Opinion on a notification for Prior Checking received from the Data Protection Officer of F4E regarding the "*Invalidity procedure before the Invalidity Committee*".

1. Proceedings

On 8 October 2012, the European Data Protection Supervisor ("the EDPS") received a notification for prior checking within the meaning of Article 27(3) of Regulation 45/2001 ("the Regulation") concerning the "Invalidity procedure before the Invalidity Committee" from the Data Protection Officer ("the DPO") of Fusion for Energy ("F4E").

On 9 November 2012, the EDPS requested further information on the basis of the notification. The replies were provided on 21 February 2013. On 26 February 2013, the EDPS sought some clarifications from the DPO and full replies were provided on 31 May 2013.

The draft Opinion was sent to the DPO for comments on 19 June 2013. No comments were received.

2. Facts

On the basis of Article 59(4) of the Staff Regulations of Officials of the European Communities (Staff Regulations), F4E "*may refer to the Invalidity Committee the case of any official whose sick leave totals more than 12 months in any period of three years*". The data processing operation will be performed by the external service provider - F4E medical control officer, under specific contracts. [1]

Data subjects and Purpose

F4E has initiated a procedure in order to establish the invalidity of staff members, determine the causes of any such invalidity and decide on the need for and frequency of follow-up medical examinations. A decision will be obtained from the Invalidity Committee as to whether the official, temporary member of staff or contract member of staff concerned should be retired of the service, or resume his/her duties.

Legal basis

The legal basis of the processing consists of:

- Articles 59(4) and 78 of the Staff Regulations;
- Articles 7, 8 and 9 of Annex II to the Staff Regulations;
- Articles 13, 14 and 15 of Annex VIII to the Staff Regulations;
- Articles 16, 32, 33, 91, 100, 101 and 102 of the Conditions of Employment of Other Servants.

[1] These contracts have already been reviewed by the EDPS as part of cases 2011-1088-91 relating to the processing of health data in light of the EDPS Guidelines.

These should be read in conjunction with Article 6 of Council Decision 198/2007/Euratom establishing F4E, and Article 10(2) of the Statutes annexed thereto.

Procedure

According to F4E's procedural handbook for invalidity committees, the procedure may be launched either at the request of the person concerned or at the request of the Appointing Authority (AA). In the latter case, the AA may consult the medical control officer with a view to determining whether there are grounds for convening an Invalidity Committee.

The AA sends the person concerned an official letter containing a request that he/she should appoint a doctor to represent him/her on the Invalidity Committee, along with information on the nature of that doctor's remit.

The Invalidity Committee consists of three doctors:

- the first is a medical control officer appointed by F4E;
- the second is appointed by the staff member concerned;
- the third is appointed by common agreement between the first two doctors.

The Invalidity Committee has a threefold task:

- to establish invalidity;
- to determine the causes of that invalidity;
- to indicate whether follow-up examinations are required and how frequently they should be carried out.

Once the proceedings have been completed, the Invalidity Committee's conclusions are provided to the Administration and the staff member in question. These do not contain any medical information. A summary medical report is also annexed to the staff member's medical file -this is generally drafted by the third doctor but contains the signatures of all three doctors on the committee. It must not be consulted by the Administration.

At the end of its proceedings, the Invalidity Committee may decide either:

(i) that the data subject will be reinstated immediately if he/she is deemed as suitable to work, in which case a letter will be sent to the concerned staff member with a copy to HR, or;
(ii) that the data subject will be deemed as unsuitable to return to work, in which case the staff member will be informed that a later assessment will be performed and in what time frame (1, 2 or 3 years).

It might be the case that the data subject's state of health could improve. The Staff Regulations therefore allow the data subject to return to the institution or body if he/she no longer satisfies the requirements for payment of an invalidity allowance. As such, the F4E medical control officer will carry out periodic medical examinations. If the Committee accepts that the person can return to work, a letter will be sent to the concerned staff member with a copy to HR.

Recipients

According to the above procedure, the recipients of the data processed are the following:

Administrative data:

- the medical control officer who is an external service provider and member of the Invalidity Committee;

- the doctors of the Invalidity Committee, who deliver their medical opinion on the status of invalidity;
- outside experts (doctors) who are not members of the Invalidity Committee, if need for consultation with such experts arises;
- the Leave Manager(s) and their alternates (Human Resources officers and group leader);
- the data subject's immediate superior;
- the Head of the Administration Department along with their secretary;
- the Heads of Departments (in case of unjustified absence) and their secretaries;
- the Appointing Authority;
- the Director and Assistant to the Director;
- the F4E Legal Advisor: in case of a dispute;
- the internal auditor and Court of Auditors, for auditing purposes only;
- the European Ombudsman: upon justified request;
- the Court of Justice of the European Union: upon justified request;
- OLAF: upon justified request;
- EDPS: upon justified request.

