancy, and the state of health of family members (parents, brothers and sisters, as well as husband/wife and children). Certain "lifestyle" questions are also included in the questionnaire, including the daily consumption of alcoholic beverages and tobacco, as well as sporting activities. Candidates are also asked whether they have, at any time in the past, had to change jobs for reasons of health.

In addition, the EFSA MA carries out a direct physical examination and completes the medical overview form. This form evidences the results of the examination (weight, height, blood pressure, reflexes, status of tongue, tonsils, lungs, etc.), and describes the candidate's current state of health based on the examination.

The EFSA MC, in turn, performs a chest X-ray and an electrocardiogram test, as well as a series of laboratory examinations on the candidate's blood and urine samples. At the MC, the candidate also visits an ophthalmologist.

The candidate's blood is tested for the following: blood count + leukocytic formula, ESR, PT, glucose, azotaemia, creatinine, cholesterol (total cholesterol, LDL, HDL), triglyceride, total proteins, aspartate-alanine aminotransferase, alkaline phosphatase, gamma glutamyl transferase, iron, ferritin, total bilirubin, albumin, electrolytes, uric acid, anti-HCV, HBsAg, anti-HBc, and TPHA. The candidate's urine is tested for the following: appearance, pH, bilirubin, ketones, erythrocytes leukocyte, cellule epithelial, protein, glucose.

Testing for HIV is subject to the candidate's written consent. A candidate may also express a strong preference not to participate in any other particular medical exam, which shall be documented by EFSA MC.

In addition to the standard medical check-up, if necessary, the EFSA MA may require that the candidate takes complementary exams. These may include a hearing test, a Pap smear, pelvic examination, rectal examination, glaucoma test, mammography, fundus, faecal occult blood test, rectoscopy, or the repetition of exams already included in the standard list of tests. Other exams may also be prescribed if their necessity is justified.

Organization of the pre-employment medical-check up. The detailed procedure for the pre-employment medical check-up is the following:

Invitation and scheduling. The pre-employment medical check-up is carried out only after the candidate has already received a formal offer of employment. The candidate, thus, first receives a letter from EFSA with a job offer, confirming that the recruitment is conditional on the outcome of the medical check-up. The candidate subsequently receives the invitation to the medical check-up.

The medical check-up is scheduled by EFSA HR. To facilitate scheduling, EFSA HR has "read" access to the Outlook calendar of the EFSA MA. Once a date has been agreed, EFSA HR forwards a signed "purchase order" to the EFSA MC. The purpose of this document is, first, to order the medical services from EFSA MC, and second, to provide evidence that the medical check-up has been carried out. The purchase order contains the following data: name, sex and date of birth of candidate; type of medical check-up ("standard pre-employment check-up"); languages spoken by candidate; and date of pre-employment medical check-up.

EFSA HR, simultaneously, sends the candidate an official invitation letter specifying the time and date of the medical check-up. The invitation letter has two annexes: One annex contains additional practical information including the list of medical exams. This annex also contains a data protection notice to the candidates. A second annex contains a copy of the medical history

questionnaire, which the candidates are requested to fill in prior to the medical check-up, and hand over to the EFSA MA during the check-up.

Communicating test results to EFSA MA and to the candidate. The EFSA MC forwards two copies of the medical results to the EFSA MA. If the candidate strongly expresses a preference not to participate in a particular medical exam, the EFSA MC documents this and sends the document, together with the medical results, to the EFSA MA.

The EFSA MA notifies EFSA HR in case he does not receive the results from EFSA MC with respect to a particular candidate. For all other candidates, the EFSA MA forwards a copy of the medical results to EFSA HR in a sealed envelope addressed to the candidate, marked "Confidential" and "To be opened by addressee only". EFSA HR then forwards this envelope to the candidate. EFSA MA retains the remaining copy of the medical results in the medical file of the candidate. The EFSA MA also retains the medical overview form and the medical history questionnaire on the medical file of the candidate. None of these documents (test results, medical overview form or medical history questionnaire) are disclosed to EFSA HR.

Complementary exams. The EFSA MA may decide, either based on his direct physical examination of the candidate, or subsequently, after receipt and analysis of the medical results from the EFSA MC, that further, so-called "complementary" exams are necessary. In both cases, the EFSA MA prescribes the necessary complementary exams for the candidate. The prescription is provided directly to the candidate, rather than to EFSA HR. The EFSA MA notifies EFSA HR that the candidate has to undergo a complementary exam and that the certification of suitability is pending. The notification to EFSA HR is carried out using a standard form that does not provide any information about the nature of the complementary exams.

If it is not possible to arrange an appointment at the EFSA MC in a timely manner, the candidate takes the complementary exams privately. In this case, he/she sends the results directly to the EFSA MA for analysis.

Reimbursement for complementary exams taken privately. The candidate may request the reimbursement of his/her expenses by submitting the original prescription written by the EFSA MA, together with the receipts as proof of payment, directly to the EFSA MA. The EFSA MA verifies the tests, stamps and signs the request for reimbursement (with a stamp indicating "approved by EFSA Medical Adviser") and forwards the request for reimbursement and the proof of payment to EFSA HR. The EFSA MA retains the prescription and the medical results on the medical file of the candidate.

Certification. Once all results are available and have been analysed, the EFSA MA certifies whether or not the candidate is physically fit to perform his/her duties, by issuing a so-called "certificate of suitability" ("Giudizio di idoneità").

Rather than merely stating whether "the candidate is physically fit/unfit to perform his/her duties," the form initially submitted to the EDPS by EFSA offered several options, including (i) fit, with the following prescriptions ("idoneo con le prescrizioni seguenti"), (ii) fit, with the following limitations ("idoneo con le limitazioni seguenti"), and (iii) temporarily unfit ("temporaneamente non idoneo"). In the meantime, EFSA revised its procedures, and replaced options (i) and (ii) with the following option: "fit for assignment with the following observations".

EFSA has not provided specific guidelines to the EFSA MA on the method to assess a candidate's suitability for service. EFSA is also not planning to set different suitability requirements for different types of positions in the organization, or guidelines to the EFSA MA what should be the consequences if a candidate/staff member refuses to take certain tests. EFSA explained that

regarding these aspects, it relies on the professional capacity and the expertise in occupational health of the EFSA MA.⁴

The EFSA MA retains a copy of the certification on the medical file of the candidate and forwards two copies (not including medical data) to EFSA HR. EFSA HR forwards a copy of the certificate to the candidate and retains the remaining copy on the personal file.

Invoicing by EFSA MC. According to the revised procedures for invoicing, the EFSA MC sends two different invoices to EFSA, one covering the standard exams that are carried out with respect to all candidates, and another invoice covering the complementary exams.

The EFSA MC sends the first type of invoice directly to EFSA HR at the end of each month indicating the number of the contract between EFSA and EFSA MC and the names of the candidates who participated in the standard tests. The EFSA MC attaches to its invoice a copy of the purchase orders.

At the end of each month, the EFSA MC also sends to EFSA a second invoice, with respect to the complementary exams. This invoice, however, is sent indirectly, via EFSA MA, in a sealed envelope marked "Confidential". The invoice indicates the number of the contract between EFSA and EFSA MC, mentions "complementary exams for pre-employment medical check-ups", and lists each exam carried out as well as the individual price with respect to each exam. The invoice does not indicate the names of the candidates who participated in the complementary exams. Instead, the EFSA MC attaches a copy of the medical prescriptions written by the EFSA MA where the names of the candidates are shown.

The EFSA MA verifies the invoices and stamps and signs them (with a stamp indicating "approved by EFSA Medical Adviser") to certify that the amounts are correct. He then sends them on to EFSA HR. However, he retains the medical prescription on the medical file of the candidate and does not forward it to EFSA HR. The invoices are ultimately sent to the EFSA Finance Department (EFSA Finance) by EFSA HR, for processing and payment. EFSA HR provides the EFSA MA with a copy of the financial proposal of the EFSA MC to enable him to verify the prices charged for the complementary exams.

Invoicing by EFSA MA. The EFSA MA also sends an invoice to EFSA HR each month indicating the number of the contract. The EFSA MA attaches a timesheet describing the type of service provided, and indicating the number of pre-employment medical check-ups carried out, and the names of the participating candidates. The invoice is verified by EFSA HR, and then forwarded to EFSA Finance for processing/payment.

2.1.4. Annual medical check-up at EFSA

As provided in the Staff Regulations, each year, all temporary agents and contractual agents working for EFSA are required to participate in an annual medical check-up.⁵ In addition to taking part in the annual medical check-up, staff members can also sign up for a separate voluntary medical prevention scheme, administered by the Commission Medical Service. This scheme, however, is not subject to this Notification.

⁴ EFSA further explained to the EDPS that it does not have the required in-house expertise in occupational health to set guidelines for the EFSA MA and hiring external consultancy on this matter would not be proportionate to the scope and size of the organization. However, EFSA informed the EFSA MA that HIV testing can be carried out only subject to written consent of the candidate/staff member. In addition, the EFSA MA was introduced to the counterparts at the European Commission, in order to be able to clarify uncertainties or specific questions. EFSA MA also participates as an observer in the quarterly meetings with doctors of the Commission and other EU agencies.

⁵ As noted in 2.1.3 above, EFSA employs no permanent staff.

Purpose of the annual medical check-up. EFSA defined the purpose of the annual medical check-up similarly to the purpose of the pre-employment medical check-up: (i) occupational health purposes (yet to be defined in more detail, but including ascertainment whether staff members need specific accommodations in the workplace due to their health conditions or disabilities), and (ii) certification of continued fitness for service.

Certification. Just as in case of the pre-employment medical check-up, the EFSA MA issues a certificate. Instead of a "certificate of suitability", EFSA refers to this certificate as a "certificate of confirmation" that the staff member has completed his/her annual visit.

EFSA's 11 January 2006 email includes a sample copy of this certificate. It is, indeed, different from the certificate issued following the pre-employment check-up. In particular, there is no field for a yes or no answer to the question whether the employee is fit for service. Instead, the document, first, certifies that the medical-check-up has been carried out, and second, includes a field for "observations related to current assignment". EFSA provided the following two examples of what these observations might consist of: "staff member must wear glasses to work on the PC; cannot lift weights" and emphasized that the observations must be relevant to the job that is currently being carried out by the employee. The observations, as EFSA explained further, must not be of diagnostic nature, but must include "behavioural recommendations" only.

The format and the content of the certificate of confirmation suggest a partially revised approach compared to EFSA's initial Notification. In fact, EFSA confirmed that it no longer requires certification of fitness, as a positive statement, each year following the annual check-up. Instead, "observations" are noted on the certificate only when the staff member is unsuitable for assignment or needs special accommodations. This revised approach, thus, although in a different and less intrusive form, continues to serve the purpose of ascertaining whether the employee continues to be fit for service.

