EUROPEAN DATA PROTECTION SUPERVISOR

WOJCIECH RAFAŁ WIEWIÓROWSKI
ASSISTANT SUPERVISOR

Head of Administration
Fusion for Energy
Torres Diagonal Litoral
Edificio B3
08019 Barcelona
Spain

Brussels, 28 March 2017
WW/ALS/xx/ D(2016) xxx **C 2016-0535**

**Subject: Prior-checking Opinion regarding 360° feedback exercise for managers at Fusion for Energy (EDPS case 2016-0535)**

Dear Mr Jahreiss,

On 14 June 2016, the European Data Protection Supervisor ("EDPS") received a notification for prior checking under Article 27 of Regulation (EC) No 45/2001[1] ("the Regulation") on 360° feedback exercise (the "Exercise") for managers from the Data Protection Officer ("DPO") of the European Joint Undertaking for ITER and the Development of Fusion for Energy ("F4E").[2]

As mentioned by your DPO in the cover email of the notification, this processing operation is similar to other notified cases of feedback tools for managers already prior checked by the EDPS.[3] For this reason, this Opinion does not contain a full analysis of all data protection aspects, but focuses on pointing out those that diverge from other cases or otherwise require improvement.

**Facts and analysis**

## 1. Lawfulness of the processing

As grounds for lawfulness, F4E has stated that the processing of personal information is based on Article 5(a)[4] and (d)[5] of the Regulation.

[1] OJ L 8, 12.1.2001, p. 1.
[2] As this is an ex-post case (cf. email from the DPO of 22 June 2016), the deadline of two months does not apply. This case has been dealt with on a best-effort basis.
[3] Cases 2009-0215, 2013-1290, 2014-0906, 2014-1146, 2015-0733, 2015-0772 and 2016-1007.
[4] Personal data may be processed only if the processing is necessary for the performance of a task carried out in the public interest on the basis of the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof or in the legitimate exercise of official authority vested in the Community institution or body or in a third party to whom the data are disclosed.
[5] Personal data may be processed only if the data subject has unambiguously given his or her consent.

As regards Article 5(d), the data subject's consent is defined in Article 2(h) of the Regulation as "*any freely given specific and informed indication of his or her wishes by which the data subject signifies his or her agreement to personal data relating to him or her being processed"*. In this regard, the EDPS underlines that consent should be used with caution in the employment context. Such consent is valid only in exceptional circumstances where the employee has a genuine free choice and is subsequently able to withdraw the consent without negative consequences.[6]

In this case, the program is presented as voluntary to managers[7] who must fill in a consent form to which a privacy statement is attached. However, the consent form does not correspond to a freely given consent as regards the sharing of his/her data in particular with other people inside F4E, as it requires from the applicant to initial all boxes[8], including the one referring to the following statement:

> "*The 360° exercise serves the professional development within Fusion for Energy. I understand that for this reason the information collected during the exercise may be looked at and used by my superior, the Head of the HR Unit, the HR responsible officer responsible for the career development of the manager and the external provider contracted to administer the survey. I give permission for these individuals to have access to the results of the survey*."

In this regard, the manager should be able to choose whether their hierarchy and members of F4E HR services should have access to his/her personal data collected during the Exercise. The processing primarily aims at helping managers enhance their personal development by receiving individual reports and is not part of their mandatory appraisal under the Staff Regulations, which is a different purpose pursued through a separate processing. Therefore, the automatic communication of the personal data processed in the framework of the Exercise to the manager's superiors, the Head of HR and the officer in charge of career development would be excessive in relation to the purpose with the processing activity and therefore not compliant with Article 4(1)(c) of the Regulation.

Furthermore, the notification, the privacy statement and the consent form should make clear that participating managers may revoke their consent and consequently stop the Exercise at any time of the process.

***Recommendations***:

1. Modify the consent form so as to (i) delete the obligation for managers to initial all boxes, and to (ii) allow the managers to opt in as regards the access to their personal data to others than the external service provider;
2. Clarify in the notification (under Section 4 - purpose of the processing), the privacy statement and the consent form (paragraph 2) that participants can decide to opt-out from the exercise at any time of the process.

[6] Article 29 Data Protection Working Party Opinion 8/2001 of 13 September 2001 on processing of personal data in the employment context.
[7] cf. Section 4 of the notification; and privacy notice.
[8] See form attached to the notification: "*Please initial all boxes*".

## 2. Processing of group reports

According to the notification, the group report includes anonymous aggregated compiled results for all of the managers who have participated and will only show the overall quantitative results for the group of participants and no open comments from the individual report are included.

The group report is provided to the F4E management. As to the understanding of the EDPS, the sharing of the group report corresponds with the purpose mentioned in the notification to give a picture of the management culture within F4E, which is another purpose than for the processing of individual reports. These two different purposes should be clarified in the notification and privacy statement.