Medical data:

- the medical control officer;
- the doctor (who is a member of the Invalidity Committee) appointed by the data subject;
- the doctor (who is a member of the Invalidity Committee) appointed by common agreement between the medical control officer and the data subject's doctor;
- the outside expert(s) who are not members of the Invalidity Committee, if need for consultation with such an expert arises.

Rights of access and rectification

Both the notification and the specific privacy notice state that data subjects may request access to their personal or medical file by contacting the controller. Data subjects also have the right to rectify their data (except for medical data) that is inaccurate or incomplete, and to obtain from the controller the blocking or erasure of their data.

Right of information

A Specific Privacy Notice is attached to the standard letter/email sent to the data subject by F4E inviting him/her to an initial meeting. The Privacy Notice makes reference to the invalidity procedure and contains the following information:

- identity of the controller;
- purposes of the data processing;
- legal basis of the processing;
- categories of data processed;
- recipients and to which data they have access;
- existence of the rights of access and rectification;
- retention periods of data;
- the fact that the processing is carried out in part by a named external service provider;
- the right of the data subjects to have recourse to the EDPS at any time.

Retention policy

The notification states that medical files are kept for a maximum of 30 years after the last medical document is inserted in the file, in the light of Article 4(1)(e) of the Regulation. This is the case for both favourable and unfavourable opinions.

Security measures
[…]

3. Legal aspects

3.1. Prior checking

Applicability of Regulation 45/2001 ("the Regulation"): The processing of data under analysis constitutes a processing of personal data ("*any information relating to an identified or identifiable natural person*"- Article 2(a) of the Regulation). The data processing is performed by an agency of the European Union, Fusion for Energy, in the exercise of activities which fall within the scope of EU law. The processing of the data, which forms part of a filing system, is manual. The Regulation is therefore applicable.

Grounds for prior checking: Article 27(1) of the Regulation subjects to prior checking 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*" by the EDPS. Article 27(2) of the Regulation contains a list of processing operations that are likely to present such risks. According to Article 27(2)(a) of the Regulation "*the processing of data relating to health*", as involved in this case, is subject to prior checking by the EDPS.

Notification and due date for the EDPS Opinion: The notification of the DPO was received on 8 October 2012. 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 199 days for further information from the controller and 23 days for comments. Consequently, the present Opinion must be delivered no later than 19 July 2013.

3.2. Lawfulness of the processing

According to Article 5 of the Regulation, data may be processed only on one of the specified grounds.

Of the five grounds listed in Article 5, the processing under analysis satisfies the conditions set out in Article 5(a) of the Regulation, to the effect that 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* (…)".

In the present case, **the legal basis** for the processing is found in the legal provisions of the Staff Regulations and Conditions of Employment of Other Servants as indicated in the facts.

The necessity for processing is also mentioned in paragraph 27 of the preamble to 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*". The processing of personal data at stake is considered as necessary in order to obtain the Invalidity Committee's conclusions as to whether the data subject should be retired of the service on grounds of invalidity, or resume professional activities. This processing therefore may be considered as contributing to the sound management and functioning of F4E.

3.3. Processing of special categories of data

Article 10(1) of the Regulation states that the processing of personal data on health is prohibited, except where it is justified by reasons provided in Articles 10(2) and 10(3) of the Regulation.

Article 10(2)(b) applies in this case: "*Paragraph 1* (prohibition of the processing of data on health) *shall 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...*". The processing under analysis is considered as necessary in order to comply with the specific obligations and rights of F4E as an employer under labour law. F4E therefore carries out this processing in accordance with the provisions of the Staff Regulations pursuant to Article 10(2)(b) of the Regulation.

In addition, according to the notification, medical data are only processed by the F4E medical control officer, members of the Invalidity Committee, and in exceptional cases, outside medical experts. It follows that the medical data are communicated to health professionals, who themselves are bound by professional secrecy for the purpose of concluding a medical diagnosis. Article 10(3) of the Regulation is therefore respected.

