September 2009

Guidelines concerning the processing of health data in the workplace by Community institutions and bodies

Introduction

Community institutions and bodies collect and use health data. Most of the rules defining the conditions and hypothesis in which health data are collected and used by Community institutions and bodies are provided by the Staff Regulations[1]. The Staff Regulations, however, do not define the rules ensuring the protection of the fundamental rights and freedoms of the persons concerned, and in particular their right to privacy with regard to the processing of personal data. To the extent that certain activities of the Community institutions and bodies may process health data relating to identified or identifiable persons, they are subject to the respect of Regulation (EC) 45/2001 as an instrument of primary legislation.

Objectives of the guidelines

Processing operations involving health data are subject to prior-checking in conformity with Article 27 (2)(a) of Regulation (EC) 45/2001, since they are likely to present a specific risk to the rights and freedom of data subjects. The EDPS envisages that these guidelines will be used as a practical guidance for Community institutions and bodies and they will assist the Data Protection Officers (DPOs) and controllers in their task of notifying the EDPS existing and/or future health-related data processing.

The content of the guidelines is to a large extent based on the EDPS Opinions issued so far regarding processing operations related to health data carried out by various Community institutions and bodies (see annex). The objective is to present in a **clear and concise way the outcome of the EDPS positions and recommendations** regarding each fundamental principle established in Regulation (EC) 45/2001 and to underline particular issues and/or practices of interest.

The EDPS is aware that in some agencies no medical service has been set up and the agency relies on the medical service of the European Commission for the processing of all medical data. In these cases, in principle no medical

[1] These guidelines do not apply to the possible processing of health data by Community institutions and bodies in their core business activities i.e. in the external activities of the Community institutions and bodies. This typically will not cover processing of health data to produce European statistics in this field.

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

data in the strict sense should be processed by the Agency. This is not to say that the guidelines should not be followed as concerns health related data which may be handled by the administrative unit of the Agency (e.g. indication of number of days of sick leave, requests for special leave).

Concepts

Health data generally refers to personal data that have link with the health status of a person This would normally include medical data (e.g. doctor referrals and prescriptions, medical examination reports, laboratory tests, radiographs), as well as administrative and financial data relating to health (e.g. medical appointments scheduling, invoices for healthcare service provision, indication of the number of days of sick leave, sick leave management).[2]

To this end, the notion of health data in the context of these guidelines mainly refers to two different forms of data. First, it refers to medical files that are kept at a doctor's practice or at the medical service of an EU institution. Medical files include medical reports, laboratory tests, medical questionnaires (e.g. at the pre-recruitment medical examination phase). Second, it refers to administrative documents that include personal data relating to the health status of a person. Amongst those documents are medical certificates (e.g. documents certifying medical aptitude for work), forms concerning sick leave or the reimbursement of medical expenses.

The **data subjects** are members of permanent staff, temporary agents, contractual agents, national experts, trainees of these bodies, candidates for the positions mentioned before and visitors of the EU institutions.

Guidelines

1. Lawfulness of the processing operation

In respect with Regulation (EC) 45/2001, any processing of health data which relates to an identified or identifiable person must find a legal basis in Article 5 of the Regulation to be considered as lawful.

Article 5(a) of the Regulation stipulates that personal data may be processed only if the *"processing is necessary for the performance of a task carried out in the public interest on the basis of the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof"*. Recital 27 of the Regulation further specifies that *"processing of data for the performance of tasks carried out in the public interest of the Community institutions and bodies includes the processing of personal data necessary for the management and functioning of those institutions and bodies"*.

[2] See EDPS Opinion on the Proposal for a Directive of the European Parliament and of the Council on the application of patients' rights in cross-border healthcare, November 2008, p.4.

In order to determine whether the processing operations comply with Article 5(a) of the Regulation two elements must be taken into account: **first**, whether either the Treaty or other legal instruments foresee the data processing operations carried out by the institution as a task in the public interest; **second**, whether the processing operations are indeed necessary for the performance of this task.

As far as the **first** element is concerned, the legal basis for the processing of health related data by the institutions and bodies for employment purposes will generally be found in the Staff Regulations of officials of the European Communities (hereinafter "Staff regulations") or in the Conditions of Employment of Other Servants, (hereinafter "CEOS"), the Rules on the Secondment of National Experts to the Commission and the Rules governing the Official Traineeship Scheme[3].

In some cases the legal basis can also be found in mandatory national legislation. Indeed, according to the established ECJ jurisprudence, national law applies within EU institutions where there is a void in the legal framework of the Community institutions and bodies and in so far as it does not run counter to the smooth functioning of these institutions. In fact, the privileges and immunities granted to the Communities on a basis of Article 291 of the Treaty, as implemented in the 1965 Protocol *"have a purely functional character, inasmuch as they are intended to avoid any interference with the functioning and independence of the Communities"*[4].

