Opinion on the notification for prior checking received from the Data Protection Officer of the Council regarding the eHEST training (Computer based Hostile Environment Security Training)

Brussels, 22 October 2008 (Case 2008-0387)

1. Proceedings

On 23 June 2008, the European Data Protection Supervisor received a notification for prior checking from the Data Protection Officer of the Council, concerning a data processing related to the eHEST training (Computer based Hostile Environment Security Training).

The EDPS requested additional information on 3 September 2008 and 11 September 2008, and the answers were received on 12 September 2008. On 18 September 2008, the draft Opinion was sent to the controller for comments, and the feedback was received on 7 October 2008. On 7 October 2008 the DPO of the Council also transmitted a modified version of the notification. Modifications were related to the categories of the data subjects, procedures to grant rights of data subjects and to the storage media of data.

2. Facts

Purpose of the processing

The purpose of the eHEST training is to raise the security awareness in order to mitigate risks for all personnel (officials and other agents of the EU Institutions, Member States and third countries) deployed on EU-led missions (European Security and Defence Policy - EUDP or/and European Union Special Representative - EUSR) outside the EU in an operational capacity under Title V of the EU Treaty.

The eHEST training is designed to mitigate against the risks of deployment to a hostile environment and to protect the General Secretariat of the Council, in case of a serious incident, from any claims of breach of duty of care or negligence.

The eHEST training is supposed to serve as an EU-wide security training standard which will be applied as a norm for all EU-led missions.

Description of the processing

The eHEST is a web-based training application with an automated evaluation function. Users are required to submit their data as part of the online registration process. The eHEST training programme envisages three tests. Only if the two first tests are passed with success, the final test can be accessed. The final test leads to certification which is a condition to the deployment in some areas.

The controller of the processing is the head of the Directorate Security Office.

Legal basis

According to the notification the specific legal base for the processing operation can be found in the Council document 9490/06 concerning the draft EU's policy which applies with regard to personnel deployed outside the EU in an operational capacity under title V of the TEU. This document provides an overall policy framework for deployment or operation outside the EU (cf. paragraph 36).

According to the notification other relevant legal bases include:
- Article 14 of the TEU;
- Article 207, paragraph 2, of the EC Treaty
- Article 23, paragraph 2, sub-paragraph 2 of the Council's Rules of Procedure (Council Decision 2006/683/EC) stating that "*Under its authority the Secretary-General and the Deputy Secretary-General shall take all the measures necessary to ensure the smooth running of the General Secretariat*."

Automated / manual processing operation

The processing envisages a mixed manual/automated process. The identification data are introduced to the system by the data subject and the request to create an account is issued. Then, the registration process is evaluated manually by the GSC Security Office and the registration request is either approved or rejected. Only those applications that are validated by the Security Office shall be granted access to the system. On the contrary, the grading of the training programme is registered automatically. Answers to the questions are automatically evaluated by the system without manual intervention. The final certificate is generated automatically for the candidate whilst at the same time notifies the eHEST secretariat within the GSC of the pass. Finally, the results and answers to the questions are to be stored in the eHEST electronic database.

Categories of data subjects

Officials and other agents of the Council and of other EU institutions and Member State Delegates.

Data categories

The categories of data collected are the following: surname, name, email address, organisation (employer), mission type and destination (ESDP, EUSR mission), course results and certification. The final certificate contains the name, the date of passing the course and the final result (course passed).

Information to be given to data subjects

Information is supplied to the data subjects in a Privacy Disclaimer during the registration process before the data subject enters his or her data.

The Privacy Disclaimer provides information about:

- The identity of the data controller;
- The purposes for which personal data are processed ("*validating the user registration and facilitating the follow-up of the electronic training services offered*")
- Categories of personal data collected;
- Categories of recipients of personal data;
- The possible consequences of failure to reply/to successfully pass the evaluation ("*failure to supply the GSC with your correct personal data or failure to successfully complete the eHEST course may have an impact in your deployment in the field*");
- The rights of data subjects to access and how to assert that right; and
- The conservation of data.

Procedures to grant rights of data subjects

In general, implementing rules relating to Regulation (EC) No 45/2001 contained in the Council decision of 13 September 2004 provide for the rights of data subjects in its Section 5 (Articles 16-24). There are no specific rules established for this particular processing operation.

The controller specifies that on request from the data subject, the controller can supply a detailed breakdown of his/her answers question by question.

The controller also specifies that requests to the GSC Security Office to block or delete the data will be treated immediately.

Retention policy

The user and training data are retained in the system for a variable period of time, which is evaluated on the case by case basis according for instance to duration of the mission, the length of the contract with the data subject, the length of the data subject's insurance coverage, or the need to produce training statistics.

