EUROPEAN DATA PROTECTION SUPERVISOR

GIOVANNI BUTTARELLI
ASSISTANT SUPERVISOR

Mr Udo HELMBRECHT
Executive Director
European Network and Information
Security Agency (ENISA)
PO Box 1309
781001 Heraklion
GREECE

Brussels, 01 October 2013
GB/RDG/sn D-2013)2167 **C 2013-0715**
Please use edps@edps.europa.eu for all correspondence

Subject: Prior checking notification of the processing of personal data in the framework of administrative inquiries and disciplinary proceedings at ENISA (Case 2013-0715)

Dear Mr Helmbrecht,

I refer to the prior check ex-post notification on the processing of personal data in the framework of administrative inquiries and disciplinary proceedings at the European Network and Information Security Agency (ENISA), which ENISA's Data Protection Officer (DPO) notified to the European Data Protection Supervisor (EDPS) on 25 June 2013. The notification included also the draft Decision of the Executive Director of the Agency on administrative inquiries and disciplinary procedures (the EDD). We asked further information to the DPO on 22 July and 13 August 2013, to which the DPO replied on 3 and 5 September 2013.

The notification contains the following comment: "*Please note that this is a real prior-check and the EDD has not been published yet at ENISA, subject to the EDPS recommendations, which will be taken into account*". In further exchanges with the EDPS, ENISA's DPO clarified that while the EDD has not yet been adopted the processing of personal data in the framework of administrative and disciplinary proceedings is not per se new. The notification relates therefore to a processing operation which is already in place.

The EDPS has adopted guidelines regarding the processing of personal data in administrative inquiries and disciplinary proceedings (AI&DP).[1] He also issued a number of prior-check opinions in this area. We will therefore highlight in the present Opinion only those aspects

[1] The Guidelines are available on EDPS website (www.edps.europa.eu) under the section Supervision/Thematic Guidelines.

that do not seem to be in conformity with the principles of the Regulation and with the Guidelines and limit the legal analysis to those practices. In light of the accountability principle guiding his work, the EDPS would nonetheless want to highlight that *all* relevant recommendations made in the Guidelines apply to the processing operations under consideration.

Having regard to **special categories of data**, Article 25 of the EDD stipulates that these data cannot be processed "*unless it is necessary for the purposes of complying with specific rights and obligations of ENISA in the field of employment law or if absolutely necessary for conducting the investigation at stake*" (emphasis added). Under Article 10(2)(b) of Regulation (EC) No 45/2001 (the "Regulation") special categories of data can be processed where the processing is necessary for the purposes of complying with the specific rights and obligations of the controller in the field of employment law insofar as it is authorised by the Treaties establishing the European Union or other legal instruments adopted on the basis thereof. As it is formulated as an alternative condition ("or"), the second part of Article 25 of the EDD, pointing to the absolute necessity for the investigation at stake introduces a new exception which is not foreseen in the Regulation. We therefore recommend replacing the conjunction "or" with "and" or to delete the second part of Article 25(1) of the EDD.

Having regard to **data quality**, we are pleased to see that the EDD contains a specific provision requiring that the personal data collected and processed be restricted to what is necessary and proportionate for the purpose of establishing the facts. In addition to this welcomed specification, we would also recommend that investigators be specifically instructed when taking up their tasks about the existing data quality requirements and restrictive rules concerning the processing of special categories of data.

The EDPS would like to emphasise the rules concerning the **storing of disciplinary related information** in the staff's personal files. ENISA should keep in these files only the final decisions taken in the disciplinary proceedings which can have an impact on the disciplinary relationship, i.e. the disciplinary decision and possibly the interim decision to suspend an agent from his/her duties. If the decision is contested before the Court of Justice of the EU (CJEU), the staff member may request to include in the file the proposed appeal and/or a note mentioning thereof. The decision to close with no further action should not be stored in the personal file, unless the data subjects requests otherwise. The same applies whenever the disciplinary decision is annulled by the CJEU in appeal.

Having regard to the **retention periods**, ENISA should take into account the provision of Article 27 of Annex IX of the Staff Regulations concerning the request for deletion of such data. In case of refusal to delete, the Agency should duly motivate the necessity of keeping the data for a longer period. The Agency should also consider setting up a maximum retention period for disciplinary related information stored in personal files. Once disciplinary related information has been deleted from the personal file (for example in light of Article 27 of Annex IX of the Staff Regulations), the EDPS sees no need to store such information in the parallel disciplinary file. It should therefore be deleted also from the latter.

