Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Commission regarding the "PowerLab Management of Clinical and Toxicological Laboratories Environment"

Brussels, 17 January 2008 (Case 2007-649)

1. Procedure

On 26 October 2007, the European Data Protection Supervisor (**EDPS**) received a notification from the Data Protection Officer (**DPO**) of the European Commission concerning the PowerLab Management of Clinical and Toxicological Laboratories Environment used in Directorate-General Joint Research Centre (**JRC**).

The notification was accompanied by the following documents:
- a copy of the relevant provisions of the Staff Regulations;
- Italian Legislative Decree 626/94 transposing Directives 89/391/EEC, 89/654/EEC, 89/655/EEC, 89/656/EEC, 90/269/EEC, 90/270/EEC, 90/394/EEC, 90/679/EEC, 93/88/EEC, 97/42/EEC and 1999/38/CE concerning improvement of health and security during work (conventional risks),
- Italian Legislative Decree 230/95 transposing Directives 89/618/Euratom, 90/641/Euratom, 92/3/Euratom and 96/29/Euratom concerning ionising radiation,
- Italian Legislative Decree 241/00 transposing Directive 96/29/Euratom concerning the protection of general public and workers against the dangers arising from ionising radiation,
- "Privacy statement",
- "Clinical Laboratory - List of Tests",
- "Radio-toxicological Laboratory - Test Report",
- "Clinical Data Process in the Medical Service Ispra in 2006",
- "Radio-toxicology process flowchart in the Medical Service Ispra in 2007",
- "Clinical Laboratory - Test Report - Acceptance Form",
- "Employee's declaration of consent form",
- "Data fields sent to PowerLab".

The draft opinion was sent to the Commission DPO and the DG JRC DPC for comments on 19 December 2007. The comments containing considerable modifications of previously submitted information were received directly from the controller on 14 January 2008.

2. Facts

2.1. Purpose of the processing

The purpose of the processing of personal data within the software environment PowerLab is the management of the work cycle of the clinical and radio-toxicological laboratories at the DG JRC in relation to laboratory tests needed during pre-employment, periodic and other

occupational risks related visits. It also includes the production and/or storage of the respective test reports.

2.2. Description of the processing

According to the information provided in the notification, the PowerLab software is a Windows based data acquisition database system that is interfaced to seven analysers in the clinical laboratory, as well as to MeDeL software[1]. Processing operations during normal activity include the following:

- automatic or manual data input from MeDeL;
- automatic transfer of validated clinical data from the analysers to PowerLab;
- manual input of test results of PowerLab;
- printing of laboratory tests schedules by the laboratory staff;
- printing and filling of completed test reports in the individual medical files[2].

The following test reports are produced by the **clinical laboratories**:

- For EC employees, two final tests reports are printed. One is archived and the other one is given to the person concerned during the medical visit, accompanied by a letter signed by the person concerned and the physician.
- For employees of external companies, one test report is printed and signed by the physician. The report is then handed over to the responsible person of the external company in an envelope marked "medical secret". A copy of the report is archived and an electronic version of the report is stored in PowerLab.
- For pensioners and relatives, one final test report is printed and signed by the physician. The report is then given to the person concerned by the secretary. The electronic version of the report is stored in PowerLab.

The following reports are produced by the **radio-toxicological laboratories**:

- For EC employees, one final test report is printed and signed by the approved medical practitioner. This report is sent by internal post to the JRC Qualified Expert[3] who assesses the report and signs it. Then, it is returned by internal post to the JRC Medical Service and archived in the individual medical file in the JRC Medical Service archives.
- For employees of external companies, one test report is printed and signed by the approved medical practitioner in the JRC Medical Service. This report is sent by internal post to the JRC Qualified Expert who assesses the report, signs it, scans it and emails the report to the company's Qualified Expert.

The controller is the Head of the "Occupational Health and Safety" Unit C2 of the Ispra Site Directorate (**ISD**) of the DG JRC who is an occupational health physician and an approved medical practitioner

[1] The MeDeL software is subject to a separate prior checking - cf. EDPS opinion in case **2007-504**.

[2] The Individual Medical Files at DG JRC Ispra and Seville are subject to a separate prior checking - cf. EDPS opinion in case **2007-329**.