Recipients of data

The data are transferred to the GSC Training Department (DGA 1A) and to the service "Consultation/modification rights" (DGA 5 "Information and Communication System"). The DGA 5 services have the possibility to access the personal data only in the context of system maintenance and functional support.

The final certificate of passing the eHEST test is provided to the data subject only.

No transfer is foreseen to the recipients outside the GSC.

Security measures

[...]

3. Legal issues

3.1. Prior checking

The prior checking relates to the processing of personal data carried out by a Community institution, in the framework, at least partially, of Community law (Article 3.1 of the Regulation (EC) 45/2001). In fact, even if the eHEST training is provided to personnel deployed on EU-led missions under Title V of the TEU and not under the Community Law, it constitutes a professional training activity which is a part of a human resources management by the services of the Council. This training is obviously not an operational activity conducted under the Title V of the TEU but a human resources management activity whose legal basis is provided by the Community Law (see section 3.2 below).

The data are processed mainly by automatic means (Article 3.2 of the Regulation).

As a consequence, the Regulation (EC) 45/2001 is applicable.

Article 27 of Regulation subjects processing operations presenting specific risks to the rights and freedoms of data subjects to prior checking by the EDPS. Article 27(2) contains a list of processing operations likely to present such risks.

Article 27(2)(b) states that the processing operations likely to present such risks include "*processing operations intended to evaluate personal aspects relating to the data subject, including his or her ability, efficiency and conduct*".

According to the notification received, eHEST is not a simple training but includes also an evaluation module and a final certification. It is a compulsory training for some categories of staff and the result of the evaluation may have an important impact for the carrier of a staff member concerned.

Therefore, processing operations are intended to evaluate personal aspects including ability. The aim of the operation is thus to evaluate the data subject. As such, eHEST must be understood as falling within the scope of Article 27(2)(b) of Regulation (EC) No 45/2001.

The notification for prior checking was received by the EDPS on 23 June 2008. According to Article 27.4, the present Opinion must be delivered within a period of two months. The Opinion should therefore be issued not later than on 22 October 2008 (including 22 days of suspension, plus the month of August).

3.2. Lawfulness of the processing and legal basis

Regulation (EC) 45/2001 provides that processing of personal data must find grounds in Article 5 in order to be considered as lawful.

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 the processing is instituted to serve a specific task provided for in a Treaty provision or another legal instrument adopted on the basis of the Treaties. The second issue is whether the activity at stake is carried out in the public interest. The third issue is to determine whether the processing operation is indeed necessary for the performance of such a task.

There is a general power of organisation of the services of the institution. The legal basis for this general power is Article 23, paragraph 2, sub-paragraph 2 of the Council's Rules of Procedure (Council Decision 2006/683/EC) stating that "*Under its authority the Secretary-General and the Deputy Secretary-General shall take all the measures necessary to ensure the smooth running of the General Secretariat*."

Specifying this general legal basis, the Council document 9490/06 provides an overall policy framework for deployment or operation outside the EU. Its paragraph 36 states that *"The General Secretariat of the Council, acting under the responsibility of the Secretary-General/High Representative assisted by the Deputy Secretary-General, will: [...] (i) ensure that appropriate measures are taken for the security of personnel not assigned to a crisis management operation visiting the field under the administrative authority of the Secretary-General/High Representative to a crisis or potential crisis area. Such measures include, but are not limited to, relevant training, [...]"*

The eHEST training falls within the legitimate exercise of official authority vested in the institution, provided that it can reasonably be considered to be necessary and that it makes a useful contribution to the running of the institution. Also, the preamble to the Regulation explicitly 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*" (recital 27).

Then, the processing of personal data in the present context can be considered as an activity conducted in the public interest.

Furthermore, the necessity of the processing has to be evaluated in the light of the purpose. In the present case, the processing is, in principle, necessary for the purposes described.

3.3. Data Quality

According to Article 4(1)(d) personal data must be *"adequate, relevant and non excessive in relation to the purposes for which collected and/or further processed".*

Given that only limited identification data are collected, this rule is respected in the present case.

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."*

This principle is very much connected to the exercise of the right of access, rectification, blocking and erasure (see section 3.7. below).

Lastly, data must also be *"processed fairly and lawfully"* (Article 4(1)(a) of the Regulation). The question of lawfulness has already been considered. As for fairness, it is related to the information to be given to the data subject (see section 3.8. below).

