Opinion on notifications for prior checking received from the Data Protection Officers of certain EU agencies concerning the *"processing of health data in the workplace"*.

Brussels, 11 February 2011 (Case 2010-0071)

1. Procedure

On 4 September 2008, the European Data Protection Supervisor (EDPS) sent a letter to all EU agencies (agencies) announcing the new procedure for ex post prior checking analysis regarding common procedures within the agencies.

On 28 September 2009, the EDPS sent "*Guidelines concerning the processing of health data in the workplace by Community institutions and bodies*" (EDPS Guidelines) to all EU agencies. These agencies were requested to submit their notifications on health data accompanied by a cover letter from the Data Protection Officer (DPO) highlighting the specific aspects vis-à-vis the EDPS Guidelines in this field. The deadline to submit notifications was 16 November 2009, but very few agencies respected it. The EDPS has subsequently continued to receive notifications, the latest being on 20 September 2010.

The EDPS received notifications for prior-checking (within the meaning of Article 27(3) of Regulation 45/2001) and a cover letter from the DPO's of the following 18 agencies:

- European Training Foundation (**ETF**),
- European Centre for Disease Prevention and Control (**ECDC**),
- European Union Agency for Fundamental Rights (**FRA**),
- Research Executive Agency (**REA**),
- European Centre for the Development of Vocational Training (**CEDEFOP**),
- Tran-European Transport Network Executive Agency (**TEN-T EA**),
- European Railway Agency (**ERA**),
- Executive Agency for Health and Consumers (**EAHC**),
- Community Fisheries Control Agency (**CFCA**),
- European Research Council Executive Agency (**ERCEA**),
- European Agency for the Management of Operational Cooperation at the External Borders (**FRONTEX**),
- Executive Agency for Competitiveness and Innovation (**EACI**),
- European Agency for Safety and Health (**EU-OSHA**),
- European Chemicals Agency (**ECHA**),
- European Foundation for the Improvement of Living and Working Conditions (**EUROFOUND**),
- European Environment Agency (**EEA**),
- European Aviation Safety Agency **(EASA**),

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 63
E-mail : edps@edps.eu.int - Website: www.edps.eu.int
Tel.: 02-283 19 00 - Fax : 02-283 19 50

- European Maritime Safety Agency (**EMSA**).

The draft opinion was sent to the 18 DPOs of the agencies concerned for comments on 10 January 2011. Some DPO's comments were received on 11 February 2011, following a request for extension from the DPO of an agency.

2. Legal aspects

2.1. Prior checking

The processing operations under examination cover various procedures namely pre-recruitment medical examinations, annual medical check-ups and sick leave absences, and involve different categories of data subjects (members of permanent staff, temporary agents, contractual agents, national experts, trainees, candidates for any of these positions and visitors to the EU agencies). These processing operations are subject to prior-checking according to Article 27(2)(a) of Regulation 45/2001 ("the Regulation "), since they concern the processing of medical data as well as administrative and financial data related to or in connection with health.

The EDPS analysed each agency's practice with reference to the data protection principles of the Regulation and evaluated whether each agency followed the EDPS Guidelines or not. In view of the similarities of the procedures, and of similarities presented by some agencies in terms of data protection practices, the EDPS decided to examine all the notifications in the same context and issue one joint opinion. In this joint opinion the EDPS highlights any agency's practice which does not seem to be in conformity with the principles of the Regulation or the EDPS Guidelines and provides the agency(ies) concerned with relevant recommendations. Some examples of good practice are also highlighted. For instance, the EDPS notes the thorough analysis of data processing operations and practices carried out by **CEDEFOP** in light of the EDPS Guidelines. Furthermore, the **ETF** has prepared a comprehensive booklet including procedures on the management of personal and medical files.

An important element in all the notifications received is that with the exception of **FRA**, all agencies outsource the medical and laboratory tests to an external medical advisor or contractors. Most of the agencies use the Commission's medical services in Brussels and Luxembourg and they have concluded SLAs (Service Level Agreements) accordingly, even those which use other external medical providers. In addition, all agencies (except **FRA**) use the medical questionnaire approved by the EDPS in July 2008 in cooperation with the Inter-institutional Medical College in the context of pre-recruitment examinations. In terms of security measures, the EDPS notes that no agency seems to have adopted a specific security policy regarding the processing of data related to health (see further on point 2.9 on security).

The EDPS considers it useful to indicate the different parties involved in the processing operations under analysis. In this way, the relevant agencies may have a clear picture of the relationship between controller and processor and which of them is responsible for keeping the medical files of staff members.

i) Medical files kept by the Commission's medical services

REA, TEN-T, ERA, CFCA, ERCEA, FRONTEX and **EACI** have concluded a SLA with the Commission's medical service in Brussels; **EAHC** has an SLA with the Commission's service in Luxembourg. The medical files are kept at the Commission's medical services.

ii) Medical files kept by an external medical centre

ECHA, EASA, CEDEFOP, EUROFOUND, EEA, **EU-OSHA** and **EMSA** have also concluded an SLA with the Commission's medical services. Some of them, namely **EUROFOUND, EEA, EU-OSHA** and **ECDC** have also concluded contracts with external medical centres which hold the medical files of the agencies' staff members.

iii) <u>Medical files kept by an external medical advisor</u>
ECHA and **EASA also** have contracts with external medical centres, but the medical files of their staff members are kept by external medical advisors who perform their activities at the agencies' premises. **CEDEFOP** and **ETF** have concluded contracts with external advisors who keep the staff members' files.

FRA has no medical officer or service. Staff members keep their medical data.

The **ECDC, EASA** and **EAHC** indicated in their notifications that the processing operations regarding the pre-recruitment medical examinations and annual check-ups involve not only data related to health, but also data intended to evaluate personal aspects relating to the data subjects, namely to determine whether a staff member is fit for the service or not (Art. 27(2)(b)). The EDPS clarifies that as Article 28(e) of the Staff Regulations of the officials of the European Communities (Staff Regulations) provides, determining whether a person is apt or not involves an assessment of whether the person is physically fit to perform his/her tasks, not an evaluation of the individual's ability, efficiency or conduct in terms of work performance. Article 27(2)(b) is therefore not relevant in this context.

