Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Commission on "AGS-EDV Database at JRC-ITU in Karlsruhe"

Brussels, 10 January 2008 (Case 2007-378)

1. Procedure

On 5 June 2007, the European Data Protection Supervisor (**EDPS**) received from the Data Protection Officer (**DPO**) of the European Commission a notification for prior checking concerning "the AGS-EDV Database" at Joint Research Centre (**JRC**) - Institute for Transuranium Elements (**ITU**) in Karlsruhe. The notification was accompanied by the following documents:

- *Gesetz über die friedliche Verwendung der Kernenergie und den Schutz gegen ihre Gefahren (Atomgesetz)* - Atom Act of 15 July 1985 (**AtomG**);
- *Verordnung über den Schutz vor Schäden durch ionisierende Strahlen (Strahlenschutzverordnung)* - Ionising Radiation Protection Regulation of 20 July 2001 (**StrlSchV**);
- Privacy Statement.

On 11 July 2007, the EDPS sent a request for additional information to the Commission's DPO. A partial reply was provided on 8 November 2007. A second information request together with the draft facts was sent to the Commission's DPO on 16 November 2007. The reply provided on 26 November was accompanied by the following documents:

- *Einbeziehung des ITU in die Sicherheitsorganisation des Kernforschungszentrums Karlsruhe* - Incorporation of the ITU in the Security Organisation of the Nuclear Research Centre in Karlsruhe (**FZK**) dated of 25 October 1967;
- *Neuregelung für die Personendosimetrie durch Verlagerung der Geschäftsbereiche von FZK auf das Forschunszentrum für Umwelt und Gesundheit* - New Regulation of Personal Dosimetry related to the transfer of competences from the FZK to the Research Centre for Environment and Health (**GSF**) dated of 29 September 2005;
- *Allgemeine Verwaltungsvorschrift zu §40 (2), §95 (3) StrlSchV und §35 (2) der Röntgenverordung* - Administrative Regulation on Radiation Passbook of 20 July 2004 (**AVV StrlPass**).

The draft opinion was sent to the Commission's DPO for comments on 19 December 2007 and these were received on 8 January 2008.

2. Facts

2.1. Context

The present notification concerns the dosimetry management at the ITU in Karlsruhe. It covers activities from the handling of personal radiation exposure data coming from internal

and external dosimetry measurements to the management of the AGS[1]-EDV[2] database. These data are being handled by the "radioprotection service" located in the "Nuclear Safety" Unit E7 of the ITU as supported by the "security service" (surveillance personnel collecting the operational pen dosimeters etc.).

The purpose of this data processing is to meet the legal requirements of the radiation protection legislation concerning (external and internal) workers and visitors accessing controlled areas.

The controller of this data processing is the Head of the Unit E7 "Nuclear Safety / Health and Radiation Monitoring Section of the ITU in Karlsruhe.

Processors: The processing of the actual dosimetry data on behalf of the controller is carried out by two external research centres established in Germany. The GSF (Research Centre for Environment and Health) is in charge of reading the official dosimeter values (external dosimetry), whereas the FZK (Research Centre Karlsruhe) is in charge of conducting incorporation measurements (internal dosimetry).

2.2. Legal requirements in the area of ionising radiation

The legal requirements in the area of protection against the dangers arising from ionising radiation are laid down in Directive 96/29/Euratom[3] and Directive 90/641/Euratom[4] (external workers) as implemented into the German Ionising Radiation Protection Regulation (StrlSchV).

Individual monitoring: For exposed category A workers[5], there should be a systematic individual monitoring based on individual measurements established by an approved dosimetric device (Article 25 (1) of the Directive 96/29, Article 6 (d) of the Directive 90/641 - §§ 40, 41, 42, 54, 55, 56, 57, 58, 59 StrlSchV).

Monitoring for category B workers shall be at least sufficient to demonstrate that such workers are correctly classified in category B; individual monitoring may be required (Article 25 (2) of the Directive 96/29 - §§ 40, 41, 42, 54 StrlSchV).

The operational protection of apprentices and students aged 18 years and over shall be equivalent to that of exposed workers of category A or B as appropriate. The operational protection of apprentices and students between 16 and 18 years shall be equivalent to that of exposed workers of category B (Article 39 of the Directive 96/29 - §§ 40, 41, 42, 45, 55 StrlSchV).

