GIOVANNI BUTTARELLI
ASSISTANT SUPERVISOR

Mr Philippe RENAUDIERE
Data Protection Officer
European Commission
BRU BERL 08/180
B - 1049 BRUSSELS

Brussels, 3 September 2010
GB/ZB/et D(2010)1309 **C2009-0012**

Subject: your consultation on the need for prior checking "EURES", EDPS case ref 2009-012

Dear Sir,

Thank you for consulting us on the need for prior checking EURES, the European Job Mobility Portal. We would like to confirm that - based on the information made available to us in your email of 6 January 2009 - the EDPS concluded that "EURES" is not subject to prior checking.

You informed us that the purpose of EURES is to provide information, advice and recruitment/placement (job-matching) services for the benefit of workers and employers as well as any citizen wishing to benefit from the principle of the free movement of persons. In particular, and in part relevant to this consultation, the EURES job mobility portal offers a tool to help jobseekers find employers and employers find jobseekers across the EU. Jobseekers can register and post their resumes on the site. Potential employees, in turn, can register, and then access, browse and search the site for matching profiles when they are looking to fill vacancies. The EURES job portal is managed by the Commission and hosted on Commission servers.

You requested us to confirm whether or not EURES is subject to prior checking on the basis of Article 27.2(b) of Regulation (EC) No 45/2001 ("**Regulation**"), which requires prior checking when processing operations are "intended to evaluate personal aspects relating to the data subject, including his or her ability, efficiency and conduct".

There is no doubt that the resume information that jobseekers upload on the job portal are subsequently used to "evaluate personal aspects relating to the data subject, including his or her ability, efficiency and conduct". This evaluation, however, is carried out by the employer organizations, rather than by the Commission, as separate and individual controllers with respect to the processing of data for evaluation purposes. These organizations are subject to their own national data protection laws (which must be in conformity with Directive 95/46/EC) and their processing of personal data is supervised by their national data protection authorities.

Data processing in EURES, insofar as it concerns the activities of the Commission, falls under the scope of the Regulation and the supervision of the EDPS. The Commission, as an "operator" of EURES, has its own responsibilities, as one of the controllers. Its main role is to provide the IT infrastructure where individuals can post their resumes. There is no "evaluation" under Article 27(2(b) that the Commission would carry out using the information uploaded. For example, the Commission does not "pre-screen" these applications. Any evaluation is done by the employers, subject to their own national laws.

For these reasons, the EDPS concluded that EURES is not subject to prior checking. 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.

Despite our conclusion that EURES is not subject to prior checking, please find below a couple of observations. These comments relate to two areas: data protection safeguards in general, and security aspects in particular.

1. Data protection safeguards. Considering the multiple actors involved and their different tasks and responsibilities, we recommend that you continue to work closely with your data protection officer ("**DPO"**) to ensure that adequate safeguards are offered for data subjects. For example, it must be ensured that they are informed in a clear and efficient manner of the data processing and that there are mechanisms put in place to ensure that they can access their personal data or correct any inaccurate data. With regard to notice, we welcome the user-friendly language that you used on the data protection notice posted on the EURES website for applicants wishing to upload their resumes and other personal information.

In the same context, the EDPS emphasises that in any situation where personal data are processed, it is crucial to correctly identify who the controller is. This has recently been emphasized by the Article 29 Data Protection Working Party in its Opinion 1/2010 on the concepts of "controller" and "processor", which was adopted on 16 February 2010. The primary reason why the clear and unambiguous identification of the controller is so crucial is that it determines who shall be responsible for compliance with data protection rules. As noted in the Working Party Opinion[1], "[i]f it is not sufficiently clear what is required from whom - e.g. no one is responsible or a multitude of possible controllers - there is an obvious risk that too little, if anything, will happen and that the legal provisions will remain ineffective". Clarity is especially needed in situations where multiple actors are involved in a cooperative relationship. This is often the case with EU information systems used for public purposes where the purpose of processing is defined in EU law.

For these reasons, the EDPS urges the Commission to lay down, in a clear, transparent and unambiguous manner, the tasks and responsibilities of each party involved in the data processing.

When allocating responsibilities, in particular, the following issues need to be addressed:

- Who are responsible for ensuring the quality (proportionality, accuracy, etc) of the data?
- Who can determine retention periods?
- Who determines who can have access to the database?
- Who are authorized to make a transfer of the data to third parties?
- Who are providing notice to data subjects?
- Who are responsible for acting when access, rectification, blocking, or erasure is requested by data subjects?

[1] See page 7, Section II.3.

- Who bears ultimate responsibility for the security of the system?
- Who makes decisions regarding the design of the system?

Finally, we point out that controllers and processors must be clearly indicated in a way which corresponds to the effective role as well as the legal status of the organizations involved.

2. Security aspects. In the case of EURES the issue of the integrity of information is the most critical one. In particular, the jobseeking individuals (or the employers, for their own registration data) are usually best placed to check and correct their own data. It is therefore important that the data stored by EURES is adequately protected against any unauthorized modification.

In this respect, first, it is important to note that similar services of the Commission (see, for example, the EPSO website) already implemented registration and log-in to the user account (in this case, "my EURES" services) using an SSL protocol. This is recommended for EURES as well.

Second, we call your attention to this most sensitive dimension here, the issue of integrity, to encourage you to pay special attention to this aspect whenever making any routine security reviews or updates, for example, to include this issue on your checklist next time when you will renegotiate your Service Level Agreement with the Commission data centre in Luxembourg.

Please note that our advice in this matter is based on the facts of the case as explained to us and should not prejudice any further comments or action from the part of the EDPS. If you have any further questions or comments, please do not hesitate to contact us again.

Yours sincerely,

(**signed**)

Giovanni BUTTARELLI