With regard to pre-recruitment medical examinations, the **ECDC, EASA** and **EEA** stated that the processing also falls under Article 27(2)(d) of the Regulation, since it intends to exclude individuals from a contract. The EDPS underlines that the recruitment of a successful candidate is based on a number of conditions specified in Article 28 of the Staff Regulations. In particular, Article 33 of the Staff Regulations provides that *"before appointment, a successful candidate shall be medically examined by one of the institution's medical officers in order that the institution may be satisfied that he fulfils the requirements of Article 28(e)"*. Hence a pre-recruitment medical examination intends to fulfil one of the six requirements of recruitment, as stated in Article 28(e) of the Staff Regulations, that "*an official may be appointed only on condition that ... he is physically fit to perform his duties*" and is not intended to exclude an individual from a contract. It follows that the processing operation on pre-recruitment medical examinations is prior-checkable due to the specific risks presented under Article 27(2)(a) and not Article 27(2)(d) of the Regulation.

According to Article 27(4) of the Regulation, the EDPS will issue his opinion within two months following receipt of the notification. Due to the fact that the last notification was submitted to the EDPS on 20 September 2010, the EDPS considers this date as the date of receipt for all notifications. Following the expiry of the deadline, the EDPS has sought answers to questions and further information from the DPO's. On 6 December 2010 the EDPS sent an e-mail to all DPOs concerned informing them that due to the complexity of the case in light of Article 27(4) of the Regulation, the EDPS had decided to extend the period of suspension for one month, until the 9 January 2010.(due to the fact that this is a Sunday, the draft for comments was sent to the DPOs on 10 January 2011). Hence the prior-checking period was suspended for 18 days (taking into account only the suspension period of the last notification received), one month due to complexity and for 15 days to allow for comments from the DPOs. The present opinion must therefore be issued no later than the 11 February 2011. The EDPS will also send each agency an individual letter underlining the necessity to inform the EDPS of the measures taken in response to the recommendations of this opinion within a period of 3 months.

2.2. Lawfulness of the processing

Personal data may only be processed if lawful grounds can be found in Article 5 of the Regulation. The processing operations under examination fall under Article 5 a), pursuant to which data may be processed if the processing is "*necessary for performance of a task carried out in the public interest on the basis of the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof or in the legitimate exercise of official authority vested in the Community institution or body or in a third party to whom the data are disclosed*".

It follows that the first issue under Article 5(a) is to determine whether there is a specific legal basis for the processing and the second issue is to verify whether the processing operation is necessary for the performance of a task carried out in the public interest.

Relevant lawful grounds in the Treaty or other legal instruments
The legal basis for carrying out a pre-recruitment examination can be found in Articles 28 and 33 of the Staff Regulations and Articles 12(d), 13(2) and 83(2) of the Conditions of Employment of other servants of the European Communities (CEOS).

In the case of annual medical check-ups, the legal basis is Article 59(6) of the Staff Regulations and Articles 16(1), 59 and 91 of the CEOS.

Article 59(1) of the Staff Regulations constitutes the legal basis for the processing of health data in any medical check-up during an absence due to sickness or accident.

TEN-T EA and **EEA** do not seem to have indicated in the notification or the privacy statement the specific legal basis for processing personal data in relation to pre-recruitment medical examinations, annual check-ups or sick leave. The EDPS recommends that, as clearly explained in his Guidelines, the specific provisions are made visible to all concerned staff members through the privacy statements (see below "Information to be given to the data subject", point 2.8).

EUROFOUND has indicated Article 59(6) of the Staff Regulations as the legal basis of the annual medical visits. **EUROFOUND** should also add the legal basis of the annual check-ups in the case of temporary and contract agents according to the provisions of CEOS. Moreover, the EDPS recommends that the exact legal basis of a pre-recruitment examination which is applicable to potential staff members should also be indicated in the notification and privacy statement (see further on privacy statement, point 2.8).

As was highlighted in the Guidelines, the further processing of medical data collected on the basis of the Staff Regulation provisions can only be considered lawful provided that it is based on the informed and freely given consent of the data subject or if the processing is necessary to protect the vital interests of the data subject. The data subject should be given the possibility to refuse and/or withdraw his/her consent with respect to further processing of his/her medical data for medical follow up purposes. In the present case, the consent is valid only if it is based on the information that each agency should provide to its staff members in line with Articles 11 and 12 of the Regulation (see "Information to be given to the data subject", point 2.8).

Necessary to perform a task carried out in the public interest
In considering whether the processing operations under analysis fulfil the second condition of Article 5 of Regulation 45/2001, the EDPS notes that the pre-recruitment medical examinations and specific medical check-ups are necessary for the purpose of managing and monitoring the aptness and sick leave of the agencies' staff members. Furthermore, the annual medical check-ups can be considered as necessary and thereby lawful for other purposes, notably for the purpose of

setting up a joint sickness insurance scheme (Articles 72 and 73 of the Staff Regulations). Such processing operations fall therefore within the context of the performance of the agencies' mission in the public interest in conformity with Article 5 (a) of the Regulation.

In any event, all agencies should ensure that the staff member concerned is:

- informed of the outcome of the annual exam from the examining doctor,
- invited to receive additional information/clarifications from the doctor if he/she wishes,
- entitled to have the annual exam carried out with a medical practitioner of his/her choice and be reimbursed in the same way as if the exam had been carried out within the agency's medical centre.

2.3. Processing of special categories of data

Within the framework of the selection and recruitment procedures the processing of certain data belonging to the "*special categories of data*" under Article 10 of Regulation 45/2001 is prohibited unless an exception can be found in the same Article 10, sub-paragraphs (2) to (5).

Some of the agencies claim that they do not receive any medical data in the strict sense and therefore the processing operations should not be subject to a prior-checking analysis. In particular, the **EU-OSHA, REA, TEN-T** and **EAHC** argue that they only process aptitude certificates, administrative data on sick leave, medical certificates, annual check-ups and the purchase of medical equipment for some staff members' daily professional activities.