As far as the **second** element of Article 5(a) is concerned, the necessity of the processing has to be evaluated in the light of its purpose on a case by case basis.

The following section examines the legal basis of the most common processing of health related data by the Community institutions and bodies.

1.1. Pre-recruitment medical examination

Articles 28 and 33 of the Staff Regulations and Articles 12(d), 13 (2) and 83 (2) of the CEOS serve as legal basis for pre-recruitment medical exams: "An official may be appointed only on condition that: ... (e) *he is physically fit to perform his duties*" (Article 28*)." 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)*" (Article 33).
In addition, Article 1 of Annex VIII of the Staff Regulations provides that if *"the medical examination made before an official takes up his duties shows that he is suffering from sickness or invalidity, the appointing authority may, in so far*

[3] The Civil Service Tribunal has interpreted "legal instrument" as any act of normative value (see Vinci v. ECB, F-130/07, §119)

[4] cf. ECJ, 1/88, SA Générale de Banque/ Commission [1989] ECR 857, §9; ECJ, C-2/88, Zwartveld and Others [1990] ECR I-3365, §§ 19 and 20; CFI, T-80/91, Campogrande/ Commission [1992] ECR II-2459, §42,

as risks arising from such sickness or invalidity are concerned, decide to admit that official 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" (i.e. decide that expenses arising from such sickness or invalidity are to be excluded from the reimbursement of expenditure provided for in Article 72 of the Staff Regulations).

The regime for temporary and contractual staff foresees the possibility to refuse reimbursement of expenses concerning such sickness and invalidity detected at the pre-recruitment medical exam (Articles 28d.2, 32, 95,100 of CEOS).

The Staff Regulations **do not foresee that the pre-recruitment medical examination also serves for prevention purposes**. Having said this, the EDPS recognises that the data collected during this medical examination could additionally serve to alert a future member of staff of a specific issue concerning his/her health and therefore could also serve for prevention purposes. **This does not, however, imply that additional data should be requested for the purpose of prevention.**

1.2. Annual medical visits

In this case Article 59 (6) of the Staff Regulations, Articles 16 (1), 59 and 91 of the CEOS usually serve as the legal basis for the processing of personal data: "*officials shall undergo a medical check-up every year either by the institution's medical officer or by a medical practitioner chosen by them*".

The Staff Regulations do not seem to specify the purpose of the annual medical check-up. The EDPS can deduce from this lack of specification of the purpose that the annual medical check-up does not serve to determine the physical aptitude of the person concerned as is the case for pre-recruitment medical visits. Furthermore, no procedure for revision of the conclusions of an annual medical visit has been put into place.

If the annual medical visit does not pursue the same purpose as the pre-employment medical examination, the processing of personal data can still 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). According to the elements examined, the EDPS also recognises that a medical service at work, as a measure of preventive medicine, can be seen as beneficial for the employer as it helps maintain human resources in better health. It also serves staff members who benefit from a medical service at their disposal.

In order to ensure a correct balance between these two interests, it is important **to intervene as little as possible in the self-determination of each person as regards their health**. In this respect the EDPS recommends as good administrative practice, that the staff member concerned **should be informed of** the outcome of the exam from the examining doctor and **should**

be invited to receive additional information/clarifications from the medical officer if he or she so desires.

As mentioned in the Staff Regulations, the annual medical visit to the Medical service of the institution or body must be optional and the person concerned should also be entitled to have this examination carried out with a medical practitioner of his/her choice. This also implies that any costs resulting from the medical visit to a practitioner of his/her choice should be reimbursed in the same way as if the annual visit had been carried out within the Institution or body.

1.3. Consent based processing

The further processing of medical data collected on the basis of the provisions of the Staff regulations or other legal instruments adopted on the basis of the Treaties for the purpose of ensuring medical follow up, must be examined in light of Article 5(d) of the Regulation according to which the processing must be based on the *"unambiguous consent"* of the data subject.

In terms of Article 2(h) of the Regulation, the data subject's consent is *"any freely given specific and informed indication of his or her wishes by which the data subject signifies his or her agreement to personal data relating to him or her being processed".* It should be also noted that the present case concerns consent in the employment context and therefore, the value of consent of the data subject must be adequately assessed. The EDPS underlines that if there is no possibility for the staff member to refuse his/her consent, this is not a freely given consent. This is supported by the findings of the Article 29 Working Party in its Opinion 8/2001 according to which: "*where consent is required from a worker, and there is a real or potential relevant prejudice that arises from not consenting, the consent is not valid in terms of satisfying either Article 7 or Article 8 [of the Directive 95/46/EC] as it is not freely given. If it is not possible for the worker to refuse, it is not consent. Consent must all times be freely given. Thus a worker must be able to withdraw consent without prejudice*". Moreover the consent must be fully informed and therefore based on information provided in line with Articles 11 and 12 of the Regulation (see point information to the data subject).