EFSA is aware of the fact that the Staff Regulations, while mandating the annual check-ups, do not require the annual certification of fitness of all staff members, or that unfitness, when it occurs, would be communicated to EFSA HR. EFSA explained to the EDPS that its policy to require certification of continued fitness (or, at least, of communication of unfitness) is stemming from a specific provision of Italian occupational health and safety legislation. When asked to explain the requirements in further detail, EFSA provided the EDPS with a copy of Italian Law 626/94, and called the EDPS' attention, in particular, to Articles 16 and 17.⁶ These provisions, in EFSA's interpretation, might require EFSA to periodically ascertain whether its employees continue to be fit for employment, or might require EFSA to have EFSA MA communicate to EFSA HR should a staff member be unfit for service. With that said, EFSA noted that it is currently in the process of evaluating how particular provisions of this law and related Italian health and safety legislation and regulations, including the requirement of certification of fitness or unfitness, can be, or should be, applied to its activities.

⁶ Article 16(1) and (2), which is the part most relevant to this discussion, reads as follows: "(1) La sorveglianza sanitaria è effettuata nei casi previsti dalla normativa vigente. (2) La sorveglianza di cui al comma 1 è effettuata dal medico competente e comprende: (a) accertamenti preventivi intesi a constatare l'assenza di controindicazioni al lavoro cui i lavoratori sono destinati, ai fini della valutazione della loro idoneità alla mansione specifica; (b) accertamenti periodici per controllare lo stato di salute dei lavoratori ed esprimere il giudizio di idoneità alla mansione specifica." An unofficial translation of these provisions reads as follows: "(1) The medical surveillance is carried out in cases provided for in the applicable laws in force (2) The surveillance referred to in paragraph 1 is carried out by the competent medical doctor and includes the following: (a) preventive verifications to ascertain the absence of contraindications to the work to which the employees are intended, to assess their suitability for their specific tasks; (b) periodic verifications to control the employees' state of health and express suitability for their specific tasks." The EDPS notes that EFSA provided, as additional information, a CD-ROM containing a comprehensive compilation of Italian occupational health and safety legislation including detailed implementing regulations.

EFSA further explained that the consequences of any particular observations made by the EFSA MA on the certificate may vary depending on the circumstances of the case, and will be decided individually. EFSA has not discussed or specifically provided for any opportunity for employees to request a review of a “negative certificate” or a review of any observations made. Other than providing a certificate of confirmation, EFSA MA does not otherwise transfer health-related data to EFSA HR.

Content of the annual medical check-up. As in the case of the pre-employment medical check-up, during the annual medical check-up, the EFSA MA carries out a direct physical examination and completes a medical overview form. The medical overview form is identical to the one used during the pre-employment medical check-up. However, no medical history form needs to be filled in by the candidate, although the initial medical history form may get updated if necessary. The EFSA MC, as in the case of the pre-employment medical check-up, performs a series of laboratory examinations on the candidate's blood and urine samples, and offers an examination by an ophthalmologist. However, no chest X-ray or electrocardiogram test is carried out. The candidate's blood is tested less comprehensively than at the pre-employment check-up. Only the following tests are carried out: blood count + leukocytic formula, ESR, azotaemia, creatinine, cholesterol (total cholesterol, HDL), triglycerides, aspartate-alanine aminotransferase, alkaline phosphatase, gamma glutamyl transferase. In particular, no HIV test is carried out routinely at the annual medical check-up. Urine is tested for the same indicators as during the pre-employment medical check-up.

In addition to the standard medical check-up, if necessary, the EFSA MA may require that the candidate participates in complementary exams. These may include all those listed as a possible complementary exam for the pre-employment medical check-ups (a hearing test, a Pap smear, pelvic examination, rectal examination, glaucoma test, mammography, fundus, faecal occult blood test, rectoscopy) but may also include a chest X-ray, an electrocardiogram test, and blood test for PT, glucose, total proteins, iron, ferritin, total bilirubin, albumin, electrolytes, uric acid, anti-HCV, HBsAg, anti-HBc, and TPHA or the repetition of exams already included in the standard list of tests. Other exams may also be prescribed if their necessity is justified. Testing for HIV is subject to consent of the staff member, even if prescribed as a complementary exam.

Organization of the annual medical check-up. The procedure for the annual medical check-up is similar to the procedure for the pre-employment check-ups.

Private testing. EFSA does not currently promote the possibility under Article 59(6) of the Staff Regulations to take the annual medical check-up privately and expressed a "preference" that its staff members undergo the medical check-up at EFSA MA and EFSA MC. EFSA explained its approach by the fact that it needs to first put in place the reimbursement scheme for private testing.

In any event, EFSA explained that if the staff member chose to proceed to an examination by an independent medical practitioner, the EFSA MA would receive the medical report and the results of the medical exams prescribed under the standard package for the annual medical visit. This transfer would take place for the following purposes: (i) so that there would be evidence that the staff member actually undertook the medical check-up, (ii) so that the EFSA MA could ascertain whether complementary exams are required (which must be prescribed by the EFSA MA) in order to confirm the completion of the annual medical check-up, (iii) so that the medical file would be kept up-to-date, and finally, (iii) so that the EFSA MA have an overview of the medical status of all staff members.

2.1.5. Information provided to data subjects

Prior to the pre-employment or annual check-up, EFSA HR sends the candidate or staff member an invitation letter specifying the time and date of the medical check-up. An annex to the

invitation letter contains additional practical information including the list of medical exams. This annex also contains a data protection notice to the candidates. In particular, it describes the purpose and the legal basis for the medical check-up, the legal basis for data processing, the recipients of the data, the controller of the data, as well as information on rights of recourse to the EDPS. A copy of the medical history questionnaire is provided as a separate annex.

In addition, with respect to the annual medical check-up, all temporary agents and contractual agents are invited to an information session during which the EFSA MA is presented, and the procedures are explained. On this occasion, employees will also receive a document explaining the procedures. This document is also available for staff on the EFSA intranet. The first information sessions for EFSA staff are planned for April 2007 and will be repeated periodically, as needed.

2.1.6. Access rights

EFSA confirmed that in accordance with Article 26a of the Staff Regulations, staff members, on request, have the right to acquaint themselves with all documents in their medical files. They also have the right to take copies of the files. If justified, they are also entitled to request that incomplete or incorrect data be rectified.⁷ The medical files can only be consulted in the presence of the EFSA MA in the infirmary. EFSA has not specifically mentioned in its Notification that it would provide access rights to candidates as well, but noted that, in any event, the medical files of those candidates who are not ultimately employed will be returned to them within a short time-frame. (EFSA MA will place such results in a sealed envelop marked "Confidential", "To be opened by addressee only" and send it to EFSA HR, who will forward them to the candidate).

2.1.7. Conservation period

Data of candidates not found physically fit for service are retained for the following periods:

(i) If the candidate has not exercised his/her right under Article 33 of the Staff Regulations to request a review by a medical committee, files will not be retained longer than 2 months following the date when the EFSA MA issued the negative medical opinion.

(ii) If the candidate has exercised his/her right to request such a review, but the negative opinion is confirmed, files will not be retained longer than 2 months following the confirmation of a negative opinion, except if the candidate exercises further appeal rights.

Data of employed staff are kept for an indefinite period, even after termination of employment or death. After the end of employment, the medical files are archived using EFSA's general archiving system. No data are stored for historical, statistical or scientific purposes.

2.1.8. Recipients and data transfers

In addition to the processors (EFSA MA and EFSA MC) and - with respect to a certain limited range of data and documents - EFSA HR and EFSA Finance, no other recipients of the data are foreseen. If unforeseen data transfers are requested by any third party, EFSA stated that it would require EFSA MA to allow transfers subject to the written consent of the data subject only.⁸

⁷The language of the tender specifications discussing EFSA MA's obligations in this regard were slightly ambiguous and can be interpreted to require justification also in case of a simple access request, although this was presumably not intended.

⁸ EFSA noted that the transfer of data may also be possible in the future if the staff member applies to another EU institution, body, or agency. EFSA explained to the EDPS that inter-agency mobility is an issue currently under discussion among EU agencies, but the practical implementation is not yet elaborated. It may be possible that such inter-agency mobility leads to mutual recognition and exchange of medical clearance certificates of staff. Such procedure would be agreed among agencies, probably with involvement of the European Commission. If this

2.1.9. Information security

Data are processed manually. Templates of the medical history questionnaire and the medical overview form are available electronically, and the questionnaire and the forms may be completed electronically, but they must subsequently be printed, signed, and placed on the medical file. No data are saved or stored electronically. The medical files are kept in paper form in a locked filing cabinet in a separate, locked room within the infirmary located on EFSA premises. The keys to the filing cabinet are held by the EFSA MA. There is no back-up for the medical files.

In the infirmary, the EFSA MA has access to a PC with printer, telephone and fax on the internal EFSA network, an EFSA email account, MS Outlook calendar, and Internet. Three EFSA HR staff members have "read" access to the calendar of the EFSA MA via Outlook. The PC of the EFSA MA is password-protected. The EFSA MA is not part of any mailing group or distribution list within EFSA.

2.2. Legal aspects

2.2.1. Prior checking

Scope of Notification. The scope of the notified processing operation, and thus, also the scope of this Opinion, is expressly limited to EFSA's pre-employment and annual medical check-ups. The EDPS points out that if the EFSA MA and the EFSA MC will provide additional medical services to EFSA in the future, or if the data obtained from the medical check-ups will be used for additional purposes, then these additional data processing operations may need to be submitted for prior checking.

Grounds for prior checking. 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) contains a list of processing operations that are likely to present such risks. This list specifically includes, under paragraph (b), the processing of data relating to health. The data collected in connection with the medical check-ups constitute health-related data, and therefore, requires prior checking by the EDPS.

Notification and due date for the EDPS Opinion. The Notification was received on 17 July 2006. According to Article 27(4) of the Regulation this Opinion must be delivered within a period of two months. The procedure was suspended for a total of 158 days and was also extended by one month. Thus, the Opinion must be rendered no later than 23 March 2007.

