Opinion on the notification for prior checking received from the Data Protection Officer ("DPO") of the European Commission ("Commission") regarding the optional "Leadership Feedback" procedure established by the European Administrative School ("EAS") in connection with its management courses

Brussels, 15 December 2008 (Case 2008-527)

1. Proceedings

On 2 September 2008, the European Data Protection Supervisor ("**EDPS**") received from the Commission's DPO the hard-copy of a notification, complete with its attachments, regarding an optional "Leadership Feedback" procedure established by the EAS in connection with its management courses ("**Notification**").

On 24 September 2008 the EDPS sent to the Commission's DPO a summary of his understanding of the facts along with his remaining questions. EAS replied on 28 October 2008.

The EDPS sent to EAS his draft Opinion for comments on 4 December 2008. The Commission replied on 12 December 2008.

2. The facts

2.1. Scope of the Notification and summary of the "Leadership Feedback" procedure. The Notification concerns an optional "Leadership Feedback" procedure established by the EAS in connection with its management courses.

EAS, as part of its mandate, organizes management courses for Commission officials and officials of other European institutions and bodies. In connection with each management course, EAS offers participants an opportunity to receive anonymous feedback about their management skills from other participants. Participation in the exercise is anonymous and entirely voluntary. The information is not used by EAS or the Commission for their own purposes and is processed entirely for the benefit of the participants.

EAS outsourced the provision of management courses to a private company established in a European Union Member State. This company, in turn, outsourced the organization of the Leadership Feedback procedure to another private company, also established in a European Union Member State. EAS has, itself, no access to any data processed during the procedure. The outsourced processor organizes and manages the feedback procedure. In particular, it makes available to participants a secure website tool to collect feedback, aggregates feedback into reports (while the anonymity of those providing feedback is ensured), and provides each participant with a report regarding the group's feedback on his/her own management skills.

Participants, if they so wish, may also complete a questionnaire assessing their own management skills and may also allow access to the feedback information to their trainers.

2.2. Privacy statement and description of the processing operation. Course participants will receive an information pack in paper form, which will also include a description of the feedback procedure. This document will contain a link to the specific data protection declaration quoted below, which is available on the EAS website. In this document, which is entitled "Privacy statement in the framework of training activities organised by the European Administrative School (EAS) and the use of leadership feedback", EAS summarises the most significant aspects of the processing operation as follows:

> This statement explains how all personal data provided are dealt with in the framework of regulation (EC) N° 45/2001 of the European Parliament and of the Council of 18 December 2000. It is submitted individually to staff of the EU institutions, agencies and offices who participate in training courses organised by the EAS and who choose voluntarily to seek feedback from colleagues on their management and leadership styles. It also applies to the staff who provide that feedback. In accordance with articles 11 and 12 of this regulation, EPSO and EAS provide the participants in this activity with the following information:
>
> **Controller identity**[1] : Mr Nicholas David BEARFIELD, Director of EPSO.
>
> **Purpose(s) of the processing**: to allow participants in EAS training courses to obtain anonymous feedback on their management and leadership style from their colleagues with the aim of helping them improve their management and leadership skills. This type of tool is commonly used internationally by training providers in courses on management and leadership. The data will not be used in any form of evaluation (appraisal) process of any of the persons involved.
>
> **Data concerned:** Data concern those staff of the EU institutions, agencies and offices participating in the training courses organised by the EAS. Data requested from the staff participating in the training courses or from their colleagues about them is collected on a purely voluntary basis.
>
> Course participants are offered the opportunity to use a feedback tool in the form of a self-assessment of their skills and an assessment by colleagues that they choose to be consulted. Participation in this activity by the person concerned and their colleagues is entirely voluntary and participants are free to choose the persons whom they wish to invite to take part in this activity. The persons so invited may choose whether or not to take part. It is a facility offered by the EAS to help participants learn about their professional skills and enhance their own personal development in a professional context. Participants participate in the activity.
>
> The personal data concerned is four-fold.
>
> Firstly, the course participant is given full information about the feedback activity and invited to choose whether or not to participate. If they so choose, they must provide details (name and electronic address) about themselves and those colleagues who will be invited to provide feedback. These details are provided at present to Innotiimi, Finland, one of the members of the consortium contracted by to provide management training programmes. Any change in or addition to the company providing this service will be notified to the DPO. Innotiimi passes this data to its sub-contractor Feedback OY who is

[1] By reason of the administrative attachment of EAS to the EPSO for the first three years following its establishment, the Director of EPSO is jointly responsible for control.

responsible for the website where the subsequent feedback exercise will take place. This data serves purely to identify the course participant and those colleagues participating in the exercise and to allow the contractor to contact them. The course participant is provided at this stage with full information about the exercise and the nature and steps of data processing. The participant is provided with an information sheet giving the same information, which is to be given to colleagues who agree to participate in the exercise. The participant is also asked to indicate whether they would prefer to receive the final report from the exercise individually, or whether it can be shared with the trainer from the training course. There is no obligation for the participant to share the final report.