The EDPS is of the opinion that the further processing of medical data collected on the basis of the Staff regulation provisions can only be considered as lawful provided that it is based on **an 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 a 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 as much as data are processed upon request of the respective EC staff members, employees of external companies or their family members, the processing is based on consent and Article 5 (d) of the Regulation is also applicable.

1.4. Specific medical check-ups

1.4.1. Medical check to verify absence because of sickness/accident

Article 59 (1) of the Staff Regulations constitute the legal basis for the processing of health data in any medical check during an absence because of sickness or accident: "*An official who provides evidence of being unable to carry out his duties by reason of illness or accident shall be entitled to sick leave.*

...

The official may at any time be required to undergo a medical examination arranged by the institution".

This provision serves as legal basis to justify the performance of a specific medical check up in the event of sickness or absence for sick leave and, if necessary, possibly to evaluate the need to provide for certain accommodations in the workplace in view of the state of health of the person concerned. However, no legal basis would seem to justify the further use of the data collected in the medical report following the specific medical examination for other purposes.

Furthermore, in line with Article 5 of Regulation (EC) 45/2001, it is recommended that **no medical data in the strict sense is contained in the medical examination report** may be sent to Human Resources.

1.4.2. Medical check for specific medical risks

As mentioned above, in some cases national law may serve as legal basis for the processing of health data by Community institutions and bodies. For example, national law may apply to workers exposed to ionising radiation[5] or to certain specialised staff working in crèches or in canteens.

1.5. Visitors/trainees/others

With regard to visitors, trainees, etc and treatment administered to them in medical incidents during visits to institutions, the processing of their health data by the medical service of an institution or body can usually be based on the consent of the data subject (Article 5.d). Should the person not be in a position to give this consent, the processing may be based on the need to protect the vital interests of the data subject (Article 5.e.) if a vital diagnosis is at stake[6].

[5] See for e.g. Council Directive 96/29/EURATOM and Council Directive 90/641/EURATOM, implemented in *Règlement Grand Ducal 14 Decembre 2000 concernant la protection de la population contre les dangers résultants des rayonnements ionisants* which served as legal basis for the processing of personal data in the frame of radiation tests (see Opinion of 5 November 2008 from the European Commission on "Occupational radiation exposure data" (case 2007-383)

[6] Furthermore, most Member States provide that all physicians shall, irrespective of their function or area of specialisation, provide emergency aid to a sick person in immediate danger and so the processing of personal data could be based on a legal obligation.

The EDPS reminds institutions and agencies that the same data protection principles apply to these persons notably as regarding data quality and rights of the data subjects (see below right of access and rectification).

1.6. Medical certificates

Article 59 (1) of the Staff Regulations, provides that: "*An official who provides evidence of being unable to carry out his duties by reason of illness or accident shall be entitled to sick leave... He shall produce a medical certificate if he is absent for more than three days. This certificate must be sent on the fifth day of absence at the latest, as evidenced by the date as postmarked. Failing this, and unless failure to send the certificate is due to reasons beyond his control, the official's absence shall be considered as unauthorised.*"

This provision therefore serves as legal basis according to Article 5.a of Regulation (EC) 45/2001 for the processing of medical or health related information contained in the medical certificate produced by the person concerned. It must be ensured that only relevant data for the purpose of justification of a medical absence or initiation of a control of an absence be requested in such a medical certificate (see below data quality).

1.7. Administrative data

Claims for reimbursement of medical expenses are also processed by Community institutions and bodies notably according to the Joint Insurance Sickness Scheme the purposes of which are defined in Articles 72 and 73 of Staff Regulations. In accordance with Article 5.a and 10.3 of Regulation (EC) 45/2001, these claims contain medical information and should only be processed by the specific department responsible for handling these claims. In no circumstances should any data contained in these claims be communicated to the Human resources unit.

The same is true of medical expenses generated by the annual medical visit to a medical practitioner of the choice of the person concerned (Article 59.6 Staff Regulations). No data indicating the type of exam carried out should be communicated to the budget and payment unit.

In this regard, the EDPS recommends that these claims are sent to the medical service that validates the exams carried out and the costs inferred and forwards to the payment unit only a total cost for reimbursement with no indication of the tests carried out.

