

Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Commission concerning "Leadership Effectiveness"

Brussels, 7 April 2010 (Case 2010-0002)

1. Proceedings

On 4 January 2010, the European Data Protection Supervisor (EDPS) received from the Data Protection Officer of the European Commission a Notification for prior checking concerning the processing operation "Leadership Effectiveness".

The EDPS requested additional information on 27 January and 17 March 2010. The responses were received on 12 February and 29 March 2010 respectively. The EDPS sent the draft opinion to the Data Protection Officer for comments on 30 March 2010, which were received on 7 April 2010.

2. Facts

- Purpose of processing

The purpose of processing is to allow participants in Ispra Site Management Directorate (ISM) 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. The exercise is conducted with the use of a web-based tool: the "LeaderView 360". 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 person involved. Participation in this activity by the person concerned and their colleagues is entirely voluntary (no negative consequence will derive if the participant chooses not to take part in the web-based test).

- Description of Emotional IntelligenceView 360 degree assessment

LeaderView360 assesses 35 critical leadership behaviours in 7 core competencies required for effective leadership in today's organisations: *Planning, Problem solving Controlling, Self management, Managing relationships, Leading, Communicating* LeaderView360 is aimed at middle to senior managers and can help to focus on enhancing overall leadership effectiveness.

- Description of the processing activity

Firstly, the participant will receive full information from the ISM training manager about the leadership effectiveness programme and the nature and steps of data processing. They are invited to choose whether they agree to participate. If they choose so, they propose a list of assessors including name, internal postal address, electronic address and role (peer, senior or direct report -staff managed and supervised by the participant-) to the ISM training manager. The assessors will then receive full information about the programme, the nature and steps of data processing, and furthermore, they are invited to choose whether or not to participate. The participants are asked to indicate whether they would prefer to receive the final report from the exercise individually, or whether it could be shared with the coach from the contractor. There is no obligation from the participant to share the final report.

The data of the course participants and those colleagues participating as assessors in the exercise will be sent to the contractor, Greenhouse Group.

Secondly the subcontractor, Consultingtools, will provide the contractor with a list of anonymous user accounts (user ID) for participants, and assessors (seniors, peers and direct reports).

The third data processing arises when the participants and the assessors need to provide input. Both the participants and the assessor will receive a letter from the contractor with the link to the user entry page for the online questionnaire with the user ID and password. In addition, the letter to the assessors will also include the name of the participant to assess.

The data collected, to rate the observed leadership behaviour, take the form of the following 5-point scale: (1 Needs Considerable Development, 2 Needs Development, 3 Competent, 4 Effective, 5 Very Effective, and NA Not Observable or Not Applicable). The participant and assessor can choose to complement the numerical data with individual comments. The participant and assessor have the option to provide these comments or not.

The fourth data processing arises when the subcontractor processes the anonymous¹ data supplied by the participants and their assessor. The numerical data are amalgamated into a single report. This is done automatically by the IT system. This anonymous² report together with the user ID is then sent to the contractor. The contractor identifies the participant by the user ID and then sends the report directly to the participant as letter by post or shares the report during the following individual coaching sessions with the participant, as requested. Only in the phase, where the contractor identifies the participant and sends the report, the contractor has access to the report.

- Data subjects

The data subjects concerned are the officials and other Commission Staff participating in courses organised by the Ispra Site Management Directorate.

- Categories of data

The categories of personal data are the following:

¹ The subcontractor can not identify itself who is the person that has provided the input. The contractor can make such identification.

² The report issued by the sub-contractor does not identify the data subjects.

- Name, first name, electronic address, internal postal address; these personal data are held both by ISM and the contractor.

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

- Information provided by assessors on their perception of the participant's management and leadership skills in areas such as performance management, change management, issue management and people management; is held anonymous by the subcontractor. This information is rendered anonymous and amalgamated into a feedback report, except for the information provided by the senior, considering the fact that normally each participant has only one senior manager where he refers to. The contractor has access to the report.

- Information to the data subjects

The data subjects will be provided by the ISM training manager with the following information:

- the identity of the controller;
- the purposes of processing;
- the recipients of the data;
- the fact that the reply to questions is purely voluntary
- the existence of the right of access and rectification;
- the legal basis of the processing
- the time limits for storing the data;
- the right to have recourse at any time to the EDPS.
- security measures

- Procedures to grant rights to data subjects

The data subject can use the functional mailbox:

JRC-ISD-Suggestions-and-Complaints@ec.europa.eu to exert his/her rights.

Data subjects concerned may send a request to ISM to indicate any changes to their personal data (for the data held by the ISM, that is, the list of interested participants and assessors).