As the EDPS explained in his Guidelines, the notion of health data refers mainly to two different forms of data, medical data and administrative documents that include personal data relating to the health status of a person. Many agencies collect and process, for instance, administrative notes certifying medical aptitude for work, invoices stating that a person carried out an annual medical visit or a vaccination, notes for a possible request for a follow-up medical examination, or simply information sent to the HR department for administrative purposes stating that a person is on medical leave. Such data are related to the health status of a person and may lead to the possible identification of a specific data subject's illness or disability. Although the exact type of illness is not indicated on a medical certificate, the data subject can be identified as having been absent due to a short or long term illness on medical treatment or due to special sick leave of a medical nature.

Consequently, even if no medical data *stricto sensu* are processed, the processing operations under analysis are related to health, thus falling under Article 27(2)(a) of the Regulation, and are subject to a prior-checking

The EDPS therefore recommends that all HR staff of **ETF, ECDC, FRA, REA, CEDEFOP, TEN-T, EAHC, ECHA, EU-OSHA, EACI, EUROFOUND, EEA, EASA** and **EMSA** who are responsible for collecting aptitude certificates and any other information related to their staff members' health status are reminded to process them in accordance with the principles of medical confidentiality. The EDPS invites these agencies to prepare declarations of confidentiality to be signed by the staff in charge that they are subject to an obligation of professional secrecy equivalent to that of a health professional in compliance with Article 10(3) of Regulation 45/2001. (This issue should be linked with Article 7(3) of the Regulation, see more in point 2.6 of this opinion).

The EDPS notes the declaration of confidentiality prepared by **CEDEFOP** and recommends that a sentence is added in the declaration, namely "*I am subject to an obligation of professional secrecy equivalent to that of a health professional in compliance with Article 10(3) of Regulation*

45/2001". This additional sentence refers specifically to the health data processed and underlines their sensitivity.

2.4. Data Quality

Adequacy, relevance and proportionality: According to Article 4(1)(c) of Regulation 45/2001 *"personal data must be adequate, relevant and not excessive in relation to the purposes for which collected and/or further processed"*.

It seems that the data related to health collected by the agencies under analysis, and the medical data collected and processed by the external providers of some of the same agencies are in principle adequate, relevant and not excessive to the purpose for which they are collected in compliance with Article 4(1)(c) of the Regulation.

Nevertheless, the EDPS draws the attention to the principle of proportionality in particular to **ECHA, EASA, CEDEFOP, EUROFOUND, EEA, EU-OSHA, EMSA, ECDC** and **ETF**. These agencies are not exclusively bound by the medical services of the Commission and process medical data in the framework of a pre-recruitment examination and annual check-up through their external providers. They should therefore ensure the prohibition of the collection of data for any purposes other than those of determining the physical fitness for employment, determining the entitlement to guaranteed benefits in relation to invalidity or death, or protecting the health of their staff members. The EDPS therefore recommends that the agencies "*in general terms undertake a thorough reassessment of the questions put in the questionnaire for the pre-recruitment medical examination and annual medical check-up in the light of the principles of adequacy, relevance and proportionality, for the purposes of judging fitness for service*"[1].

1) Pre-recruitment medical examination

The EDPS notes that the medical questionnaire used by ***ECHA*** requires a photo of the data subjects who are invited to undergo the pre-recruitment medical examinations. The EDPS does not see the relevance of such information to the purpose of the processing, that is whether the successful candidate is fit or not for the job position.

2) Medical check-up performed by a general practitioner

In cases where staff members wish to carry out an annual check-up at a medical practitioner of their own choice, the **ETF**, **FRONTEX, EACI, EU-OSHA, ECHA, EUROFOUND, EEA, EASA** and **EMSA** should set up a policy according to which the data subject's private practitioner should not communicate their results to the agencies' doctor or the Commission's medical service without the data subject's own freely given and informed consent. The practitioner should only send a declaration to the agencies' HR confirming that the examinations were carried out and if necessary, specifically mention the fact that the data subject concerned needs special accommodations.

CEDEFOP put forward that the annual medical examinations is not primarily preventive, but to ascertain whether the staff member is fit for his/her duties or whether some adjustments need to be made in the workplace. The agency therefore considers that all medical results should be communicated to the **CEDEFOP**'s external medical officer as only they are able to certify the

[1] See EDPS Opinion of 14 July 2007 on the processing of medical data by the EP medical services in Brussels and Strasbourg (case 2004-205).

fitness to work in the work environment and from an occupational medicine perspective. The EDPS highlights that from a data protection perspective, the data subjects should be free to decide whether their medical results should be communicated from their private practitioner to the agency's doctor. A declaration confirming that the staff member is apt should be sufficient for the agency. Nevertheless, the EDPS considers that in some problematic cases, where a staff member's health status may be a risk to his/her colleagues or to his/her own work performance, those specific results could be sent to the agency's doctor under the condition that the data subject is informed before the transfer of those medical data.

Accuracy: Article 4 (1) (d) of the Regulation provides that personal data must be "*accurate and when necessary, kept up to date*". In addition, "*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* ".

This principle should be applied both to medical files and personal files.

The **ETF, ECDC, REA, CEDEFOP, ERA, EAHC, CFCA, ERCEA, FRONTEX, EACI, EU-OSHA, ECHA, EUROFOUND, EEA, EASA** and **EMSA** should ensure that the pre-recruitment aptitude certificates and the annual check-up declarations should be kept in the personal files. The files should be completed with up-dated health status documents where necessary, namely in the case of an annual check-up. Internal notes should be addressed accordingly to the responsible HR staff.

The **ETF, ECHA** and **EASA** should ensure that the quality principle is respected by adding for instance a clause in the contract with their external medical advisors and medical centres. The **ECDC**[2]**, EU-OSHA, EUROFOUND, EEA** and **EMSA** should do likewise with their respective external medical services. This clause should list specific methods which can guarantee that the medical data of the data subjects are kept **accurate, complete** and **up-to-date,** namely that:

- the consent and signature of the data subjects as regards information concerning contacts with their attending physician or specialist may help to ensure that the medical data contained in the medical report are complete;
- the data subjects can sign their medical examination reports so that the accuracy of their administrative data can be verified;
- the data subjects may submit other medical opinions to the medical advisors and medical services of the above agencies in order to ensure the completeness of their medical file;
- the medical advisor should ensure that no comment or annotation should be added to any medical form by any third party.

