EUROPEAN DATA PROTECTION SUPERVISOR

GIOVANNI BUTTARELLI
ASSISTANT SUPERVISOR

Mr Udo HELMBRECHT
Executive Director
European Network and Information
Security Agency (ENISA)
PO Box 1309
71001 Heraklion
Greece

Brussels, 05 February 2014
GB/MV/sn/D(2014)0301 **C 2013-0594**
Please use edps@edps.europa.eu for all correspondence

Subject: **Opinion on the notification for prior checking from the Data Protection Officer of the European Network and Information Security Agency in the field of leave management**

Dear Mr Helmbrecht,

On 4 June 2013, the European Data Protection Supervisor ("EDPS") received from the Data Protection Officer ("DPO") of the **European Network and Information Security Agency ("ENISA")** a notification for prior checking covering processing of data related to leave management.

The notification was accompanied by 16 annexes.

The notification was sent to the EDPS following the adoption on 20 December 2012 of the Guidelines on Leave and Flexitime (the "Guidelines"). The EDPS sent the draft for comments on 8 November 2013 and these were received on 4 February 2014. As the processing operations are already in place, the deadline of two months for the EDPS to issue his Opinion does not apply. This case has been dealt with on a best-effort basis.

Legal aspects

This Opinion deals with the already existing leave procedures at ENISA. It is based on the Guidelines, which allows the EDPS to focus on ENISA practices that do not seem to be compliant with the Guidelines and the principles of Regulation EC No 45/2001.
Based on the notification, the purpose of the leave procedure is the management of absences and leave of ENISA statutory (TA, CA, SNE) and non-statutory staff (interims, trainees) in application of Commission Decision C(2004) 1597 and Commission Decision C(2010) 7495.

As described in the notification, ENISA is making use of different databases in its leave management[1].

The legal basis of the processing operations is described as based on the Articles 57-61 of the Staff Regulations and Annex V thereof, as well as on the Articles 16 and 91 of the CEOS. As good practice, ENISA may consider adopting specific implementing rules of the Staff Regulations to ensure the correct implementation of these Articles. In general, these are often based on decisions from the managing boards/steering committee of the relevant agencies. ENISA should provide these decisions as they should be part of the legal basis.

Regarding **information** of the data subjects, the notification states that staff is informed via intranet announcement and emails: the Leama manual is available on the intranet, there is guidance to staff in various documents on the use of flexitime, teleworking, working regimes, there is publication of the relevant ED Decisions and regular information to staff in staff meetings. The EDPS considers that such information does not fulfil the requirements of Articles 11 and 12 of Regulation 45/2001 and that ENISA should therefore ensure that the information is provided in a privacy statement made available to staff members.

Moreover, the EDPS would like to draw the attention of ENISA to the case where a leave/teleworking request is linked to the health situation of a family member. In such case, the EDPS considers that the privacy statement should foresee the communication of information to this family member whose personal data are processed by ENISA. If the EDPS admits that direct provision of such information would involve disproportionate efforts by ENISA, he considers that the Agency, amongst other appropriate steps, could at least ask staff members submitting such data to inform the family members concerned about the processing of their personal data and their rights in that respect. Therefore, besides adopting the privacy statement regarding leave/teleworking as mentioned above, this should include that family members may have access to data concerning them, and ask that officials/staff members providing such data inform the persons concerned of those rights.

Regarding the **retention policy**, the notification states that there is no retention policy at ENISA in place yet. As regards leave, the EDPS refers to the Guidelines on leave and flexitime where he is setting acceptable retention policy for all EU institutions and bodies. The notification also states that ENISA would appreciate guidance of the EDPS in this field, and as regards retention policy as a whole. Other Guidelines on health data at work, recruitment, etc. have been adopted by the EDPS and can also serve as guidance for ENISA to draft its retention policy.

Such retention policy is even more relevant as ENISA states that anonymised statistics on leave are kept by HR and provided to Management whenever requested. Given that this should apply

[1] Among others, ENISA has a central HR repository, an electronic database for leave management (Leama), an electronic database for missions regarding fitness to travel before or during missions (Mima), an electronic project management system (Matrix), etc.

for instance to data kept for a longer term than the established retention, the need for a retention policy is required. This should not, however, impede ENISA to draw statistics of the current year in the management of leave.

As to security measures, the EDPS notes that the declaration of confidentiality to be signed by the HR staff that they are subject to an obligation of professional secrecy equivalent to that of a health professional, in compliance with Article 10(3) of the Regulation is missing. As stated in the Guidelines (under point 10): "given the particular sensitivity of the processing of health related data and considering that data indicating the health status of a person are processed by HR services during a leave request procedure (e.g. reason for the absence, forms concerning sick leave, medical certificates, etc), the EDPS recommends that all persons within HR services who are responsible for processing information related to the staff members' health status are reminded to process them in accordance with the principles of medical confidentiality". Therefore, the EDPS invites ENISA to adopt such declaration of confidentiality.

Conclusion

In view of the above, the EDPS recommends that ENISA:
1- provides a privacy statement covering the processing operations described in the notification, including the comments made above;
2- adopts retention policy as regards the processing operations at stake taking into account the Guidelines already adopted by the EDPS in this field;
3- provides the EDPS with a copy of the declaration of confidentiality to be signed by ENISA staff dealing with health related data.

The EDPS would like to invite ENISA to inform him about the implementation of these recommendations within three months after receipt of this letter.

(**signed**)

Giovanni BUTTARELLI

Cc: Mr Konstantinos MOULINOS, Data Protection Officer, ENISA