Accidental and emergency exposure: In the case of accidental exposure, the relevant doses and their distribution to the body shall be assessed (Article 26 of the Directive 96/29 - § 57 StrlSchV). In the case of emergency exposure, individual monitoring or assessment of the

---

1 *Abteilung für Gesundheit und Strahlenüberwachung* - Health and Radiation Monitoring Section

2 *Elektronische Datenverarbeitung* - Electronic Data Processing

3 Council Directive 96/29/Euroatom of 13 May 1996 laying down basis safety standards for the protection of the health of workers and the general public against the dangers arising from ionising radiation

4 Council Directive 90/641/Euroatom of 4 December 1990 on the operational protection of outside workers exposed to the risks of ionising radiation during their activities in controlled areas

5 Exposed workers who are liable to receive an effective dose greater than 6 mSv per year or an equivalent dose greater than 3/10 of the dose limits for the lens of the eye, skin and hands, forearms, feet and ankles in terms of Article 21 (a) of the Directive 96/29 / § 54 (1.) StrlSchV

individual doses shall be carried out as appropriate to the circumstances (Article 27 of the Directive 96/29 - §§ 58, 59 StrlSchV).

Recording and reporting of results: A record containing the results of the individual monitoring shall be made for each exposed category A worker. It shall be retained during the working life involving exposure to ionising radiation of exposed workers, and afterwards until the individual has or would have attained the age of 75 years, but in any case not less than 30 years from the termination of the work involving exposure (Article 28 of the Directive 96/29, Article 6 (f) of the Directive 90/641 - § 12c AtomG / §§ 42 (1), 112 StrlSchV).

The results of individual monitoring shall be made available to the competent authorities, to the undertaking, to the worker concerned and to the approved medical practitioner or approved occupational health services in order to interpret their implications for human health as provided in Article 31. In the case of an accidental or emergency exposure, the results of the individual monitoring shall be submitted without delay (Article 29 of the Directive 96/29 - §§ 41, 42, 57 StrlSchV).

All doses relating to specially authorised exposures of category A workers shall be separately recorded in the medical record referred to in Article 34 and the individual record referred to in Article 28 (Article 12 (1) (e) of the Directive 96/29 - §§ 42, 60, 61, 62, 63, 64 StrlSchV).

Upon request, workers shall have access to the results of their individual monitoring (Article 38 (2) of the Directive 90/29 - §§ 40, 42 StrlSchV).

Information and training: The exposed workers, apprentices and students shall be informed on the health risks involved in their work, i.e. the general radiation protection procedures and precautions to be taken, as well as the importance of complying with the technical, medical and administrative requirements. They shall also be given a training in the field of radiation protection (Article 22 (1) (a) and (2) of the Directive 96/29, Article 6 (b) Directive 90/641 - §§ 38, 9 (1) 4. StrlSchV).

Visitors: The competent authority can request that visitors present in the controlled areas are subjected to a dosimetric measurement (§ 40 (5) StrlSchV).

2.3. Description of the processing

Radioprotection information session: Each professionally exposed person must follow a compulsory radiation protection information session which is given by a member of the radioprotection service. During this course, the person has to provide some personal data which are collected on a paper form. On this form also appear different parameters which are given by the member of the radioprotection service (see data listed below in point 2.5).

External dosimetry: Workers professionally exposed to ionising radiation at the ITU must wear a dosimeter. Every month, the dosimeters are sent to the GSF who has to determine and record the personal dose, as well as report it to the employer. Upon request, the GSF has to provide the measurement results to the competent authorities. In case of an overexposure, the GSF has to inform the competent authorities, as well as the person concerned without delay.

Internal dosimetry: The incorporation measurements (whole body counting etc.) are carried out by the FZK who has to record and report it to the employer. Upon request, the FZK has to provide the measurement results to the competent authorities. In case of an overexposure, the FZK has to inform the competent authorities, as well as the person concerned without delay.

Radiation passbook: In addition, the external workers working at ITU must be in possession of a radiation passbook (§ 40 (3) StrlSchV).

AGS-EDV Database: The AGS-EDV[6] database consists of records of persons who work in controlled areas of the ITU Karlsruhe. It is set to detect persons who are **exceeding** predefined dose limits and therefore, reports with the names of the persons are produced automatically in order to inform as quickly as possible and to maintain doses as low as possible.

In addition, periodical reports are produced in order to inform responsible and authorised bodies in the different companies and supervisory authorities about the received doses.

Any kind of report can be made manually after authorisation of access to the database, that is if necessary.