For the data held by the contractor, the data subject will have to exercise the right of access and rectification directly with the contractor. The data subject may also choose to send the request to the ISM. In this case, the ISM will forward the request to the contractor to arrange for the access and possible rectification as necessary. A functional e-mail address has been established for this purpose.

Colleagues providing input may also 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. The same procedure as for the participant will be followed.

The answer from the contractor is sent directly to the data subject. The data subject may obtain a copy of his or her personal data as registered by the contractor, to allow them to check that the information they supplied was accurately recorded. The contractor would do this directly with the participant without passing through the data controller to ensure that the

controller has no access to any data. The controller will be informed by the contractor that he has fulfilled the request, without including further personal data.

- Type of processing (automated and/or manual)

The processing activity conducted is automated.

- Storage media

Electronic and paper media. The agreements (paper form) to participate in the programme including the proposed list of assessors, and the agreements to participate as assessor in the programme are stored by ISM training manager in a locked cabinet.

- Recipient(s) of the Processing

The ISM Contractor

The contractor of the ISM receives the data. The contractor will receive from the ISM, a list of participants and assessors who expressed interest in taking part in this exercise.

Furthermore, if the participant so wishes, the course facilitator (trainer) also receives the amalgamated report of the feedback. The trainer is not part of the ISM, but part of the contractor.

- Retention policy

Data (electronic and paper media) will be deleted 3 month after the report has been sent to the data subject.

- Time limit to block/erase data on justified legitimate request from the data subjects

Upon a justified request by the data subject the personal data will be modified/blocked within 14 days.

- Security and organisational measures

(...)

3. Legal aspects

3.1. Prior checking

Applicability of Regulation (EC) 45/2001: The assessment done with the use of the "Leader View 360" web-based test tool constitutes processing of personal data ("*any information relating to an identified or identifiable natural person*" - Article 2 (a) of the Regulation). The feedback received by the participant will not reveal the way in which the colleagues completed the answers ("who said what"). Nevertheless, these data can not be considered "anonymous" because the contractor has the possibility to link the answers with the colleagues who have produced them (see Recital 26 of Directive 95/46/EC: "*(...); whereas, to determine whether a*

person is identifiable, account should be taken of all the means likely reasonable to be used either by the controller or by any other person to identify the said person; (...)". Furthermore, as mentioned in point 2 above, the answers from the senior manager will easily identify the data subject from whom they emanate, because normally each participant has only one senior manager where he refers to.

The EDPS recommends that the Commission explores the possibilities for making the use of this web-tool an anonymous exercise from the processor perspective (the contractor in this case). In this regard, variables such as IT development, procedures and cost will have to be taken into account.

The data processing is performed on behalf of a former "Community institution" in the exercise of activities which fall within the scope of former "Community law" (Article 3 (1) of the Regulation).³

It has to be noted that even though the Commission has no access to the data processed by the contractor (data used for performing the "LeaderView 360"), the contractor has to act according to the instructions given by the Commission. The Commission is the data controller of this processing activity because it determines the purposes (as specified under point 2 above) and the means (the use of the web-based tool) - Article 2 (d) of the Regulation. The contractor is therefore not authorised to undertake any further processing activity beyond what is determined by the Commission and specified in the contract.

The processing of the data is done electronically. Therefore, Regulation (EC) 45/2001 is applicable.

Grounds for prior checking: According to Article 27 (1) of the Regulation, "*processing operations likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purpose shall be subject to prior checking by the European Data Protection Supervisor*". Article 27 (2) of the Regulation contains a list of processing operations that are likely to present such risks. This list includes Article 27 (2) (b): "*processing operations intended to evaluate personal aspects relating to the data subject, including his ability, efficiency and conduct*". The assessment done with the use of the web-based tool, although not part of a formal appraisal, clearly represents such a processing operation and is therefore subject to prior checking by the EDPS.

Deadlines: The notification of the DPO was received on 4 January 2010. 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 36 days to require additional information and to allow for comments from the data controller. Consequently, the present opinion must be delivered no later than on 8 April 2010..

3.2. Lawfulness of the processing

Article 5 of Regulation 45/2001 provides criteria for making processing of personal data lawful. One of the criteria provided in Article 5 (a) is that the "*processing 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*

³ The concepts of "Community institutions and bodies" and "Community law" were abolished by the entry into force of the Lisbon Treaty on 1st December 2009. Article 3 of Regulation 45/2001 must therefore be read in the light of the Lisbon Treaty.

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).