3.4. Data Quality

Adequacy, relevance and proportionality: According to Article 4 (1)(c) of Regulation 45/2001, personal data must be "*adequate, relevant and non excessive in relation to the purposes for which they are collected and/or further processed*". It should therefore be verified that the data collected are relevant in relation to the purpose for which they are being processed.

The EDPS considers that the data as described in this Opinion satisfy these conditions regarding the purpose of the processing explained above.

Accuracy: Article (4)(1)(d) of the Regulation provides that data must be *"accurate and, where necessary, kept up to date*". According to this 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*".

Invalidity is an inability to work for a fixed or indeterminate period. Depending on the case, the Invalidity Committee may decide to set a special timetable for a re-evaluation of the person's situation (unfit/fit to work), taking into consideration that the data subject must be re-examined periodically (Article 15 of Annex VIII to the Staff Regulations).

In the present case, the procedure in place enables one to conclude that the system itself gives a reasonable guarantee of data quality. Furthermore, the rights of access and rectification are available to the data subject, in order to make the file as comprehensive as possible. These rights constitute the second means of ensuring that data concerning the data subjects are accurate and updated (see section 3.7 on "the right of access").

Fairness and Lawfulness: Article (4)(1)(a) of the Regulation provides that personal data must be *"processed fairly and lawfully"*. The lawfulness of the processing has already been discussed in section 3.2 of this Opinion. As to fairness, this is linked to the information that must be provided to the data subject (see section 3.8 on "the right to information"). Some information on the invalidity process is provided to the data subjects by F4E within the medical service guide to procedures and the procedural handbook. Although not strictly

required by the Regulation, the EDPS would suggest that it would be good practice to supply more comprehensive information on each step of the process, including how and when communication will take place between the parties (for example by email, letter etc). It would also be helpful to provide more details on what will happen if the staff member's duties are ceased, continued or resumed, to ensure that he or she is fully aware of the potential outcomes.

3.5. Conservation of data

Article 4 (1) (e) of Regulation 45/2001 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*".

The EDPS notes that F4E does not make a distinction between the cases of a favourable or unfavourable opinion by the Invalidity Committee; in both cases, medical files are retained for a maximum of 30 years.

F4E has made reference to the 2009 EDPS "Guidelines concerning the processing of health data in the workplace". Although these guidelines do not, in general, strictly extend to invalidity proceedings, Article 4 recommends that 30 years is the absolute maximum that medical data should be kept in this context. However, the Guidelines go on to state that any such conservation periods should be considered on a case by case basis, in relation to the specific documents and the reasons for retaining them. Article 4(1)(e) of the Regulation stresses the idea of necessity in relation to the purpose of collection. As such, F4E should carefully consider whether there is a valid justification to retain all invalidity documentation for up to 30 years, including both favourable and unfavourable opinions. If appropriate justification cannot be provided, it is likely that F4E will be in breach of the Regulation.

In terms of retention, distinctions should also be made between:

- documents containing health related data (record of sick leave absences, whether the staff member suffers from permanent invalidity, and general reason for the invalidity);
- the Invalidity Committee decision to be kept in the personal file with other related documentation.

3.6. Transfer of data

Articles 7, 8 and 9 of the Regulation set forth certain obligations that apply when data controllers transfer personal data to third parties. The rules differ depending on whether the transfer is made (i) to or within Community institutions or bodies (based on Article 7), or (ii) to recipients subject to Directive 95/46 (based on Article 8), or (iii) to other types of recipients (based on Article 9).

Internal transfers: In accordance with Article 7(1), F4E is required to verify both that all the recipients possess the appropriate competences and that the transfer of the personal data is necessary to the performance of these competences. In this instance, the case is one of a transfer both within the F4E- in particular within the various departments responsible as indicated above- and between the F4E and other EU institutions and bodies. Each recipient has its own specific competence and the data transferred to each one appear to be necessary to the lawful performance of their assignments. The EDPS points out, however, that only the data they require for the performance of their missions must be transferred. In addition, in

accordance with Article 7.3 the recipients shall be reminded to process the personal data only for the purposes for which they were transmitted.

External transfers: In the context of the invalidity procedure, health data are also communicated to the doctor appointed by the data subject, and to a doctor appointed by agreement between F4E's medical control officer and the data subject's doctor. These external recipients are health professionals subject to the obligation of professional secrecy, which takes into consideration the particular nature of the data communicated and satisfies the conditions of Article 10(3) of the Regulation.

