Opinion on the notification for prior checking received from the Data Protection Officer ("DPO") of the European Commission ("Commission") regarding the Management of Safety at Work at the Joint Research Centre's ("JRC") Institute for Health and Consumer Protection[1] in Ispra ("Institute")

Brussels, 20 May 2009 (Case 2008-541)

1. Proceedings

On 26 August 2008, the Commission's DPO submitted to the European Data Protection Supervisor ("**EDPS**") via e-mail his Notification regarding the Management of Safety at Work at the JRC Institute for Health and Consumer Protection in Ispra, complete with its attachments ("**Notification**").

On 25 September 2008 the EDPS sent to the Commission's DPO a summary of his understanding of the facts along with his remaining questions. Until the Institute's written confirmation of the facts and response to the questions on 16 October 2008, the case was suspended. The EDPS sent to the Institute his draft Opinion for comments on 20 November 2008. The EDPS sent a reminder to the DPO regarding the comments on 11 May 2009 requesting a reply by 18 May 2009. As no response was received, the EDPS issued his Opinion on 20 May 2009.

2. The facts

2.1. Scope of the Notification and outline of the processing operations. The Notification and the EDPS Opinion concern a dedicated filing system: "Management of Safety at Work" used by the Institute. This filing system is maintained by the "Prevention and Protection Service Responsible" ("**RSPP**")[2] of the Institute. Personal data with an implication for safety at work are collected and stored in this filing system and consulted when needed. The purpose of the processing is to comply with the employer's obligations on safety at work under Italian laws. The processing operation covers all employees of the Institute.

Distinct, but related processing operations are analysed in the following EDPS Opinions:

- Opinion of 6 February 2008 on a notification for prior checking concerning the Dosimetry Management System at DG JRC Ispra (Case 2007-505),

[1] The Institute for Health and Consumer Protection (IHCP) is part of the Directorate General Joint Research Centre (DG JRC) of the European Commission. Its mission is to protect the interests and health of the consumer in the framework of EU legislation on chemicals, food and consumer products by providing scientific and technical support including risk-benefit assessment and analysis of traceability.

[2] The Institute explained that the RSPP currently consists of a single individual who hierarchically depends from the management support unit but who reports directly to the Institute's Director.

- Opinion of 6 February 2008 on a notification for prior checking on individual medical files at Joint Research centre in Ispra and Seville (Case 2007-329),
- Opinion of 23 January 2008 on a notification for prior checking concerning the Occupational Medicine (MeDeL) at DG JRC (Case 2007-504),
- Opinion of 17 January 2008 on a notification for prior checking concerning the Management of Clinical and Toxicological Laboratories Environment (PowerLab) at DG JRC (Case 2007-649), and
- Opinion of 25 January 2008 on First aid, accidents at work and other medical examinations at JRC (Joint Research Centre) in Ispra (Case 2007-372).

2.2. Privacy statement and description of the processing operations. The Notification explains that information on safety at work is available on the intranet of the Institute at http://ihcp-agora.jrc.it. The information includes documents and procedures to prevent so-called "residual risks". In addition, a privacy statement is also available at the same website. This document is entitled "Management of Safety at Work at the JRC-IHCP Institute in Ispra Privacy Statement" and summarises the most significant aspects of the processing operations as follows:

1. Description

The Prevention and Protection Service Responsible (RSPP) of the Institute for Health and Consumer Protection (IHCP) of the Joint Research Centre (JRC) is dealing with the collection and consultation of personal data for updating and verification of the fitness to work for each employee of the JRC Institute in the frame of safety at work. Personal data is collected and further processed for the purpose detailed hereafter under point 2.

This processing of personnel data is under the responsibility of the Director of the Institute for Health and Consumer Protection (IHCP) at the JRC.

For this collection and further processing of personal data, Regulation (EC) 45/2001, of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, is applicable.

2. What personal information do we collect, what is the legal basis, for what purpose and through which technical means?

Identification data

The personal data collected and further processed are: name, surname, birthday, nationality, sex, taxpayer's code, direction/institute/unit, employer/supervisor, start contract date, job description, scientific/technical/administrative action/activity, Commission Login User Name, personal number, office/laboratory location/building, type of contract, employee and employer scheme.