Furthermore, the following reports are produced every month:
- list of persons wearing dosimeters;
- list of decreasing doses in order to identify the highest exposition;
- collective doses for the institute;
- production of statistical graphs showing how doses are received over a period of time;
- detailed reports on demand (exposed persons, hierarchy or medical service).

2.4. Data subjects

Data subjects are those individuals who are occupationally exposed to ionising radiations (members of JRC staff and external staff under contract), apprentices and students, as well as visitors exposed to ionising radiation.

2.5. Categories of data processed

Identification data: name, surname, date and place of birth, sex, nationality, unique identification number and registered number of the radiation passbook (if applicable).

Organisational and occupational data: name and address of the employing company, working group and area inside the ITU; date of start and end of work at the ITU, follow-up of periodical compulsory information sessions.

Radiological data: radiation category, dosimeter type, results of dose readings from personal dosimeters, results of radioactivity measurements in the body and in excretion samples, date and results of dose values (official and operational).

"Medical data": type of medical and incorporation analysis to be organised, date of the last medical clearance, periodical medical clearance certificates, result of body fitness, reports in case of incidents or accidents in conjunction with radioactivity.

2.6. Recipients

According to the information provided in the privacy statement, the data are disclosed to the qualified and experienced radiation protection and medical officers (Health Physics Experts and Medical Officers as identified in the Directive 96/29, the AtomG and the StrlSchV).

[6] *Elektronische Datenverarbeitung* - Electronic Data Processing

According to the information provided in the notification, the data may be transferred to the following recipients:
- National supervisory authorities;
- Director of the ITU;
- external companies (employers of the external workers);
- "ADMIN medical service" / "Health Physics Experts and Medical Officers as identified in the Directive 96/29, AtomG, as well as StrlSchV";
- "ITU nurses linked to ADMIN";
- GSF and FZK (processors acting on behalf of ITU / "radioprotection experts from the outside").

2.7. Data retention

The individual dosimetry records shall be retained until the individual has or would have attained the age of 75 years, but in any case not less than 30 years from the termination of the work involving exposure to ionising radiation. In any case, they shall be deleted at the latest 95 years after the birth of the data subject (§ 42 StrlSchV).

Data kept for further statistical purposes are kept in anonymous form.

2.8. Rights of data subjects

According to the information provided in the notification, the data subjects' rights (access, rectification, blocking and erasure) can be exercised upon a request to the controller. After a justified and legitimate request, the modification of personal data is made within a month. However, the official dose values cannot be changed or deleted.

2.9. Information to data subjects

According to the information provided in the notification, JRC staff members, external workers, apprentices and students are being given information listed in Articles 11 and 12 of the Regulation during their compulsory radiation protection information sessions (at the beginning of their work in the controlled areas and then every six months). The privacy statement distributed during these information sessions provides for the following information: identity of controller, purpose, categories of data collected, certain recipients, existence of possibility to verify, modify or delete their information, data storage period, JRC DPC's and Commission DPO's contact information and the right of recourse to EDPS.

Furthermore, all data subjects (including visitors) are informed about the received radiation dose in case of overexposure (§ 42 (2) StrlSchV).

2.10. Security measures

(...)

3. Legal Aspects

3.1. Prior checking

Applicability of the Regulation: The present notification relates to the processing of personal data (*"any information relating to an identified or identifiable natural person"* -

Article 2 (a) of the Regulation) carried out in the exercise of activities falling within the scope of Community law (Article 3 (1) of the Regulation). The processing is partly automatic (the AGS-EDV database) and the personal data collected are kept in structured files (individual dosimetry records; Article 3 (2) of the Regulation). Therefore, the Regulation (EC) 45/2001 is applicable.

The scope of the prior checking analysis is restricted to the processing of dosimetry data[7]. The medical surveillance of workers exposed to ionising radiation will be analysed in a separate opinion.

Grounds for prior checking: Article 27 (1) of Regulation (EC) No 45/2001 subjects to prior checking by the EDPS all "*processing operations likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes"*. Article 27 (2) of the Regulation contains a list of processing operations that are likely to present such risks. This list includes *"processing of data relating to health"* (Article 27 (2) (a) of the Regulation). Processing of dosimetry data clearly concerns health related data and thus needs to be subjected to prior checking.

Ex-post prior checking: Since prior checking is designed to address situations that are likely to present certain risks, the opinion of the EDPS should be given prior to the start of the processing operation. In this case however the processing operation has already been established. In any case, this is not a serious problem in that any recommendations made by the EDPS may still be adopted accordingly.