Having regard to **traffic data**, we would like to stress the importance of a balanced and proportionate approach by ENISA when processing such data. We welcome the fact that EDD limits access to e-communications data only in exceptional circumstances where no other less invasive methods could be used and after the DPO is consulted. It should be considered that precautions should be followed also in respect of access to the contents of ENISA owned computers, as they may well contain personal files or information having no relationship with the purpose of the investigation. Whenever access to files that are apparently of a private

nature appears to be necessary for the investigation, this access should be subject to adequate guarantees. In order to consolidate this principle in tangible investigative practices, we recommend the adoption of a formal protocol for the processing of electronic evidence (forensic investigations) by ENISA, which will also contribute to the safeguard of the data quality principle. With respect to the retention period of traffic data, we would recommend adding a reference in Article 26(1) of the EDD to the possibility to derogate from the six month rule, pursuant to Article 20 of the Regulation.

Having regard to **data-transfers**, we consider the situations giving rise to transfers listed in Article 27 of the EDD as in line with Article 7 of the Regulation. We would suggest adding the EDPS as a possible recipient, next to the European Ombudsman, in case of complaints lodged concerning the alleged breach of personal data. Article 27 of the EDD does not contemplate cases of transfers to national authorities, which however are likely to occur where the investigation leads to the conclusion that a criminal offence may have been committed. In these cases, Article 8 of the Regulation has to be respected, or Article 9 in cases where the Member State concerned has not extended the application of Directive 95/46/EC to judicial activities. In this respect, we refer you to the recommendations provided in the EDPS Guidelines on AI&DP.

Concerning the **information** of data subjects, the notification simply refers to the publication of the EDD. The DPO further clarified that "*ENISA provides all the information staff concerned may request in a disciplinary procedure. No additional information is provided*". This approach is not compatible with the Regulation. Under Articles 11 and 12 of the Regulation, the controller has to provide the information listed therein in all cases on its own motion, not only upon request from the data subject. The only exception to this rule is where one of the derogations foreseen in Article 20 applies. In order to ensure compliance with these provisions, we recommend that ENISA draws up standardised privacy statements to be provided individually to all relevant data subjects (investigated persons, whistleblowing, witnesses, etc) whenever ENISA processes data relating them.

Having regard to the **right of access**, Article 28(2) of the EDD states that "*the staff member can request access and copies of all documents directly related to the allegations made against him*". We draw your attention to the fact that the data subject should in principle be granted full access to the *personal data* included in his disciplinary file. The restrictive wording used in the above provision ("*all documents directly related to the allegations*") should therefore not affect the full character of the data subject right. Limitations may only be justified in light of Article 20(c) of the Regulation, for example where it is necessary for the protection of the rights and freedom of others, which encompasses privacy and data protection but possibly also other rights and freedoms. Furthermore, the right of access of any person whose data are processed in the framework of the procedure, other than the data subject, should be taken into account.

Having regard to **whistleblowers' protection**, we would like to stress that the confidentiality rules should apply not only to whistleblowers but also to other individuals providing information in the framework of AI&DP, such as witnesses or simple informants. The identity of these persons should not be disclosed, except when this would contravene national rules on judicial procedures and/or where they maliciously make a false statement. In those cases, these personal data could only be disclosed to judicial authorities.

In relation to the possible **restriction** of access and information rights pursuant to Article 20 of the Regulation, these restrictions cannot be applied systematically. In particular, ENISA should assess the necessity of the restriction on a case by case basis and be able to

demonstrate it upon request. ENISA should also take into account that the restriction can only be temporary and comply with the other prescriptions of Article 20.

We would appreciate if you could inform us of the follow up measures taken concerning the above recommendations within three months of reception of this letter. Considering that this is an ex post prior-check, the recommendations need to be immediately applied by ENISA to ongoing processing activities.

We remain at your disposal should you have any questions concerning this matter.

Yours sincerely,

(**signed**)

Giovanni BUTTARELLI

Cc: Ulrike Lechner (Data Protection Officer) - ENISA