Other data are training data from SYSLOG FORMATION, data related to safety at work like exposures to work risks, data about accidents at work, data about medical and professional fitness

Legal Basis

- Directive 89/391/CEE
- Decreto Legislativo nr 81/2008 (replacing Italian Law 626/94 regarding matters pertaining to safety at work)

Purpose

The purpose of the processing of updating and verification of employee data is necessary in order to comply with the employer's obligations on safety at work.

Technical Information

The user's data are collected through paper forms/sheets but or by using electronic media.

3. Who has access to your information and to whom is it disclosed?

The access to all personal data is only granted through UserId/Password to a defined population of users. These users typically are: the Director, the Unit Head and the Safety Officer and the staff member. No personal data is transmitted to parties, which are outside the recipients and the legal framework mentioned.

4. How do we protect and safeguard your information?

The collected personal data is stored on the servers of JRC and underlie the Commission Decision C (2006) 3602 of 17/08/2006 "concerning the security of information systems used by the European Commission" defines IT security measures in force. Annex I defines the security requirements of EC Information Systems. Annex II defines the different actors and their responsibilities. Annex III defines the rules applicable by users.

5. How can you verify, modify, block or delete your information?

In case you want to verify which personal data is stored by the responsible controller, have it modified, corrected, blocked or deleted, please write an e-mail message to the functional mailbox address mentioned hereafter under "Contact Information", explicitly specifying your request.

6. How long do we keep your data?

Personal data are retained as long as the employee is under contract.

7. Contact Information

Should you have any queries concerning the processing of your personal data, please address them to the controller under the following mailbox: jrc-ihcp-dir-sec@ec.europa.eu

On questions relating to the protection of personal data, you can contact:
- the DG JRC Data Protection Co-ordinator: jrc-data-protection-coordinator@ec.europa.eu
- the Commission's Data Protection Officer: data-protection-officer@ec.europa.eu

8. Recourse

In the event of a dispute, you can send a complaint to:
- the European Data Protection Supervisor: edps@edps.europa.eu

2.3. Data collected in the filing system. The Notification explains that three types of employee data are collected in the filing system, as follows:

First, personal and administrative data are imported for each employee as available in a database called "DATAPOOL":

- name,
- birthday,
- nationality,
- sex,
- taxpayer's code,
- direction/institute/unit,
- employer/supervisor,
- start contract date,
- job description,
- scientific/technical/administrative action/activity,
- Commission Login User Name,
- personal number,
- office/laboratory location/building,
- type of contract,
- employee and employer signatures/dates on forms/sheets/documents.

Second, training data are linked from a database called "SYSLOG FORMATION":

- data from the training map (courses requested) and
- the training passport (courses followed)
- about language courses,
- general courses,
- compulsory safety courses and
- others from the e-learning database.

Third, data related to safety at work are also included in the filing system. These include the following data:

- exposures to work risks,
- data about accidents at work, including date of accident, location, witnesses, accident details, period of absence, injuries,
- possible exposure to substances/radiations: exposure time/single operation, number operations/month, quantity/single operation, environ exposure method, substance used,
- compulsory protective equipment devices or safety measures,
- physical/sensory fitness: Cat A., Cat B, medical fitness/professional fitness

Data in this third category come from the following sources:

- New Arrivals Administrative Checklist Admin (documenting administrative procedures)
- New Arrivals Safety and Laboratory (documenting safety and laboratory related items)
- Data about accidents at work (Rapporto d'Infortunio)
- Leaving Checklist
- Risk Assessment Sheet (Scheda Blu Inglese)
- Professional Hazard Sheet V.1
- Data Sheet about Exposure to Carcinogenic Substances (Registro Esposizione)
- Data Sheet about Exposure to Nanoparticles (Modulo Esposti Nanoparticelle)

- Data about medical and professional fitness.

3. Legal aspects

3.1. Prior checking

Scope of Notification. As discussed under Section 2.1 above, the scope of the Notification and of this Opinion covers a dedicated filing system: "Management of Safety at Work" used by the Institute.

Applicability of the Regulation. Regulation (EC) No 45/2001 (the "**Regulation**") applies to the "processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system" and to the processing "by all Community institutions and bodies insofar as such processing is carried out in the exercise of activities all or part or which fall within the scope of Community law" (Article 3).