Deadlines: The present notification was received on 5 June 2007. According to Article 27 (4) of the Regulation, the EDPS opinion must be delivered within a period of two months. The procedure was suspended for a total of 158 days (107 + 20 + August). Consequently, the present opinion must be delivered no later on 11 January 2008.

3.2. Lawfulness of the processing

The lawfulness of the processing operations must be examined in light of Article 5 of Regulation 45/2001. The notification for prior checking stated that the processing is necessary according to Article 5 (a) and (b) of the Regulation. Although there is a "grey zone" between Articles 5 (a) and (b) of the Regulation, the EDPS considers that in the present case, Article 5 (b) of the Regulation allowing for *"processing necessary for compliance with a legal obligation to which the controller is a subject"* is applicable. Indeed, the controller of the processing operation is subject to very specific legal obligations laid down in the German Ionising Radiation Protection Regulation of 20 July 2001 (StrlSchV) implementing the Directives 96/26 and 90/641[8] (cf. point 2.2 above).

3.3. Processing of special categories of data

Pursuant to Article 10 (1) of the Regulation, the processing of health related data is prohibited except in specific predefined circumstances, such as when 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 EC or other legal instruments adopted on the basis thereof"* in terms of Article 10 (2) (b) of the Regulation or

[7] As suggested by the name and the description of the processing operation as submitted in the prior checking notification

[8] The German legislation shall be applicable pursuant to the ITU Foundation Agreement signed between the European Commission and the German government in 1964.

"necessary to protect the vital interests of the data subject" in terms of Article 10 (2) (c) of the Regulation.

As explained above, the purpose of the processing in question is the compliance with the mandatory rules imposed on the controller with respect to the protection of occupationally exposed persons as laid down in the German Ionising Radiation Protection Regulation (StrlSchV) implementing the Directives 92/26 and 90/641. In any case, the processing of health-related data of visitors accessing controlled areas could be justified with respect to the necessity to protect their life and health. Article 10 of the Regulation is therefore fully complied with.

3.4. Data Quality

The data quality principles enshrined in Article 4 (1) (a), (c) and (d) of the Regulation require that the data are *"processed fairly and lawfully"*, they are *"adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed"*, as well as *"accurate and, when necessary, kept up to date"*.

Lawfulness has already been discussed (cf. point 3.2) and fairness will be dealt with in relation to information provided to data subjects (cf. point 3.7).

As to adequacy and relevance, the EDPS notes that the purpose of collection of the various categories of personal data (identification, organisational and occupational, radiological and "medical") is the surveillance of persons exposed to professional risks in the area of ionising radiation. The EDPS is of the opinion that the data collected and processed for this aim are in compliance with Article 4 (1) (c) of the Regulation.

As to accuracy, the EDPS notes that several measures are put in place in order to comply with this data quality principle, ranging from the attribution of a unique identification number to each professionally exposed person to the possibility to request rectification of inaccurate or incomplete data processed (cf. also point 3.8). Article 4 (1) (d) of the Regulation is therefore duly complied with.

3.5. Data retention

Article 4 (1) (e) of the Regulation states 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"*. In addition, *"the personal data which are to be stored for longer periods for statistical purposes should be kept either in anonymous form only, or if that is not possible, only with the identity of the data subject encrypted"* and *"shall not be used for any other purpose"*.

As indicated above, the individual dosimetry records are being kept for at least 30 years from the termination of the work involving exposure to ionising radiation and are in any case deleted 95 years after the birth of the data subject (§ 42 StrlSchV). In addition, the data stored for further statistical purposes are kept in anonymous form.

Considering that the storage of accurate dosimetry data may have significant relevance later in the context of medical treatment of the person concerned and/or in view of possible occupational diseases' related claims, the EDPS considers the legally prescribed time limit as reasonable. Article 4 (1) (e) of the Regulation is thus fully respected.

3.6. Transfer of data

Articles 7, 8 and 9 of Regulation (EC) No 45/2001 set out certain obligations that apply when the processed data are being transferred to third parties. The rules differ depending on whether the transfer is made to or within a Community institution or a body (based on Article 7), to recipients subject to Directive 95/46/EC (based on Article 8), or to other types of recipients (based on Article 9).