Ex-post prior checking. The processing operations started after the EDPS had been notified but before the EDPS issued its opinion. To recapitulate the chronology of the events, the two public procurement procedures for the selection of the EFSA MC and the EFSA MA were conducted in the first part of 2006, and two separate contracts were signed with the EFSA MC and the EFSA MA on 26 June 2006 and 6 July 2006. The Notification was submitted on 17 July 2006. The first pre-employment check-ups took place during September 2006 and the annual medical check-ups started in November 2006. Based on the initial experience, on 9 January 2007, EFSA HR made a preliminary evaluation of the process together with the EFSA MA and also involving EFSA's DPO.

procedure is introduced, EFSA nevertheless plans to seek the unambiguous consent of the staff member to transfer the certification of suitability to the new agency. The underlying medical file, kept with the EFSA MA, will never be transferred, but on request of the data subject, it will be handed over to him/her. EFSA added that as regards other international organizations, the matter is probably not relevant since each international organization applies its own rules for examining the physical fitness of recruited staff.

The EDPS emphasizes that since prior checking is designed to address situations that are likely to present risks, the opinion of the EDPS should normally be requested and given prior to the start of the processing operation. Therefore, notifications should normally be submitted at the planning stage, in such time that considering the two months deadline for the EDPS to issue his Opinion, as well as the eventual time needed for EFSA to fulfil any requests for information, the case could be brought to an end before the processing operations begin.

However, as the project is still in its pilot phase, the EDPS does not view the delay as a serious problem in the current case, provided that all recommendations that EDPS makes will be taken into account to further improve the procedures. The EDPS also welcomes EFSA's practice to involve the DPO in the planning and refining of the procedures relating to the medical check-ups and appreciates that EFSA already revised some of its procedures before the EDPS issued this Opinion.

2.2.2. Lawfulness of the processing

A. Introduction. Article 5(a) of the Regulation provides that personal data may be processed if "processing is necessary for the performance of a task carried out in the public interest on the basis of the Treaties ... or other legal instrument adopted on the basis thereof".

The first issue under Article 5(a) is to determine whether the processing is instituted to serve a specific task provided for in a Treaty provision or another legal instrument adopted on the basis of the Treaties. The second issue is to determine whether the processing operation is indeed necessary for the performance of such a task. To address the first issue in the present case, Recital 27 of the Regulation needs to be taken into account, which specifies that "processing of personal data for performance of tasks carried out in the public interest includes the processing necessary for the management and functioning of those institutions and bodies". Taken together, the issue in the present case is whether the processing is necessary for the management and functioning of EFSA, and in particular, whether it is necessary for the performance of the tasks set forth in the Staff Regulations regarding the organization of the medical-check ups.

The requirement to undergo the annual and pre-employment medical check-ups is based on the provisions of the Staff Regulations. Thus, a specific legal instrument adopted on the basis of the Treaties permits, and in fact, mandates, the check-ups. The Staff Regulations, as it will be shown below, also clearly designate the purposes of the pre-employment check-up. However, they fail to designate the purposes of the annual check-up.

The fact that the medical check-ups are mandated by a longstanding and directly applicable Council Regulation suggests, although does not conclusively determine, the lawfulness of the organization of the medical check-ups. Similarly, the fact that the Staff Regulations clearly define the purposes of the pre-employment check-up suggests the lawfulness of the use of data for such purposes. At the same time, the fact that the Staff Regulations fail to designate the purpose of the annual check-up suggests that the lawfulness of any implied purposes must be carefully assessed to determine whether the processing is necessary for the management and functioning of EFSA.

Under the two headings immediately following (Sections B and C), the EDPS first discusses the relevant provisions of the Staff Regulations. Subsequently (in Sections D, E, F, G and H), the EDPS will assess the lawfulness of the purposes of EFSA's processing operations on the facts of the case. EFSA designated several purposes for its data processing operations, as discussed in Sections 2.1.3 and 2.1.4 above. The EDPS will discuss which of these purposes are lawful for each of the two types of medical check-ups. As a preliminary remark, the EDPS emphasises that both the function and the regulation under the Staff Regulations of the two types of medical check-up are fundamentally different, and therefore, what may be viewed as a lawful purpose for

one, may be deemed unlawful for the other. Finally, Section I provides conclusions on the issue of lawfulness.

B. Pre-employment medical check-up under the Staff Regulations. The pre-employment medical check-up is based on Article 33 of the Staff Regulations.⁹ The primary purpose of the pre-employment medical check-up is to satisfy the appointing authority that the candidates are physically fit to perform their duties. In addition, it may, in the circumstances set forth in Article 1 of Annex VIII of the Staff Regulations, help determine whether candidates will receive benefits in case they become invalid or die during the first five years of their employment.¹⁰

With respect to fitness for service, Article 28(e) of the Staff Regulations¹¹ requires that candidates be appointed for office only if they are physically fit to perform their duties. Article 33 of the Staff Regulations¹², therefore, provides that before appointment a successful candidate must be medically examined in order that the institution may be satisfied that he/she fulfils the requirements of physical fitness.

These provisions must be read together with the anti-discrimination provisions set forth in the Staff Regulations. In particular, Article 1d provides that any discrimination based on disability is prohibited in the application of the Staff Regulations, and that "a person with a disability meets the conditions laid down in Article 28(e) if he can perform the essential functions of the job when reasonable accommodation is made".¹³

With respect to invalidity or death benefits, Article 1 of Annex VIII of the Staff Regulations¹⁴ provides that if the medical examination shows that the candidate is suffering from sickness or invalidity, the appointing authority, insofar as risks arising from such sickness or invalidity are concerned, may decide to admit that candidate to guaranteed benefits in respect of invalidity or death only after a period of five years from the date of his entering the service of the Communities. The pre-employment medical check-up, thus, to this limited extent, may also contribute to the determination of guaranteed benefits in respect of invalidity or death.

Pursuant to Article 33 of the Staff Regulations, where a negative medical opinion is given as a result of the pre-employment check-up, the candidate may, within 20 days of being notified of this opinion, request that his/her case be submitted for the opinion of a medical committee composed of three doctors chosen by the appointing authority from among the institution's medical officers. The medical officer responsible for the initial negative opinion shall be heard by the medical committee. The candidate may refer the opinion of a doctor of his choice to the medical committee.

C. Annual medical check-up under the Staff Regulations. The annual medical check-up is based on Article 59(6) of the Staff Regulations, which requires officials to undergo a medical

⁹ Articles 13 and 83 of the Conditions of Employment also require temporary agents and contractual agents to undergo a similar medical-check-up. In both cases, Article 33 of the Staff Regulations applies, by analogy.

¹⁰ Similar provisions apply for temporary agents and contractual agents pursuant to Articles 32 and 100 of the Conditions for Employment.

¹¹ Article 12 of the Conditions of Employment in case of temporary agents, and Article 82 in case of contractual agents.

¹² Article 13 of the Conditions of Employment in case of temporary agents, and Article 83 in case of contractual agents.

¹³ These provisions also apply to temporary agents pursuant to Article 10 of the Conditions of Employment. Article 82 of the Conditions of Employment provides similar, although less specific anti-discrimination provisions with respect to contractual agents.

¹⁴ Similar provisions apply for temporary agents and contractual agents pursuant to Articles 32 and 100 of the Conditions for Employment.

check-up every year either by the institution's medical officer or by a medical practitioner chosen by them.¹⁵ The Staff Regulations do not specify the purpose of the annual medical check-up.

D. Ascertaining fitness for service during the pre-employment medical check-up. As noted above, in the case of the pre-employment medical check-up, the Staff Regulations make it clear that its primary purpose is to ascertain fitness for service. Processing health data for this purpose can be considered necessary "for the management and functioning" of EFSA, and inasmuch as data processing is limited to what is necessary for purposes of ascertaining fitness for service, the EDPS considers that the processing operation is lawful.

The EDPS, however, emphasizes the importance of safeguards to prevent that the data obtained during the pre-employment medical check-up will be used to discriminate against candidates based on disability, chronic illness, health conditions, or life-style.

In this respect, the EDPS welcomes the practice of EFSA that it first provides a written offer to successful candidates and schedules the pre-employment medical check-up only thereafter. The EDPS views this chronological order as an important guarantee that disability, chronic illness, other medical conditions, or lifestyle (so long as the candidate remains fit to perform his/her duties) do not interfere with the selection of the candidate. Indeed, to reduce the risks of discrimination based on disability or other medical conditions, the recommended practice is to inform candidates that they hold a valid offer (conditional only on the results of the medical tests) prior to the time they undergo the medical check-up. EFSA HR should assess all other conditions of employment (e.g. requisite educational background, professional experience, criminal records, etc.) before the medical tests take place.

For the same reason, in order to limit the possibilities of discrimination, EDPS also recommends that during the pre-employment check-up no data should be collected solely for purposes of prevention. This applies especially to life-style questions, such as the amount of regular exercise or alcohol and tobacco consumption.¹⁶ With that said, the EDPS acknowledges that data collected for purposes of ascertaining fitness, can, secondarily, be used for purposes of occupational health and prevention, subject to the limitations discussed in Section G below.

E. Limitation of benefits as a result of the pre-employment medical check-up. In addition to ascertain fitness, the Staff Regulations also clearly specify that data obtained during the pre-employment medical check-up can also be used to determine benefits with respect to death or invalidity during the first five years. This purpose is also lawful, provided that the following considerations are taken into account:

EFSA informed the EDPS that it has not yet developed a policy as to the implementation of this specific provision. The EDPS recommends that pending the development of a more complete policy on this issue, should these provisions need to be invoked, EFSA implements at least some data protection safeguards. As a minimum, EFSA should ensure that the appointing authority decides whether to invoke these provisions without undue delay, and in any event, before the employment contract is signed. The information disclosed to the appointing authority regarding the nature of the illness or other medical condition should also be limited to what is strictly necessary to carry out an assessment. In addition, it must also be carefully considered whether the decision can be delegated to EFSA MA or other medical professionals, thus avoiding the need to disclose sensitive health-related data to EFSA HR, the appointing authority, or others within EFSA. In addition, it should also be ensured that candidates are not treated discriminatorily, that is, comparable conditions will lead to comparable limitations on death or invalidity benefits.

¹⁵ Article 59(6) of the Staff Regulations also applies by analogy to temporary agents and contractual agents pursuant to Articles 16 and 91 of the Conditions of Employment.

¹⁶ These issues will be discussed in more detail in Section 2.2.4 discussing adequacy, relevance, and proportionality.

F. Ascertaining continued fitness for service during the annual check-up. From the data protection and privacy perspective, it is essential that any interference from the employer to such a private matter as one's health be limited to the extent strictly necessary. This is especially important at times when due to a serious illness (such as cancer or Parkinson's disease), or an illness that might be carrying a stigma (such as AIDS, or mental illness) an employee is undergoing extreme stress.

