Opinion on the notification for prior checking from the Data Protection Officer of the GSC of the European Union concerning "Data processing with regard to accident insurance"

Brussels, 14 September 2009 (Case 2004-0257)

1. Proceedings

Notification within the meaning of Article 27(3) of Regulation No 45/2001 concerning the *"Data processing with regard to accident insurance"* case was given by the Data Protection Officer (hereinafter referred to as the "DPO") of the General Secretariat of the Council of the European Union (hereinafter referred to as "the GSC") by letter dated 19 April 2007.

In connection with this notification, questions were put to the DPO of the GSC by e-mail on 11 May 2007 and a reminder and a description of the facts were sent on 26 May 2008. Replies were received on 18 December 2008. On 20 January 2009 the draft opinion was sent to the DPO of the GSC for comments. Comments were not provided until 21 August 2009 owing to the major reorganisation recently undergone by the Accident Insurance Department, as pointed out by the data processing controller.

2. Facts

This case concerns processing by the Accident Insurance Department of the GSC.

Data subjects

Data subjects are officials, temporary staff, contract staff, seconded national experts and trainees of the GSC.

Purpose

The purpose of processing is to reimburse data subjects in the event of an accident or occupational disease.

Legal basis

The legal basis is Article 73 of the Staff Regulations of the European Communities (hereinafter "the Staff Regulations"), Article 28 of the Conditions of Employment of Other Servants of the European Communities (hereinafter "the CEOS") and the common rules on the insurance of officials of the European Communities against the risk of accident and of occupational disease which came into force on 1 January 2006 (hereinafter "the common rules on accident and occupational disease insurance"). Seconded national experts are covered by Article 9 of Decision (EC) 2003/479 and trainees by Article 13 of Decision (EC) 94/04.

Under Article 18 of the common rules on accident and occupational disease insurance, decisions recognising the accidental cause of an occurrence, and decisions linked thereto,

recognising the occupational nature of a disease are taken by the appointing authority. Before taking a decision, the appointing authority notifies the data subject, or those entitled under him/her, of the draft decision and of the findings of the doctor appointed by the appointing authority. Within a period of sixty days, the data subject may request that the Medical Committee[1] deliver its opinion.

In addition, an insurance company is contracted with the GSC on the basis of a service contract concluded between the European Community, represented by the Commission, on behalf of the GSC and all the institutions, and the insurance company. This service contract applies in all European Union institutions.[2] Article 8.1 of the contract, entitled *"Data protection"*, provides that *"the personal data referred to in the contract shall be processed in accordance with Regulation (EC) No 45/2001 ... they may only be processed for the purposes of the performance, administration and monitoring of the contract by an entity appointed as data processing controller, without prejudice to their possible transmission to bodies charged with auditing or inspection functions under Community law. The policyholder has a right of access to and right to rectification in respect of personal data relating to him/her. For any question concerning these data, the policyholder shall contact the entity appointed as data processing controller. The policyholder has the right to have recourse at any time to the European Data Protection Supervisor."* Article II.9.1, concerning confidentiality, also provides that the insurance company *"shall undertake to treat as strictly confidential all information and documents relating to the performance of the contract and not to make use of them or disclose them to third parties. The contractor shall continue to be bound by this undertaking after the tasks have been completed."*

For the external doctor appointed by the appointing authority under Article 73 of the Staff Regulations and the Common Rules, a mandate is signed by the Director-General for Administration and sent to a doctor residing in Belgium. The mandate states that the complete files for the persons to be examined will be forwarded to the external doctor one week before the date of the meeting called by the insurance company. As soon as the external doctor has all the necessary information and the results of any additional examinations, he must draft his expert report. The original must be send to the GSC's Accident Insurance Department and copied to the insurance company.

Proceedings

Under the procedure and the provisions of the common rules on accident and occupational disease insurance, the person involved in the accident or those entitled under him/her must make an accident report and send it to the Accident Insurance Department together with a medical certificate filled in by the doctor who provided the first treatment. The accident report must state particulars of the date and time, the causes and the circumstances of the accident and also the names of witnesses and of any third party which may be liable. The medical certificate must specify the nature of the injuries and the probable consequences of the accident. The original and one copy of the duly completed and signed accident report and the medical certificate must be submitted to the Accident Insurance Department within ten working days of the date on which the accident occurred.