2. Processing of special categories of data

Regulation (EC) 45/2001 provides for specific rules for categories of data considered by their nature of infringing fundamental rights and freedoms. According to Article 10 of the Regulation, the processing of personal data concerning health is prohibited unless grounds can be found in Article 10(2) and 10(3).

As it has been explained above, in most cases the justification for processing of health related data is to be found in the EC Staff Regulations or in other national legal obligations in the field of employment. In those cases, the processing operation can be considered as complying with Article 10(2)(b) 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 or, if necessary, insofar as it is agreed upon by the EDPS".*

In most processing operations, as explained above, the processing can be based on the Staff regulations adopted on the basis of the Treaties[7]. As this 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 in so far 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)(c) of the Regulation, as will be explained in the Section discussing "data quality".

The prohibition regarding the processing of data concerning health can also be lifted where the processing is *"necessary for the purpose of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy"* (Article 10(3)). This provision can serve to process data in the frame of providing health services. By virtue of their function, the medical officers and nurses are health professionals subject to the obligation of professional secrecy entitled to process personal data under this capacity.

Finally, Article 10 (2) (a) of the Regulation allows for processing of the health-related data in case *"the data subject has given his express consent to the processing".* As indicated above, this provision is applicable when the data are **provided,** or further processing was **accepted, voluntarily by the data subject**. In any event, the **consent** should be based on information provided in line with Articles 11 and 12 of the Regulation.

3. Data quality

3.1. Adequacy, relevance and proportionality

According to Article 4(1)(c) personal data must be *"adequate, relevant and not excessive in relation to the purposes for which collected and/or further*

[7] As mentioned above (footnote 3), the Civil Service Tribunal interprets a "legal instrument" as any normative act thereby including the Staff Regulations.

processed". This rule implies a necessary link between the data and the purposes for which the data are processed.

3.1.1. Pre-recruitment medical examination

According to the Staff Regulations, the primary purpose of the pre-recruitment medical 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. If the employee is fit for service only subject to certain reasonable accommodations made in the workplace, then this medical check-up may also help determining what accommodations are necessary. The secondary purpose of the pre-recruitment medical check-up as defined in the Staff Regulations 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[8].

Taking into consideration these two purposes, the data quality principle implies that 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**, the EDPS recommends that during the pre-recruitment 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-recruitment medical check-ups.

The medical questionnaire completed by candidates at the medical pre-recruitment examination should not collect inappropriate or excessive data. In this respect, in July 2008 **the EDPS approved in cooperation with the College medical interinstitutionnel a template medical questionnaire for candidates that must be adopted by all institutions and bodies**.

Moreover, in application of the proportionality principle, the EDPS calls into question the practice of **HIV test performed at the pre-recruitment visit**. Indeed, the necessity of this test must be demonstrated in relation to the purpose of the pre-recruitment visit, otherwise the value of the consent can be challenged.

As mentioned above, the EDPS agrees with the Article 29 Working Party, and questions the value of consent in the context of employment when the consequence may be the loss of a job opportunity.

[8] or whether reimbursement of medical cost can be refused as concerns temporary or contract staff (see above).

3.1.2. Medical files

Even though certain standard data will always be present in medical files such as the name, date of birth and personnel number, the precise content of a medical file will of course be variable according to the case.

Guarantees must however be established in order to ensure the respect for the principle of data quality. This could take the **form of a general recommendation to the persons handling the files** reminding them of the rule and recommending that they ensure its respect.

3.1.3. Medical questionnaire of annual visits

Data quality must also be ensured in any medical questionnaire submitted to staff members during the annual medical visits. In most cases, the purpose of this medical check up is preventive. Any information requested must be relevant as concerns this purpose. In some cases, however, the purpose of the regular medical visit is to comply with health and safety regulations (for persons exposed to ionising radiation, for example).

The EDPS recommends an **evaluation** of the data in each questionnaire on medical relevance in the light of the data protection principles.

Data subject may be offered the possibility to perform an HIV test during the annual visit. It must be clearly specified that **this test is not mandatory** and that it is only based on the informed **consent** of the data subject.

3.1.4. Medical check-up performed by a general practitioner

When an official or servant chooses to have the medical examination performed by a practitioner of his/her choice he will receive the list of exams to be carried out from HR and go for the tests and the visit. The practitioner is required to forward the report on the examination and the results of any other examinations carried out.

The principle of data quality implies that only that the institution or body may only process data which are necessary for the purpose for which the data was collected and/or further processed.

The EDPS considers that the preventive purpose of the annual check-up can be served by a declaration by the doctor confirming that the examinations were carried out. If necessary, the declaration could specifically mention the fact that a person needs special accommodations. **The EDPS therefore recommends that results should not be communicated to institutions' medical service without the employees' freely given and informed consent.**

3.2. 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."*

It is not easy to evaluate the accuracy of medical data, especially of subjective data such as notes taken down by a medical officer where the accuracy does not appertain so much to the content of the information, but to the fact that a statement had been made.