[3] *"Persons having the knowledge and training needed to carry out physical, technical or radiochemical tests enabling doses to be assessed, and to give advice in order to ensure effective protection of individuals and the correct operation of protective equipment, whose capacity to act as a qualified expert is recognised by the competent authorities"* in terms of Article 2 of the Directive 96/29 (ionising radiation)

2.3. Data subjects

The following persons may be involved in the data processing in question:
- European Commission employees (civil servants, temporary agents, contractual agents, auxiliary staff, grant holders, detached national experts, trainees);
- family members of subjects working for the JRC (for clinical tests);
- employees of external companies working for the JRC.

2.4. Categories of data processed

Identification data: progressive check-in number, MeDeL check-in code, dossier number, personnel number, first name, last name, gender, birth date, check-in date in MeDeL and place of work. (According to the controller's comments on the draft opinion received on 14 January 2008, the fiscal code listed among "Data fields sent to PowerLab" is not used for people in PowerLab.)**Medical data:** laboratory tests data (clinical and radio-toxicological).

2.5. Data retention

In general, the data processed within PowerLab are kept for the whole time of employment and up to 30 (standard and/or radiation exposure) or 40 years (carcinogenic agents) after the end of occupation. In addition, data of non-recruited persons are kept for five years after the pre-employment visit.

2.6. Data transfers

The data may be communicated to the following recipients:
- JRC Medical Service in the "Occupational Health and Safety" Unit C2 of the ISD,
- authorised staff responsible for detection, measurement or radioactivity and dose estimation in the "Nuclear Decommissioning and Facilities Management" Unit C1 of the ISD / JRC Qualified Experts,
- medical consultants working for the employer of the external workers (responsible persons of the external companies referred to in point 2.2.),
- Qualified Experts working for the employer of the external workers.

2.7. Rights of the data subjects

According to the information provided in the notification, the data subjects may send a request to verify, modify or delete their administrative information to the following functional mailbox: jrc-medical-service@ec.europa.eu or contact directly the JRC Medical Service Front Desk. Upon a justified and legitimate request by the data subject, the personal data will be modified in the database within 14 days. However, the laboratory tests results cannot be modified, but comments of the data subject can be added.

2.8. Information to be given to the data subjects

According to the information provided in the notification, a privacy statement will be put on the board in the waiting hall of the JRC Medical Services, as well as will be published on the Intranet website of the "Occupational Health and Safety" Unit.

The privacy statement submitted for review of the EDPS contains information about the respective controller (Head of the ISD "Occupational Health and Safety" Unit), the purpose of the processing (survey of staff's health), categories of data processed (identification and

medical data), certain recipients (JRC Medical Service staff), the existence of rights of access and rectification, the applicable time limits for storing the data, as well as the right to sent a complaint to the EDPS.

2.9. Security measures

(...)

3. Legal aspects

3.1. Prior checking

Applicability of the Regulation: The notification received on 26 October 2007 deals with processing of personal data (*"any information relating to an identified or identifiable natural person"* - Article 2 (a) of the Regulation) within the software environment PowerLab at the DG JRC of the European Commission. The processing is carried out in the exercise of activities falling within the scope of Community law (Article 3 (1) of the Regulation). The processing is - at least partly - performed by automatic means and the data processed manually form a part of a filing system (Article 3 (2) of the Regulation). Therefore, the Regulation (EC) 45/2001 is applicable.

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). The present case clearly concerns processing of 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 notification of the DPO was received on 26 October 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 pending comments on the draft opinion from the DPO for 26 days. Consequently, the present opinion must be delivered no later than on 22 January 2008.

3.2. Lawfulness of the processing

The lawfulness of the processing operations in question has to be examined in light of Article 5 of Regulation 45/2001.

Performance of a public interest task: Pursuant to Article 5 (a) of the Regulation, the processing is lawful if it *"is necessary for performance of a task carried out in the public interest on the basis of the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof or in the legitimate exercise of official authority vested in the Community institutions or body"*. The processing of personal data for

performance of tasks carried out in the public interest includes *"the processing necessary for the management and functioning of those institutions and bodies"* (recital 27).

The PowerLab software is necessary for the management of the work cycle of the clinical and radio-toxicological laboratories at the DG JRC in relation to laboratory tests needed during pre-employment, periodic and other occupational risks related visits, all in accordance with the secondary legislation applicable in the particular area.