Data collected on the accident report form

---

[1] Article 22 of the common rules on accident and occupational disease insurance provides that the Medical Committee will consist of three doctors: one appointed by the insured party or those entitled under him/her, one appointed by the appointing authority and one appointed by agreement between the first two doctors.

[2] Article I.1.1. of the contract stipulates that *"the object of the contract is insurance against the risks of accident, occupational disease and death from natural causes for officials, temporary staff and contract staff of the institutions of the European Union"*.

The data collected on the accident report form are as follows: surname and forename of the data subject (maiden name and husband's name for married women), personal number, office address and telephone number, private address, date of birth, grade, date and time of the accident, exact place, detailed circumstances, questions relating to the accident (whether it occurred during the performance of duties or during leave on personal grounds), whether there was intervention by an authority and, if so, the name of the authority and the number of any report, whether the accident resulted in incapacity for work and whether a third party was responsible (in that case, the name and address of the third party are required, the name and address of his/her insurance company, the number of his/her insurance policy, the name and address of the injured party's insurance company and the number of his/her insurance policy).

Data collected on the medical certificate

The data collected on the medical certificate are as follows: name and address of the doctor, name and address of the data subject, date of the accident, date of first treatment, description of injuries, details of previous illnesses or disabilities which have aggravated the injuries resulting from the accident, incapacity for work resulting from the accident (percentage of incapacity and estimated duration), nature of treatment, results of any X-ray carried out, whether or not hospitalisation is necessary, probable date of recovery, percentage of permanent incapacity and comments made by the doctor.

Where the data supplied by the data subject are illegible, the ASSMAL system (reimbursement of medical expenses under Article 72 of the Staff Regulations) and the GPWIN and SAP systems (used for additional reimbursement of medical expenses to accident victims) are consulted in order to check the data supplied by the data subject.

Processing involves manual entry of declarations and medical certificates sent by the data subject to the Accident Insurance Department and all medical reports relating to them and of medical expense calculations established by that department. The two officials in the department use the usual word-processing programmes, Word and Excel.

Under Article 24 of the common rules on accident and occupational disease, staff administering accident files are required *"to observe confidentiality regarding medical documents and/or expenses which come to their attention in the course of the performance of their tasks. They shall continue to be subject to this obligation after their duties have ceased under these rules."*

Recipients

The data recipients for the purposes of the processing operation are as follows:

- the external doctor appointed by the appointing authority, who receives the data subject's file in order to issue an expert report;
- the insurance company contracted with the GSC receives the accident report, the medical certificates, the medical reports and the calculation of medical expenses for additional reimbursement under Article 73 of the Staff Regulations;
- the Medical Committee provided for in Article 22 of the common rules on accident and occupational disease insurance is a possible recipient, if the data subject so requests.

Rights of access, rectification, blocking, erasure:

As regards the right of access and rectification, data subjects may, at their request, consult the whole of the accident file relating to them in the department's office. Moreover, a staff note relating to processing refers to Section 5 of the Council Decision 2004/644/EC of 13 September 2004, entitled *"Procedure for data subjects to exercise their rights"*, and

particularly to Articles 13, 14, 15 and 16 which set out the procedures for ensuring rights of access, rectification, blocking and erasure.

Right to information
The notification refers to Staff Note No 219/05 on the procedure under the new rules on insurance against accident and occupational disease which was circulated to staff by the data processing controller on 20 December 2005.

Data storage
Data are retained throughout the lifetime of the data subject in case he/she submits an application for the file to be re-opened because his/her condition has become aggravated, as the data subject is entitled to do under Article 21 of the common rules on accident and occupational disease insurance. Each accident file contains the accident report together with the medical certificate and all the correspondence exchanged.

The data are not stored for historical, statistical or scientific purposes.

Storage and security measures
Access to the Accident Insurance Department's offices and archives requires the use of a magnetic card and a code. Accident files in them are stored in locked cupboards. Staff members' computers can be used only with a personal code.

3. Legal aspects

3.1 Prior checking

Regulation (EC) No 45/2001 applies to the processing of personal data by all Community institutions and bodies insofar as such processing is carried out in the exercise of activities all or part of which fall within the scope of Community law (Article 3(1)). In the case in point, the data processing is carried out by the GSC in the exercise of activities which fall within the scope of Community law.

