

## **Opinion on the notification for prior checking received from the Data Protection Officer of the European Parliament regarding a self-assessment tool “PerformanSe”**

Brussels, 07 April 2014 (Case 2013-0772)

### **1. Proceedings**

On 28 June 2013, the European Data Protection Supervisor (“EDPS”) received from the Parliament’s Data Protection Officer (“DPO”) a notification regarding “PerformanSe”: a self-assessment tool, offered via the Parliament’s Professional Training Unit.

On 15 July 2013, the EDPS sent the Parliament's DPO some additional questions for further information. Replies were received on 23 July. The EDPS forwarded some final queries on 13 September, and a response was provided on 4 December 2013.

The EDPS sent a draft Opinion to the Parliament for comments on 25 March 2014. The Parliament replied on 3 April 2014.

### **2. The facts**

#### **Data subjects**

The data subjects of the processing operation are EP staff members (heads of unit or service level) who are voluntarily participating in the self-assessment questionnaire.

#### **Purpose**

The purpose of the processing operation is to allow participants to obtain feedback in the form of two feedback reports and, upon request, a feedback session by telephone to establish their managerial tendencies and main motivation levers in their working environment. The assessment may be a pre-training for middle management or may be taken separately. The data will not be used to evaluate the data subjects in any way.

#### **Legal base**

- Article 24(a) of the Staff Regulations of Officials of the European Union and Articles 11, 81 and 127 of the Conditions of employment of other servants of the European Union;
- Internal rules on professional training for EP staff.

## **Outsourcing**

The Parliament outsources the processing operation PerformanSe to a private company (the contractor) called Bick CONSORTIUM established in an EU Member State. This company subcontracts the organisation of the PerformanSe procedure to another private company, also established in an EU Member State, called PerformanSe S.A.S (the sub-contractor).

In its contract with the external contractor, the Parliament included a specific data protection clause, that the contractor may act only on instruction from the controller with regard to, in particular, the purposes of the processing, the categories of data processed, the recipients of data and the means by which data subjects may exercise their rights. Furthermore, the contract explicitly mentions that the Parliament must be consulted by the external contractor in advance in order to verify if the direct or indirect subcontractor(s) satisfy the requirements of the legislation on data protection. The contract also makes reference to Article 23(2)(b) of the Regulation, and the fact that the contractor binds himself to adopt, or to have adopted by its direct or indirect sub-contractors, technical and organisational measures.

"PerformanSe" is a web-based tool. As a first step, Parliament staff members make contact with the Professional Training Unit which sends them an e-mail in order to inform them about the process and notably the fact that personal data will be collected and sent to a processor. (In future, the Parliament also plans to also attach the privacy statement to this email.) If the staff members still wish to enrol, the Unit provides their contact details to the sub-contractor enabling the company to send them an invitation containing a link to a password creation page, which is a mandatory step before being able to access the questionnaire. A subsequent message with further details is sent when emailing the link to the questionnaires. In this e-mail, they are told that following completion of the questionnaire they will be contacted by PerformanSe to arrange a telephone feedback appointment.

## **Nature of the data to be processed**

The questionnaire takes the form of a self-assessment, and the participants may answer questions associated with their professional sphere, behavioural tendencies and motivation levels. The data processed are the following:

- identification details (name, given name, electronic address, password); and
- behavioural data (answers from the data subject to the questionnaire in areas such as change management, organisational management, team management and personal resources).

Once the data subject provides input on the above questions, the information collected is converted into numerical data, which are automatically amalgamated into two reports (which are not anonymous). Participants are then able to freely access these reports through their password.

Data subjects are also informed that they may receive an additional feedback session by telephone, if required. This will be based on analysis, by the PerformanSe consultant, of the data subject's reports. No deadline is set for answering or requesting telephone feedback sessions.

## **Information to the data subjects**

When the Parliament sends an e-mail to the data subjects informing them about PerformanSe, the e-mail will contain a link to the privacy statement. The EDPS received a copy of the privacy statement.

## **Recipients of the data**

The sub-contractor of the Parliament receives the numerical data, along with its IT officers, who may intervene in case of technical problems. The latter may also have access to the questionnaires and the data subjects' replies in some cases. This is because they may need to assist users in case of any IT-related problems during the self-assessment process, and in case of report generation.

## **Data subjects' rights**

Staff members concerned may submit a demand for access, rectification, blocking, erasure or objection to the controller via a functional email, who will pass it onto the sub-contractor. Following any such request, along with proof of identity, they may obtain a copy of their personal data as registered by the sub-contractor. This will allow the data subject to check the accuracy of the data and perform any necessary changes.

## **Data retention period**

All data (including numerical data, feedback reports and questionnaires) will be retained for 90 days after completion of the questionnaire and then deleted by PerformanSe S.A.S.

## **Data storage and security**

[...]

## **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 the European Parliament, in the exercise of activities which fall within the scope of EU law. The processing of the data is automatic, since PerformanSe is a web-based tool and data subjects have individual access.