Nevertheless, the EDPS is of the opinion that any system should serve to ensure that data are sufficiently complete and kept up to date. The **signing of the medical examination report** allows the data subject to verify the accuracy of the administrative data. The **consent (and signature) of the data subject** as regards information concerning contacts with his attending physician or specialist may also help to ensure that medical data contained in the medical report are complete. **Any other medical opinions submitted by the data subject must also be kept in the medical files**, so as to ensure the completeness of the file.

Furthermore the EDPS insists that in any medical form to be filled in by the person concerned, **no comment or annotation should be added by any third party**. The data controller should ensure that **only authorized persons** have access to the medical files and that **an audit trail is in place to trace back user actions**, especially with regard to the processing of electronic data.

Lastly, the data subject has right of access and right of rectification so as to ensure that the record is as complete as possible (see point right of access and rectification below).

3.3. Fairness and lawfulness

Lastly, personal data must be *"processed fairly and lawfully"* (Article 4(1)(a) of the Regulation). The question of lawfulness has already been considered. As for fairness, it is related to the information to be given to the data subject and to the right of access and rectification granted to data subjects (see below).

4. Conservation period

Article 4(1)(e) provides 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 were collected or for which they are further processed."*

The EDPS provided guidance to the Collège medical interinstitutionnel in this respect[9]:

As a general rule, as concerns conservation of medical data, the EDPS considers that a **period of 30 years** can in most cases be considered as the absolute maximum during which data should be kept in this context.

In **specific cases** the EDPS recognises that a long retention period can be beneficial for the data subject. Conservation periods necessary for specific medical documents should be considered on a case by case basis. In particular, these conservation periods should be determined in relation to the nature of the respective document and the necessity to keep the particular data. For example:

Data related to sick leave: Article 59 (4) of the Staff Regulations could justify a conservation period of 3 years for data necessary to justify an absence due to sick leave. The only justification for keeping them any longer would be if a dispute or appeal were under way.

Specific medical check ups: The storage of accurate data related to the occupational exposure to certain risks (e.g. radiation) has significant relevance in the context of medical treatment of the individual and/or in view of possible claims for alleged occupational diseases, even several years after the end of work.

Non-recruited persons: The medical data of not recruited persons should be kept only for the period of time during which it is possible to challenge the data or the negative decision taken on the basis of the data.[10] This should also apply to candidates who, due to health reasons, are not recognised by the Medical Adviser as being able to perform the tasks.

5. Data transfer

A transfer of health data might take place, first, within or between different Community institutions or bodies (internal), and second, between a Community institution or body and recipients, other than Community institutions and bodies (external). In the latter case it has to be determined whether the recipient is subject to national law adopted pursuant to Directive 95/46/EC.[11]

[9] EDPS Recommendation issued on 26th February 2007 in response to the request of the Collège des Chefs d'administration, Case 2006-532. The issue is still pending with the Collège

[10] id.

[11] For the applicable law see Article 4 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

5.1. Internal transfers

Transfers of data between Community institutions or bodies are in accordance with the Regulation if they are necessary for the *legitimate performance* of tasks covered by the competence of the recipient (Article 7(1)).

Internal transfers of health data take place, for example, when the conclusions of a medical examination carried out in the frame of absence for a medical reason are transmitted to the Human Resources unit. In these cases, it should be noted that, in accordance with the principle of necessity as laid down in Article 7, only the conclusions of the medical exam as to whether or not the absence is justified may be communicated to the Human resources without any medical data. The same is true of the communication of the results of the pre-recruitment medical exam which should only refer to "apt/inapt/apt with reserve".

In the event that a person chooses to carry out his/her medical examination with a doctor of his/her choice and proceeds to send invoices for reimbursement in accordance with Article 59 of the Staff Regulations, as mentioned above, the EDPS recommends that no medical or health information[12] what so ever is transmitted to the administrative budget department.

The EDPS recommends a procedure whereby all medical invoices are first sent to the medical service of an institution or body, who validates them and **only transmits** to the budget department **the total sum to be reimbursed.**

Medical files can also be transmitted internally to other institutional Medical Services in case of transfer of the employee. When a request for transfer of information contained in the medical file is made, the medical service is required to verify the competence of the recipient and to make a provisional evaluation of the necessity of the transfer of data.

If health related data is transferred to third parties other than the Medical Service, compliance with Article 10 (see point 2) must also be ensured. If the data is transferred to comply with labour-law obligations arising from the Staff Regulations, Article 10(2) of the Regulation is fully complied with.