All elements that trigger the application of the Regulation are present here:

First, the notified selection and recruitment process entails the collection and further processing of personal data as defined under Article 2(a) of the Regulation.

Second, the personal data collected undergo automatic processing operations as well as manual data processing operations, which form part of a filing system (Article 3(2) of the Regulation).

Third, the processing is carried out by the Institute, a Community body, in the framework of Community law (Article 3(1) of the Regulation).

Based on the foregoing, the Regulation is applicable.

Grounds for prior checking. Article 27(1) of the Regulation 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) contains a list of processing operations that are likely to present such risks. This list specifically includes health-related data under paragraph (a). Therefore, the notified processing operation requires prior checking by the EDPS.

Notification and due date for the EDPS Opinion. The Notification was received on 26 August 2008. According to Article 27(4) of the Regulation this Opinion must be delivered within a period of two months. The procedure was suspended for a total of 6 months and 24 days. Thus, the Opinion must be rendered no later than 21 May 2009 (27 October 2008 + suspension for the rest of the month of August (5 days) + 21 days + 5 months and 28 days for comments).

Ex-post prior checking. The processing operations started before the EDPS had been notified. Since prior checking is designed to address situations that are likely to present risks, the opinion of the EDPS should normally be requested and given prior to the start of the processing operation. However, this processing operation was notified after it had already been in place for some time and therefore the prior checking needs to be carried out ex-post.

This does not represent a major problem in the present case provided that all recommendations of the EDPS are taken into account.

3.2. Lawfulness of the processing

Article 5(a) of the Regulation provides that 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 ... or other legal instrument adopted on the basis thereof".

The first issue under Article 5(a) is to determine whether there is a specific legal basis for the processing: a Treaty provision or another legal instrument adopted on the basis of the Treaties. The second issue is to determine whether the processing operation is necessary for the performance of a task carried out in the public interest. To address this second issue in the present case, Recital 27 of the Regulation needs to be taken into account, which specifies that "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". Thus, the second issue in the present case is whether the processing is necessary and proportionate for the management and functioning of the Institute.

With regard to the first issue, management of safety at work at the Institute is based on the provisions of Directive 89/391/CEE and Decreto Legislativo nr 81/2008 (replacing Italian Law 626/94 regarding matters pertaining to safety at work).

Thus, specific legal instruments adopted on the basis of the Treaties allow for the notified processing operations. As to the Italian decree, it applies to the Institute in Ispra considering that it does not interfere with the tasks and privileges provided for under Community law, as provided in the case law of the ECJ[3]. With regard to the second issue, the EDPS is also satisfied and does not question that the notified processing operation is necessary and proportionate for the management and functioning of the Institute.

To conclude, the EDPS considers that the notified processing operations are lawful, so long as the recommendations made in this Opinion are followed.

3.3. Processing of special categories of data

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and of data concerning health or sex life, are prohibited unless an exception can be found in Articles 10(2)-(4) of the Regulation.

The prohibition is lifted among others where the processing is necessary for the purposes of complying with the specific rights and obligations of the controller in the field of employment law insofar as it is authorised by the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof, or as it is agreed upon by the European Data Protection Supervisor, subject to adequate safeguards (Article 10(2)(b) of the Regulation).

The present filing system, due to its specific purpose, contains a significant amount of health-related data. This is "necessary for the purposes of complying with the specific rights and obligations of the controller in the field of employment law" and authorized in the Italian decree cited above when designating the legal basis of the processing operation. The processing of health-data is thus, lawful under Article 10(2)(b) of the Regulation.

[3] See Case 1/88 SA SA Générale de Banque v Commission [1989] ECR 857, paragraph 9, Case C-2/88 Imm. Zwartfeld and Others [1990] ECR I-3365, paragraphs 19 and 20, and the judgment in Case T-80/91 Campogrande v Commission [1992] ECR II-2459, paragraph 42.

3.4. Data Quality

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

Based on the information provided to him, the EDPS does not question the adequacy, relevance and proportionality of the data collected in the filing system.

This is with one exception: the EDPS recommends the Institute to reconsider whether the safety officer needs direct access to all of the training information listed in Section 2.3 above, including information on general courses and language courses, and "others from the e-learning database". These appear to have no bearings on safety at work.