In cases where the Commission's medical services[3] carry out some or all medical examinations for some of the agencies' staff members, and their medical files are kept at the Commission's medical services, those agencies, in particular the **REA, TEN-T, ERA, EAHC, CFCA, ERCEA, FRONTEX, EACI** and **EMSA,** should ensure that the data subjects are aware of the above practices regarding the accuracy of their medical file.

FRA should take into consideration the above recommendations in case the agency concludes a

---

[2] The EDPS took note of the **ECDC**'s DPO letter of 29 January 2010 in which she stated that the agency instructed the processor to adopt the EDPS recommendation regarding the signature of laboratory reports by the data subjects.

[3] It should be recalled that the activities of the Commission's medical service in Brussels and Luxembourg were subject to prior-checking by the EDPS. The Opinion was issued on 10 September 2007, case 2004-232).

contract with a processor for carrying out all medical examinations.

In the case of sick-leave absences where administrative data related to health are collected electronically, the **ETF, ECDC, FRA, REA, ERA, EAHC, CFCA, FRONTEX, EU-OSHA, EACI**, **EEA, EUROFOUND** and **EMSA** should ensure that an audit trail is in place to ensure traceability of user actions (see issue on security, point 2.10).

2.5. Conservation of data

Article 4(1)(e) of Regulation 45/2001 outlines the principle that *"personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are collected or for which they are further processed"*.

The EDPS would like to clarify, as pointed out in the Guidelines point out, as a general rule a period of 30 years after the last medical document inserted in the file should be considered as the absolute maximum period during which medical data should be kept in this context. Any conservation period should be assessed and determined in the light of Article 4(1)(e) of the Regulation. As recommended by the EDPS in his letter to the Board of Heads of Administration on 26 February 2007[4]**,** the nature of the medical documents should be examined in the light of the rules applicable in order to determine what conservation periods would be suitable to each type of document. It is therefore necessary to examine to what extent and for what purposes it is necessary to keep various medical documents during and after a staff member's period of employment. It is important to note that on 11 October 2010, the Board of Heads of Administration submitted a consultation to the EDPS under Article 28(1) of the Regulation regarding specific retention periods for various medical documents. Following meetings between the EDPS and the CPAS, the relevant sub-committee of the Board, the EDPS will issue soon his decision on the consultation taking into account the EDPS letter of 26 February 2007 and his prior-checking opinions.

In this regard and in order to avoid any misunderstanding, the **EACI** should add to their privacy statement that medical data are kept for a maximum 30 years *"after the last medical document is inserted in the file in the light of Article 4(1)(e) of the Regulation."* The **EACI** should also adopt specific data retention periods related to sick leave and regarding non-recruited persons in conformity with the EDPS Guidelines.

The EDPS notes that the **ECDC** keeps aptitude certificates ("certificates of health") of both recruited and non-recruited persons for a maximum of thirty years.
Furthermore, the **EUROFOUND** stated that " *a copy of the pre-recruitment certificate is kept in the personal file permanently. The original is kept in the medical file. The medical file as part of the personal file of a staff member is kept on a permanent basis*".
The **ECHA** indicated in its notification that "*the medical files of staff members are kept until 10 years after the end of the employment*".
The **EASA** also stated in its notification that "*the results are kept in the medical file, which is kept for 10 years from the date the contract of employment has ceased*".
The EDPS would like to highlight that the data which should be kept in the medical files by the agencies' processors are laboratory results of the pre-recruitment examinations and any other medical examinations that the data subject wishes to undertake. According to the above mentioned assessment, the medical files should be kept for a maximum of 30 years after the staff member left the workplace. Aptitude certificates stating the aptness or not of the staff member should be kept

[4] See http://www.edps.europa.eu/EDPSWEB/edps/Supervision/Adminmeasures.

in the personal file. According to the EDPS Guidelines on staff recruitment[5], the EDPS recommend that personal files should be kept for 10 years after the end of the period during which a staff member is in active employment or the last pension payment.
Consequently, the data retention periods adopted by the **ECDC** and the **EUROFOUND** are excessive for the purpose for which the data are collected and the data retention period indicated by the **ECHA** and the **EASA** is not in compliance with the above mentioned policies. The EDPS invites all four agencies to re-assess the data kept in the medical files and personal files and set up appropriate data retention periods as explained above.
Moreover, in light of the EDPS Guidelines, the **ECDC** and **ECHA** should adopt a retention period for the data of non-recruited persons, a period during which it is possible to challenge the data or the negative decision. In addition, the EDPS recommends that the **ECDC** and the **ECHA** adopt specific data retention periods related to sick leave data.

According to the **FRA**'s notification, the agency keeps the aptitude certificates in the personal files of recruited persons for an indefinite period as long as the personal file exists. The EDPS finds this period excessive and unnecessary under Article 4(1)(e) of the Regulation. As already pointed out, the EDPS recommends that the **FRA** should keep personal files for a maximum period of 10 years after the end of the period during which a staff member is in active employment or the last pension payment.

The **EAHC** should follow the same recommendations for the retention period of the aptitude certificates related to pre-recruitment examinations kept in the personal file and set up a data retention period for non-recruited persons as recommended in the EDPS Guidelines.

In the case of the **ETF**, the EDPS recommends that the agency should also adopt specific retention periods related to sick leave data, specific medical check-up data and regarding non-recruited persons in conformity with the EDPS Guidelines.

The EDPS invites the **REA** to consider, while establishing its own specific retention list, not only the "Common Commission-level retention list", but also the recommendations made by the EDPS in his Guidelines; **REA** should notably adopt retention periods for both recruited and non-recruited persons of data related to health (aptitude certificates and medical certificates), sick-leave and if necessary specific medical check-ups. The EDPS should be informed as soon as the list is adopted.

The **TEN-T** informed the EDPS about the retention periods for the data related to sick leave and to non-recruited persons, which seem to be reasonable. The EDPS recommends that these retention periods are indicated in both the notification and the privacy statement.

The **FRONTEX** should set up a retention period for the health related data of non-recruited persons in light of the EDPS Guidelines.