The EDPS recommends that in the context of transfers to other institutions, only **persons authorised** to have access to data relating to health, and who are **subject to professional secrecy**, receive medical files.

The recipient of the medical data shall process the data only for the purposes for which they were transmitted (Article 7(3))

[12] Such information could appear for example, by simple reference to the speciality of the medical practitioner.

In order to ensure compliance with this provision the EDPS recommends that **all recipients** are reminded of their obligation **not to use the data received for any further purpose** than the one for which they were transmitted.

5.2. External transfers

External transfers may take place, for example, if health data is transferred to external doctors appointed by the data subject. A distinction must be made between recipients within and outside the scope of Directive 95/46/EC.

Personal data may only be transferred to recipients who are subject to national law adopted pursuant to Directive 95/46/EC, if the transfer is necessary for the performance of a task carried out in the ***public interest*** or **subject to the exercise of public authority** (Article 8(a)) or if **the recipient established the necessity of having the data transferred** and if there is **no reason to assume** that the **data subject's legitimate interests** might be **prejudiced** (Article 8(b)).

This could be the case for transfers to national authorities in the context of an investigation by a national authority, for example. The necessity of the transfer will however need to be demonstrated. The cooperation with the national authorities must also respect the requisites and mechanisms imposed by national regulations on medical secrecy. Furthermore it must be ensured that only adequate, relevant and not excessive data are transferred.

Should the data be transferred to a medical practitioner at the request of the data subject, this request justifies the necessity of the transfer according to Article 8(b). Furthermore, it does not in principle go against the interests of the data subject.

Personal data may only 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** (Article 9(1)). It is possible to derogate from this principle if the **data subject** has given his/her **unambiguous consent** or if **the transfer is necessary** in order **to protect the vital interests of the data subject**.

6. Right of Access and Rectification

According to Article 13 of the Regulation, the data subject shall have the right to obtain without constraint from the controller, communication in an intelligible form of the data undergoing processing and any available information as to their source. Data subjects cannot be requested to specify the purpose of their request for access. In the case of Medical files, by virtue of Article 26(a) of the Staff Regulations, staff members have the right to acquaint themselves with their medical files, in accordance with arrangements laid down by the institutions.

The EDPS recommends that the institutions in accordance with the data protection requirements should ensure that access requests are dealt with **in a timely fashion and without constraints**. For this reason, it may be considered appropriate for institutions/agencies to establish **reasonable time limits**. Persons concerned should be entitled to receive copies of their medical file if they ask for it.

In this respect the EDPS also calls the attention to the Conclusions 221/04 of 19 February 2004 of the "Collège des Chefs d'administration", which aim at harmonizing certain aspects of access provisions across the Community institutions. This document emphasizes that access must be provided to health 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.

Data subjects should also be granted access to their data in an intelligible form, which may imply, for example, that the medical practitioner must interpret the data (such as medical codes or results of blood analysis) and/or make the data decipherable.

The EDPS would like to underline the fact that the rule as laid down in the Regulation 45/2001 is that data subjects have an access to their personal data. Any restrictions to this right must therefore be strictly limited. The restriction must be based on the protection of the data subject. As for a restriction based on the "rights and freedoms of others", this refers to the fact that the rights and freedoms of an identified third party override the access of the data subject to the information. This should be examined on a case by case basis in the light of the principle of proportionality and precludes a blanket denial of access to personal notes of medical officers contained in the medical files.

The **general rule**, in all cases, whether they concern mental or physical conditions, **remains direct access**. However, *ex* Article 20.1 (c) of the Regulation, the access to data of **psychological or psychiatric nature** can be provided **indirectly**, if an assessment made on a case by case basis reveals that indirect access is necessary for the protection of the data subject, given the circumstances at stake[13].

Non-recruited persons need to be granted access to data processed about their health status. The same applies to **visitors, trainees or other persons** who in the course of their presence in the institution were subject to medical treatment.

[13] Article 20.1 (c) of Regulation (EC) No 45/2001 reads as follows: "*The Community institutions and bodies may restrict the application of Article 4(1), Article 11, Article 12(1), Articles 13 to 17 and Article 37(1) where such restriction constitutes a necessary measure to safeguard: (c) the protection of the data subject or of the rights and freedoms of others."*

Article 14 of the Regulation provides the data subject with a right to rectify inaccurate or incomplete data. This right is somewhat limited as regards certain medical data to the extent that the accuracy or completeness of medical data is difficult to evaluate (see above).

The right of **rectification**, however, may apply to **other types of data** contained in **medical files** (administrative data, for example). Furthermore, the data subject may request that his or her medical file be **complete** – i.e. he or she may request that information such as counter opinions by another doctor are **added** to the medical file.