Data are compiled on paper, particularly the accident reports, the medical certificates and all the relevant reports, using Word and Excel. The data are therefore subject to manual processing intended to form part of a filing system. Article 3(2) is thus applicable in this case.

Accordingly, the processing falls within the scope of Regulation (EC) No 45/2001.

Article 27(1) of Regulation (EC) No 45/2001 requires prior checking by the EDPS of all *"processing operations likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes"*. The list of operations that are likely to present such risks which appears in Article 27(2) includes the *"processing of data relating to health"* (Article 27(2)(a)). In this instance, data relating to health are processed because medical expenses in the event of an accident or occupational disease can only be reimbursed on production of medical certificates and expert reports. This processing operation therefore falls within the scope of the prior checking procedure based on Article 27(2)(a) of the Regulation.

In principle, checking by the EDPS should be performed before the processing operation is implemented. In this case, as the EDPS was appointed after the system was set up, the check necessarily has to be performed ex post. This does not make it any the less desirable that the recommendations issued by the EDPS be implemented.

The formal notification was received on 19 April 2007. In accordance with Article 27(4) of the Regulation, the two-month time limit within which the EDPS must deliver an opinion was suspended. Taking into account the 717 days of suspension, the EDPS will deliver his opinion by 14 September 2009 (494 days of suspension + 3 months of August + 192 days for comments).

3.2 Lawfulness of processing

Article 5 of Regulation (EC) No 45/2001 provides that personal data may only be processed if at least one of its five conditions are met.

The processing operation under examination meets the condition in Article 5(a) of the Regulation, in accordance with which personal data may be processed if *"processing is necessary for the performance of a task carried out in the public interest on the basis of the Treaties establishing the European Communities [….] or in the legitimate exercise of official authority vested in the Community institution"*.

Two matters have to be considered in relation to this condition: firstly, whether the processing operation is provided for under the Treaties establishing the European Communities or other legal instruments and, secondly, whether the processing is necessary in the public interest (the necessity test).

The **legal basis** for this processing operation is to be found in Article 73 of the Staff Regulations, Article 28 of the CEOS, and the common rules on accident and occupational disease insurance. Seconded national experts are covered by Article 9 of Decision (EC) 2003/479 and trainees by Article 13 of Decision (EC) 94/04.

The **necessity** for the processing operation is also covered by recital 27 of the Regulation, which states that *"processing of personal data for the performance of tasks carried out in the public interest by the Community institutions and bodies includes the processing of personal data necessary for the management and functioning of those institutions and bodies"*. In the case in point, the processing operation is necessary for the management and proper functioning of the GSC. More specifically, the EDPS considers the tasks performed by the GSC's Accident Insurance Department to be in the public interest in the field of employment law in compliance with the provisions of Article 73 of the Staff Regulations. To that end, appropriate measures have been adopted to ensure that the medical costs of an official's or staff member's accident or occupational disease are covered by an insurance company.

The processing operation proposed is therefore lawful.

Moreover, data relating to health are among the data which Article 10 of Regulation (EC) No 45/2001 classes as *"special categories of data"*.

3.3 Processing of special categories of data

Under Article 10(1) of Regulation (EC) No 45/2001, the processing of personal data concerning health is prohibited unless grounds can be found in Article 10(2) and (3) of that Regulation.

The collection of medical certificates and other expert reports in this case is necessary in the context of the specific rights and obligations of the GSC in the field of employment law and is therefore justified under Articles 76 and 76a of the Staff Regulations. Processing of such data therefore complies with Article 10(2)(b) of the Regulation, which states that the prohibition

on processing data concerning health does not apply where *"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"*.

Under the procedure, the medical certificates accompanying accident reports and other medical reports are supplied by the data subjects to the Accident Insurance Department. The original of the expert report by the doctor appointed by the appointing authority must also be forwarded to the Accident Insurance Department. The documents comprise data relating to health since they state the data subject's name, the doctor's specialisation, the type of treatment, whether or not an X-ray was carried out and the result, whether or not hospitalisation is necessary, the percentage of incapacity for work, etc. The EDPS considers that insofar as Article 24 of the common rules on accident and occupational disease insurance is applicable, Article 10(3) is complied with.