An employee needs to comply with regulations governing medical leave and, if such is the case, ultimately, with regulations governing invalidity, or termination of employment. At the same time, however, it is the employee's right, both on ethical and data protection/privacy grounds, to choose the moment when he/she wishes to disclose to the employer the severity or nature of the illness. The employee should also remain free to decide in what manner and to what depth he/she wishes to speak up about it.

Therefore, the EDPS has strong doubts as to the proportionality of a blanket requirement for a certificate of continued fitness to all staff categories each year, and recommends that EFSA reconsiders whether such requirement is indeed necessary for purposes of "the management and functioning" of EFSA.

The EDPS does not question the principle that periodic communication to the employer whether the employee continues to be fit for service may be proportionate and thus, lawful in certain cases. These may include, for example, cases when the health problems of the employee pose risks to the safety or health of others (e.g. armed security guards, or staff handling food) or cases where the employees are subject to specific, increased risks at the workplace (such as radiation or certain dangerous substances).

However, the EDPS suggests that EFSA reassesses the necessity of the periodic certification requirement in cases where these specific factors are not present.¹⁷

In addition to the fundamental problem that the requirement of annual certification of continued fitness for all staff categories could be excessive, and could disproportionately interfere with the private life of employees, the EDPS has strong doubts about the lawfulness of institutionalizing the annual certification process also for the following reasons:

First, the Staff Regulations, which specifically mention the purpose of the pre-employment check-ups as ascertainment of fitness for service, are silent when it comes to the purpose of the annual check-ups. Thus, it can be deduced that the same purpose is not contemplated under the Staff Regulations, as otherwise it would be set forth specifically.

Second, even if the Staff Regulations allowed the use of medical data for certification of continued fitness for service, it is unclear what would be the consequence of a negative certification, and how the process of certification would fit into the procedures for authorization of sick leave, determination of invalidity, and termination of service, which are all carefully regulated under the various provisions of the Staff Regulations. Perhaps most importantly, the contemplated certification procedure would conflict with Article 59 (4) of the Staff Regulations, which 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. The appointing authority, thus, unilaterally may refer to the Invalidity Committee only after a long period of

¹⁷ Should EFSA conclude that annual certification is necessary with respect to certain staff categories or certain risks, the EDPS recommends that EFSA clearly specifies, both internally, and in the notice it provides to data subjects, which staff categories, and under what circumstances, will be subject to the requirement of periodic certification. The lawfulness of these processing operations will need to be separately analysed, and they may also be subject to prior checking. A review procedure must also be established. With that said, the EDPS acknowledges that in certain cases, for example, when an employee contracts a highly contagious disease, his medical information may need to be disclosed on an *ad hoc* basis. These *ad hoc* disclosures must, in any event, be limited to what is strictly necessary.

accumulated absences, and not by virtue of a single examination by the EFSA MA, which, in some cases, may have only been preceded by shorter absence from work or no absence at all.

Third, the content and scope of the pre-employment and annual check-up is different (e.g. the candidate's blood is tested much more comprehensively during the pre-employment check-up). Therefore, the reliability of the two certificates, if one would want to use them for comparable purposes, would not be comparable, in any event.

Fourth, the issuance of such an important document as a certificate of suitability would need to be subject to adequate safeguards. Importantly, the Staff Regulations provide for a review procedure against a negative certificate issued during the pre-employment check-up. No similar procedures are foreseen by the Staff Regulations in case of the annual check-ups.

Finally, the EDPS points out that based on the information that EFSA provided he sees no reason why Italian health and safety legislation referred to by EFSA to support the necessity of the annual certification process¹⁸ should justify the lawfulness of the annual certification process with respect to all staff categories.

The EDPS, first, acknowledges that the Staff Regulations allow the European institutions, agencies, and bodies to set stricter requirements in health and safety matters than those provided for in the Staff Regulations.¹⁹ Thus, the EDPS does not question that EFSA, as a general rule, is entitled to set stricter occupational health and safety regulations than other European institutions or agencies. Neither does the EDPS question that as a general rule the mandatory provisions of Italian health and safety regulations may apply to EFSA, as an entity located on Italian territory.

However, application of national law, in any event, is subject to certain limitations under the Protocol of the Privileges and Immunities of the European Communities, the principles of supremacy of Community law, and the case law of the European Court of Justice.

Accordingly, the EDPS acknowledges that in the present case certain Italian health and safety regulations may be applicable to the activities of EFSA to fill in any existing gap in regulations and to ensure a high level of health and safety protection for EFSA employees. However, and in any event, these national health and safety regulations must be interpreted and applied in a way to eliminate conflicts with the provisions of directly applicable European legislation, including (i) the Staff Regulations, and (ii) the Regulation.

The EDPS welcomes EFSA's efforts to clarify which particular provisions of Italian Law 626/94 it should apply to its activities. During such an assessment, the provisions of the Staff Regulations, as well as the data protection requirements set forth in the Regulation, must be taken into consideration. As a result of a detailed analysis, it may appear that it is possible to reconcile the strict data protection principles of the Regulation, on one hand, and articles 16 and 17 of Italian Law 626/94 on the other hand.²⁰

¹⁸ See Section 2.1.4 above for the specific provisions cited by EFSA.

¹⁹ Article 1(e) of the Staff Regulations provides the following: "Officials in active employment shall be accorded working conditions complying with appropriate health and safety standards at least equivalent to the minimum requirements applicable under measures adopted in these areas pursuant to the Treaties."

²⁰ In fact, the EDPS notes that the first paragraph of Article 16 should not be interpreted as a blanket obligation for all employers in Italy to carry out an extensive set of medical tests, similar to those required by EFSA, every year and with respect to all its employees, and subsequently certify each individual employee's continued fitness to carry out their particular tasks. The "medical surveillance" and "verification" described in Article 16 specifically states that the provisions only apply "in cases provided for in the applicable laws in force". Indeed, additional provisions of Italian law, including detailed implementing regulations, appear to require annual (or other periodic) verification and certification only in certain very specific cases. For example, Article 33 of D.P.R. 19 marzo 1956, n.303, containing the general rules for "occupational hygiene" ("Norme Generali per l'igiene del lavoro) mandates periodic medical check-ups for employees exposed to toxic, infectious, or harmful substances. Specific provisions mandating periodic check-ups are also in place, among others, to protect children, adolescents, as well as employees exposed to asbestos,

As a separate, but related matter, the EDPS welcomes the fact that, as described in Section 2.1.4 above, EFSA has already revised the certificate to be issued during the annual medical check-up, and the revised certificate does not have a specific entry stating whether or not employees are fit for continued service. Nevertheless, the EDPS calls EFSA's attention to the fact that in addition to the modification of the text of the certificate itself, the entire procedure, and the information provided to staff members must also be revised accordingly to reflect that the purposes of the two types of medical check-up are different and no annual certification of fitness takes place. The EDPS also notes that the format and content of the information provided on the document issued to HR following the annual check-up will be further discussed in Section 2.2.4 below to ensure that no medical information is unnecessarily transferred to EFSA HR.

G. Annual medical check-up: occupational health and prevention. If, as a result of its reconsideration of the lawfulness and necessity of the annual certification, EFSA concludes that a blanket requirement for the annual certification is not necessary for the management and functioning of EFSA after all, this does not, in itself, mean that no annual check-ups should be organized and the processing operations are altogether unlawful. Processing may remain lawful for certain other purposes, in particular, for purposes of prevention, as permitted in Article (10)(3) of the Regulation (see Section 2.2.3 below).

An efficient occupational health service can be advantageous to the employer, as it helps maintain a healthier, and thus, more productive workforce. At the same time, employees also enjoy the benefits of a free service offered to them. These goals, in a well-managed occupational health service, are complementary.

To keep this balance, from the data protection and privacy perspective, it is essential that the employer should limit interference with the medical self-determination of staff members to the extent strictly necessary. As a general rule, following receipt of the test results and hearing the advice of EFSA MA, staff members should remain free to decide what additional medical checks or treatments they wish to undertake, and no information about their choices should be communicated to EFSA HR or third parties. The fact whether or not they have any medical problems, and if so, what are those medical problems should remain between EFSA MA and the staff member concerned.²¹

In addition, to achieve the purpose of prevention, staff members and candidates must also receive meaningful feedback from EFSA MA about the results of the medical check-up, rather than merely receive a copy of the test results. EFSA confirmed that indeed, the EFSA MA does explain to the data subject the medical results during the medical check-up.

If used solely for purposes of prevention, subject to the limitations as described above, and further provided that staff members are allowed to take the medical exams entirely privately, as required under Article 59(6) of the Staff Regulations, the EDPS considers this processing operation necessary "for the management and functioning" of EFSA, and thus, lawful.

radiation, staff on board of commercial or fishing vessels, and employees working with compressed air. Other Italian provisions deal with the specific issue of drug testing (D.P.R. 9 ottobre 1990, n.309, Article 125) and require some employees whose activities may pose risks to the safety, security, and health of third parties, to take drug tests periodically. Finally, specific provisions apply to the armed forces, police, firemen, and other special categories of employees. The EDPS has not, in the context of this prior checking procedure, analysed whether any such specific provisions meet European data protection requirements. In any event, the fact that the requirement of periodic ascertainment of fitness is limited to specific circumstances appears to be, as a general rule, in line with the approach of EDPS according to which, in specific, well-defined and justified circumstances, the periodic certification process may be justifiable. In addition, considering the nature of the tasks carried out by EFSA employees, many of the above-referred detailed health and safety provisions will likely be irrelevant for EFSA's operations.

²¹ There may be exceptions in certain cases, as described in Section F.

As to the use of data for additional, broader occupational health purposes, as discussed in Section 2.1.3 above, EFSA is currently only in the planning stage of developing its own occupational health services that it wishes to provide to its staff, independently of the Commission Medical Service. At the time of deployment of such additional services, a separate lawfulness analysis will have to be made to assess whether the use of data for such additional purposes is permissible. As to the specific purpose of determining whether any accommodations are needed to be made in the working conditions of the employee, this purpose is permissible, subject to the limitations as discussed in Section 2.2.4 regarding data quality.

H. Pre-employment medical check-up: occupational health and prevention. The Staff Regulations do not specifically mention that the pre-employment medical check-up can be used for purposes of prevention. Nevertheless, the EDPS recognizes EFSA's argument that from the medical point of view, the earlier a patient is alerted to any potential health issue, the better it is. There is usually a year passing between the time of the pre-employment check-up and the annual check-up. For this reason, the EDPS acknowledges that it is justified to use the information obtained during the pre-employment check-up for purposes of prevention. For example, the medical check-up may indicate that the cholesterol level of a candidate is moderately higher than normal. This would not, itself, have a negative impact on his fitness for service. Nevertheless, once this test has already been made, it is helpful to alert the candidate (and the candidate alone) that he should consider consulting a medical practitioner to see whether he may need medical treatment or life-style changes.

