WOJCIECH RAFAŁ WIEWIÓROWSKI
ASSISTANT SUPERVISOR

Interim Director
European Institute of Technology & Innovation (EIT)
Infopark 1/E - Neumann Janos utca,
1117 Budapest
Hungary

Brussels, 17 January 2018
WW/XK/sn/D(2018)0115 **C 2016-1165**
Please use edps@edps.europa.eu for all correspondence

Subject: **EDPS prior-check Opinion on *"administrative inquiries and disciplinary proceedings"* at EIT (case 2016-1165).**

Dear Mr ...,

We have analysed the notification on the processing operations in the context of administrative inquiries and disciplinary proceedings at EIT sent to the EDPS for prior checking under Article 27 of Regulation (EC) No 45/2001 (the Regulation)[1] on 16 December 2016[2].

The EDPS has updated the Guidelines[3] on processing personal information in administrative inquiries and disciplinary proceedings ('the Guidelines'). On this basis, the EDPS will identify and examine the agency's practices, which do not seem to be in conformity with the principles of the Regulation, as further outlined by the EDPS Guidelines, providing EIT with specific recommendations in order to comply with the Regulation.

[1] OJ L 8/1, 12/01/2001.
[2] As this is an ex-post case, the deadline of two months does not apply. The EDPS has dealt with this case on a best-effort basis.
[3] Available on our website: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/16-11-18_Guidelines_Administrative_Inquiries_EN.pdf

Legal analysis

1) Necessity and proportionality when collecting data

On the basis of the information provided, it seems that EIT has not adopted written rules on the use of different means for collecting potential evidence in the context of administrative inquiries or disciplinary proceedings.

In light of Article 4(1)(c) of the Regulation[4] as further outlined by the Guidelines[5], investigators should rigorously apply the principles of necessity and proportionality when choosing the means of inquiry. The principle of data minimisation should be applied for all means and steps of the investigation. Investigators should limit the collection of personal information to what is directly relevant and necessary to the purpose of the inquiry and of the disciplinary proceeding. They should also retain the information only for as long as it is necessary to fulfil that purpose. In other words, investigators should collect only the personal data they really need, and they should keep it only for as long as they need it.

There are some more and less intrusive means of collecting data in the context of an inquiry or a disciplinary proceeding.

For example, the *hearing* of the person under investigation, of witnesses and victim is usually a proportionate option, as it is the least intrusive and the most transparent means to conduct an inquiry and establish the alleged facts relevant to the inquiry.

When collecting *paper information*, investigators should consider blanking out irrelevant or excessive information to the inquiry.

If *electronic information* related to the person under investigation is necessary and relevant evidence to the inquiry, the IT service should be in charge of implementing the technical aspects of the collection on instructions of the investigators. The number of authorised IT officers in charge should be strictly limited (need-to-know principle). The investigators' request should be specific so that the IT service will extract only relevant information[6].

EIT should provide guidance helping investigators choose the appropriate means for collecting evidence and reducing the amount of personal data collected to what is necessary. This guidance can be included in a manual or other instructions to investigators.

EIT should consult its DPO in this regard and take into consideration the DPO's practical guidance and advice.

---

[4] *"Personal data must be adequate and not excessive in relation to the purposes for which they are collected and/or further processed".*

[5] See para. 16-26 of the Guidelines.

[6] See also section 2.6 of another set of EDPS guidelines, the "EDPS Guidelines on personal data and electronic communications in the EU institutions" about different methods that can be employed to investigate serious offences (access to e-Communications data, covert surveillance, forensic imaging of the content of computers and other devices, available on our website: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/15-12-16_eCommunications_EN.pdf.

Recommendation:

1. EIT should provide specific guidance on applying the data protection rules when using different means for collecting potential evidence for the investigation.

2) Retention periods

In accordance with Article 4(1)(e) of the Regulation, personal data must not be kept longer than necessary for the purpose for which they are collected or further processed.