The second data treatment arises when the course participant provides input to the activity. This data takes the form of filling in an on-line questionnaire regarding their management skills. The data collected take the form of numerical data i.e. answering yes or no to a series of set questions, and textual data where the participant can choose to complement the numerical data with individual comments. The participant has the option to provide these comments or not.

The third data treatment arises when the colleagues of the course participants provide their input to the activity by completing an on-line questionnaire regarding their feedback on the management skills of the participant. The data collected take the form of numerical data i.e. answering yes or no to a series of set questions, and textual data where the person concerned can choose to complement the numerical data with individual comments.

The fourth data treatment arises when Feedback OY process the data supplied by the participant and their colleagues. The numerical data from the two sources are amalgamated into a single report.[2] This report will also include an amalgamation of any written comments made. This report is then sent to the participant to the email address that they have chosen to supply. The report will also be sent to the trainer who is delivering the course but only if the participant has given their consent. This allows the trainer to give one-to one feedback orally to the participant on the results of the report.

Nature of the data to be processed:

- Data of a personal nature allowing the identification of the staff member concerned (name, given name, electronic address);

- Information provided by the course participant on their own perception of their management and leadership skills in areas such as performance management, change management, issue management and people management.

- Information provided by colleagues on their perception of the participant's management and leadership skills in areas such as performance management, change management, issue management and people management. This information is rendered anonymous and amalgamated into a feedback report.

[2] EAS explained to the EDPS that this "amalgamation" takes place automatically. The software tool automatically formats the individual input into the aggregated data tables and chapters of the final report. EAS further explained that Feedback OY nevertheless must be able to have access to the individual data in order to delete any data at the request of the data subject. Neither Innotiimi nor EAS has access to the data.

Legal base:

- conditions of employment of servants of the European Communities, as fixed by regulation (CEE, Euratom, CECA) n° 259/68 of the Council, last modified by regulation (CE, CECA, Euratom) n° 23/2005 of the Council, and in particular articles 45b of the Staff Regulations and 7 § 2 point c) of Annex III of the Staff Regulations;

- decision n° 2002/620/CE of the European Parliament, the Council, the European Commission, the Court of Justice, the Court of Auditors, the European Economic and Social Committee, the Committee of the Regions and the European Ombudsman of 25 July 2002 culminating in the creation of the European Personal Selection Office;
- decision n° 2005/118/CE of the European Parliament, the Council, the European Commission, the Court of Justice, the Court of Auditors, the European Economic and Social Committee, the Committee of the Regions and the European Ombudsman of 26 January 2005 culminating in the creation of the European Personal Selection Office;

- decision n° 2005/119/CE of the Secretaries General of the European Parliament, the Council, the European Commission, the Court of Justice, the Court of Auditors, the European Economic and Social Committee, the Committee of the Regions and the European Ombudsman of 26 January 2005 concerning the organisation and operation of the European Administrative School;

Recipients of the data: the contractor of the EAS who receives and processes the data; the course participant him/herself who receives the anonymous, amalgamated report of the feedback; if the participant so wishes, the course facilitator who also receives the anonymous, amalgamated report of the feedback. No data is received by the EAS or any of the EU institutions, agencies or offices.

Lawfulness of processing: the processing is useful in helping staff of the EU institutions, agencies and offices to fulfil their management functions carried out in the public interest on the basis of legal instruments adopted on the basis of the treaties establishing the European Communities.

Date when processing starts: date of receipt by the contractor of the EAS of the data identifying the course participant and the colleagues participating in the feedback exercise.

Data retention period: data concerning the identity of the course participant and his/her colleagues is kept for a period not exceeding 2 months from the end of the training course in which the course participant is participating and for which the data is supplied. The data concerning the feedback of the colleagues (either individual or amalgamated) is kept for a period not exceeding 2 months from the end of the feedback session for which the data is necessary.[3]

Right of access and verification: staff members concerned may send a request to indicate any changes to their personal data. In any case, and following written request with a copy of a proof of identity, they may obtain a copy of their personal data as

[3] EAS explained that it established the retention period at two months as it believes that this is reasonable considering that new reports may need to be generated if the recipient of the report looses his/her report and wishes to obtain another copy or if the persons providing individual feedback wish to check again what information they provided.

registered by the contractor of the EAS.[4] Requests can be sent to: **epso-eas-pdp@ec.europa.eu.**

Following a written request with a copy of a proof of identity, participants may obtain a written copy of all the information which they provided in the form of feedback to allow them to check that the information they supplied was accurately recorded.