As indicated above, the data may be transferred to the following recipients:
- national supervisory authorities;
- Director of ITU;
- external companies (employers of the external workers);
- "ADMIN medical service"/ "Health Physics Experts and Medical Officers as identified in the Directive 96/29, AtomG, as well as StrlSchV";
- "ITU nurses linked to ADMIN";
- radioprotection experts from the outside;
- GSF and FZK (processors acting on behalf of the ITU).

Internal transfers: The transfers to the Director of the ITU, to the "ADMIN medical service" and to the "ITU nurses linked to ADMIN" shall be examined in light of Article 7 of the Regulation 45/2001. This Article provides that *"personal data can be transferred within or to other Community institutions or bodies if the data are necessary for the legitimate performance of the tasks covered by the competence of the recipient"* (paragraph 1) and that *"the recipient can process the data only for the purposes for which they were transmitted"* (paragraph 3).

The EDPS notes that the internal transfers fall within the legitimate performance of the tasks covered by the competence of the respective recipient. In fact, the Director of the ITU has to ensure adequate protection of persons professionally exposed to ionising radiation in the ITU whereas the "ADMIN medical service" assisted by the "ITU nurses linked to ADMIN" are responsible for the medical surveillance of the professionally exposed persons.

In order to ensure full compliance with Article 7 of the Regulation, the EDPS recommends that all recipients are reminded of their obligation to process the data only for the purpose for which they were actually transmitted.

Transfer to recipients subject to Directive 95/46/EC: The data transfers to the German supervisory authorities, to the two processors established in Germany, as well as the transfers of external workers' data to their employer established in the EU shall be examined in light of Article 8 of the Regulation. This Article allows for transfers to recipients subject to (the national law adopted for the implementation of) Directive 95/46/EC *"if the recipient establishes that the data are necessary for the performance of a task carried out in a public interest or subject to the exercise of public authority"* (Article 8 (a) of the Regulation.

The transfers to the German supervisory authorities, to the two processors acting on behalf of the ITU, as well to the external workers' employer established in the EU are necessary for the exercise of public authority and/or for the exercise of a public interest task in the area of protection against ionising radiation in accordance with the applicable national legislation. The necessity of the actual transfer is established jointly by the sender and the recipient.

Transfers to recipients <u>not</u> subject to Directive 95/46/EC: The transfers of external workers' data to their employer not established in the EU, as well as the transfers of data of

third countries nationals to the respective third countries national authorities shall be examined in light of Article 9 of the Regulation. In principle, transfers to recipients not subject to Directive 95/46/EC may occur only *"if an adequate level of protection is ensured in the country of the recipient or within the recipient international organisation and the data are transferred solely to allow tasks covered by the competence of the controller to be carried out"* (paragraph 1), unless one of the exceptions defined in paragraph 6 is applicable. In the present case, Article 6 (a, d, e) of the Regulation (transfer based on "*the unambiguous consent of the data subject"*, transfer "*necessary or legally required on important public interest grounds"*, transfer *"necessary in order to protect the vital interests of the data subject"* may be applicable.

3.7. Rights of access and rectification

Right of access: Pursuant to Article 13 of the Regulation, "*the data subject shall have the right to obtain, without constraint, at any time within three months from the receipt of the request and free of charge from the controller information at least as to the purposes of the processing operation, the categories of data concerned, the recipients to whom the data are disclosed and communication in an intelligible form of the data undergoing processing and of any available information as to their source".*

The right of access to the regular individual dosimetry results is enshrined in § 41 StrlSchV. It is specified in the privacy statement that the access request shall be addressed to the Head of the Unit E7 "Nuclear Safety / Health and Radiation Monitoring Section of the ITU acting as controller. Therefore, Article 13 of the Regulation is fully respected.

Right of rectification: Article 14 of the Regulation provides that *"the data subjects shall have the right to obtain from the controller the rectification without delay of inaccurate or incomplete information".*

The EDPS notes that the right of rectification can be somewhat limited because of the nature of the processing operation in question. It clearly applies to the updating of administrative data contained in the AGS-EDV database. Nevertheless, it is more difficult to guarantee this right with respect to dosimetry measurements. In principle, it cannot be excluded that the person concerned requests a review by another radioprotection expert. It could be a good practice to include such an expert opinion into the AGS-EDV database in order to make the processed data complete.