**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) 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 intends to evaluate the potential managerial abilities and conduct (motivation and behaviour at work) of data subjects, since

the participants are provided by the sub-contractor with feedback in the form of two feedback reports and upon request, with a feedback session by telephone. The notification should therefore be subject to prior-checking by the EDPS under Article 27(2)(b) of the Regulation.

**Ex-post prior checking:** Since prior checking is designed to address situations that are likely to present certain risks, the Opinion of the EDPS should be given prior to the start of the processing operation. In this case, the EDPS regrets that the processing operation has already been established. However, the EDPS underlines that all his recommendations given in the present Opinion should be duly implemented before the next PerformanSe assessment is carried out by the Parliament.

**Notification and due date for the EDPS Opinion:** The notification of the DPO was received on 28 June 2013. According to Article 27(4) of the Regulation, the EDPS Opinion must be delivered within a period of two months. However, this only applies to true prior checks; ex post prior checking cases are dealt with on a best effort basis.

### 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 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 (...)*".

In the present case, **the legal basis** for the processing can be found in the legal provisions indicated in the facts.

As to **the necessity** of the processing, paragraph 27 of the preamble to the Regulation should be considered, 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 in the present case falls within the framework of the training policy of the institution concerned. It can be considered as necessary, since staff members can receive feedback about their behavioural tendencies and main motivation levels within their working environment. The processing therefore constitutes a tool which aims to train and evaluate the staff members who complete the questionnaire. In this respect, it can be considered as an instrument which intends to ensure the sound management and functioning of the institution where the data subject works.

### 3.3. 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*".

The EDPS notes that the data as described in the facts seem to 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".*

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 information from the participants. The more adequate and relevant they are, the more likely it is that participants will be able to respond in a way which is meaningful so that they can be provided with useful feedback by the sub-contractor.

Second, accuracy depends on the subjective judgment of the participants who provide information, as well as the effort they put into answering the questions. Considering the optional nature of the procedure - that staff members can participate on a voluntary basis and that, if they wish, they may receive individual telephone feedback - it seems that the system itself gives a reasonable guarantee of data quality.

Furthermore, the rights of access and rectification are available to the data subjects, in order to make the information they provide as comprehensive as possible. These rights constitute the second means of ensuring that data concerning the data subjects are accurate and updated (see section 3.6 on "the rights of access and rectification").

**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 3.7 on "the right of information").

### **3.4. Conservation of data**

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*".

On the basis of the information available, the EDPS considers the 90 days retention period necessary and proportionate in light of Article 4(1)(e) of the Regulation.

### **3.5. 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 EU institutions or bodies (based on Article 7), (ii) to recipients subject to Directive 95/46 (based on Article 8), or (iii) to other types of recipients (based on Article 9).

It is noted that no Parliament unit has access to the data related to the questionnaire. There is no transfer.

### **3.6. 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.

Currently, the privacy statement does not appear to inform the data subjects of any time limits for requests and responses. The EDPS would recommend that this information is added to the document for the sake of clarity.

### **3.7. Right of information**

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 some from other persons, which is the case with regard to the data contained in the feedback reports.

In the present case, the EDPS notes that the privacy statement contains almost all necessary information in conformity with Articles 11 and 12 of the Regulation.

Nevertheless, the EDPS considers that the privacy statement does not inform the data subjects that those wishing to discuss their results during a telephone feedback session with the sub-contractor may do so, but presumably only within 90 days after completion of the questionnaire, as that is when the data are deleted. As analysed in point 3.1, the fact that the participants may receive feedback, hence evaluation by the sub-contractor, is the reason why the processing operation under analysis has been prior-checked by the EDPS. Such information, including the time limit within which they can obtain feedback, should therefore be mentioned in the privacy statement.

Furthermore, the EDPS notes that the privacy statement does not explicitly point out that the Parliament will not have any access to the data. It is suggested that this clarification is added to the text. The Parliament should also provide the EDPS with confirmation that, with immediate effect, privacy statements will be added to the initial email sent to data subjects from the Professional Training Unit.

### **3.8. Processing on behalf of the controller**

Article 2 (e) of the Regulation 45/2001 states that *"processor' shall mean any natural or legal person, public authority, agency or any other body which process personal data on behalf of the controller"*. Article 23 of the Regulation stipulates on one hand, the role of the processor and on the other hand, the obligations of the controller in ensuring sufficient guarantees in respect of the technical and organisational security measures, along with ensuring compliance with those measures.

The EDPS welcomes that the Parliament, in its contract, has included all necessary clauses and rules, as described in the facts, which are in conformity with Article 23(1) and (2) of the Regulation. In addition, all PerformanSe engineers are required to sign confidentiality statements before processing the data.

### **Conclusion**

There is no reason to believe that there is a breach of the provisions of the Regulation, provided that the additional information, as recommended by the EDPS in points 3.6 and 3.7, is indicated in the privacy statement.

Brussels, 07 April 2014

Signed

Giovanni BUTTARELLI  
Assistant European Data Protection Supervisor