However, this does not mean that additional data, which are not necessary to ascertain fitness or determine limitations on benefits, should be collected during the pre-employment medical check-up for purposes of prevention or for other occupational health reasons. The EDPS calls EFSA's attention to the dangers that broadening of the scope of data collection may pose. In particular, the danger that data collected for purposes of prevention (for example, data obtained about smoking habits, contraception use, or family medical history, which should be irrelevant to determine fitness for service) may be used to discriminate against employees based on their life-style, their increased potential for certain diseases, or the need to care for family members.

From the data protection perspective, the principle of purpose limitation set forth in Article 4(b) of the Regulation requires that "personal data must be collected for specified, explicit and legitimate purposes and *not further processed in a way incompatible with those purposes.*" If additional data, which are not necessary for assessment of fitness for service were to be collected during the pre-employment check-up specifically for purposes of prevention only, it would be very difficult to ensure that such data would not, additionally, be also used to used to unlawfully discriminate against employees.

For this reason, the EDPS recommends that no data should be collected for purposes other than determination of fitness (or limits to invalidity or death benefits within the first five years of service). However, once data have already been obtained during the pre-employment medical check-up for purposes of ascertaining fitness or determining whether any temporary limitation on benefits are necessary, such data may, secondarily, also be used for purposes of prevention, provided that data subjects are clearly informed of such secondary use.

Finally, and as a separate matter, as regards additional occupational health services, the EDPS notes that the last paragraph of Section G above is equally applicable to the pre-employment medical check-up. Thus, importantly, the data obtained may also be used to determine whether any accommodations are needed to be made in the working conditions of the employee.

I. Conclusion on lawfulness. To conclude, the EDPS considers that the notified processing operations are lawful, so long as the data obtained from the pre-employment check-up are used strictly only to ascertain fitness for service (and additionally, to determine limitation of benefits for the first five years, with respect to death or invalidity), and that the annual check-ups are

offered and used only as a preventive tool to alert staff members to any potential medical problems, but leaving it up to them what course of action they will take to protect their health. Data obtained during the pre-employment check-up may be similarly and secondarily also used for purposes of prevention. However, during the pre-employment check-up no data should be collected solely for purposes of prevention. Further, the data obtained during both check-ups can serve to help determine what accommodations need to be provided to the employees at the workplace.

The EDPS recommends that EFSA reconsiders its policy with respect to annual certification of continued fitness for service in light of the doubts that the EDPS raised regarding its lawfulness. This does not preclude EFSA from mandating an annual certification process with respect to certain staff categories if specific risks exist, especially if such are mandated by Italian health and safety regulations, provided that they are not contrary to the principle of proportionality set forth in the Regulation.

The EDPS acknowledges that EFSA has already made certain steps to revise its procedures, and it no longer requires certification of fitness, as a positive statement, each year. Instead, "observations" are noted on the certificate only when the staff member is unsuitable for service or when special accommodations are necessary. The EDPS, however, recommends that the procedures be fully revised to ensure that - except certain limited and clearly specified cases - no information relating to the health condition of the employee should be provided to EFSA HR, others within EFSA, or any third parties.

2.2.3. Processing of special categories of data

Processing of personal data concerning health is prohibited unless grounds can be found in Articles 10(2) and 10(3) of the Regulation.

As explained above concerning the legal basis, the justification for processing health data in connection with medical check-ups can be found in the Staff Regulations. Therefore, the processing falls under 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".

As it is an exception to the general prohibition, Article 10(2)(b) must be interpreted strictly. First, the rights and obligations of the controller are qualified as "specific". Thus, the processing of sensitive data is permissible only insofar as it is relevant for the specific purposes described above when discussing lawfulness. Second, 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 in Section 2.2.4 discussing "data quality".

In addition, and subject to the additional guarantee that data must only be processed by a health professional subject to the obligation of professional secrecy (or by another person also subject to an equivalent obligation of secrecy), the data obtained during the medical check-ups may also be used for purposes of preventive medicine, pursuant to Article 10(3) of the Regulation. As this is an exception to the general prohibition, Article 10(3) must also be interpreted strictly. In particular, any processing is only permissible insofar as it is "required" (in other words, necessary), for purposes of prevention.

Based on these provisions, the EDPS considers that EFSA's data processing operations are permissible, provided that they are limited to the purposes as described in Section 2.2.2 I above. In particular, the pre-employment check-ups fall under the exception provided under Article

10(2)(b) of the Regulation, while the annual check-ups will fall under Article 10(3) of the Regulation.

2.2.4. Data Quality

A. Adequacy, relevance, and proportionality. 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."

The primary purpose of the pre-employment check-up is to determine whether or not the candidate is fit for service. The main issue, thus, is what health-related data are likely to have an impact on the performance of the duties of the employee.²² If the employee is fit for service only subject to certain reasonable accommodations made in the workplace, then the medical check-up may also help determining what accommodations are necessary.

The secondary purpose of the pre-employment medical check-up is to determine whether death or invalidity benefits should be limited during the first five years of service due to a pre-existing medical condition. Any information requested during the pre-employment medical check-up should, therefore, only serve the purpose of determining whether or not a person is physically fit to perform his/her duties, needs certain accommodations at the workplace, or to assess whether a limitation on benefits is necessary.

To minimize the risks of discrimination based on health conditions family situation, or lifestyle, as discussed in 2.2.2.H, the EDPS recommends that during the pre-employment medical check-up no data should be collected solely for purposes of prevention.

The principles of adequacy, relevance, and proportionality must be ensured with respect to all categories of data collected at all stages of the procedure for the pre-employment medical check-ups.

In addition, these principles must also apply to data collected during the annual check-up. The purpose of the annual medical check-up (apart from permissible exceptions as discussed earlier) is prevention. This, however, should not mean interference with the employee's medical self-determination, and should not include collection of excessive data. As a matter of good practice, the EDPS recommends that during the annual medical check-up, in cases where the proportionality of the collection of certain data is questionable, the risk of discrimination based on health conditions, family situation, or lifestyle is present, and the data provide only limited preventive benefits (for example, consider data regarding contraception use), the questions should be eliminated altogether. Should EFSA decide, for medically justified occupational health reasons, that it nevertheless wishes to collect some such data during the annual medical check-up, the candidate should be offered the choice whether or not to provide the information. Collection of such data should be permissible only if the employee gives his/her informed consent with a clear understanding that (i) the provision of the information is entirely optional, and (ii) the data so obtained will only be used for purposes of prevention, that is, for alerting the candidate to any possible health-problems, or recommending a course of action, and will have no effect on determination of the employee's continued employment.

B. Medical history questionnaire. First, it must be ensured that the medical history questionnaire completed by successful candidates on the occasion of the pre-employment medical check-up

²² The type of data may vary according to the type of position. For example, drivers need to see well enough to drive, telephone operators need to hear well enough to handle phone calls. EFSA is not planning to set different suitability requirements for different types of positions in the organization. EFSA explained that regarding these aspects, it relies on the professional capacity and the expertise of EFSA MA. Considering that EFSA is a small organization, and that the EFSA MA can rely on the Commission Medical Service to clarify problematic issues, EDPS finds this approach adequate.

does not attempt to collect non-relevant or excessive data. The EDPS questions the relevance and proportionality of certain information requested during the pre-employment medical check-up.

Family history. Medical history of a spouse or adopted children, lacking any genetic link, has no place on the medical history questionnaire. Although the state of health of blood relatives such as parents, siblings, and children may indicate predisposition to certain genetic disorders or increased probability of developing certain conditions in the future (e.g., cancer, cardio-vascular problems, certain mental illnesses), the predicative information thus obtained is not a legitimate tool for determining fitness for service.²³ In addition, responding to the questionnaire with respect to family members would also disclose sensitive personal data of those persons without their consent. For the above reasons, the EDPS recommends that these questions should be eliminated altogether. If found useful for purposes of prevention, questions relating to blood relatives, such as parents, siblings, and children may be raised during the annual medical check-up, provided that they are clearly marked as optional, and it will be indicated on the questionnaire that the data so obtained will only be used for purposes of prevention.²⁴

Pregnancy. Article 1d of the Staff Regulations prohibits sex discrimination. This prohibition extends to discrimination against an employee or potential employee based on pregnancy. The scope of the prohibition covers asking a potential employee in an application or during an interview whether or not she is, or is planning to become, pregnant; asking an applicant if she is using birth control; and not hiring a candidate because she is, or is planning to become, pregnant.

EFSA confirmed that it does not intend to collect information about whether or not the candidate or staff member is pregnant, and does not wish to test candidates or staff members for pregnancy. Information relating to pregnancy, however, is nevertheless requested on the medical history questionnaire submitted to the EDPS. In particular, candidates are asked to respond to the question whether or not they are pregnant. In addition, their last period, as well as whether they use contraceptive (and presumably also, what contraceptive they use) are also recorded on the medical history questionnaire.

This information is indicated in the medical file kept by EFSA and is not normally transferred to EFSA HR. Nevertheless, considering the highly sensitive nature of this information and its potential for discrimination, the EDPS recommends that EFSA reassesses whether there is a genuine need, from the medical point of view, to indicate in the medical files in all cases and with respect to all staff categories, whether a candidate or staff member is pregnant, considering that the purpose of the medical check-up, after all, is to ascertain fitness for service, and that pregnancy, in any event, cannot be considered as a factor that would prevent employment.²⁵

²³ 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. EDPS notes that terms such as "potential disorders" and "foreseeable future" must be interpreted restrictively, the prognoses must be medically justified, and a clear link between a potential disorder and fitness to carry out one's duties will need to be demonstrated. Collection of genetic information or examination of family history in view of identifying potential hereditary diseases that the candidate might develop in the future with a lesser or greater degree of probability, in particular, appears to be problematic.

²⁴ This does not preclude that during the annual medical check-up the EFSA MA discuss the health conditions of blood relatives, for purposes of prevention, provided that such information will not be registered in the medical files and that the staff member will also remain free not to disclose such information at all. To protect the privacy of family members, it should also be considered, whether the detailed information obtained orally during the consultation regarding the state of each family member could be registered in the medical files in an aggregate form, without directly and personally identifying the individual family members. For example: "indication of several cases of high blood pressure and obesity in family history" or "one case of anxiety disorder in family history".

²⁵ Collecting information regarding pregnancy from all female candidates, could be, for example, proportionate, if pregnancy had, as a general rule, a significant effect on the results of the various blood tests and urine tests listed, and therefore, the tests could not be reliably evaluated without knowing whether the staff member is pregnant.