If either of these doctors is in a Member State which is subject to Directive 95/46/EC, Article 8 of the Regulation is applicable. The data related to health may only be transferred once the necessity for such a transfer has been established in light of Article 8 of the Regulation.

If either of these medical doctors is in a country that is not subject to Directive 95/46/EC, Article 9 of the Regulation is applicable. Pursuant to this provision, the data may be transferred only to a country of an adequate level of protection. If this is not the case, the exceptions stated in Article 9(6) must be taken into account. In the present case, paragraph (a) of Article 9(6) is particularly relevant: "*By way of derogation from paragraphs 1 and 2, the Community institution or body may transfer personal data if: (a) the data subject has given his or her consent unambiguously to the proposed transfer …*".

The EDPS notes that a confidentiality declaration has been signed by the contractors processing data in the context of the F4E invalidity procedure, and that data protection requirements also form part of the contracts themselves. The confidentiality declaration is in conformity with Article 23 of the Regulation.

3.7. Rights of access and rectification

Article 13 of the Regulation provides for the principle of the right of access to the data –and the procedures thereof– at the request of the data subject. Article 14 of the Regulation provides for the data subject's right of rectification.

Both the medical service guide to procedures and the privacy notice make reference to the data subjects' right to have access to their medical file by submitting a request. F4E should make clear that this access may be requested to F4E as controller, at any stage of the procedure.

Right of access: The existence of the right of access is in accordance with Article 13 of the Regulation.

Nevertheless, the EDPS draws F4E's attention to Article 20 of the Regulation, which lays down certain restrictions on this right, in particular where such restrictions constitute a necessary measure for the protection of the data subject or of the rights and freedoms of others. The right of access to the medical file is contained within F4E's specific privacy notice on invalidity. This notice states that data subjects have the right of direct access to their medical file, to be exercised on the premises of the medical service in the presence of the medical control officer. However, provision is not made for indirect access in order to consult psychiatric/psychological reports through the intermediary of a doctor appointed by the data subject. Although the medical service guide to procedures briefly mentions possible restrictions to the right of access, this is not made clear within the privacy notice. Moreover,

neither document specifically mentions Article 20(1)(c) of the Regulation, which lays down that this restriction is necessary to guarantee the protection of the data subject or the rights and freedoms of others.

The EDPS invites F4E to ensure that a restriction on access to medical files is examined on a case-by-case basis. Article 20 of the Regulation must not be allowed to result in a general refusal of access to the personal notes of doctors in the medical file. F4E should also make sure that the privacy notice makes reference to the possibility of the application of Article 20 of the Regulation, in terms of potential exceptions to the right of access.

Right of rectification: With regard to the right of rectification, F4E should explain to data subjects, for example in the privacy notice, that their right of rectification in the context of medical data includes the addition of other medical opinions of doctors to their medical file.

3.8. Information to the data subject

Articles 11 and 12 of the Regulation 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 operations, they are required 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 others from other persons.

In the present case, the privacy notice sets out most of the items included in Articles 11 and 12 of the Regulation. However, the EDPS draws F4E's attention to the following information that should be included in the notice:

- in terms of the possible recipients of processing, clarify that the "external expert" will be a doctor, and;
- provide clarification on the rights of access and rectification, as analysed in section 3.7 of this Opinion.

Moreover, it is noted that only a general description of the overall procedure is provided in the procedural handbook and privacy notice. As mentioned in section 3.4 of this Opinion, the EDPS would recommend that more details about each step of the process are given in the procedural handbook, including potential outcomes, in order that data subjects are fully informed.

3.9 Security Measures

[…]

4. Conclusion

There is no reason to believe that there is a breach of the provisions of the Regulation, provided that the following considerations are taken into account. In particular F4E should:

- reconsider the retention periods of the personal data, as explained in section 3.5 of this Opinion;

- make reference to the possibility of the application of Article 20 of the Regulation in the privacy notice, regarding the right of access to the medical file. F4E should ensure that restrictions on access to medical files are examined on a case-by-case basis;

- explain to data subjects that their right of rectification in the context of medical data means the addition of other medical opinions of doctors to their medical file;

- include in the privacy notice (and/ or other documentation relating to the invalidity procedure) the information as explained in section 3.7 and 3.8 of this Opinion.

Brussels, 16 July 2013

(**signed**)

Giovanni BUTTARELLI
Assistant European Data Protection Supervisor