7. Information to the Data Subject

Article 11 and 12 of the Regulation provide for certain information to be supplied to the data subjects in order to ensure the transparency and fairness of the processing of personal data. Article 11 is applicable if the data have been obtained from the data subject, while Article 12 foresees certain requirements in case the data have not been obtained from the data subject.

In the case of medical data, in general data processed are partly provided by the data subjects and partly by the respective Medical Service staff or external doctors.

7.1. Ways to provide the information

The EDPS recommends, given the character of the data being processed, that the data controller uses adequate means to ensure the data subject *receives* the information.

In particular, in case of medical check ups, the information listed in Articles 11 and 12 of the Regulation may be **personally** given **before the examination** of the patient. For example, this information could be provided in the medical questionnaire and in the invitation to a medical exam, in the medical questionnaire to be filled in the case of absence due to sickness, in the forms for reimbursement of medical claims, etc.

If the information is provided in a privacy statement that is available on the webpage, the **statement** should be **easily accessible**. The EDPS suggests including a link to the privacy statement at the pages that are related to the processing of health data (e.g. if forms available for downloading are provided).

Information can also be given in areas where the processing takes place, e.g. waiting rooms of medical services.

7.2. Information to be given:

In accordance with Articles 11 and 12 the data subjects should be provided with at least the following information:

- Identity of the controller
- The legal basis of the processing operation
- Information about the purpose of the processing
- The categories of data processed[14]
- The recipients of the data
- The existence of right of access and rectification
- The time limits for storing the data
- The right to recourse to the EDPS at any time

In addition, the data subject should be informed if the data provided undergo automated processing. In order to ensure full transparency and fair processing in any case it is recommended to provide the data subject with a contact address where staff members can send questions regarding the privacy statement.

In case of **Medical Check-ups**, the EDPS recommends that employees be informed of their entitlement to **choose the doctor** who will perform their annual medical check-up and of the practical steps they must take to have the check-up carried out by a doctor of their choice. The information ought to encompass the **rules on reimbursement** (including ceilings) and the rules on certifying that the check-up has been performed. In accordance with data protection requirements, it should also be made clear **whether** the medical practitioner will need to **forward any result of the medical examination** to the relevant EU institution or body, and if so, for what purpose.

In case of **Pre-employment Check-ups** it is of crucial importance to inform data subjects about the purpose of the processing of health data since especially recruitment candidates may not be familiar with the provision provided in the Staff Regulations. The EDPS further recommends **informing** the data subject that **disabilities** or other medical conditions **should not act as a bar to candidates**, as long as they are able to perform their duties when reasonable accommodation is made.

In case of **Medical Questionnaires** or as a general rule, if data subjects are asked to answer certain questions as regards their health, they should be informed if the answers are **voluntary or obligatory** and the possible consequences of a failure to reply.

8. Subcontracting

In many cases agencies do not have their own medical service but outsource this to the Commission medical service or to an external service provider. In the latter case, the agency must ensure the respect of Article 23 of the Regulation by the agency and must choose a processor providing sufficient

[14] It would be good practice to provide a detailed list of blood and urine tests and other medical exams carried out.

guarantees in respect of the technical and organisational security measures required.

Furthermore, a contract or other legally binding act must be established according to which the subcontractor must only act upon instruction of the agency. Should the service provider be subject to national law implementing Directive 95/46/EC, he will need to ensure respect of the provisions of national law as regards security and confidentiality.

Most importantly, rules must be established concerning the communication of health data to the agency concerned to the effect that only relevant data may be sent to the institution/body.

9. Security

Due to the sensitive nature of health data, all processing operations deserve careful consideration in the light of data protection principles. In this context the EDPS highlights the need to put in place appropriate security measures in order to effectively prevent data from being altered, lost or accessed by non-authorised persons.

These measures should as a minimum include:

- Definition of a **specific data security policy**, following the overall security policy and/or guidelines of the institution, which would describe a) the assets under protection (i.e. the paper and electronic medical files) and the data processing procedures related to them, b) the roles and responsibilities, as well as respective access rights, of all persons involved in the processing.
- Appointment of a **specific security officer**, which would be responsible for the implementation and review of all relevant organizational and technical measures.
- Use of **codes of conduct or confidentiality declarations** for all persons involved in the processing, who are not bound to secrecy obligation.
- Establishment of appropriate **physical access control** measures in all areas where paper medical files are processed.
- Establishment of appropriate **technical measures** to ensure confidentiality, integrity, accountability and availability of the data when electronic processing systems are in place,
- The inclusion of health related data in the personal files of members of staff may also imply the **division** of these files so as to ensure that only those persons entitled to have access to such data can in fact have access.