3.4 The controller and the processor

Pursuant to Article 2(d) of the Regulation, the controller is *"the Community institution or body, the Directorate-General, the unit or any other organisational entity which alone or jointly with others determines the purposes and means of the processing of personal data"*. The controller is responsible for ensuring that the obligations laid down in the Regulation are met (information to be given to the data subject, ensuring the rights of the data subject, choice of processor, notification of the data protection officer, etc.). The processor is the *"natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller"* (Article 2(e)).

In this case, the GSC is contracted with the insurance company via a service contract. The GSC is also bound by a mandate issued to an external doctor appointed by the appointing authority.

The GSC is considered to be the controller since it determines the purposes and means of collecting data relating to the data subjects in accordance with Article 8(1) of the service contract. The insurance company is a processor, since - on the basis of the service contract concluded – it processes the data subjects' medical data collected on behalf of the GSC i.e. it determines the amounts to be reimbursed on the basis of medical reports, insofar as the collection and subsequent processing of the data are necessary to comply with the GSC's specific obligations and rights in the field of employment law as laid down in Article 10(2)(b) of the Regulation.

The external doctor is also considered as a processor, since he processes medical data on behalf of the GSC in that he draws up an expert report and sends it both to the Accident Insurance Department and to the insurance company so that the amounts to be reimbursed can be estimated by the insurance company.

The roles of the controller and the processor therefore comply with Article 2(d) and Article 2(e) of the Regulation respectively.

3.5 Data quality

In accordance with Article 4(1)(c) of Regulation (EC) No 45/2001, personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.

Even though GSC data subjects' files will always contain certain standard data, such as administrative data relating to the data subject, the precise content of a file relating to health will obviously vary according to the case. However, there must be some guarantee that the principle of data quality is complied with. This could take the form of a general recommendation to the persons handling the files asking them to ensure that this rule is observed.

The administrative and medical data collected by the Accident Insurance Department as described in point 2 appear to be relevant and not excessive in relation to the purposes for which they are collected.

The data transmitted to the insurance company are the accident report accompanied by the medical certificate, the medical reports, including the expert report and the calculation of reimbursement of medical expenses. These data, both administrative and medical, would seem to be required to enable the insurance company to exercise all the rights and obligations deriving from the contract. The common principles of the law of contract which can be derived from general European practice include the right for the insurance company to obtain sufficient information about the accident or occupational disease to be able to exercise all the rights and actions provided for in the contract. This follows from the principle of the appropriate defence of one's rights. Moreover, in this case, it is important that all elements relating to an accident or occupational disease be taken into consideration so that the insurance company's reports are as full and as precise as possible.

The EDPS therefore considers that Article 4(1)(c) of the Regulation is complied with.

Moreover, the data must be *"processed fairly and lawfully"* (Article 4(1)(a)). The lawfulness of the processing operation has already been discussed in point 2 of this opinion. As for fairness, this relates to the information which must be transmitted to the data subject (see point 3.11 below).

Article 4(1)(d) of the Regulation stipulates that data must be *"accurate and, where necessary, kept up to date"*. Furthermore, under that Article, *"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"*. The data in question in this case are, on the one hand, administrative data (data relating to the private sphere) and, on the other hand, medical data, As regards medical data, it is not easy to ensure, or assess, their accuracy. Nonetheless, the EDPS would emphasise that every reasonable step must be taken to ensure that data are up-to-date and relevant. Data subjects' right to access and rectify their data is a second means of ensuring that their data are accurate and up-to-date (see point 3.10 on the right of access).

3.6 Data retention

The general principle set out in Regulation No 45/2001 is that 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"* (Article 4(1)(e) of the Regulation).

As stated earlier, data are retained throughout the lifetime of the data subject in case he/she submits an application for the file to be re-opened because his/her condition has become aggravated, as the data subject is entitled to do under Article 21 of the common rules on

accident and occupational disease insurance. Each accident file contains the accident report together with the medical certificate and all the correspondence exchanged.

The EDPS considers that the period for which data are retained in this case, that is throughout the data subject's career or longer, is justified under Article 73 of the Staff Regulations, depending on the nature of the accident or occupational disease. It is also explicitly stated in Article 21 of the common rules on accident and occupational disease insurance that, with regard to aggravation and cases which have been terminated, insured parties may at any time apply for the case to be re-opened.

