GIOVANNI BUTTARELLI
ASSISTANT SUPERVISOR

Ms Françoise MURILLO
Head of Resource and Service Centre
EU-OSHA
European Agency for Safety and Health at Work
Gran Via 33
E-48009 Bilbao
SPAIN

Brussels, 14 May 2013
GB/MV/kd D(2013) 978 **C 2013-0281**
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 Agency for Safety and Health at Work concerning leave management.

Dear Ms Murillo,

On 13 March 2013, the European Data Protection Supervisor ("EDPS") received from the Data Protection Officer ("DPO") of the European Agency for Safety and Health at Work ("EU-OSHA") a notification for prior checking concerning leave management. The notification was accompanied by the following documents:

1. Cover letter with an overview of the procedure;
2. Decision N. RSC(12)16 - EUHR Allegro N.2 on access rights, delegations and authorizations in "EUHR Allegro";
3. Corrigenda to Decision N. RSC(12)16 - EUHR Allegro N.2 on access rights, delegations and authorizations in "EUHR Allegro";
4. Director's Decision RSC (12)33 - EUHR Allegro N.3 regarding change of administrative workflows.

The DPO sent this notification to the EDPS following the adoption on 20 December 2012 of the Guidelines in the area of Leave and Flexitime (the "Guidelines")[1] and before the deadline given to EU institutions and bodies to submit their notification (end of March 2013). The EDPS sent the draft Opinion for comments to the DPO on 11 April 2013 and these were received on 19 April. A phone call also took place on 8 May as to clarify some of the recommendations.

[1] Guidelines concerning the processing of personal data in the area of leave and flexitime adopted on 20 December 2012 (EDPS 2012-0158).

This Opinion is also linked to a consultation by EU-OSHA on the need for prior check of the EU HR Allegro system (Case 2011-1102). The consultation covered various aspects on personal files, flexitime and leave. On the aspect of leave, the EDPS stated that this point would be treated following the adoption of the Guidelines.

1. Legal aspects

This Opinion deals with the already existing leave management processing operations at EU-OSHA. It is based on the Guidelines, which allows the EDPS to focus on EU-OSHA practices that do not seem to be compliant with the leave and flexitime Guidelines and the principles of the Data Protection Regulation 45/2001.

The purpose of the processing operations covers the management of all leave categories (annual leave, special leave, sick leave, family leave, parental leave, part-time leave, leave on personal grounds) for EU-OSHA statutory staff members (Temporary Agents (TA), Contract Agents (CA) and local staff) and Seconded National Experts (SNE)). Concerning trainees, HR receives and keeps only information regarding absences and leaves. Trainees' working time information is kept by their respective supervisors.

The EDPS notes that the processing in question is lawful in terms of Article 5(a) of the Regulation[2] and that the leave management data are processed in compliance with data quality principles set out in its Article 4(1).

The EDPS notes that the notification foresees not only the applicability of Article 27.2.a) (health related data) but also of Article 27.2.d) (excluding individuals from a right, benefit or contract) of the Regulation. The EDPS considers that it is not the purpose of leave management as such to exclude people from a right, benefit or contract. Therefore only Article 27.2.a) should apply here.

Furthermore, the EDPS notes that, regarding processing of health related data, the procedure in place at EU-OSHA is in line with Article 10 of the Regulation, on the basis of Article 10.2.b).

As described in the notification, in case of sick leave, family leave and some types of special leave, special categories of data may be processed, such as administrative data (not medical data) related to the health status of the staff member or his family/relatives (i.e., the fact that a person is sick or hospitalized and number of related days of absence) which is submitted to the Agency by the external medical advisor; and sexual orientation (through the names of the partners).