The notification refers to a maximum period of 20 years from the closing date of the inquiry or from the date of the disciplinary decision. The EDPS invites EIT to consider three possible scenarios in light of the revised Guidelines[7]:

1) Pre-inquiry file: For cases in which EIT makes a preliminary assessment of the information collected and the case is dismissed, EIT should set up a maximum retention period of two years after the adoption of the decision that no inquiry will be launched. This maximum retention period could be necessary for audit purposes and complaints to the Ombudsman.

2) Inquiry file: When EIT launches an inquiry including the collection of evidence and interviews of individuals, there are three possibilities: i) the inquiry is closed without follow-up, ii) a caution is issued or iii) the Appointing Authority of the institution adopts a formal decision that a disciplinary proceeding should be launched.

For cases i) and ii), a maximum of five-year-period from closure of the investigation is considered to be a necessary retention period, taking into account audit purposes and legal recourse from affected individuals.

For case iii), EIT should transfer the inquiry file to the disciplinary file, as the disciplinary proceeding is launched on the basis of the evidence collected during the administrative inquiry.

3) Disciplinary file: EIT carries out a disciplinary proceeding with the assistance of internal and/or external investigators (Disciplinary Board). In principle, EIT should take into consideration the nature of the sanction, possible legal recourses as well as audit purposes and set up a maximum retention period, after the adoption of the final Decision.

If the staff member submits a request, under Article 27 of Annex IX to the Staff Regulations, for the deletion of a written warning or reprimand (3 years after the Decision) or in the case of another penalty (6 years after the Decision, except for removal from post) and the Appointing Authority grants the request, the disciplinary file which led to the penalty should also be deleted. If the Decision on the penalty stored in the personal file is deleted, there is no reason to keep the related disciplinary file. The Appointing Authority should assess whether to grant this request in light of the severity of the misconduct, the seriousness of the disciplinary measure imposed and possible repetition of the misconduct.

[7] See para. 52-53 of the EDPS Guidelines.

Recommendation:

2. EIT should distinguish between different retention periods according to the possible scenarios explained above.

3) Information to be given to the individuals concerned

Informing individuals concerned

EIT has prepared a privacy statement, which is communicated to the individuals concerned before an administrative inquiry.

Content of the data protection notice

EIT has prepared a detailed and comprehensive privacy statement including relevant information listed in Articles 11 and 12 of the Regulation.

Recommendation:

3. Under Articles 11(1)(f)(ii) and 12(1)(f)(ii) of the Regulation, EIT should also indicate clearly in the privacy statement the three different scenarios and their respective retention periods, as outlined above.

Possible limitations to the rights of information, access and rectification of the individuals concerned:

EIT refers in the privacy statement to possible restrictions to the right of information, access and rectification in light of Article 20 of the Regulation.

Reminder:

In cases where EIT decides to apply a restriction of information, access, rectification etc. under Article 20(1) of the Regulation, or to defer the application of Article 20(3) and 20(4)[8], such decision should be taken strictly on a case by case basis. In all circumstances, **EIT should document the reasons for taking such decision (i.e. motivated decision).** These reasons should prove that the restriction is necessary to protect one or more of the interests and rights listed in Article 20(1) of the Regulation and they should be documented before the decision to apply any restriction or deferral is taken[9].

4) Security measures

EIT has put in place some technical and organisational security measures.

In addition to the organisational measures, due to the sensitive nature of the data processed (for example, it might be the case that data related to health are processed), the EDPS recommends that **all authorised officers involved sign confidentiality declarations stating that they are**

[8] under Article 20(5) of the Regulation.

[9] This is the kind of documentation the EDPS requests when investigating complaints relating to the application of Article 20.

subject to an obligation of professional secrecy equivalent to that of a health professional. These declarations will contribute in maintaining the confidentiality of personal data and in preventing any unauthorised access within the meaning of Article 22 of the Regulation.

Conclusion

The EDPS considers that there is no reason to believe that there is a breach of the provisions of the Regulation provided that the recommendations made in this Opinion are fully taken into account.

In light of the accountability principle, the EDPS **expects EIT to implement the above recommendations** accordingly and has therefore decided to **close the case**.

Yours sincerely,

(**signed**)

Wojciech Rafał WIEWIÓROWSKI

Cc: Data Protection Officer, EIT
Acting Head of Service and Finance Unit, EIT