In fact, the **legal basis** confirming the lawfulness of the processing can be found in the following provisions:

- Article 33 of the Staff Regulations, Articles 13 (2) and 83 (2) of the Conditions of Employment of Other Servants (pre-employment visits),
- Article 59 (6) of the Staff Regulation, Articles 16 (1), 59 and 91 of the Conditions of Employment of Other Servants (periodical visits of officials, temporary, auxiliary and contract agents),
- Italian Legislative Decrees 626/94, 230/95 and 241/00 (occupational risks related visits, including periodical visits of seconded national experts, trainees, grant holder and external workers).

As to the applicability of the Italian Legislative Decrees within the DG JRC of the European Commission, it has to be recalled that in line with the established ECJ jurisprudence, national law applies within EU institutions insofar 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]. Therefore, in the present case, the above mentioned Italian Legislative Decrees can be invoked as legal basis for processing of personal data in relation with professional risks related visits.

Consent of the data subject: As much as data processed within PowerLab are processed upon request of the family members of subjects working for the JRC, Article 5 (d) of the Regulation is applicable as well. According to this provision, the processing of personal data is lawful if *"the data subject has unambiguously given his or her consent"*.

The data subject's consent is defined in Article 2 (f) of the Regulation pursuant to which it is *"any freely given specific and informed indication of his wishes by which the data subjects signifies his agreement to personal data relating to him being processed."* The consent is therefore based on information provided in line with Article 12 of the Regulation (that is discussed in point 3.9.).

3.3. Processing of special categories of data

Pursuant to Article 10 of the Regulation, *"the processing of personal data concerning health is prohibited"* unless in specific predefined circumstances.

Obligation of the controller acting as employer: The processing of health-related data in PowerLab can be considered as *"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"* (Article 10 (2 (b) of the Regulation).

[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 explained above, the processing is necessary for the internal management of the clinical and radio-toxicological laboratories at the DG JRC in accordance with the relevant provisions of the Staff Regulations, the Conditions of Employment of Other Servants, as well as the Italian Legislative Decrees 626/94, 230/95 and 241/00.

Secrecy obligation imposed on health professionals: In addition, in the present case Article 10 (3) of the Regulation may be applicable. This provision allows for *"processing of health related data for the purpose of preventive medicine, medical diagnosis, the provision of care or treatment by a person subject to an obligation of secrecy equivalent to the one imposed on health professionals"*.

The EDPS notes that the physicians working in the JRC Medical Service, as well as the medical consultants working for the employer of the external workers are bound by an obligation of secrecy by virtue of their profession.

As to the other JRC Medical Service staff (nurses, laboratory staff, secretaries), as well as the Qualified Experts that may be involved in the processing of the medical data within PowerLab, the EDPS recommends that these persons are reminded of their specific professional secrecy obligation in terms of Article 10 (3) of the Regulation.

Consent of the data subject: 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 inasmuch the data are provided voluntarily by the respective family member of subject working for the JRC. In any case, the consent is based on information provided in line with Article 12 of the Regulation (discussed in point 3.9.).

3.4. Data Quality

Fairness and lawfulness: Article 4 (1) (a) of the Regulation also provides that personal data must be *"processed fairly and lawfully"*. 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 3.9.).

Adequacy, relevance and proportionality: According to Article 4 (1) (c) of the Regulation, personal data must be *"adequate, relevant and non excessive in relation to the purposes for which they are collected and/or further processed"*.

The EDPS notes that in PowerLab, the fiscal code is not being used in connection with natural persons and therefore cannot be considered as personal data in terms of Article 2 (a) of the Regulation and does not pose problems of excessiveness as it would if used for natural persons. The data processed within PowerLab are of administrative and/or medical nature and comply with Article 4 (1) (c) of the Regulation.

Accuracy: Article 4 (1) (d) of the Regulation provides that personal data must be *"accurate and, where necessary, kept up to date"* and that *"every reasonable step must be taken to ensure that data which are inaccurate or incomplete are erased or rectified"*.

The EDPS acknowledges that it is difficult to assess the accuracy and completeness of the medical data processed in the present case. In any case, the rights of access and rectification

also contribute to ensuring the quality of data processed within PowerLab (cf. point 3.8. in detail).

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"*.