If there is no such demonstrated need, the EDPS recommends that any question on the medical history questionnaire relating to pregnancy would be limited to those staff members who apply for positions which would be unsafe if they were to be pregnant (for example, due to exposure to radiation). This should be, however, clearly indicated on the medical history questionnaire. In addition, EFSA should also make sure that it is clearly understood by all affected female candidates what the consequences of their pregnancy on their employment will be (for example, that pregnancy will not affect their employability but that they will temporarily be assigned to other duties). The medical history questionnaire should be revised accordingly.

The EDPS notes that this does not preclude the EFSA MA or EFSA MC asking female candidates whether they are pregnant, for purposes of ensuring that any examinations are safe to take, waive certain tests (e.g. chest-X-ray) or prescribe alternative, safer test methods. However, if safety of tests is the only reason to record pregnancy in the medical file with respect to a certain candidate or staff member, the EDPS suggests that EFSA reassesses whether there is a genuine need to record or retain this information in the medical file.

Finally, considering the continued risk of discrimination on account of pregnancy even during employment, the EDPS recommends that the above considerations should also apply to collection of data during the annual medical check-up. In particular, EFSA should reconsider whether it is necessary to collect data on pregnancy during the annual medical check-up for purposes of prevention or occupational health only, with respect to all staff categories. In its assessment, EFSA should consider whether raising this question can genuinely add value. If so, the question may be completed during the annual medical check-up, provided that it is clearly marked as optional and that it will be indicated on the questionnaire that the data so obtained will only be used for purposes of prevention, or in order to provide accommodation at the workplace.

As a related matter, the EDPS also suggests that EFSA reassesses whether there is a genuine need, from the medical point of view, to indicate in the medical files the date of the last menstrual period of female candidates and the use of contraception. This evaluation should go beyond the simple mention of the fact that some forms of contraception (in particular, oral contraception) constitute pharmacological treatment. The assessment should show a genuine need for or benefit derived from collecting this type of information in the context of the pre-employment medical check-up.²⁶ Unless this assessment suggests otherwise, these questions should be eliminated.²⁷

Lifestyle. Lifestyle-questions such as those related to the amount of alcohol or tobacco consumed or physical exercise undertaken, although they may prove to be useful for prevention, also appear to be excessive for purposes of ascertaining fitness for service.²⁸ Again, the EDPS recommends that any such question on the medical history questionnaire would be eliminated. If found useful for purposes of prevention, the questions may be completed during the annual medical check-up, provided that they are clearly marked as optional, and it will be indicated on the questionnaire that the data so obtained will only be used for purposes of prevention.

²⁶ Collecting of this information could be, for example, proportionate, if the contraception had, as a general rule, a significant effect on the results of the various blood tests and urine tests, and therefore, the tests could not be reliably evaluated without knowing whether the staff member takes contraceptive pills.

²⁷ Should EFSA's assessment conclude that collecting information on contraceptive pills is necessary, the EDPS notes in this respect that there is a question on the medical history form which asks what regular medication the candidates take. It may be appropriate to revise the question and include in it reference to contraceptive pills. For example, the question could be modified as follows: "Do you take regular medication or contraceptive pills?"

²⁸ The EDPS notes that this Opinion does not address the issue whether, and to what extent, data can be collected in cases where there may be an increased risk to public safety if persons addicted to alcohol or drugs are employed (e.g. the Opinion does not address the issue of drug testing of armed security guards).

Prior job changes due to health reasons. Finally, the information whether or not the candidate at any time had to change job for reasons of health is overly intrusive, and thus, disproportionate. Therefore, it should be eliminated.

The EDPS, thus, recommends that the data in the medical history questionnaire are re-assessed in the light of the principles of adequacy, relevance, and proportionality for purposes of assessment of fitness for service.

C. Medical overview form, blood and urine tests. Next, the medical overview form evidencing the results of physical examination and the list of required tests (including detailed breakdown of blood and urine tests) provided must also be assessed in the light of the principles of adequacy, relevance, and proportionality.

D. "Certificates of suitability" and "certificates of confirmation". Finally, the principles of adequacy, relevance, and proportionality must also be ensured in the "certificates of suitability" and "certificates of confirmation" that EFSA MA provides to EFSA HR and that will be kept in the personal file.

As discussed in Sections 2.1.3 and 2.1.4, EFSA revised the form and content of the certificate of suitability and the certificate of confirmation. The certificate, in case of the pre-employment check-up now includes only the statement whether or not the candidate is fit for service (with a possible indication of temporary unfitness), although a field is still provided for "observations". The certificate for the annual check-up is silent on the fact whether the employee continues to be fit for service, and instead, simply confirms that the medical exams have been carried out. It also contains a field for "observations".

EFSA emphasised that any "observations" made on the certificates must relate to the specific job assignments and tasks of the staff member, and must be of "behavioural" rather than of descriptive or diagnostic nature (see Section 2.1.4).²⁹

The EDPS welcomes EFSA's efforts to improve its procedures, and makes the following additional recommendations.

First, as a general rule, any information regarding disabilities or health conditions should be disclosed only insofar as it can, and in fact, will be, used by EFSA HR to make improvements or accommodations in the working conditions of the employee, or help protect the health and safety of others. In cases where there is no clear need for EFSA HR to know about the specific treatment or prescription required for the employee to perform his/her duties or about the specific limitation, there is no reason for this sensitive medical information to be included on the certificate, and thus, in the personal file. This should be true even in case if otherwise the information may have some relevance to the specific job of the employee. For example, there is no need for EFSA HR to be informed whether a secretary needs contact lenses or glasses to read and type³⁰, whether the head of unit uses a cardiac pacemaker, or a lawyer-linguist, by taking medication, successfully manages to live with his depression.

²⁹The EDPS notes that the concept of "personal data concerning health" in Article 10(1) of the Regulation is not limited to medical data of a descriptive or diagnostic nature (for example, specific figures of blood cholesterol levels or the fact that a candidate is diabetic). In particular, in the context of occupational health, the accommodation to be provided by the employer normally also constitutes health-related information. For example, if an annual certificate of confirmation specifies that "the employee cannot lift weights heavier than 5 kg", this information itself constitutes health-related information, even though the recipient may not know precisely what the underlying medical reason for such a recommendation is.

³⁰The EDPS acknowledges that in certain cases when the employee needs special accommodations (other than his/her regular glasses) to work in front of the screen, the need for such accommodation needs to be communicated to the employer.

Even if an accommodation or safeguard measure is needed, however, the EDPS recommends that information should be strictly limited to what is necessary to provide the accommodation or take the safeguard measures. For example, if an employee is reliant on daily or weekly medical procedures at the local hospital, and the nature of the requested accommodation is to offer flexitime allowing the medical procedures to take place, there is no need for EFSA HR to be informed about the precise nature of the medical condition.

Second, with respect to both the pre-employment and the annual check-ups, the EDPS suggests that EFSA reassess whether any "observations" regarding the medical condition of the staff member should be necessarily made via the certificates. The certificate will be placed on the personal file, and as part of the file, it will be available to a broader group of recipients than what may be strictly necessary to achieve the purpose of the communication. As part of the personal file, it will also be retained for a considerable length of time, which may also not be necessary for the purpose of the communication. During this assessment, EFSA should consider that any information relating to medical conditions should be kept confidential as much as possible, with a strict limitation of disclosure on a need-to-know basis.

Third, when the EFSA MA considers that any disclosure needs to be made to EFSA HR regarding the need for specific accommodations in the workplace, the EDPS also recommends that the EFSA MA discusses individually with the employee concerned the form and content of the disclosure that EFSA MA will make to EFSA HR, in order to ensure that no more health-related data will be disclosed than what is strictly necessary and acceptable to the employee.

E. Data transfers to EFSA MA in the framework of private testing. Article 59(6) of the Staff Regulations allows the annual medical check-up to be carried out by a medical practitioner chosen by the official.

In this context, the EDPS recommends that EFSA reassesses whether or not EFSA MA needs to receive the test results or any other health-related information from the practitioner chosen by the employee. The EDPS is of the opinion that the preventive purpose of the medical check-up itself outlined in Section 2.2.2 can be achieved by a statement by the medical practitioner confirming that the exams have been carried out. If necessary, the statement could include, subject to the limitations set forth in Section D above, whether the employee needs special accommodations.

If additional information will be necessary, for additional occupational health purposes yet to be specified by EFSA, data transfers may be permissible for those purposes. However, the proportionality of those transfers will need to be separately evaluated. "Completeness of the medical files" or the "need for EFSA MA to have an overview of the staff members' health records", without more, are not sufficient grounds for mandating the data transfer. Neither it is self-explanatory that it must be, in any event and in all cases, the EFSA MA who should prescribe the complementary exams. For now, the EDPS recommends as good practice that a freely-given and informed consent of the employees should be requested for the transfer. Some employees might decide to give such consent, whereas others may prefer to keep their health-related data to the medical practitioner chosen by them.

F. Fairness and lawfulness. Article 4(1)(a) of the Regulation requires that data must be processed fairly and lawfully. The issue of lawfulness was analysed above (see Section 2.2.2). The issue of fairness is closely related to what information is provided to data subjects (see Section 2.2.8 below).

G. Accuracy. 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."

In this case the data include the results of complex medical examinations carried out by the EFSA MC, results of the physical examination carried out by the EFSA MA and the information relating to the employee's clinical history. Given the nature of most of these data, it is not easy to ensure, assess, or prove accuracy. However, the EDPS emphasises that EFSA nevertheless must take every reasonable step to ensure that data are up to date and relevant. For example, so as to ensure the completeness of the file, any other medical opinions submitted by the data subject must also be kept in the medical files.

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 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).

As for the data of candidates whose certificates of suitability were negative, the EDPS finds that the two months period following the issue of the negative certificate (and the equivalent provisions in case of exercising appeal rights) is reasonable. The EDPS, additionally, calls the attention of EFSA that a similar conservation period should also be established for the data of those candidates whose certificates of suitability were positive, but who, for any reason, did not join the service after all.

As for the data of staff members, the EDPS recommends that EFSA evaluates to what extent and for what purposes the content of a medical file needs to be kept. The EDPS also recommends that a definitive time-limit is set for keeping the data, rather than allowing EFSA to keep the data indefinitely.

In this respect, the EDPS calls EFSA's attention to his recommendations issued on 26 February 2007 in case 2006-532 in response to the request of the Collège des Chefs d'administration to comment on the Collège's proposal of a uniform 30-year conservation period for all medical data across the Community institutions. In his recommendations, the EDPS invited the Collège to reassess its initiative and examine, on a case by case basis, what conservation periods are necessary for specific medical documents, considering that Article 4(e) of the Regulation requires that data should be kept no longer than is necessary for the purposes for which they are processed. The recommendation will be available on the EDPS website shortly.