For a more detailed description and specific examples of security measures, the EDPS refers to his **Guidelines on security for processing of personal data** [15].

[15] Currently under adoption

Annex: List EDPS prior checking opinions relating to the processing of health data

Opinion of 6 April 2005 on the notification for prior checking relating to procedures regarding the administrative management of medical expenses (Case 2004-305)

Opinion of 17 June 2005 on "Medical Files" at the European Court of Justice, Case 2004-280.
Opinion of 15 November 2005 on a notification for prior checking on "SUIVI: sick leave of translation directorate" of the Court of Justice (Case 2004-279)

Opinion of 28 April 2006 on the transfer of medical files at OHIM, Case 2005-168

Opinion of 29 May 2006 on the notification for prior checking regarding the "Medical files" and "Clinic daybook" at the Council (Cases 2004-254 and 2005-363)

Opinion of 25 July 2006 on a notification for prior checking regarding the "accident record" at the Council (Case 2005-379)

Opinion of 20 October 2006 on "Medical Files kept by the ECB's Medical Adviser" and "Recording of Medical Information in the Personal File" (Case 2006-240/241)

Opinion of 23 March 2007 on the notification for prior checking regarding EFSA's pre-employment and annual medical check-ups (Case 2006-365)

Opinion of 14 June 2007 on "Medical Files-Luxembourg" at the European Parliament Case 2004-203.

Opinion of 14 June 2007 on the notification for prior checking from the Data Protection Officer (DPO) of the European Parliament regarding the "Camed-Brussels" dossier (Case 2004-205)

Opinion of 10 July 2007 on "Management of the Sickness Insurance Scheme" at the European Commission (Case 2004-238)

Opinion of 27 July 2007 on a notification for prior checking regarding the dossier "Asbestosis: screening and follow-up - 'Asbestos' database (Medical service and psychological/social measures BXL)" (Case 2004-227)

Opinion of 27 July 2007 on a notification for prior checking related to Administration of the Accidents and Occupational Disease Insurance (Case 2007-157)

Opinion of 3 August 2007 on a notification for prior checking on the modification of the data processing operations concerning "gestion du temps" and "medical records" (Case 2007-373)

Opinion of 10 September 2007 on the notification for prior checking on the "Management of the activities of the Medical Service in Brussels and Luxembourg, in particular via the SERMED computer application" (Case 2004-232)

Opinion of 13 September 2007 on the notification for prior checking regarding pre-employment and annual medical check-ups at EMCDDA (Case 2007-348)

Opinion of 11 October 2007 on the notification for prior checking regarding the "Checks on absences due to illness - Brussels, Luxembourg" at the European Commission (Case 2004-226)

Opinion of 29 November 2007 on the notification for prior checking regarding the "Invalidity procedure - Medical service in Brussels and Luxembourg" of the European Commission (Case 2007-125)

Opinion of 5 January 2008 on "Occupational Radiation Exposure" (Case 2008-385)

Opinion of 7 January 2008 on a notification for prior checking on recording of the leave of temporary, auxiliary and contract agents, national experts and trainees at the European Medicines Agency (Case 2007-420)

Opinion of 23 January 2008 on a notification for prior checking concerning the Occupational Medicine (MeDeL) at DG JRC (Case 2007-504),

Opinion of 25 January 2008 on "First aid, accidents at work and other medical examinations" at JRC (Joint Research Centre) in Ispra (Case 2007-372),

Opinion of 6 February 2008 on a notification for prior checking on individual medical files at Joint Research centre in Ispra and Seville (Case 2007-329),

Opinion of 6 February 2008 on the notification for prior checking regarding the "checks on absences from work due to illness or accident - Directorate-General Joint Research Centre Ispra and Seville" dossier (Case 2007-508)

Opinion of 4 March 2008 on a notification for prior checking concerning "CAME - management of absences due to illness" (Case 2007-688)

Opinion of 4 June 2008 on the notification for prior checking regarding CPVO's pre-employment and annual medical check-ups (Case 2007-176)

Opinion of 3 September 2008 on a notification for prior checking on "Dosimetry management system of radiological workers at JRC-IE in Petten" (Case 2008-020)

Opinion of 16 September 2008 on partial subcontracting of medical insurance scheme at the EIB (Case 2008-323)

Opinion of 5 November 2008 on the notification for prior checking regarding occupational radiation exposure data at the Commission (Case 2007-385)

Opinion of 11 November 2008 on the procedure in the event of absence due to sickness or accident at the Council (Cases 2008-271 and 2008-283)

Opinion of 18 November 2008 on the notification for prior checking regarding individual medical files at the European Commission Brussels- Luxemburg (Case 2004-225)