The **ERA** and the **EU-OSHA** should set up a specific retention period for the data related to sick leave in conformity with Article 59(4) of the Staff Regulations and in light of the EDPS Guidelines.

The **EEA** has not indicated in the notification any retention periods for:
- aptitude certificates in the personal files,
- data related to sick leave,
- specific medical check-ups and

[5] Guidelines concerning the processing operations in the field of staff recruitment, 10 October 2008.

- data of non-recruited persons.

The EDPS recommends that the **EEA** adopts specific retention periods for these data and ensure that the external medical provider of the agency keeps the medical data of its staff members for a maximum period of 30 years after the last medical document in the staff member's file in the light of Article 4(1)(e) of the Regulation.

The **ERA** indicated in the notification that "*data on leave on medical grounds are processed for statistical purposes in an anonymous manner, thus Regulation 45/2001 is not applicable.*" In order to avoid any confusion, the EDPS draws attention to Article 4(1)(e) of the Regulation which explicitly provides that " *... personal data which are to be stored for longer periods for historical, statistical or scientific use should be kept ... in anonymous form only ...In any event, the data shall not be used for any purpose other than for historical, statistical or scientific purposes*". It is clear from this provision that the **ERA** should ensure that the data are rendered anonymous if they are used for statistical purposes. Only if this is done is the Regulation no longer applicable. The EDPS requests that **ERA** provides evidence of the method by which it achieved the anonymisation of the data for statistical purposes.

2.6. Transfer of data

The processing covered by Article 7(1) is the transfer of personal data within or to other Community institutions or bodies *"if the data are necessary for the legitimate performance of tasks covered by the competence of the recipient"*.

Internal communication of data within the agency:

i) Medical invoices
The EDPS welcomes the specific policy adopted by the **ECDC** according to which the controller forwards only the total cost that should be paid to the external medical contractor to the agency's Financing/Accounting Section. A declaration of confidentiality is also signed by the accounting officer of the agency's department.

FRA should ensure that the reimbursement document (Annex 2 of the notification) should be filled in by the medical practitioner of the data subject who then transmits only the total sum to be reimbursed to the joint insurance claims office of the agency.

There was no information provided by **ETF, FRONTEX, EU-OSHA, EEA** and the **EASA** as to whether any specific procedure is established regarding the possible transfer of health data to the administrative budget department of the agency in the context of reimbursement. The EDPS insists that the above agencies set up a procedure whereby all medical invoices are first sent to the medical service of the agency, which validates them and then only transmits the total sum to be reimbursed to the budget department.

REA, **ERA** and **FRONTEX** should set up a procedure whereby the Commission's medical service should validate all medical invoices and then fill in a document which would indicate the total sum to be reimbursed. This document should be transferred directly to the agencies' responsible finance department only by the Commission's medical service.

As concerns **CEDEFOP's** position, the EDPS recalls that the objective of the Guidelines is to harmonise good practice and ensure consistency among all agencies. The EDPS therefore invites **CEDEFOP** to reconsider the policy regarding medical invoices and adopt the recommendations made in the Guidelines.

ii) Transfers to other institutions
Moreover, in the context of transfers to other institutions, agencies should ensure that the recipients of medical files are only persons authorised to have access to data relating to health and who are subject to professional secrecy.

This should be the case for the **FRA**, **REA**, **TEN-T**, **ERA, EAHC**, **CFCA**, **ERCEA**, **FRONTEX**, **EACI, EU-OSHA, ECHA, EEA** and **EASA** when the agencies need to transfer aptitude certificates of staff members, or other documents related to their health, to another institution.

iii) Compliance with Article 7(3) of the Regulation
Furthermore, Article 7(3) of the Regulation provides that "*the recipient shall process the personal data only for the purposes for which they are transmitted*". According to the notifications, the **ETF, ECDC**[6]**, FRA, REA, TEN-T, ERA EAHC, CFCA, ERCEA, FRONTEX, ECHA, EU-OSHA, EACI, EUROFOUND, EEA**, **EASA** and **EMSA** have not provided any document or any other reference which show that the principle of Article 7(3) is respected. The EDPS recommends that for instance an internal note is prepared by each agency or a declaration is signed by the potential recipients, which explicitly reminds them of their obligation not to use the data received for any other purpose than the one for which they were transmitted.

The EDPS recommends that the above two points (ii) and (iii) be implemented together with the recommendation in point 2.3. This means that the agencies concerned should prepare internal notes or declarations to be signed by the staff regarding both Article 10(3) and Article 7(3) of Regulation 45/2001.

External transfer

i) Transfer in light of Article 8 of the Regulation
Article 8 of the Regulation provides the conditions under which personal data may be transferred to recipients subject to the national law adopted for the implementation of Directive 95/46/EC.

The notifications of the **ETF, ECDC, FRA, REA, TEN-T, ERA, EAHC, CFCA, ERCEA, FRONTEX, EACI, EU-OSHA, ECHA, EUROFOUND, EASA** and **EMSA** do not provide any information as to a possible transfer to any recipients within the scope of the Directive. Although rare, these transfers cannot be excluded. In case the agencies need to transfer health data for instance to national authorities in the context of an investigation carried out by a national authority, the necessity of the transfer should be demonstrated under Article 8(a) of the Regulation. Moreover, the EDPS highlights that cooperation with national authorities should also respect the requisites and mechanisms imposed by national regulations on medical secrecy. In all cases, it is fundamental that only adequate, relevant and not excessive data should be transferred.

ii) Transfer in light of Article 9 of the Regulation
Article 9 of the Regulation provides that personal data may be transferred to recipients who are not subject to national law adopted pursuant to Directive 95/46/EC, if the third country or organisation provides an adequate level of protection. Adequacy of protection should be assessed in view of the criteria set forth in Article 9(2). Exceptional cases are provided for in Article 9(6).

---

[6] The EDPS notes that according to the notification, the **ECDC**'s staff members have been informed about confidentiality in processing data. They have received instructions by the DPO and the agency is in the process of carrying out training/information sessions. Such practices are encouraged and should be adopted by all agencies.

In all cases of transfers outside the scope of the Directive, the agencies should ensure respect for Article 9.

In the event of such a transfer, the agencies should ensure respect of Article 9.