The EDPS takes note that the need to know principle is applied by EU-OSHA as regards the procedure to grant access to specific recipients to the personal data in Allegro. EU-OSHA clarified that the platform Allegro is not hosted on the Agency's server, but on the service provider's that both HR and staff can access through the Internet. In the SLA that the Agency signed with the service provider, EU-OSHA added a data protection clause by which the service provider commits to comply with all the requirements foreseen by the Regulation. The IT department of EU-OSHA is not managing the system in place for the management of leave. In this case, however, the service provider should be considered as a recipient as they would fall in any case under the definition of Article 2.(g) of Regulation 45/2001. This implies that they should be mentioned in the list of recipients in the notification/privacy statement.

[2] Based on Articles from the Staff Regulations, the Conditions of Employment of other servants of the European Communities, Council Regulation N°2062/34 establishing EU-OSHA, Commission Decisions C(2010) 7495 on leave, C(2010) 7572 on parental leave and C(2010) 7494 on family leave adopted by analogy by EU-OSHA and EU-OSHA Decisions.

EU-OSHA also states that in order to ensure an appropriate level of confidentiality, HR section staff members, Heads of Unit (including the Director) and their assistants (delegates) have signed a declaration of professional secrecy equal to that of a health professional. The EDPS welcomes this procedure, as described in the Guidelines.

It is also stated that in case of any type of leave for which staff members have to provide a medical certificate, the HR section neither processes nor stores health data and staff members are requested to send any medical certificate directly to the Agency's medical adviser, or indirectly, through the HR section in a sealed envelope clearly stating "'confidential", who, in turn, forward it unopened to the medical adviser.

Besides, the EDPS notes that, in accordance with Articles 13 and 14, the rights of access, rectification and erasure are granted to the data subjects. As stated by EU-OSHA, these rights are embedded in the Allegro application, whereas blocking can be solicited through a dedicated channel for communication with the HR Section, also available in Allegro. It is mentioned that three snapshots will be taken of the contested data. The EDPS notes however that neither the notification nor the privacy statement contain information regarding the time needed to handle such request. Therefore, he recommends amending this point on the notification and privacy statement.

The EDPS analysed the privacy statement that was provided and he considers that information in respect of Articles 11 and 12 is provided to the individuals. He has no further comment on the privacy statement.

According to the notification, the retention period covering data related to annual, special and sick leave are stored for 4 years, whereas the decision related to part-time, parental leave, family leave and leave on personal grounds are stored in the data subject's personal files and follows its retention period.

If the EDPS welcomes that EU-OSHA established a clear difference of retention periods between the different categories of leave, he would like to remind that, as a reasonable conservation period and in view of aligning retention periods, a three years retention period was considered as a maximum by the Guidelines, especially regarding retention of data in the context of annual leave This approach should nonetheless also apply in the context of sick leave, as underlined in the Guidelines (point 5.1 and 5.2 of the Guidelines).

In the Guidelines, the EDPS considered that the proportionality of a retention period exceeding the three years is to be considered to be appropriate only where this would be strictly required in order to cover periods when a dispute or an appeal is underway. [3] Therefore, the EDPS invites EU-OSHA to revise its retention policy to conform it to the Guidelines.

Finally, the security measures that are described in the notification seem in line with the requirements of Article 22, also as regards the existence of the declaration of professional secrecy equal to that of a health professional.

[3] See also the EDPS Guidelines concerning the processing of health data in the workplace, page 12: "Article 59 (4) of the Staff Regulations could justify a conservation period of 3 years for data necessary to justify an absence due to sick leave. The only justification for keeping them any longer would be if a dispute or appeal were under way".

2. Conclusion

In view of the above, the EDPS recommends that the EU-OSHA:

1 - clarifies the time needed to block data in the case of justified requests;
2 - amends its retention periods with respect to the Guidelines on leave and flexitime, as analysed above.
3 - completes the list of recipients, as analysed above

The EDPS invites EU-OSHA to inform him about the implementation of these recommendations within three months after receipt of this letter.

Done at Brussels, 14 May 2013

(**signed**)

Giovanni BUTTARELLI
Assistant European Data Protection Supervisor

Cc: Ms Ilaria PICCIOLI, Data Protection Officer, EU-OSHA