It should be emphasised that in the case of medical reports relating to occupational diseases, the possibility of data being stored for more than 30 years was raised in a note from the Board of Heads of Administration on 4 October 2006 concerning time-limits for storing data. In his opinion on the conservation of medical documents, the EDPS emphasised that the conservation for more than 30 years of medical documents acquired under Article 73 of the Staff Regulations was to be regarded as justified[3].

It is also important to note that data retention for such a long period must be accompanied by appropriate guarantees. As for all sensitive data, appropriate arrangements need to be made for their transmission and storage.

3.7 Change of purpose/compatible use

In this instance, the ASSMAL, GPWIN and SAP databases are sometimes consulted to check the data supplied by the data subject. The processing operation under consideration does not entail a general change in the intended purpose of the databases and is not incompatible with that purpose, since those databases are tools used by the staff of the GSC. Accordingly, Article 6(1) of the Regulation does not apply in this instance and the conditions of Article 4(1)(b) of the Regulation are fulfilled.

3.8 Transfer of data

The processing operation should also be scrutinised in the light of Article 7(1) of the Regulation. The processing covered by Article 7(1) is the transfer of personal data between or within Community institutions or bodies *"if the data are necessary for the legitimate performance of tasks covered by the competence of the recipient"*.

To comply with Article 7(1), the GSC must ensure that all the recipients have the appropriate competence and that the transfer is necessary. Here a transfer takes place within the GSC itself, to the Medical Committee. The recipient has a specific competence and the data transferred to the Committee are necessary for the legitimate performance of the tasks falling within its competence. The EDPS therefore considers the transfer acceptable under Article 7(1) of the Regulation.

Moreover, Article 7(3) of the Regulation provides that *"the recipient shall process the personal data only for the purposes for which they were transmitted"*. In this instance, it is specifically stipulated in Article 24 of the common rules on accident and occupational disease that staff administering accident files are required to observe confidentiality regarding medical documents and continue to be subject to this obligation after their duties have ceased

[3] Opinion of the EDPS of 26 February 2007 on conservation periods for medical documents.

under those rules. The EDPS considers that, provided that this provision is applied in practice, Article 7(3) of the Regulation is complied with.

Since the external doctor appointed by the appointing authority and the insurance company designated by the appointing authority are external to the institution and are governed by Belgian law, they are recipients subject to national law, i.e. the Belgian law adopted for the implementation of Directive 95/46/EC. The data transfers in the processing operation will therefore be scrutinised under Article 8 of Regulation (EC) No 45/2001. The transfer is covered by Article 8(b), which stipulates that data may be transferred if *"the recipient establishes 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"*. The necessity of transferring the data to the two recipients (the external doctor and the insurance company) is justified, respectively, by the service contract and the mandate by which the SGC is bound. Since the principle of data quality is complied with (see the analysis in point 3.5), the transfer will not prejudice the legitimate interests of data subjects (see point 3.12 for security measures).

3.9 Processing including the personal or identifying number

Article 10(6) of Regulation (EC) No 45/2001 states that *"the European Data Protection Supervisor shall determine the conditions under which a personal number or other identifier of general application may be processed by a Community institution or body."*

The data subject's personal number may be collected in connection with the administration of accident and occupational disease insurance The EDPS considers that the personal number can be used in this context since it allows identification of the data subject and facilitates the follow-up in an appropriate way. There is no reason to set other conditions in this instance.

3.10 Right of access and rectification

Article 13 of Regulation (EC) No 45/2001 establishes a right of access – and the arrangements for exercising it – upon request by the data subject. Under Article 13 of the Regulation, the data subject has the right to obtain from the controller, without constraint, communication in an intelligible form of the data undergoing processing and any available information as to their source.

Article 14 of Regulation (EC) No 45/2001 allows the data subject the right of rectification. In addition to being given access to their personal data, data subjects may also have the data amended if necessary.

For the record, data subjects may, at their request, consult the whole of the accident file relating to them in the Accident Insurance Department's office. Under Article 21 of the common rules on accident and occupational disease insurance, they may also submit an application for the file to be re-opened because of an aggravation of their condition. Moreover, a staff note relating to processing refers to Section 5 of the Council Decision of 13 September 2004 and particularly to Articles 13, 14, 15 and 16 which set out the procedures for ensuring rights of access, rectification, blocking and erasure.

The EDPS is consequently pleased to note that the obligations laid down in Articles 13 and 14 of Regulation (EC) No 45/2001 are being complied with.