2.7. Rights of access and rectification

Article 13 of the Regulation provides for a right of access and sets out the modalities of its application following the request of the staff member concerned. Article 14 of the Regulation provides that *"the data subject shall have a right to obtain from the controller the rectification without delay of inaccurate or incomplete personal data".*

Right of access

Recruited staff members

i) Right of access within reasonable time limits and without constraints
Most of the agencies outsource the processing of medical data of their staff members and they therefore do not keep any medical files. It is therefore necessary to make a clear distinction between the right of access to a staff member's medical file and a staff member's personal file.

- **to the staff member's medical file**

The EDPS considers appropriate that the **ECHA, EU-OSHA**, **EEA, EASA** and **EMSA** ensure through the contract with their external medical provider/advisor that the latter establish a reasonable time limit within which an access request should be dealt with without any constraints pursuant to Directive 95/46/EC. This should be explicitly indicated in the privacy statements informing the data subjects about their rights (see point 2.8).

- **to the staff member's personal file**

The **ETF**, **ECDC, CEDEFOP, TEN-T, ERA, EAHC, ECHA, EEA** and **EMSA** should explain in the privacy statement or in another note that all aptitude certificates of both pre-recruitment examinations and annual check-ups are accessible in the personal file (kept by the agencies' HR) within a reasonable time and without constraints following the access request in conformity with Article 13 of Regulation 45/2001.

ii) Access in an intelligible form
Those agencies which have external medical providers, namely **ECHA, EASA, CEDEFOP, EUROFOUND, EEA, EU-OSHA, EMSA, ECDC** and **ETF** should ensure that the medical practitioners in charge of undertaking medical examinations communicate the medical results to the data subjects in an intelligible form. This implies that they should interpret the data (such as medical codes or results of blood analysis) and/or make the data decipherable.

iii) Copies of medical files
When data subjects request copies of their medical file, the **ECHA, EU-OSHA**, **EASA** and **EMSA** should ensure that the medical practitioners in charge of their medical files grant this request to their staff members.

iv) Access to data of a psychological or psychiatric nature
In cases where the data processed are of a psychological or psychiatric nature, the **ETF, ECDC, REA, TEN-T, ERA, EAHC, CFCA, ERCEA, FRONTEX, ECHA, EU-OSHA, EACI, EUROFOUND**, **EASA** and **EMSA** should ensure that data subjects have access indirectly, if it is

assessed on a case by case basis that indirect access is necessary for the protection of the data subject ex Article 20.1.c) of the Regulation. The possibilities for indirect access should take place in light of the Conclusions 221/04 of 19 February 2004 and the above agencies should inform the data subjects of those possibilities (see point 2.8).

Non-recruited staff, visitors, trainees

According to the notifications, some other categories of data subjects are not catered for, such as non-recruited persons, visitors, trainees or other persons who might be subject to a medical treatment in the course of their presence in the agencies. Therefore the **ECDC, REA, TEN-T, ERA, EAHC, CFCA, FRONTEX, ECHA, EU-OSHA, EACI**, **EASA** and **EMSA** should grant the right of access to those data subjects of their data processed related to their health status when they request so. This information should be indicated in the privacy statement.

Right of rectification

The **ETF, FRA, REA, CEDEFOP, TEN-T, ERA, EAHC, CFCA, ERCEA, FRONTEX, ECHA, EU-OSHA, EUROFOUND**, **EEA, EASA** and **EMSA** should ensure that this right is understood by data subjects (for instance, by providing information in the privacy statement) and is granted to them, in particular their entitlement not only to correct any administrative errors in their medical file but also to supplement it by adding the second opinions of other doctors.

2.8. Information to be given to the data subject

Articles 11 and 12 of Regulation 45/2001 provide that data subjects must be informed of the processing of data relating to them and list a range of general and additional items. The latter apply insofar as they are necessary in order to guarantee fair processing in respect of the data subject having regard to the specific circumstances of the processing operation. In the present case, medical data are partly provided by the data subject and partly by the Commission's medical services or external doctors and medical providers.

Privacy statement

The information provided by the **ETF** in point 1.7 of the letter sent to the EDPS is irrelevant to the right to information. Furthermore, although the **ETF** listed in the notification all the elements of information under Articles 11 and 12, the agency did not prepare a privacy statement explaining to the data subjects concerned, the relevant information under these provisions. Consequently, in light of the EDPS Guidelines, the EDPS invites the **ETF** to provide the data subject with a privacy statement which should be easily accessible and explain all the information listed in Articles 11 and 12.

The **ECDC** should amend the data retention periods in the privacy notices on both pre-recruitment and annual medical examination (see point 2.5 above) and clarify to data subjects that an external medical service keeps their medical files, whereas personal files are kept by the agency's HR.

The EDPS recommends that **FRA, REA, TEN-T, FRONTEX, EU-OSHA, EUROFOUND, EEA** and **EASA** prepare, as soon as possible, a privacy statement listing all the rights of the data subjects provided by Articles 11 and 12 of the Regulation.

The **CEDEFOP** has indicated the information that the agency envisages including in the privacy statement in compliance with Articles 11 and 12 of the Regulation. A copy of the privacy statement referring thoroughly to all the appropriate information, should be sent to the EDPS as soon as it is prepared.

The EDPS finds that the "*specific privacy statement e-HR*" provided by the **ERA** is irrelevant to the processing of data related to health carried out by the agency. It is therefore recommended that an appropriate privacy statement is prepared concerning the specific processing operations carried out by the agency. This should explain clearly to data subjects all the relevant information under Articles 11 and 12.

The **EAHC** indicated in the notification that relevant information can be found on their intranet. The **EMSA** provided the EDPS with some links to documents on the intranet, which do not seem to be relevant to Articles 11 and 12 of the Regulation. The EDPS therefore invites both the **EAHC** and **EMSA** to prepare a privacy statement regarding pre-recruitment, annual check-ups and sick leave processing operations. This privacy statement should provide clear and detailed information regarding the rights to information of the data subject as they are enumerated in Articles 11 and 12 of the Regulation.