2.2.6. Recipients and data transfers

As described in Section 2.2.9, the EFSA MA and the EFSA MC act as processors, under contract with EFSA, while EFSA remains the controller of the data. The medical files, including the test results, the medical overview form and the medical history questionnaire are kept under lock and key by the EFSA MA.

Data transfers to EFSA HR and EFSA Finance. EFSA HR receives only a very limited amount of medical information about the data subjects. First, EFSA HR made sure that it receives the certificate from EFSA MA without the background information contained in the medical file. Second, EFSA HR made significant efforts to develop procedures to minimize its role in the organization of medical-check ups and complementary exams, and its role in communications between the EFSA MA, EFSA MC and the candidate or staff member, which could otherwise risk disclosure of sensitive data. The EDPS welcomes these efforts, as well as the efforts made to ensure that for invoicing purposes, EFSA does not receive a detailed breakdown of complementary exams per candidate/staff member from EFSA MC but instead, involves EFSA MA in the verification of the invoices.

The EDPS has the following recommendations to further improve the procedures:

First and foremost, the EDPS recommends, as discussed above in Section 2.2.4, that care should be taken so that the certificate of suitability/certification of confirmation should not contain health-related information beyond what is strictly necessary.

Second, EFSA HR should ensure that during the reimbursement workflow for complementary exams taken privately, no sensitive data are processed either by EFSA HR or by EFSA Finance. This applies both to reimbursement for exams taken privately in the framework of the pre-employment medical check-up, and reimbursement for exams taken privately in the framework of the annual check-ups, for which there is not yet a reimbursement procedure in place.

The potential risk in such cases is due to the fact that the invoice itself might indicate the type of exam or the speciality of the physician or medical establishment carrying out the exam. This information might in itself be highly sensitive (for example, consider mention of “syphilis test” “oncologist”, “mental health institute”). One option, if the candidate/staff member submits such an invoice to EFSA MA, is for EFSA MA to alert the candidate to the possibility that such information will be incidentally disclosed to EFSA HR and EFSA Finance, and request consent of the candidate/staff member or that the invoice would be resubmitted without the sensitive mentions. Other alternatives could include obliterating parts of the invoice by EFSA MA, before forwarding to EFSA HR. However, in the present case, taking into account, especially, that less privacy-intrusive alternatives are available, the EDPS does not consider it as a sufficient guarantee to simply impose confidentiality requirements on the staff processing the invoices within EFSA HR and EFSA Finance.

Third, the EDPS also recommends that in case the data transfer is not systematic, whenever possible, the consent of the employee should be sought for any *ad hoc* disclosure of health-related data by EFSA MA to EFSA HR or others within EFSA.³¹ If such consent cannot be obtained, EFSA must assess case by case whether EFSA MA can nevertheless disclose the requested information. This is possible in certain cases, for example, in case of a highly contagious disease that poses risks to health and safety of others. In case of doubt, the EDPS recommends that EFSA MA consults the DPO before he makes the requested disclosure.

Data transfers to third parties. The EDPS welcomes the requirement set by EFSA that if unforeseen data transfers are requested by any third party, EFSA MA should allow transfers subject to the written consent of the data subject only. However, he points out that the language of the Regulation suggests a more nuanced approach, and at least in certain cases, data transfer must be allowed even without consent. Just as in case of disclosures to EFSA HR, in case of doubt, the EDPS recommends that EFSA MA consults the DPO before he makes the requested data transfer.

As a general guidance, the EDPS calls EFSA’s attention to the following:

Article 7 of the Regulation provides that personal data may be transferred within or to other Community institutions or bodies if the data are necessary for the legitimate performance of the tasks covered by the competence of the recipient. Further, Article 8 of the Regulation provides that personal data can be transferred to recipients other than Community institutions and bodies, subject to Directive 95/46/EC, if (i) the data are necessary for the performance of a task carried out in the public interest or subject to the exercise of public authority or (ii) if the data are otherwise necessary and if there is no reason to assume that the data subject's legitimate interests might be prejudiced.

³¹ EFSA already requires EFSA MA to provide medical data to third parties only subject to the consent of the data subjects (see heading immediately below).

Based on the foregoing, when a request for transfer of information contained in the medical file is made pursuant to Article 7 or 8, the consent of the staff member is not always mandatory. However, in absence of consent, EFSA HR, as controller, together with EFSA MA, as processor, will be required to verify the competence of the recipient and to make a provisional evaluation of the necessity of the transfer of the data. For example, transfers to the medical committee reviewing the decision to issue a negative certificate of suitability, or transfers to the Invalidity Committee are provided for in the Staff Regulations and are within the competence of the recipient. Other transfers, such as transfers to the legal counsel of EFSA may also be permissible in the context of a case taken by a staff member against a decision in this field. The recipient shall only process the data for the purposes for which they were transmitted.

Finally, 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, the exceptions foreseen by Article 9(6) may be considered. Of these, paragraphs (a) and (e) are particularly relevant here: "By way of derogation from paragraphs 1 and 2, the Community institution or body may transfer personal data if: (a) the data subject has given his or her consent unambiguously to the proposed transfer, ... or (e) the transfer is necessary in order to protect the vital interests of the data subject,"

2.2.7. Right of access and rectification

Right of access. According to Article 13(c) of the Regulation, the data subjects have the right to obtain from the controller, without constraint, communication in an intelligible form of the data undergoing the processing and any available information as to their source. Article 20 provides for certain restrictions to this right including the case when 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 26(a) of the Staff Regulations, staff members also have the right to acquaint themselves with their medical files, in accordance with arrangements laid down by the institutions.

The Notification confirms that EFSA provides access to the medical files to staff members, and refers to Article 26(a) of the Staff Regulations, but does not establish any specific arrangements in this respect, other than providing that the medical files must be consulted only in the presence of the EFSA MA in the infirmary. The EDPS welcomes that EFSA allows access to the medical files without setting any specific restrictions. However, the EDPS recommends that EFSA sets safeguards to ensure that any access requests will be dealt with in a timely fashion and without constraints. This may include, for example, setting a reasonable timeline for EFSA MA in which to schedule an access visit, or provide copies of documents, and an obligation on EFSA MA to consult the EFSA DPO should he wish to limit access to any data requested. When establishing these safeguards, it must also be ensured that access cannot be limited to "justified cases" and must be allowed for any or no reason at all. Data subjects also cannot be required to specify the purpose of the request.

The EDPS also calls EFSA's attention to "Conclusion 221/04" of 19 February 2004 of the Collège des Chefs d'administration, which aims at harmonizing certain aspects of access provision across the Community institutions. This document emphasises that access must be provided to health-related data to the maximum extent possible. The document provides, among others, that access

should also be provided to data of psychological or psychiatric nature, although, in such cases, access may be granted indirectly, through the intermediary of a medical practitioner designated by the data subject. The document also specifies that access should also be given to the personal notes of the medical professional who carries out the medical check-up; provided that such access may be denied after examination of the circumstances of the given case if limitation of the disclosure is necessary to protect the interests of the person concerned or the rights of others. The EDPS, however, emphasises that this limitation must not be read to allow arbitrary restrictions on access.

Finally, the EDPS points out that not only staff members, but also candidates must be granted access to their data pursuant to Article 13 of the Regulation.

Additional recommendations. Finally, the Notification provides that EFSA MA forwards one copy of the EFSA MC test results to the candidate and retains one copy in the medical file of the candidate. The EDPS would recommend, as a good practice, to provide candidates also with a copy of the medical history questionnaire and a copy of the medical overview form automatically without the data subject having to specifically request these documents. This can be done, for example, by providing a copy to the candidate/staff member immediately at the end of the medical check-up. Alternatively, a copy of the document can be placed in the same sealed envelope in which the medical tests are communicated to the candidates/staff members.

Right of rectification. Article 14 of the Regulation provides the data subject with a right to rectify inaccurate or incomplete data. As mentioned above when discussing data quality, the data subject should be able to request that opinions by another medical officer or a Court decision are placed in the medical files so as to ensure that the files are complete and up-to-date. The same rules should apply to the medical certificates kept in the recruitment file.

2.2.8. Information to the data subject

Articles 11 and 12 of the Regulation require that certain information be given to data subjects in order to ensure the transparency of the processing of personal data. Article 11 is applicable to data obtained from the data subject, whereas Article 12 is applicable to cases where the data have not been obtained from the data subject. On the facts of the case, Article 11 is applicable to data contained in the medical history questionnaire, whereas Article 12 applies to the data contained in the certificate of suitability/certificate of confirmation, to the medical overview form completed by EFSA MA, and to the test results.

Timing and format of the data protection notice. Article 11 provides that when the data are obtained from the data subject, the information must be given at the time of collection. For the case when the data have not been obtained from the data subject, Article 12 provides that the information must be given when the data are first recorded or disclosed, unless the data subject already has it.

The EDPS welcomes EFSA's good practice of providing the required data protection notice at the time candidates or employees are invited to the medical check-up, in an attachment to the invitation letter. This allows data subjects to arrive at the medical check-up with the reassurance that their medical data will be processed fairly and lawfully.

The EDPS also welcomes (i) EFSA's practice of carrying out informational sessions for staff members regarding the annual medical check-up, which also includes information about data protection, and (ii) EFSA's initiative to provide a detailed description of the procedures for the annual medical check-up on the intranet, again, including data protection aspects of the processing.

Content of the data protection notice. Articles 11 and 12 of the Regulation provide a detailed list of information that needs to be provided to data subjects. In essence, the controller must inform data subjects about who processes what data and for what purposes. The information must also specify the origins and recipients of data, must specify whether replies are obligatory or voluntary and must alert the data subjects to the existence of the right of access and rectification. Further information, including the legal basis of processing, the time limits for storing the data, and the right of recourse to the EDPS must also be provided if necessary to guarantee fair processing. This may depend on the circumstances of the case.

Finally, both Articles 11 and 12 allows exceptions from the notification requirement in case when the data subject already has the information. Article 12 allows for further exceptions in a limited number of cases, including when the provision of information proves impossible or would involve disproportionate effort.

Considering that (i) none of the Article 11 or 12 exceptions apply to the facts of the case (data subjects do not already have the required information available to them, and the provision of information would not involve disproportionate efforts), and that (ii) all items listed in Articles 11 and 12 (including the legal basis of processing, time-limits for storing the data, and the right of recourse to the EDPS) are necessary to guarantee fair processing, the EDPS is of the opinion that all items listed under Articles 11 and 12 respectively must be provided in the data protection notice.