Article 2 of Commission Decision of 7 May 2002 on staff training refers to the objectives of training activities: *"Staff training in the Commission shall have as fundamental objective to expand and improve individuals' competencies so that each staff member can contribute optimally to achievement of the Institution's goals. At the individual level, training should serve to improve professional effectiveness and should contribute to every staff member's sense of fulfilment, belonging and commitment at the workplace. By developing relevant knowledge, skills and attitudes, training should further help individuals to make desired career moves, both laterally (mobility) and vertically (promotion, including change of category)"*. Nevertheless, even if the assessment conducted in the context of the web-based tool might be useful, it is not "necessary" for the performance of the task described in the mentioned rule. This is demonstrated by the fact that participation in this activity is optional.

Therefore, the processing activity under analysis has to be based on Article 5(d) of the Regulation, which states that personal data may be processed only if *"the data subject has unambiguously given his or her consent"*. The *"data subject's consent"* is defined in Article 2(h) of the Regulation as follows: *"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 the present case, the data subject is specifically informed about the processing activity in the light of Article 11 of the Regulation and the fact that he or she is free to participate or not in the exercise. Furthermore, no negative consequences can affect the data subject if he or she decides not to participate.

3.3. Data Quality

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 information presented to the EDPS on the data processed appears, *prima facie*, to meet those requirements.

The controller has to instruct the processor to respect this principle in regard to the web-tool's questions.

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"*. As indicated above, an important part of the information processed is provided by persons other than the participant (colleagues). In this respect, it is important that the data subjects (participant and colleagues) can make use of their rights of access and rectification to ensure the accuracy of their personal data processed (cf. point 3.6 in detail). In any event, it has to be noted that most of the data processed is of a subjective nature, and therefore, it is difficult to evaluate the "accuracy", particularly in the context of the present case.

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 3.7)

3.4. 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"*.

The EDPS is of the view that the three months retention period is reasonable *vis-à-vis* the purpose of the processing.

3.5. Transfer of data

In line with Article 8 of the Regulation, personal data shall be transferred to recipients subject to the national law adopted for the implementation of Directive 95/46/EC *"(...) (b) if the recipient establishes the necessity of having the data transferred and if there is no reason to assume that the data subject's legitimate interests might be prejudiced"*.

The necessity of having the data transferred is proven by the fact that if the personal data is not communicated to the provider of the web-test and the trainer (contractor), these recipients are not able to perform the tasks requested by the controller with the consent of the data subject. As to the legitimate interests of the data subject, compliance with the data quality principle, as well as with the obligations of the controller and the rights of the data subject, as described in the present Opinion, ensure that there is no reason to assume, in principle, that they might be prejudiced. Furthermore, the data can not be used in any evaluation procedure by the institutions and bodies, and the data subject has given his consent to the processing. As a consequence, there is no reason to believe that the transfer would affect the data subject's legitimate interests.

3.6. Right of access and rectification

Article 13 of Regulation 45/2001 grants the data subject the right of access to personal data being processed. Article 14 of Regulation 45/2001 provides a right to rectification without delay of inaccurate or incomplete data.

As described in point 2 above, procedures have been established to grant these rights to the data subjects. It has to be noted that, when the request of access will be done directly to the functional mailbox of the Commission, the Commission will have to forward the request directly to the contractor, and will not receive an answer with the content of it. The contractor has nevertheless to inform Commission that it has provided access and proceeded to rectify the data, if appropriate. The data subjects should also have the possibility to exercise this right directly with the contractor. Therefore, the EDPS recommends the controller to offer also this possibility.

Regarding the right of rectification, the EDPS points out that given the subjectivity involved in the feedback reports and the purpose that these reports are intended to serve, the room for rectification is relatively limited. For example, the person concerned providing feedback may later realize that he or she made a mistake in providing feedback. Therefore, a case-by-case analysis is recommended should there be a request for rectification.

3.7. Information to the person concerned

Pursuant to Articles 11 and 12 of Regulation (EC) No 45/2001, those who collect personal data are required to inform individuals that their data are being collected and processed unless the data subject already has this information. Individuals are further entitled to be informed of, inter alia, the purposes of the processing, the recipients of the data and the specific rights that individuals, as data subjects, are entitled to.

The EDPS received a copy of a draft Privacy Statement, where most of the requirements are specified. However, some further points have to be mentioned/modified, as follows:

- the statement has to specify that the data subject will suffer no negative consequences if he or she decides not to participate in the web test;
- regarding the "purpose of processing", it has to be clarified that "anonymous feedback" means that the colleagues who have contributed will not be identified, neither in the feedback received by the participant, nor in the feedback received by the trainer (when they so chose);
- the subcontractor does not process "anonymous data" because the contractor is able to "identify" the data subjects to which it relates. Therefore, any reference to "anonymity" has to be deleted;
- taking into account the way in which the system is set up so far, the following statement is not appropriate: "The 360° feedback is (...) anonymous, (...)" , therefore, this part has to be amended;
- it has to be mentioned that the course facilitator (trainer) is also a contractor to the Commission, therefore, another recipient;
- as to the right of access and rectification, it has to be mentioned, that even if the request of access could be made directly to the Commission, the Commission will forward the information to the contractor, and will not receive an answer with the content of it. Furthermore, the data subjects have to be informed about the means to contact the contractor (e.g. e-mail address) in case they decide to exercise their rights directly with him;
- there is no obligation to provide information about the security measures adopted. Therefore, the EDPS recommends the deletion of the details related to the specific security measures adopted.