The purpose of the processing, "*to manage the rights and obligations of CFCA staff and SNE's*", as defined by **CFCA** in the privacy statement is vague and can be misleading. The EDPS recommends that the agency adds a clause/sentence which explains that the purpose of the processing concerns the rights and obligations of the agency's *staff in the context of the processing of their data related to health.*

The EDPS finds that the privacy statement of the **ERCEA** concerns the recruitment procedure and the constitution of personal files. This is not sufficient, since it does not concern the data related to health processed by the agency. Consequently, the EDPS recommends that an appropriate privacy statement is drafted listing all rights of Articles 11 and 12 in relation to the specific processing operations under analysis.

The **ECHA** included a data protection notice on the invitations addressed to the data subjects regarding pre-recruitment examinations at the Commission's medical service and Helsinki's medical centre. The same data protection clauses are stated in the invitations regarding annual check-ups, special leave for medical treatment and sick leave away from the place of employment.
The **ECHA** should also prepare a data protection notice regarding the medical examinations carried out by the external medical advisor.
The **ECHA** should include the EDPS recommendations concerning the right of access and rectification (see point 2.7 above) in all its data protection notices. It should also add the following information in light of the EDPS Guidelines on health data:

- the legal basis of each processing operation on health data;
- the retention period of medical data kept by the external medical advisor for both recruited and non-recruited persons;
- the retention period of data related to sick leave and
- the right of data subjects to have recourse at any time to the EDPS.

The EDPS points out to all agencies that the privacy statement should not only be addressed to all newly recruited staff (as the **REA** indicated in its notification), but to all the staff of the agencies. It should for instance be easily accessible on an agency's website.

Additional information to be given

Apart from the rights listed in Articles 11 and 12, the privacy statement should provide some further information regarding the processing operations under analysis. The EDPS reiterates the recommendations as highlighted in his Guidelines on health data.

The **REA**, **TEN-T**, **ERA**, **ERCEA**, **FRONTEX, EAHC, EU-OSHA, EUROFOUND, EEA, CEDEFOP, EASA** and **EMSA** should clarify in the privacy statement which party (Commission's medical service, external provider, agency's doctor) is responsible in carrying out the pre-recruitment exams, annual and other check-ups, as well as where the staff members' medical files are kept.

The **REA**, **CEDEFOP**, **TEN-T**, **ERA**, **EAHC**, **ERCEA**, **FRONTEX, EU-OSHA, EUROFOUND, EEA** should furthermore indicate what data related to health are collected and stored by the HR of the agencies and for what purposes.

Medical questionnaires

ETF should indicate on the two questionnaires "sorveglianza sanitaria" and "visite periodiche" (used during an annual check-up by the agency's medical advisor) whether the answers to the questions are voluntary or mandatory and the possible consequences of a failure to reply.

Medical check-ups

i) Choice of a private medical practitioner

In the case of medical check-ups, the **ETF, REA, TEN-T, ERA, EAHC, ERCEA, FRONTEX, ECHA, EU-OSHA, EACI, EUROFOUND, EEA**, **EASA** and **EMSA** should inform data subjects of their entitlement to choose their own private practitioner and of the practical steps they must take to have the check-up carried out by a practitioner of their choice.

ii) Transfer of medical examinations' results

Furthermore, the **ETF, REA, CEDEFOP, TEN-T, ERA, EAHC, ERCEA, FRONTEX, ECHA, EU-OSHA, EACI, EUROFOUND, EEA**, **EASA** and **EMSA** should specify in the privacy statement whether the data subject's private medical practitioner will need to forward any result of the medical examination to the agency's doctor or Commission's medical service, or any other external medical provider, and if so for what purpose. As explained in the Guidelines, the EDPS must insist that medical results of an annual check-up should not be communicated to the agency's doctor or Commission's medical service without the data subjects' freely given and informed consent.

iii) Indirect access to psychological or psychiatric data

Finally, the EDPS recommends that the **ETF, ECDC, FRA, REA, CEDEFOP, TEN-T, ERA, EAHC, CFCA, ERCEA, FRONTEX, ECHA, EU-OSHA, EACI, EUROFOUND, EEA**, **EASA** and **EMSA** inform data subjects through the privacy statement or an internal note of the possibilities of indirect access to psychological or psychiatric data in light of the Conclusions 221/04 of 19 February 2004.

2.9. Security

According to Article 22 of Regulation 45/2001,*"the controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected".*

The EDPS notes that the Commission has signed a "Memoranda of Understanding" (MoU) about the application of the European Commission Information Systems Security Policy with a number of agencies, such as the **EACI, EAHC, ERCEA, REA** and **ERA**. Furthermore, the **ERCEA** provided a short "state of art" in relation to the preparation of the IT Security Policy by its Local

Information Security Officer[7]. However, this MoU is not meant to provide or replace the agency's own IT security policy or any security measures they should adopt under Article 22 of the Regulation.

As mentioned in point 2.4, the **ETF, ECDC, FRA, REA, ERA, EAHC, CFCA, FRONTEX, EU-OSHA, EACI**, **EUROFOUND**, **EEA** and **EMSA** do not seem to have adopted an audit trail in order to be able to trace user actions, in particular in the case of sick-leave absences where administrative data related to health are collected electronically. This security measure should be implemented in compliance with the technical and organisational measures provided in Article 22 of the Regulation.

Furthermore, the EDPS notes that a few agencies provided documents related to their information and communication IT policy. These documents are irrelevant to the specific requirement of Article 22 of the Regulation. Consequently, the EDPS recommends that all agencies should adopt their own specific security policy taking into account the list of elements provided in Article 22(2)(a - j) of the Regulation. This specific security policy should be based on a risk assessment exercise which should be conducted by each agency and should be implemented in the framework of the actual processing of medical or/and health related data at their premises. Each agency should send a copy of their specific security measures to the EDPS.

2.10. Subcontracting

In light of Article 23 of the Regulation, agencies should choose a processor who can guarantee that adequate technical and organisational security measures can be provided in the framework of the processing of medical data.

The EDPS has identified three categories of outsourcing:
i) the Commission's medical service acts as processor to the agency and the processing is governed by a SLA,
ii) an external medical centre carries out some or most of the medical exams on behalf of the agency and
iii) the medical advisor processes medical data at the agency's premises on behalf of the agency.