Additional recommendations. The annexes to the invitation letters provide useful summaries of the data processing operations and include a brief mention of much of the information required in Articles 11 & 12 of the Regulation. As a copy of the data protection notice was made available to the EDPS, he can now provide specific recommendations: improvements that can be implemented at the practical level. The EDPS will discuss below only those items listed under Articles 11 and 12 where he suggests further changes.

Information about the purpose of the processing. The data protection notice regarding the pre-employment medical check-up under its first heading clearly designates the purpose of the visit to be ascertainment of physical fitness to perform duties. This is good practice. The EDPS additionally recommends that a reference should be made to the anti-discrimination provision in the Staff Regulation (Article 1d) and that it be clearly stated that disabilities or other medical conditions will not disqualify candidates so long they are able to perform the essential job functions when reasonable accommodation is made.

The data protection notice also briefly refers to the secondary purpose of the medical check-up: the possible use of the data for purposes of limiting guaranteed benefits in respect of invalidity or death for the period of the first five years of service. The communication of this secondary purpose and important potential limitation on benefits should be improved: the notice should describe to the reader what Articles 32 and 100 of the Conditions of Employment are about, rather than merely refer to them. Without this, the candidates are provided no warning unless they look up the Staff Regulations prior to the pre-employment medical-check-up, which may be cumbersome for many candidates, especially before entry into service.

With respect to the purposes of the annual check-up, the EDPS suggests that these should be designated and characterized as a free preventive service offered to employees.

Information about the categories of data concerned. Article 12 (but not Article 11) also requires that information be given to data subjects about the categories of data concerned. This information enables candidates to assess whether the data collection is proportionate to the purpose of the medical check-up. In particular, candidates, when their blood or urine samples are taken, should know for what indicators, thus, for what purposes, these samples are tested for. The EDPS welcomes EFSA's practice to provide a detailed breakdown of the various indicators that

blood samples are tested for. Similar breakdown should also be provided for the urine tests, to reassure candidates/employees that they are not tested for non-disclosed purposes (e.g., for pregnancy, or substance abuse).

Candidates must also be informed about the content of the certificate of suitability/certificate of confirmation. Candidates must also be informed about the consequences of a certificate, which states that the candidate is "temporarily unfit" for performance.

Consequences of failure to reply. Article 11 requires that data subjects should be informed whether replies to questions are obligatory or voluntary as well as what will be the possible consequences of failure to reply. This provision is relevant with respect to both the responses to the medical history questionnaire and the right to object to taking any particular tests.

As for the HIV tests, candidates are clearly advised that the HIV test is optional. As for the rest of the medical exams, the information provided could be improved to include reassurance that expressing strong preference not to take a particular test is not, in itself, a reason to issue a negative certificate, provided that the EFSA MA can otherwise reasonably ascertain fitness for service.

As for the medical history questionnaire, as noted above in Section 2.2.4, certain information should, as a matter of good practice, not be requested at all during the pre-employment check-up. If EFSA concludes that the information should be nevertheless requested for overriding medical reasons, it must be clearly indicated on the form that the information provision is optional and not mandatory, and that there are no adverse consequences of failing to reply to them.

Information about access rights. Data subjects must also be informed about the existence of the right of access to, and the right to rectify the data concerning them. This right is not specifically addressed in the data protection notice. The notice, therefore, needs to be complemented. The EDPS also recommends that information should go beyond merely mentioning the existence of this right, and should explain how, in practice, data subjects can exercise such rights.

Information about the legal basis. The data protection notice designates Article 5(c) of the Regulation as the legal basis of the processing with respect to both the annual and pre-employment medical check-ups.³² This provision should be replaced with references to the specific legal basis of the processing, that is, to the provisions of the Staff Regulations relating to the pre-employment and annual medical check-ups.

Information about the time-limits for storing the data. With respect to the pre-employment check-up the data protection notice provides that in case the candidate is not recruited, the medical files will be transferred to the candidate and no medical information will be retained by EFSA MA. The EDPS recommends that the notice should also specify the retention periods in case the candidate enters into the service.

With respect to the annual medical check-up, the data protection notice in its current form provides no information about conservation periods. The necessary information should be included in the notice.

Information about right of recourse to the EDPS. The data protection notice mentions that the data subject has the right of recourse to the EDPS. The EDPS additionally recommends that EFSA adds that such right of recourse can be exercised "at any time". This information may also

³² The EDPS also notes that in any event, the reference should have been to Article 5(a), as discussed above in connection with the lawfulness and legal basis, although Article 5(c), in addition to Article 5(a), constitutes an additional, secondary legal basis with respect to the pre-employment medical check-ups (but not with respect to the annual check-up).

be accompanied by a recommendation to contact the EFSA DPO first, before filing any complaint with the EDPS, while at the same time making it clear that this procedural step is not legally required.

Possibility of arranging for the annual check-up privately. Article 59(6) of the Staff Regulations provides that the annual medical check-up may either be carried out by the institution's medical officer or by a medical practitioner chosen by the staff member. Although this right is set forth in the Staff Regulations, as a good practice, the EDPS recommends that employees be advised (via the information posted on the intranet and during the information sessions organized) that they can choose the doctor who will carry out the annual medical check-up, and informed what practical steps they need to take to take the exams privately. Information should cover the rules for reimbursement (including maximum amounts) as well as the rules for certification that the medical check-up has been carried out. It should also be clearly provided whether the medical practitioner chosen will need to forward the staff member's medical records to EFSA MA, and if so, for what purpose.

Languages used. The EDPS emphasises that it is important that the information should be given to data subjects, EFSA's multinational staff, in a language that they will understand. Therefore, the EDPS welcomes that (i) EFSA targets contracting multi-lingual service providers, that (ii) it emphasised the language requirements in the specifications of the calls for tenders, and that (iii) the EFSA Staff Committee involved in the selection process has drawn special attention to these aspects.

The EDPS additionally recommends that all documents used by EFSA MA and EFSA MC in their interaction with data subjects should be translated into English or another language that the candidates will understand. This includes, importantly, the certificate of suitability/certificate of confirmation, and the medical history questionnaire form (both of which EFSA already submitted to the EDPS in English as supplemental information). As for the medical overview form, EFSA explained that it is intended to be used as a personal working tool of the EFSA MA. However, as it contains important health-related data (including all results of the physical examination, such as blood pressure and others), the EDPS recommends that this document, which also forms part of the medical file, should also be translated into a language/or languages that the candidates understand.

2.2.9. Processing data on behalf of controllers

EFSA is the controller of the processing operation in the meaning of Article 3(1) of the Regulation. EFSA MA and the EFSA MC should be considered as "processors" within the meaning of Article 2(e) of the Regulation who "process personal data on behalf of the controller".

Article 23 of the Regulation requires that the processing operation must be governed by a contract binding the processor to the controller. EFSA submitted two service contracts to the EDPS as supplementary information: a 26 June 2006 contract between EFSA and the EFSA MC and a 6 July 2006 contract between EFSA and the EFSA MA.

The EDPS calls EFSA's attention to the fact that for purposes of data protection, the processor can act only on instructions from the controller while at the same time the professional discretion of the medical adviser has to be respected in medical matters. The obligations set out in Articles 21 and 22 of the Regulation on security are also incumbent on the processor. Article 23 requires that these two requirements must be clearly specified in the contract. The EDPS points out that although the contracts contain some provisions on data protection and confidentiality (Articolo I.8 Protezione dei dati and Articolo II.9, Obbligo di riservatezza), these relate to data protection and confidentiality issues surrounding the conclusion of the contracts themselves, rather than the processing of health-related data based on the contracts. Therefore, the EDPS recommends that the contracts be modified to include the requirements set forth in Article 23 of the Regulation.

2.2.10. Security measures

According to Articles 22 and 23 of the Regulation, the controller and the processor must 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 unauthorized disclosure or access, accidental or unlawful destruction or accidental loss, or alteration, and to prevent all other forms of unlawful processing.

The EDPS considers that the security measures adopted by EFSA are adequate in the light of Article 22 of the Regulation, provided that confidentiality of communications is guaranteed when transferring information from and to the EFSA MA and EFSA MC. In this respect, the EDPS finds it a good practice and an appropriate measure to mark the term "confidential," "to be opened by addressee only" or similar, on the sealed envelop whenever it contains medical information.

Conclusion

There is no reason to believe that there is a breach of the provisions of the Regulation provided that the considerations noted in Sections 2.2.2 through 2.2.10 are fully taken into account. The recommendations of the EDPS include, most importantly, the following:

- The purposes of processing must be clearly specified and limited to the following:
 - The primary purpose of the pre-employment medical check-up is ascertaining fitness for service. A secondary purpose is assistance in determination of limitations with respect to death or invalidity benefits for the first five years of service. No data should be collected solely for purposes of prevention.
 - The purpose of the annual medical check-up, until EFSA develops its policy on occupational health, must be limited to prevention. Importantly, EFSA should reconsider whether the annual check-ups should serve to determine whether individual employees continue to be fit for service. Exceptions include cases when the health, safety or security of third parties are at stake or when employees are subject to certain specific work conditions, including exposure to toxic, infectious, or otherwise harmful substances.
 - If, due to information obtained during the pre-employment or annual medical check-up, the EFSA MA concludes that certain accommodations need to be made to accommodate the health condition of the employee, then these conclusions may be communicated to EFSA HR. However, if any health-related data needs to be disclosed, it should be limited to what is strictly necessary, and if possible, the consent of the employee must be obtained prior to disclosure.

Additional recommendations:

- Data Quality:
 - The scope of data collected on the medical history questionnaire and the information included on the certificate of suitability/certificate of confirmation should be revised to comply with the principles of relevance and proportionality.
 - If the annual check-up is carried out privately, the resulting health-related data should not be forwarded to EFSA MA without the consent of data subject unless the purposes of such transfer are clearly specified and proportionate.
- Conservation of the data:
 - A reasonable, definite time frame must be established by EFSA for the conservation of employee medical data.
- Information to data subjects:
 - Clear and specific information needs to be provided to data subjects regarding all items listed under Articles 11 and 12 of the Regulation. The EDPS also emphasizes the need to provide clear information about anti-discrimination rules and the possibilities of undergoing the medical-check-up privately.
- Processing data on behalf of controllers:
 - The service contracts concluded with EFSA MA and EFSA MC should be modified to address data protection aspects pursuant to Article 23 of the Regulation.

Done at Brussels, on 23 March 2007

Peter HUSTINX
European Data Protection Supervisor