EUROPEAN DATA PROTECTION SUPERVISOR

GIOVANNI BUTTARELLI
ASSISTANT SUPERVISOR

Mr Emmanuel MAURAGE
European Network and Information
Security Agency (ENISA)
P.O. BOX 139
71001 HERAKLION
GREECE

Brussels, 14 January 2011
GB/MV/ktl/D(2011) 67 **C 2010-0932**

Dear Mr Maurage,

On 23 November 2010, the European Data Protection Supervisor (EDPS) received by e- mail a notification for prior checking (Notification) under Article 27 from the Data Protection Officer (DPO) of the European Network and Information Security Agency (ENISA) on Training Programme. This notification follows a visit by the EDPS to ENISA and discussions with his staff in order to discuss cases which may be subject to prior checking .

According to the notification, the purpose of the processing is to accommodate the training needs of personnel in order to meet the requirements of the service. It is also stated that "*attribution of candidate rights might be affected by means of processing made*". ENISA submits the case for prior-checking considering that the processing falls within the processing operations intended to evaluate personal aspects relating to the data subject (Article 27.2(b)).

The data collected relates to the candidates that request training within the ENISA policy framework for training on individual initiative in the interest of the service. The data processed are related to their name, grade and training course. Rights of access, rectification, blocking, erasure and objection can be made by contacting ENISA service in charge of the processing. Although an evaluation of the training course followed by the candidates is made, the produced report is not intended to evaluate individual trainers. This is only made for quality management purposes.

The EDPS does not consider that such processing operations in the framework of the training programme are intended to evaluate personal aspects relating to the data subject, including his or her ability, efficiency and conduct. Article 1 of the Decision of the Executive Director on Training Policy foresees that: "*Trainings at ENISA do not serve the objective of rewarding*

staff members for their performance; they are simply carried out in the interest of the service, which is the determining factor for authorising a training or not". Furthermore, there is clearly no mention of any evaluation in the decision.

Instead, it is rather in the context of the general evaluation procedure of staff members that references to the trainings followed by them may be used in their evaluation.

Therefore, in the light of these comments, the EDPS concludes that the described Training Programme of ENISA is not subject to prior checking. On the other hand, as you are aware of, the evaluation procedure is subject to prior checking and will cover the aspect of evaluation of the data subject regarding the training followed or not[1]. Should you identify any specific reasons or risk factors why this processing operation should nevertheless be subject to prior checking, please do not hesitate to contact us again and we would be ready to reconsider our position.

Although not subject to prior check, after having analysed the elements of the procedure which was submitted to him, the EDPS would nevertheless like to make the following recommendations in order to ensure that there is no breach of the provisions of Regulation 45/2001:

1) Different elements of the notifications should be amended.

For instance:
- in box 7 regarding information to data subject, it is not sufficient to underline that "Rights are determined as per Regulation (EC) 45/2001", but ENISA should underline the steps taken by the data controller to inform the staff member of the processing operations, in line with article 11 and 12 of Regulation (EC) 45/2001 (privacy notice given to staff, information available on the intranet, etc);
- in box 12 of the notification, the recipients of the data should be more clearly determined (head of unit of the staff member/department of HR, etc).

2) As regards the conservation period, guidance was requested by ENISA.

The EDPS has considered, in other cases, as compliant with Regulation (EC) 45/2001 the following conservation periods:
- when paper and electronic training records are kept for the duration of the staff member's career according to the Staff Regulations, i.e. for certification purposes (see art. 45.2 SR) and that records are disposed of 1 year after the staff member's departure (resignation / contract expiry));
- training applications and presence lists which are justification documents for the payment of the external contractor and therefore are kept for the periods determined under the Financial Regulation as justification for the payment of contractors/training providers invoices (5 years after discharge);
- evaluation documents on the training action kept according to the duration of the contract with the service provider.

3) ENISA should adopt a privacy statement on the Training Programme, to be circulated to staff and containing information in line with Regulation (EC) 45/2001 (especially information elements as foreseen by Articles 11 and 12).

[1] See for instance PC 2010-0936 on annual appraisal of temporary agents and contract agents (to be adopted).

4) Guidance with regard to the time limits for blocking and erasure of the different categories of data was requested.

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, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified"*.

With regard to data provided by participants about themselves such as contact details and purposes for participation, there is no substantive reason to believe that they are inaccurate. With regards to time limits for blocking and erasure of the different categories of data on justified legitimate requests from the data subject, no time limit should apply.

In any case, a further guarantee of accuracy is implemented as participants may exercise their rights of access and rectification, as mentioned in the notification.

Article 13 of Regulation (EC) No 45/2001 establishes a right of access upon request by the data subject. Article 14 of Regulation (EC) No 45/2001 provides the data subject with a right of rectification.

5) The notification does not foresee training by external contractors (only internal training and training by the Commission services are mentioned). ENISA should however keep in mind that if such situations were taking place, external contractors would be involved in the processing of personal data in connection with staff training at ENISA. In fact, these contractors would process personal data on behalf of ENISA who would determine the purposes and means of the actual data processing (Article 2(d) and (e) of Regulation 45/2001). Moreover, all agreements with external contractors should provide for the confidentiality and security obligations set out in the applicable national data protection legislation (Article 23 of the Regulation).

The EDPS invites ENISA to amend its notification in line with these recommendations regarding the training policy. To facilitate our follow-up, it would therefore be appreciated if you could provide the EDPS with all relevant documents within 3 months of the date of this letter to evidence that the recommendations have been implemented.

Yours sincerely,
(Signed)

Giovanni BUTTARELLI

Cc : Mr Udo HELMBRECHT , Director, ENISA