As indicated above, the data are kept for the whole time of employment of the data subject and up to 30 (standard and radiation exposure) or 40 years (carcinogenic agents) after the end of occupation. The data of non-recruited persons are kept for five years after the pre-employment visit.

With respect to the fact that the PowerLab storage time limits were set out in accordance to the time limits applicable to the conservation of individual medical files at JRC Ispra and Seville, the EDPS would like to refer to its remarks provided in the respective opinion (EDPS 2007-329). In particular, EDPS would like to underline that the conservation periods shall be determined in relation to the nature of the respective document, as well as the necessity to keep the particular data[5].

3.6. Transfer of data

As indicated above, the data processed within PowerLab may be transferred to the following recipients:
- JRC Medical Service in the "Occupational Health and Safety" Unit C2 of the IDS,
- authorised staff responsible for detection, measurement or radioactivity and dose estimation in the "Nuclear Decommissioning and Facilities Management" Unit C1 of the ISD / JRC Qualified Experts,
- medical consultants working for the employer of the external workers,
- Qualified Experts working for the employer of the external workers.

Internal transfers: The data transfers within the Ispra Site Directorate of the DG JRC shall be examined in light of Article 7 of the Regulation. This provision allows for transfers of personal data within Community institutions *"if the data are necessary for the legitimate performance of the tasks covered by the competence of the recipient"* (paragraph 1). The recipient can process the data "*only for the purposes for which they were transmitted"* (paragraph 3).

The EDPS considers that all these transfers are necessary for the legitimate performance of the recipients' tasks in the area of protection against professional risks (as determined in the Italian Legislative Decrees 626/94, 230/95 and 241/00). Therefore, Article 7 (1) of the Regulation is being complied with.

In order to ensure the full compliance with Article 7 (3) of the Regulation, the EDPS recommends that all recipients are reminded of their obligation not to use the data received for any further purposes than the one for which they were transmitted.

[5] cf. also EDPS opinion **2006-532** on conservation period for medical documents of 26 February 2007

Transfers to the external companies: The transfers of personal data of external workers to the medical consultants, as well as Qualified Experts of their employers have to be examined in light of Articles 8 and 9 of the Regulation.

In case the external companies are subject to (the national measures adopted for the implementation of) Directive 95/46/EC[6], Article 8 of the Regulation is applicable. Pursuant to Article 8 (a) of the Regulation, intra-Community transfers are possible *"if the recipient establishes that the data are necessary for the performance of a task carried out in the public interest or subject to the exercise of public authority"*.

EDPS is of the opinion that such a transfer may lawfully occur on a basis of Article 8 (a) of the Regulation since the external company needs the data in order to comply with its public interest task in the area of protection against professional risks as laid down in the Italian Legislative decrees 626/94 and 230/95. In fact, in their quality as employer, the external companies have to ensure adequate protection of their workers against conventional and ionising radiation related occupational risks, such as to ensure that only medically fit workers are exposed to the respective health risks.

In case the external companies are not subject to Directive 95/46/EC, Article 9 of the Regulation is applicable. In principle, transfers to such recipients 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 an exception laid down in paragraph 6 can be applied.

3.7. Processing of personal number

Article 10 (6) of the Regulation provides that "*the EDPS determines the conditions under which a personal number or other identifier of general application may be processed by a Community institution or body*".

The PowerLab database contains the personal number of the data subject The EDPS considers that the personal number can be used in this context since it allows for the identification of the respective staff member and facilitates the follow-up in an appropriate way. There is no reason to determine any further conditions in this case.

3.8. Right of access and rectification

Right of access: Article 13 of the Regulation establishes the right of access of the data subjects. In particular, the data subject has *"the right to obtain, without constraint, at any time within three months from the receipt of the request and free of charge form the controller, communication in an intelligible form of the data undergoing processing and any available information as to their source"*.

As indicated above, all data processed within PowerLab can be accessed upon a request addressed to the controller (functional mailbox jrc-medical-service@ec.europa.eu or the Medical Service Helpdesk. Article 13 of the Regulation is therefore complied with.

Right of rectification: Article 14 of the Regulation provides the data subject with *"the right to rectify inaccurate and incomplete data"*.