The EDPS stresses that the means of implementing security measures is different in each of the above categories of outsourcing:

- in the case of SLAs, the security measures are already in place at the Commission. This of course does note mean that the agencies should not also ensure a security system within their own premises (see point 2.9 above);
- in cases where agencies concluded contracts with external medical centres, they should ensure that an appropriate level of security is adopted and implemented by the external contractor under Articles 23(2)(b) and 23(3) of the Regulation; and
- in cases where the medical advisors carry out their tasks at the premises of the agencies, the agencies should ensure through their contract with the medical advisor that the latter respects the agency's internal security measures which should be in conformity with Article 22 of the Regulation as Article 23(1) provides.

In particular, the ***EU-OSHA*** should ensure that a contract or other legally binding act must be established between the external medical service and the agency in conformity with Article 23 of the Regulation. This legal act should provide that the processor must only act upon instruction

[7] The **ERCEA** Local Information Security Officer informed the EDPS with a note of 23 September 2010 of the on-going work for preparing the IT Security Policy in the field of health related data.

from the agency. Moreover, the provider should be subject to national law implementing Article 16 or 17(3), second indent of Directive 95/46/EC, and it will need to ensure respect for the provisions of national law regarding security and confidentiality. The **EU-OSHA** should send a copy of the contract including these elements to the EDPS as soon as it is concluded.

The **EAHC** and the **EASA** concluded an SLA with the Commission's medical service in Luxembourg in 2006. However, this SLA does not make reference to the applicability of the Regulation. The EDPS highlights that the SLAs signed with the Commission's medical service in Brussels in 2008 by the agencies concerned do refer to the Regulation 45/2001. The EDPS therefore recommends that both the **EAHC** and the **EASA** update their SLA with the Commission's medical service in Luxembourg and indicate that the medical service applies the provisions of the Regulation.

The **ETF, ECHA, CEDEFOP, EUROFOUND** and **EASA** provided the EDPS with similar copies of the contracts they concluded with their external medical providers and medical advisors, acting as processors. The EDPS recommends that the following elements are included in their contracts:

- in their contracts with external medical centres, the **ECHA, EASA** and **EMSA** should include an addendum which should clearly indicate the measures of security required by the agency and to be adopted by the processor in conformity with Article 23(2)(b) and Article 23(3) of the Regulation;
- in their contracts with medical advisors, the **ETF**, **ECHA** and **EASA** should include the measures of security that the agency has adopted at its premises, and both agencies should ensure that the level of security required is respected by the medical advisor in light of Article 23(1) of the Regulation;
- as concerns Articles I.9 of the contracts related to data protection, the EDPS points out that mere reference to the contractor's personal data and right of access to them is not sufficient. The data subjects should also be included since they are part of the execution of the contract. The EDPS therefore recommends that where in Articles I.9 of all contracts there is reference to "the Contractor", the **ETF**, **ECHA**, **EASA** and **EMSA** should add the phrase "*and the data subjects whose data are processed by the Contractor"*.

As for **EUROFOUND**, where in Article I.8 of its contract there is reference to "the Contractor", the agency should add the phrase "*and the data subjects whose data are processed by the Contractor".*

The **ECDC** and the **CEDEFOP** should include in their contracts with the external medical providers, a data protection clause as well as an addendum on the measures of security that the agencies require their processors to implement in conformity with Articles 23(2)(b) and 23(3) of the Regulation.

The **EEA** has not provided the EDPS with a copy of the contract with the external medical provider. The EDPS recommends that the EEA ensures that the contract is in conformity with the requirements of Article 23 of the Regulation and invites the agency to send a copy of the contract accordingly.

Conclusion

The EDPS Guidelines have been a useful tool for agencies to reflect on how the data protection

principles of Regulation 45/2001 have an impact on processing related to pre-recruitment examinations, annual check-ups and sick leave absences. As stated in point 2.1, despite the clear explanation provided in the EDPS Guidelines regarding the wide concept of "health data", there were a few agencies which maintained that the data they were processing did not present specific risks under Article 27(2)(a) of the Regulation.

The EDPS would draw particular attention to two other issues derived from the present analysis: the legal basis of outsourcing and the privacy statement. The EDPS notes that some agencies omitted common elements from their contracts with external medical providers, notably security measures and data protection clauses. These are fundamental elements to be included in the contracts with the processors.

Moreover, agencies have not grasped the importance of a privacy statement. Only the **EACI** drafted an almost complete privacy statement in line with Articles 11 and 12 of the Regulation. The EDPS highlights the principle that the data subject must be fully informed for the processing to be lawful, and it should therefore be based on information provided in conformity with Articles 11 and 12 of the Regulation. It follows that the controller should provide the data subjects with all the necessary information about the processing, and their rights in relation to it, before the processing operation begins. This is especially true in those cases where the processing is based on the data subject's consent.

In analysing the DPOs' cover letters, the information indicated in the notifications and some remarks on the draft opinion sent to them for comments, the EDPS finds it necessary to underline that the mere intention or confirmation that a specific data protection practice will be applied in conformity with the EDPS Guidelines and recommendations is not sufficient for the implementation of the EDPS recommendations. Instead, concrete measures are required. After the EDPS opinion is issued and sent to the controller, the latter should take the EDPS recommendations fully into consideration, adopt concrete measures to implement them as soon as possible and inform the EDPS of those measures. This part of the procedure is the follow-up of the EDPS recommendations for a processing operation subject to prior-checking. The follow-up should take place within 3 months of issuing the opinion.

Consequently, in light of the EDPS' recent policy paper on monitoring and ensuring compliance with Regulation 45/2001[8]**,** the controller of each agency concerned is now invited to adopt specific and concrete measures in order to implement the EDPS recommendations regarding the processing of data related to health. This implies that in the context of the follow-up, each agency must provide the EDPS with documents which demonstrate that the EDPS recommendations have actually been implemented.

Done at Brussels,

(**signed**)

Giovanni BUTTARELLI
Assistant European Data Protection Supervisor

8 Monitoring and Ensuring Compliance with Regulation (EC) 45/2001 Policy paper, Brussels, 13 December 2010, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/10-12-13_PP_Compliance_EN.pdf.