3.8. Information to the data subject

In order to ensure transparency and fairness of the processing of personal data, Articles 11 and 12 of Regulation 45/2001 provide for certain information to be supplied to the data subjects. The provision of Article 11 is applicable in case *"the data have been obtained from the data subject"*, the provision of Article 12 in case the data have been obtained from other source. In the present case, both Articles are applicable since the data processed are being obtained from the person concerned, as well as from the various parties involved in the process (GSF and FZK).

As indicated above, during the mandatory initial and periodical radiation protection information session, **JRC staff members, external workers, apprentices and students** are being given a privacy statement containing the following information:

- identity of controller,
- categories of data collected,

- certain recipients ("Health Physics Experts and Medical Officers as identified in the Directive 96/29, AtomG, as well as StrlSchV"),
- existence of possibility to verify, modify or delete their information,
- data storage period,
- JRC DPC's and Commission DPO's contact information,
- the right of recourse to EDPS.

In addition, in case of overexposure, all data subjects (including visitors) are being informed about the received dose without delay (§ 42 (2) StrlSchV).

Nevertheless, no information about the communication of the privacy statement to **visitors** exposed to ionising radiation is provided in the notification.

Therefore, in order to ensure the full compliance with Articles 11 and 12 of the Regulation, the EDPS recommends that
- the privacy statement is completed as to information about possible data recipients (by adding a reference to the national supervisory authorities, Director of ITU, external companies (employers of the external workers), "ITU nurses linked to ADMIN", GSF and FZK) and information the legal basis applicable,
- the revised privacy statement is also being posted to those parts of the buildings where they can be well perceived by visitors (such as at the entrances to the controlled areas, at the distribution sites of personal dosimeters, in the waiting rooms of the GSF and the FZK).

In addition, the revised privacy statement should be placed on the ITU Intranet.

3.9. Processing data on behalf of controllers

Determination of the controller and the processor: As indicated above, two processors are being involved in the processing of data of individuals exposed to ionising radiation in controlled areas of the ITU in Karlsruhe: the GSF and the FZK. These two German research centres process the relevant data on behalf of the Head of "Nuclear Safety" Unit E7 of the ITU who determines the purpose and the means of the actual processing (Article 2 (d) and (e) of the Regulation).

Contract concluded between the controller and the processor: Article 23 of the Regulation 45/2001 stipulates that the controller must "*choose a processor providing sufficient guarantees in respect of the technical and organisational security measures required by Article 22 of the Regulation"* (paragraph 1) and that "*the carrying out of a processing operation by way of a processor must be governed by a contract or legal act binding the processor to the controller"* stipulating, in particular, that the processor has also to comply with **obligations of confidentiality and security** as set out in the national law transposing Articles 16 and 17 (3) of the Directive 95/46/EC (paragraph 2) .

According Article 16 of the Directive 95/46/EC, the processor *"shall not process personal data except on instructions from the controller, unless required to do so by law"* ("confidentiality of processing").

Article 17 (3) of the Directive 95/46/EC specify that appropriate technical and organisational measures must be adopted by the controller and the processor *"to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected. Such measures shall be taken in particular to prevent any unauthorised*

disclosure or access, accidental or unlawful destruction or accidental loss, or alteration, and to prevent all other unlawful forms of processing".

In order to ensure the full compliance with Article 23 of the Regulation, the contracts concluded between the ITU and the FZK and/or the GSF ("licence agreements", ITU foundation agreement) shall provide for the above mentioned confidentiality and security obligations as set out in the applicable German data protection legislation.

3.10. Security measures

(...)

4. Conclusion

There is no reason to believe that there is a breach of the provisions of Regulation 45/2001 provided that the above considerations are fully taken into account. In particular,

- the Director of the ITU, the "ADMIN medical service" and the "ITU nurses linked to ADMIN" should be reminded of their obligation to process the data only for the purpose for which they were actually transmitted (Article 7 (3) of the Regulation);

- the privacy statement should be revised in light of Articles 11 and 12 of the Regulation in order to provide complete information about the possible recipients, as well as the legal basis applicable;

- the revised privacy statement should be posted to those parts of the buildings where they can be well perceived by visitors (such as at the entrances to the controlled areas, at the distribution sites of personal dosimeters, in the waiting rooms of the GSF and the FZK), as well as on the ITU Intranet;

- the contracts concluded between the ITU and the FZK and/or the GSF should include the confidentiality and security obligations as set out in the applicable German legislation (Article 23 of the Regulation);

(...)

Done at Brussels, 10 January 2008

Peter HUSTINX
European Data Protection Supervisor