EUROPEAN DATA PROTECTION SUPERVISOR

GIOVANNI BUTTARELLI
ASSISTANT SUPERVISOR

[…]

Brussels, 09 January 2014
GB/DG/sn/D(2014)0030 **C 2013-1337**
Please use edps@edps.europa.eu for all correspondence

**Subject: Consultation under Article 46(d) on the notification of a data breach involving the mass disclosure of e-mail addresses**

Dear […],

On 27 November 2013, the EDPS was made aware of an apparent breach of Regulation EC No 45/2001 involving the disclosure of candidates' e-mail addresses following a recruitment application process at […]. The EDPS was informed of this error after being copied in on an e-mail sent from one of the affected candidates to the […] recruitment team, asking whether the EDPS had been made aware of the incident. […]'s Data Protection Officer (DPO) subsequently acknowledged the candidate's e-mail on 28 November, again with the EDPS in copy. On 4 December, the EDPS sent a letter to the DPO requesting […]'s position, with several additional questions. A reply was received on 10 December 2013.

[…] explained that on 19 November 2013, an assistant in the HR selection and recruitment team sent out an e-mail to inform all 205 non-selected candidates that they had not been successful in application for a specific post. […]'s usual procedure is to use one e-mail template that is sent to all candidates using the blind copy function (BCC). In this particular case, a manual mistake was made by an assistant in the HR team who, instead of copying all the addresses in the 'BCC' field of the email, accidentally included them in the 'TO' field. The error was identified approximately 1.5 hours later, when a candidate replied with additional questions. On the same day, […] sent an e-mail to all affected candidates apologising for the mistake, and the DPO was also informed.

[…] has since confirmed that a number of measures were already in place at the time of the incident, to minimise any risk to personal data:

1. a detailed work instruction describes the procedures for the selection and recruitment process, so HR staff have clear guidance on how to manage any such procedures;
2. all […] staff have signed confidentiality declarations, with a specific declaration for staff members participating in selection panels;
3. data protection and IT training is provided on a regular basis and is available to all staff;

4. a data protection workshop was recently organised for the HR team leaders, as well as a compulsory refresher training session for all HR staff; and
5. an internal data protection audit was carried out in 2012 to assess the selection and recruitment procedures in the Agency. No "critical" issues were identified, but a series of recommendations were made, and an action plan is underway to address the findings.

A number of further measures have been (or will be) implemented following the incident, to mitigate the risk of any other disclosures:

1. […] has recently signed a contract for the development of an e-HR tool, which will cover all HR processes including the selection and recruitment process. This means that manual copy-pasting of e-mail addresses will no longer take place. Instead, the system will create individual messages based on a standard template to be sent to different categories of recipients (for example selected candidates, non-selected candidates etc). This will completely eliminate the risks involved with mass mailing, and the disclosure of other candidates' personal data will no longer be possible. The development of the tool will begin in early 2014, with the selection and recruitment module activated the following year;
2. […]'s DPO has drafted a recommendation on data breaches for all staff, which will be formally issued shortly. The document is based on a paper produced by the DPO network on the topic, taking into account any stipulations in existing legislation and (mainly) the current proposal for a review of the Data Protection Regulation. This recommendation recognises the need for a uniform procedure in dealing with data breaches, including keeping track of any such incidents by the DPO, transparency guarantees towards the data subjects, and proper follow-up and improvement actions.

E-mail addresses often enable identification of the person they belong to. Sometimes, they can also indicate other information (such as the current employer). They are thus personal data as defined in Article 2(a) of the Regulation. Article 22 of the Regulation contains provisions relating to the security of data processing, and stipulates that measures should be taken to mitigate any risk of unauthorised access or disclosure (amongst other things).

The actions taken by […] to avoid and mitigate such incidents in the future seem to be sufficient, and it would appear that adequate preventative measures were in place at the time. Notably, the future e-HR tool will prevent such breaches from recurring, although in the unlikely event that something similar was to happen again, the DPO's data breach recommendations will help to manage any such incidents.

The EDPS would just like to highlight one issue in relation to data controllership. The DPO recommendations state that data controllers are the responsible Heads of Unit. Legally speaking however, […] as an Agency is the controller of the processing operation, with the various Heads of Unit entrusted with the processing of personal data. While the Heads of Unit are good contact points for internal and external enquiries, the ultimate responsibility of controllership rests with […] itself. […] should consider amending the text accordingly, to avoid any confusion.

[…] has demonstrated that it has already taken steps to prevent a repetition of this kind of breach, and to mitigate the consequences should it recur. It is important to ensure that such incidents are prevented, as the confidential handling of applications protects both the privacy of applicants as well as ensuring a fair selection procedure. However, the EDPS recognises that this particular data breach was caused by a manual error, which does not seem to have occurred as a result of

any negligence on […]'s part in terms of data security. As such, the EDPS now considers this case as closed.

Thank you for your assistance in this matter.

Yours sincerely,

(**signed**)

Giovanni BUTTARELLI

Cc: […] – Data Protection Officer, […]