3.4. Conservation of data

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 Community institution or body shall lay down that personal data which are to be stored for longer periods for historical, statistical or scientific use should be kept either in anonymous form only or, if that is not possible, only with the identity of the data subjects encrypted. In any event, the data shall not be used for any purpose other than for historical, statistical or scientific purposes"* (Article 4(1)(e) of the Regulation).

As indicated above, data are retained for variable period of time, established on the case by case basis. The EDPS recommends establishing an effective procedure which will allow erasing data which conservation is not necessary for the purposes of the processing. In this context, the EDPS would suggest establishing a unified time-limit for storing the data which would facilitate their management and erasure. The EDPS also reminds that only anonymous data can be kept for statistical purposes.

3.5. Automated individual decisions

Article 19 of Regulation (EC) 45/2001 provides that *"the data subject shall have the right not to be subject to a decision which produces legal effects concerning him or her or significantly affects him or her and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him or her, such as his or her performance at work, reliability or conduct, unless the decision is expressly authorised pursuant to national or Community legislation or, if necessary, by the European Data Protection Supervisor. In either case, measures to safeguard the data subject's legitimate interests, such as arrangements allowing him or her to put his or her point of view, must be taken".*

This provision applies to the present processing operation. In fact, the evaluation of the abilities of the data subjects is exclusively automated. The tests are evaluated and the certification generated by automatic means without human intervention.

The EDPS authorises this processing provided that the controller takes the necessary measures to safeguard the data subject's legitimate interests. Those measures in this particular case are basically the right of access to and rectification of the evaluation

data and the appropriate information of the data subjects. There are specified in sections 3.7. and 3.8.

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. In the present case, the controller does not transfer data outside the General Secretariat of the Council. Transfer within or between Community institutions and bodies covered by Article 7 of the Regulation

The EDPS recalls that Article 7(1) of the Regulation requires that personal data are only transferred "*if the data are necessary for the legitimate performance of tasks covered by the competence of the recipient*." In order to comply with this article in sending personal data, the controller must ensure that (i) the recipient has the appropriate competence and (ii) the transfer is necessary.

In the present case the data are transferred to the GSC Training Department (DGA 1A) in order to produce the training statistics, and to the service "Consultation/modification rights" (DGA 5 "Information and Communication System"). The DGA 5 services have the possibility to access the personal data only in the context of system maintenance and functional support. Those transfers are necessary for the legitimate performance of tasks covered by the competence of the recipient and therefore comply with the Article 7 of the Regulation.

3.7. Right of access and rectification

According to Article 13 of the Regulation, the data subject shall have the right to obtain without constraint from the controller, communication in an intelligible form of the data undergoing the processing and any available information as to their source.

As described in point 2 of the present Opinion, the data subject can access their eHEST account containing the identification data. As to the access to the answers of tests questions, the controller will supply on request a detailed breakdown of data subject's answers question by question.

Article 14 of the Regulation provides the data subject with a right to rectify inaccurate or incomplete data. Given the fact that the identification data are entered directly into the system by the data subject and that the other data (examination results) are generated automatically by the system, there is a low risk that the data would need to be rectified.

In the unlikely case of the human error or the software malfunction, the data subjects have the possibility to address the controller and have their data corrected.

Therefore, the EDPS considers that Articles 13 and 14 of the Regulation are complied with.

3.8. Information to be given to the data subject

Under Articles 11 and 12 of the Regulation, certain information must be provided to

the data subject. In the case in question, data are mainly obtained directly from the data subject. The examination/certification data are generated automatically by the system. Therefore, both Articles 11 and 12 are applicable.

As already mentioned in section 2, the privacy disclaimer provides to persons concerned some information requested in the Articles 11 and 12 of the Regulation.

In order to fully comply with those provisions, the EDPS recommends including in the privacy disclaimer a reference to:
- the legal basis of the processing operation;
- whether replies to the questions are obligatory or voluntary;
- specific list of potential recipients of data (names of GCS services);
- the existence of the right to rectify the data and how to assert that right (in respect of the identification data as well as the evaluation/certification data);
- the precise time-limits for storing data;
- the right to have recourse at any time to the EDPS.

3.9. Security measures

Security measures have been put in place to counter any data alteration or destruction and any non-authorised access to data. In this connection, the EDPS has received information allowing him to state that the security measures appear to be satisfactory in this case.

Conclusions

The proposed processing does not appear to infringe Regulation (EC) No 45/2001 provided that the following recommendations are taken into account:

- The specific procedure should be established to allow erasing data whose conservation is not necessary for the purposes of the processing.

- The Privacy Disclaimer should be amended as stated in section 3.8 of this Opinion.

Done at Brussels, 22 October 2008

(signed)

Joaquín BAYO DELGADO
Assistant European Data Protection Supervisor