3.11 Information to the data subject

Articles 11 and 12 of Regulation (EC) No 45/2001 relate to the information to be given to data subjects in order to ensure transparency in the processing of personal data. These articles list a series of compulsory and optional items of information. The optional items are applicable insofar as, having regard to the specific circumstances of the processing operation, they are required in order to guarantee fair processing in respect of the data subject. In the present case, some of the data are collected directly from the data subject and some from other persons.

The provisions of Article 11 (*Information to be supplied where the data have been obtained from the data subject*) on information to be provided to the data subject apply in this case insofar as data subjects themselves supply the accident report and medical certificate for the purposes of reimbursement.

The provisions of Article 12 (*Information to be supplied where the data have not been obtained from the data subject*) on information to be provided to the data subject also apply in this case, since data are collected by the external doctor and the insurers and possibly via the ASSMAL, GPWIN and SAP databases.

For the record, the notification refers to Staff Note No 219/05 on the procedure under the common rules on accident and occupational disease insurance. However, neither that staff note nor any other document contains the information set out in Articles 11 and 12 of Regulation (EC) No 45/2001.

The EDPS therefore recommends that all the information set out in Articles 11 and 12 of Regulation (EC) No 45/2001 be the subject of an internal note for forthcoming communications on processing to be sent to the data subjects.

3.12 Processing by a processor

Where a processing operation is carried out on its behalf, Article 23 of Regulation (EC) No 45/2001 stipulates that the controller must choose a processor providing sufficient guarantees in respect of the technical and organisational security measures required by the Regulation. The carrying out of an operation by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that the processor shall act only on instructions from the controller and that the confidentiality and security obligations with regard to the processing of personal data shall also be incumbent on the processor.

For the record, it should be pointed out that the service contract concluded by the Commission, on behalf of the GSC and all the institutions, and the insurance company, includes provisions concerning data protection (Article I.8) and confidentiality (Article II.9). However, Article I.8 is confined only to data *"referred to in the contract"*, which is not sufficient as regards data transferred as a consequence of the performance of the contract. Article II.9 is also inadequate since there is no reference to security measures within the meaning of Article 23(2)(b) of the Regulation. The EDPS therefore considers that the provision on data protection (Article I.8 of the contract) needs to be reworded to include a reference to the data transferred and processed as part of the processing operation in question. Article II.9 of the service contract also needs to be supplemented by a reference to the level of security adopted within the meaning of Article 23(2)(b) of the Regulation. It is necessary, in

particular, that it be subject to the obligations in respect of security laid down in Belgian legislation pursuant to the second indent of Article 17(3) of Directive 95/46/EC.

Nor does the GSC mandate to the external doctor designated by the appointing authority make provision for security measures. While the obligation laid down in Article 23(2)(b) of the Regulation may already be covered by the rules on medical ethics, it is nevertheless an explicit legal requirement in the context of the protection of personal data. The EDPS therefore recommends that the external doctor as processor be subject to a security obligation under Belgian legislation as provided for in Article 23(2)(b) of Regulation No 45/2001 (see above).

3.13 Security measures

In accordance with Article 22 of Regulation (EC) No 45/2001 on the security of processing, the controller is to *"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"*.

With regard to the information communicated, the EDPS has no reason to believe that the security measures adopted by the GSC do not comply with the provisions of Article 22 of the Regulation.

Conclusion:

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

- establish guarantees to ensure that the principle of data quality is complied with in respect of all data relating to health. This could take the form of a general recommendation to the persons handling the files asking them to ensure that this rule is observed;

- ensure that all data relating to health are kept up to date by those administering them in the Accident Insurance Department;

- ensure that long-term data retention is accompanied by appropriate guarantees. In cases where certain occupational disease files are kept for historical purposes, the data must be rendered anonymous;
- prepare an internal note containing all the information set out in Articles 11 and 12 of Regulation (EC) No 45/2001 and send it to the data subjects in forthcoming communications on processing;

- ensure that the provision concerning data protection (Article I.8 of the service contract) is reworded to refer to data transferred and processed in the course of the processing operation in question. It is also essential that both Article II.9 of the contract and the mandate be supplemented with a reference to the level of security laid down in Belgian legislation.

Done at Brussels, 14 September 2009

(Signed)

Giovanni BUTTARELLI
Assistant European Data Protection Supervisor