The EDPS understands that the group reports do not allow for the identification of individual answers provided by the participants and the contributors. However, in view of the optional character of the exercise, one cannot entirely exclude that the group report will contain identifiable information on participating managers. The participants should therefore be properly informed that the group report communicated to the F4E management could potentially contain identifiable information related to them.

***Recommendations*:**

3. Amend the notification and the privacy statement, which should be more appropriately designated as a 'data protection statement', to clearly define the respective purposes of the processing of the individual and group reports.
4. Add to the data protection statement information about that it cannot be entirely excluded that the group report communicated to F4E management would not potentially contain identifiable information related to the participants.

## 3. Recipients v. internal processors

According to the Regulation, a processor is "*a (...) person* (...) *which processes personal data on behalf of the controller*"[9].

The notification and data protection statement identifies managers that participate in the Exercise as "internal processors" of their consent forms, their individual report and the group report[10]. Furthermore, other staff members[11] are also mentioned as "internal processors" of the consent forms, individual reports and group reports. Please note that under the Regulation the term "processor" refers to situations such as outsourcing processing operations to external parties, and not to the simple fact that F4E staff members process personal data under instruction from the controller. Moreover, as mentioned above (Section 1), it should be up to the participating manager to decide if he/she wishes to share the personal information with other recipients ("internal processors"). This should be reflected in the notification and data protection statement.

[9] Article 2(e) of the Regulation.
[10] See Section 12 of the notification and pp. 3-6 of the privacy statement.
[11] The Director, concerned Head of Department, Head of Unit, Head of HR, HR responsible Officer and the direct superior of the participating manager.

***Recommendations***:

5. Modify the terminology used in the notification and data protection statement (in sections on the recipients) so that managers participating in the Exercise and other F4E staff members having access to the data are not considered as "internal processors" of personal data;
6. Indicate in the notification and data protection statement that the individual reports will not be communicated to recipients other than the external service provider without the explicit consent of the participating manager.

**4. Information of data subjects**

In the data protection statement under "*Lawfulness of the processing*", the first paragraph mentions Article 5(a) for this specific processing operation. The second paragraph refers to Article 5(d) but in relation to the annual check-up.

***Recommendation***:

7. F4E should amend this paragraph so it refers to the Exercise and indicate that consent may be revoked at any time in the course of the exercise. (As regards the data protection statement's denomination and content, see also recommendations 2-6 and 8.)

**5. Processor and sub-processor**

F4E has a Service Level Agreement (the "SLA") on training of staff with the European School of Administration ("EUSA"). The SLA includes a data protection clause (Article 14) mentioning that EUSA shall process all personal information supplied to them by F4E in line with the Regulation and that the data supplied to EUSA shall be exclusively for the purpose of the registration of participants and evaluation. Article 9 of the SLA states a possibility for EUSA, upon request by F4E, to provide consultancy services in the area of training.

From the information provided, we understand that the Exercise involves two processors: the Commission's (EUSA) contractor, Bick Consortium ("Bick"), and a sub-contractor, Cubiks. Cubiks collects evaluations on the managers that participate in the Exercise through its own assessment tool and produce individual and group reports whereas Bick are conducting individual debriefing sessions with the participating managers. However, the identity of these (sub-) processors are not mentioned in the notification and the privacy statement. Additionally, it appears that F4E does not have a direct contractual relationship with Bick (nor with Cubiks, for that matter), but instead directly uses the contract between Bick and EUSA.

For this specific procedure, F4E requested EUSA under Article 9 of the SLA to provide them with the Exercise as a consultancy service. EUSA is therefore the processor to F4E and Bick the sub-processor. F4E has provided the signed order forms between them and EUSA with the cost proposal for the Exercise[12]. The data protection clause in Article 14 of the SLA does not explicitly oblige EUSA to only act upon instructions from F4E (as mentioned in Article 23(2)(a)), and to have proper security measures in place (Article 23(2)(b)), also in relation to the sub-processor(s). F4E should therefore remind EUSA about its responsibilities in relation to Article 23(2) for this processing activity and for future contracts explicitly include the obligations to be imposed on the controller under Article 23.

[12] by email of 23 January 2017.

***Recommendations***:

8. Indicate the identity of the (sub-)processors and their respective roles in the notification (under Section 12 - Recipients) and the privacy statement;
9. Remind EUSA in writing, as processor of the Exercise, of their obligations in relation to Article 23(2) and include an explicit obligations for the processor in future contracts.

* *
*

In this Opinion, the EDPS has made several recommendations to ensure compliance with the Regulation. Provided that they are implemented, the EDPS sees no reason to believe that there is a breach of the Regulation.

The EDPS expects **implementation and documentary evidence** thereof within **three months** of the date of this Opinion for the above-mentioned recommendations.

Yours sincerely,

**(signed)**

Wojciech Rafał WIEWIÓROWSKI

Cc: Data Protection Officer - F4E