[6] in case they are established in the EU - cf. Article 4 (1) (a) of the Directive 95/46/EC

As indicated above, the administrative data processed within PowerLab can be rectified upon a request addressed to the controller, whereby the modification in such data occurs within 14 days. The medical data processed within PowerLab (laboratory tests results) cannot be modified, but comments of the data subjects can be added.

The EDPS welcomes the JRC practice as regards rectification of administrative data, as well as acknowledges that the possibility of rectification of medical data can be limited due to the difficulty to assess their accuracy and completeness (cf. point 3.4.). He also recognises that for quality control reasons, it may be inappropriate to include external laboratory tests results submitted by the data subject into PowerLab itself. Nevertheless, the EDPS is of the opinion that JRC Medical Service should consider whether references to external laboratory test results provided by the data subjects and kept in the respective medical files could be provided in PowerLab (in particular in the comments of the data subjects on the medical data processed).

3.9. Information to the person concerned

In order to ensure the transparency and fairness of processing of personal data, Article 12 of the Regulation 45/2001 provides for certain information to be supplied in case the *"the data have not been obtained from the data subject"*. This information shall be provided "*at the time of the recording"* of the respective personal data or, in case of disclosure to third parties, *"no later than at the time when the data are first disclosed"*.

Privacy statement: As indicated above, a privacy statement will be put on the board in the waiting hall of the JRC Medical Services, as well as will be published on the Intranet website of the "Occupational Health and Safety" Unit. It contains the following information:

- identity of the controller (Head of the ISD "Occupational Health and Safety" Unit),
- certain information about the purpose of the processing (survey of staff's health),
- certain recipients (JRC Medical Service),
- categories of data processed (identification and medical data),
- the existence of rights of access and rectification,
- the time limits for storing the data,
- the right to send a complaint to the EDPS (including reference to the email address edps@edps.eu.int).

Therefore, in order to ensure full compliance with Article 12 of the Regulation, the EDPS recommends that the privacy statement posted in the JRC Medical Service waiting hall, as well as the JRC Intranet is modified in order to provide for a complete information about possible data recipients (cf. points 2.6. and 3.6.), the legal basis of the processing (cf. point 3.2.), the exact purpose of processing (cf. point 2.1.), as well as for the correct contact details of the EDPS (edps@edps.europa.eu). Only then an informed consent for the purpose of Articles 5 (d) and 10 (2) (a) of the Regulation can be assumed.

Information about test results: According to the information provided in the notification, data subjects (or physicians of their choice) are not informed about their radio-toxicological test results by the controller. In addition, the test reports produced by the clinical laboratories are communicated only to the employer of the external worker, but not to the data subject itself. This practice raises the EDPS concerns that the data subjects may not receive certain data relevant for their health status (or only with a delay).

In this respect, the EDPS acknowledges that it could be a good practice

- to communicate the radio-toxicological tests reports to the respective data subjects (or physicians of their choice) once they are completed (signed by the Qualified Expert) and put into the individual medical file, as well as
- to communicate the clinical test reports to the external workers concerned (or physicians of their choice) at the same time as the are being transmitted to their employer (i.e. disclosed to a third party in terms of Article 12 of the Regulation).

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 JRC Medical Service staff (nurses, laboratory staff, secretaries), as well as the Prevention and Protection Service (Qualified Experts) should be reminded of their professional secrecy obligation laid down in Article 10 (3) of the Regulation,

- the JRC Medical Service should consider the possibility of including a reference to external laboratory test results submitted by the data subject into PowerLab (Articles 4 (1) (d) and 14 of the Regulation),

- the JRC Medical Service should reconsider the current storage periods in order to comply with Article 4 (1) (e) of the Regulation,

- the data recipients within the Ispra Site Directorate should be reminded of their obligation not to use the data received for any other purposes than the one for which they were transmitted (Article 7 (3) of the Regulation),

- the privacy statement posted in the Medical Service waiting hall, as well as on the JRC Intranet, should be modified in order to provide for a complete information about possible data recipients, the legal basis of the processing, the exact purpose of processing, as well as for the correct contact details of the EDPS (Article 12 of the Regulation),

- the possibility of direct transmission the radio-toxicological and clinical tests reports to the respective data subjects (or physicians of their choice) should be considered (Article 12 of the Regulation).

Done at Brussels, 17 January 2008

Peter HUSTINX
European Data Protection Supervisor