Following a written request with a copy of a proof of identity, colleagues providing feedback may obtain a written copy of the information which they provided in the form of feedback to allow them to check that the information they supplied was accurately recorded.

This entails any right of rectification under article 14 of regulation (EC) N° 45/2001 of the European Parliament and of the Council of 18 December 2000

Staff also have the right to have recourse at any time to the European Data Protection Supervisor (edps@edps.europa.eu).

2.3. Data transfers to processors, data security. EAS provided the following additional information on data transfers to processors and on data security:

- Innotiimi has a written contract with EAS, which includes a specific data protection clause. This clause provides that
  - data must be processed in accordance with the provisions of Regulation (EC) No 45/2001,
  - data may be processed solely for the purposes of the performance, management and follow-up on the contract with EPSO/EAS, and upon instruction of the data controller,
  - data are confidential, the contractor must limit access to the data to staff on a strictly as-needed basis, and
  - the contractor undertakes to take appropriate technical and organisational security measures (with a detailed list of what those measures should ensure).

- The text of the clause does not limit Innotiimi's ability to choose its subcontractors and does not specifically oblige Innotiimi to pass on these obligations to its subcontractors. However, EAS confirmed that if the EDPS considers it necessary, it is still possible to include this in written form in the contractual obligations of Innotiimi. EAS further explained that Innotiimi has a written agreement and a non-disclosure agreement with Feedback OY.

- In Feedback all employees have to sign a non-disclosure agreement ("NDA") when they come into the company and only those who have been appointed to this project will have access to the data. Feedback OY also has an NDA with the computer server hosting company and only those who have signed an NDA have access to the server and the database.

- The data server is in a secured room and only authorized personnel have access to it.

[4] EAS explained that each participant who provided feedback regarding the performance of one of the other participants can have access only to the information that he/she himself or herself provided. That is, they cannot have access to the final aggregate report that was provided to the participant receiving the aggregate feedback information.

- Maintenance of systems takes place under SSL- or SSH-secured connection. The data transfers to participants are sent by email in a zip file. The password to this file is then sent in a separate email.

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 an optional "Leadership Feedback" procedure established by the EAS in connection with its management courses.

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 data processing entails the collection and further processing of personal data as defined under Article 2(a) of the Regulation.

The EDPS points out that although feedback is provided in an anonymous format this does not mean that these data would be considered anonymous in the sense of Article (4)(1)(e) of the Regulation. In particular, Feedback OY at all times during the two-months retention period can verify who provided what feedback information. In addition, the aggregate reports, although contain no personal data of those providing the feedback, contain the personal data (evaluation data) of those receiving the reports.

Second, the personal data collected undergo automatic processing operations (Article 3(2) of the Regulation).

Third, the processing is carried out on behalf of EAS, 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, under paragraph (b), "processing operations intended to evaluate personal aspects relating to the data subject, including his or her ability, efficiency and conduct." The purpose of the notified processing operation is the evaluation of the applicants' leadership skills. First, applicants evaluate each other, anonymously as described above. Second, applicants may also evaluate themselves and discuss the feedback with their trainers. Therefore, the notified processing operation requires prior checking by the EDPS.

Notification and due date for the EDPS Opinion. The Notification was received on 2 September 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 42 days. Thus, the Opinion must be rendered no later than 15 December 2008 (3 November 2008 + suspension for 34 days + 8 days for comments).

True prior checking. The processing operation was notified before it was put into place, and therefore, constitutes a true prior checking case. Since prior checking is designed to address situations that are likely to present risks, EAS may only commence the processing operations after it has considered and implemented the recommendations set forth in this Opinion.

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.

With regard to the first issue, the privacy notice quoted above devotes a specific heading to this issue ("legal base") and lists a number of documents. Although none of them specifically provides for a leadership feedback procedure, the EDPS is satisfied that it is within the competence of EAS to offer such a procedure. With regard to the second issue, the EDPS is also satisfied and does not question that the notified processing operation is necessary and proportionate, considering also its optional and anonymous character, that EAS and Innotiimi have no access to any personal data and that the feedback data are used only for the benefit of the participants receiving feedback.