3.8. Processing of personal data on behalf of the controller

In the present case, the processing activity is mainly conducted by processors (contractor and sub-contractor), on behalf of the Commission. Article 23 of the Regulation stipulates that: *"1. Where a processing operation is carried out on its behalf, the controller shall choose a processor providing sufficient guarantees in respect of the technical and organisational security measures required by Article 22 and ensure compliance with those measures.*

2. The carrying out of a processing operation by way of a processor shall be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:

(a) the processor shall act only on instructions from the controller;

(b) the obligations set out in Articles 21 and 22 shall also be incumbent on the processor unless, by virtue of Article 16 or Article 17(3), second indent, of Directive 95/46/EC, the processor is already subject to obligations with regard to confidentiality and security laid down in the national law of one of the Member States.

3. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in Article 22 shall be in writing or in another equivalent form".

The EDPS received a copy of the draft contract with the contractor. The EDPS recommends, nevertheless, the inclusion of a clause specifying that the applicable law for the obligation of confidentiality and security of the processing is the law of the Member State where the processor is established, in this case, Belgium. Furthermore, the clause has to include the following wording in order to be in line with Article 23:

"Where the present contract requires the processing of personal data, the contractor may act only on instruction from the data controller (the official responsible for supervising the performance of the contract and appointed by the Commission), notably as concerns the purposes of the processing, the categories of data which may be processed, the recipients of the data and the means by which the data subject may exercise his/her rights.

The data are confidential within the meaning of Regulation (EC) No 45/2001 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by Community institutions and bodies and on the free movement of such data. The contractor will limit access to the data to staff strictly necessary for the performance, management and follow-up of the contract.

The contractor undertakes to take appropriate technical and organisational security measures in view of the risks inherent in the processing and of the nature of the personal data concerned with the aim of:

- (a) prevent any unauthorised person from gaining access to computer systems processing personal data;*
- (b) prevent any unauthorised reading, copying, alteration or removal of storage media;*
- (c) prevent any unauthorised memory inputs as well as any unauthorised disclosure, alteration or erasure of stored personal data;*
- (d) prevent unauthorised persons from using data-processing systems by means of data transmission facilities;*
- (e) ensure that authorised users of a data-processing system can access no personal data other than those to which their access right refers;*
- (f) record which personal data have been communicated, at what times and to whom;*
- (g) ensure that it will subsequently be possible to check which personal data have been processed, at what times and by whom;*
- (h) ensure that personal data being processed on behalf of third parties can be processed only in the manner prescribed by the contracting institution or body;*
- (i) ensure that, during communication of personal data and during transport of storage media, the data cannot be read, copied or erased without authorisation;*
- (j) design its organisational structure in such a way that it will meet the special requirements of data protection.*

In the event of any infringement of these clauses, the institution may terminate the contract immediately without prejudice to any possible damages.

The contractor is required to ensure that its obligations in matters of data protection are transferred to any sub-contractors."

3.9. Security measures

According to Article 22 of Regulation (EC) No 45/2001, *"the controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks presented by the processing and the nature of the personal data to be protected"*.

These security measures must *"in particular prevent any unauthorised disclosure or access, accidental or unlawful destruction or accidental loss, or alteration, and to prevent all other unlawful forms of processing"*.

The EDPS has no reason to believe that the measures mentioned are no adequate in light of Article 22 of the Regulation.

4. Conclusion:

There is no reason to believe that there is a breach of the provisions of Regulation 45/2001 provided the above considerations are fully taken into account. In particular, the ISM should:

- explore the possibilities for making the use of this web-tool an anonymous exercise. In this regard, variables such as IT development, procedures and cost will have to be taken into account;
- instruct the processor to respect the data quality principle (adequacy, relevance, proportionality) in regard to the web-tool's questions;
- offer the data subjects the possibility to exercise their rights directly with the contractor;
- conduct a case-by-case analysis should there be a request for rectification;
- amend the Privacy Statement as recommended above;
- include a clause in the contract with the processor specifying that the applicable law for the obligation of confidentiality and security of the processing carried out by the controller is the law of the Member State where the processor is established, in this case, Belgium; as well as include the recommended wording to the data protection clause as mentioned above.

Done at Brussels, 7 April 2010

(signed)

Peter HUSTINX
European Data Protection Supervisor