Fairness and lawfulness. Article 4(1)(a) of the Regulation requires that data must be processed fairly and lawfully. The issue of lawfulness was analysed above (see Section 3.2). The issue of fairness is closely related to what information is provided to data subjects (see Section 3.8 below).

Accuracy. According to Article (4)(1)(d) of the Regulation, personal data must be "accurate and, where necessary, kept up to date", and "every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified."

Based on the information provided to him, the EDPS does not question the accuracy of the data collected during the selection and recruitment procedures.

3.5. Conservation of data. The general principle in the Regulation is that personal data may 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).

Based on the information provided to him, the EDPS does not question the necessity to keep the data collected in the filing system for the duration of the employee's employment with the Institute.

3.6. Recipients and data transfers. The EDPS welcomes the fact that access to the filing system is limited on a need-to-know basis.

The EDPS additionally calls the Institution's attention to the requirement that if unforeseen data transfers are requested by any third party, the Institution should allow transfers subject to (i) either the unambiguous (with respect to sensitive data, explicit) and informed consent of the data subject, or (ii) as otherwise specifically allowed by the Regulation. The EDPS also emphasizes that pursuant to Article 7(3), the recipients may only process the personal data transferred for the purposes for which they were transmitted.

In case of doubt, the EDPS recommends that the controller consults the Institution's DPO before he/she makes the requested data transfer.

3.7. Right of access and rectification. Article 13 of the Regulation grants a data subject the right of access to personal data held about him. Article 14 provides a right of rectification of personal data.

In this respect the EDPS recommends that a minimum set of safeguards would be established and communicated in the privacy notice to ensure that any requests are granted in a timely manner and without constraints. If in doubt whether to grant access, the controller should consult the Institution's DPO.

3.8. Information to the data subject. Articles 11 and 12 of the Regulation require that certain information be given to data subjects in order to ensure the transparency of the processing of personal data. Article 11 is applicable to data obtained from the data subject, which is the case, for example, with regard to data contained in the documents that the controller requested the data subjects to complete. Article 12 applies when the data have not been obtained from the data subject. This is the case, among others, of the data contained in documents which were not completed by the data subject himself, at the request of the controller, for example, training data from the SYSLOG training database.

The EDPS welcomes that the privacy statement is posted on the Institution's intranet along with the relevant "safety-at-work" information. With regard to the content of the privacy notice, the EDPS makes the following additional recommendations:

Item 2 ("What personal information do we collect, what is the legal basis, for what purpose and through which technical means?) should be more clearly drafted. First, as regards the data collected, whereas "identification data" are discussed in great detail, similar detail is not given with respect to the data related to safety at work. The EDPS recommends that the categories of data collected would be described in the privacy notice at least in the same detail as above in Section 2.3 of this Opinion. Second, under "Technical Information" the statement "*The user's data are collected through paper forms/sheets but or by using electronic media"* should be clarified. Again, the level of detail as set forth in Section 2.3 of the Opinion would be appropriate or a summary could be provided.

3.9. Security measures. According to Article 22 of the Regulation, the controller must implement the 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. These security measures must in particular prevent any unauthorized disclosure or access, accidental or unlawful destruction or accidental loss, or alteration, and to prevent all other forms of unlawful processing.

The EDPS has not encountered any facts which would raise doubts about the adequacy of the security measures for data processed in the framework of the Institution's "Safety at work" filing system. In any event, the EDPS calls attention to the fact that the Institution should ensure that personal data in the filing system are not accessible by and disclosed to anyone other than those specified in this Opinion.

Conclusion

There is no reason to believe that there is a breach of the provisions of the Regulation provided that the considerations noted in Sections 3.2 through 3.9 are fully taken into account. The recommendations of the EDPS include the following:

- Data quality & proportionality:
  The Institute should reconsider whether the safety officer indeed needs direct access to general training data in SYSLOG Formation, as well as training data on languages and e-learning, in addition to training information directly relevant to safety at work.

- Rights of access:
  The Institution should establish a minimum set of safeguards to ensure that access requests will be addressed in a timely manner and without restraints.

- Information to data subjects:
  Notice with respect to certain items under Articles 11 and 12 of the Regulation should be provided in a more specific manner.

Done at Brussels, on 20 May 2009

(signed)

Giovanni BUTTARELLI
Assistant European Data Protection Supervisor