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. 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."

The adequacy, relevance and proportionality of the data collected for purposes of providing feedback must be evaluated on a case by case basis and may depend on the material taught at the specific management course.

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 3.7 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."

Accuracy may have different meanings in the context of the present processing operation. First, it is closely related to the issues of the adequacy and relevance of the questions asked when requesting feedback information. The more they are adequate and relevant, the more likely it is that participants will be able to respond in a way which is meaningful for purposes of providing useful feedback to each other. In this sense, accuracy must also be evaluated on a case by case basis and may depend on the material taught at the specific management course.

Second, accuracy depends on the subjective judgment of the participants who provide feedback, as well as the effort they put into answering the questions. Considering the optional character of the feedback procedure, that participants can choose themselves whom to invite to provide feedback, and that they can also decide themselves whether or not to share the final report with their trainer, the EDPS does not consider the subjectivity inherently involved in the feedback procedure as a major problem.

3.4. 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).

The EDPS does not question that the two-month retention period contemplated by EAS is reasonable.

3.5. Recipients and data transfers. The EDPS welcomes the fact that access to the data is strictly limited and serves for the benefit of the person receiving feedback only. The EDPS particularly welcomes that it is clearly stated that EAS and other EU Institutions have no access to the data.

The external specialist companies which are involved in the outsourced task of feedback provision are subject to Member States laws and thus, subject to Directive 95/46/EC. The EDPS welcomes that EAS also has a specific data protection clause in its contract with Innotiimi.

The EDPS further recommends that the clause would specifically refer to Article 23(2)(b) of the Regulation and Articles 16 and 17(3) second indent of Directive 95/46/EC (even if the contents of these provisions are already summarised in the text of the data protection clause itself).

Further, the EDPS recommends that the contract between EAS and Innotiimi, which already contains a data protection clause, will also include that

- Innotiimi is obliged to ensure that all its direct and indirect subcontractors will undertake the same obligations in writing and that
- the choice of Innotiimi's direct or indirect subcontractors is subject to the approval of EAS, which can be withheld in case the security of the data or maintenance of other data protection safeguards are not ensured.

3.6. 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.

The EDPS does not question the adequacy or sufficiency of the measures put in place by EAS to ensure the data subjects' rights of access and rectification. However, he points out that given the subjectivity involved in the feedback reports and the limited use that these reports are intended to serve, the room for rectification is relatively limited. For example, a person providing feedback may later realize that he made a mistake in providing feedback (e.g. noted the worst marks instead of the best ones for his course colleagues as he negligently thought mark 1 meant best and 5 meant worst or the other way around). Or a confident participant who received an aggregate report reflecting poorly on his skills may request Feedback OY to check again whether there was not a computational error in compiling the report.

3.7. 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 with regard to the participants' responses to the feedback questionnaires. Article 12 applies when the data have not been obtained from the data subject, which is the case with regard to data contained in the aggregate reports.

The EDPS welcomes that the privacy statement is posted on the website of EAS and that a link is provided to it in the documentation received by course participants. As an additional recommendation, the EDPS suggests that at least the following minimum information would also be provided among the printed materials in the information package to guarantee the fairness of the processing:

- the feedback procedure is entirely optional and anonymous,
- all data are processed solely for the purposes of providing feedback,
- will be deleted within 2 months, and that
- all data are processed by subcontractors and that EAS or others within the Institutions have no access to any data.

3.8. 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 suggest doubts about the adequacy of the security measures. Note, however, the recommendations made regarding outsourcing in Section 3.5 above.

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 3.8 are fully taken into account. The recommendations of the EDPS include the following:

- The contract between EAS and Innotiimi, which already contains a data protection clause, should also include that (i) Innotiimi is obliged to ensure that all its direct and indirect subcontractors will undertake the same obligations in writing and that

(ii) the choice of Innotiimi's direct or indirect subcontractors is subject to the approval of EAS, which can be withheld in case the security of the data or maintenance of other data protection safeguards are not ensured.

- In addition to the detailed privacy statement on the EAS website, at least the following minimum information should also be provided among the printed materials in the information package: (i) the feedback procedure is entirely optional and anonymous, (ii) all data are processed solely for the purposes of providing feedback, (iii) data will be deleted within 2 months, and (iv) all data are processed by subcontractors and that EAS or others within the Institutions have no access to any data.

Done at Brussels, on 15 December 2008

(signed)

Peter HUSTINX
European Data Protection Supervisor