EUROPEAN DATA PROTECTION SUPERVISOR

WOJCIECH RAFAŁ WIEWIÓROWSKI
ASSISTANT SUPERVISOR

(...)
Director Administration
EFTA Surveillance Authority
Rue Belliard 35
1040 Brussels

Brussels,
WW/XK/sn/D(2018)2139 **C 2017-1142**
Please use edps@edps.europa.eu for all correspondence

Subject: **EDPS prior-check Opinion on *"HR Administrative, B, H and V, Disciplinary and Grievance investigations"* at EFTA Surveillance Authority (case 2017-1142)**

Dear (...),

On 14 December 2017[1], the EDPS received an ex-post prior-checking notification under Article 27 of Regulation (EC) No 45/2001 (the Regulation)[2] on the processing operations in the context of administrative inquiries and disciplinary proceedings[3] at EFTA Surveillance Authority (ESA). The notification was sent from the Data Protection Officer (DPO) of ESA for ex-post prior-checking under Article 27 of EFTA Surveillance Authority decision of 15 December 2016 laying down rules on data protection ('the Decision')[4].

The EDPS has issued Guidelines[5] on processing personal information in administrative inquiries and disciplinary proceedings ('the EDPS Guidelines'). Although, the EDPS Guidelines are primarily based on the Regulation, given the strong similarities between the Regulation and the Decision, the main elements of the Guidelines are also applicable in this case. On this basis, the EDPS will identify and examine ESA's practices, which do not seem to be in conformity with the principles of the Regulation, as further outlined by the EDPS Guidelines, providing ESA with specific recommendations in order to comply with the

[1] 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.
[2] OJ L 8/1, 12/01/2001.
[3] It was indicated in the notification: "*HR Administrative, B, H and V, Disciplinary and Grievance investigations*".
[4] College Decision 235/16/COL.
[5] 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

Regulation. The EDPS invites ESA to consult the EDPS Guidelines when it implements the EDPS recommendations.

ESA has sent the following documents attached to the notification:
i) EFTA Surveillance Authority Staff Regulations & Rules (ESA's SF and Rules) and
ii) a privacy statement entitled "new starters, staff and leavers".

Legal analysis

1) Grounds for prior checking

The notification states that the processing operations under analysis are justified for prior checking under Article 27(a) and (c) of the Decision.

Article 27(2)(a) of the Decision is indeed considered a legal ground for prior-checking, as the processing operations under analysis may entail the processing of data relating to suspected offences, criminal convictions or security measures within the meaning of the provision.

The EDPS stresses that, the processing operations are also intended to evaluate personal aspects relating to the individuals involved, in particular their alleged misconduct within the meaning of Article 27(2)(b) of the Decision.

The notification refers to Article 27(2)(c) of the Decision stating "where data collected and used in the investigation as evidence will normally have been collected for different purposes than such an investigation". Article 27(2)(c) of the Decision applies in processing operations which allow linkages not provided for pursuant to legislation between data processed for different purposes[6]. In the present case, an administrative inquiry or disciplinary proceeding entails the processing of different categories of personal data (i.e. allegations, testimonies etc.) from different individuals concerned (i.e. alleged victim, person under investigation, witness, other staff concerned at ESA etc), who are bound by ESA's SR and Rules. These data may either (1) be collected directly for the administrative inquiry or disciplinary proceeding (e.g. a witness statement) or (2) be used for the administrative inquiry or disciplinary proceeding after initially having been created for different purposes (meaning a change of purpose, see below; e.g. a document containing personal data used as evidence). Article 27(2)(c) of the Decision targets situations such as interconnecting different databases without a proper legal basis.[7]

An administrative inquiry or disciplinary proceeding does not entail linkages of different sources of data extracted from different databases or platforms not provided for by legislation, in the sense of Article 27(2)(c) of the Decision.

[6] For example, when the purpose of a processing is to monitor what various social media users say and how they react about an EU institution, such processing entails linkages of different sources of data from different social media platforms.
[7] See EDPS prior-check Opinion in case 2016-0674: https://edps.europa.eu/data-protection/our-work/publications/opinions-prior-check/import-export-and-transit-directory-olaf_en.

The processing operations are therefore subject to prior-checking by the EDPS because they fall within the category of risky processing operations under Article 27(2)(a) and (b) of the Decision[8].

2) Lawfulness of administrative inquiries

The lawfulness of a processing must be justified on the basis of one of the five legal grounds under Article 5 of the Decision.

Processing operations for administrative inquiries and disciplinary proceedings can in principle considered to be lawful under Article 5(a) of the Decision.

Article 5 (a) of the Decision requires two elements: the processing must be based on the "EEA Agreement or legal acts incorporated into that Agreement" (a legal basis must be provided) and the processing must be necessary for the performance of a task carried out in the public interest (a necessity test must be established).

Legal basis

The notification refers to ESA's SR and Rules. Article 44 of those rules concerns only the disciplinary measures that the "Responsible Member" may authorise. ESA's SR and Rules do not provide a legal basis for the conduct of administrative inquiries and disciplinary procedures[9]. A legal basis means a legally binding decision, policy or implementing rules regarding administrative inquiries and disciplinary proceedings. The EDPS therefore recommends that ESA adopt such a specific legal instrument; this should define the purpose of an administrative inquiry and of a disciplinary proceeding, establish the different stages of the procedures and set out detailed rules and principles to be followed in the context of an inquiry and a disciplinary proceeding. A specific legal instrument is fundamental, as it will set out the process of an administrative inquiry or a disciplinary proceeding with legal certainty, safeguards and clarity. It should also enable those involved in the process to have the necessary information about their rights and how to exercise them. This legal instrument could then serve as a specific legal basis for administrative inquiries and disciplinary proceedings, which is missing from ESA's SR and Rules.

Necessity test

Provided that ESA adopts a legal basis which implements the procedures applicable in administrative inquiries and disciplinary proceedings, the processing of personal data in this context can be considered as necessary in compliance with the adopted rules.

Recommendation:

2. ESA should adopt a legal instrument setting out the different stages of the procedures as well as the rules and principles to be followed in the context of an administrative inquiry and a disciplinary proceeding.

[8] Article 27(2) of the Regulation contains a list of processing operations that are likely to present risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, including point (c) processing operations allowing linkages not provided for pursuant to national or EU legislation between data processed for different purposes.

[9] See para. 9-10 of the EDPS Guidelines.

In the meantime, in case ESA needs to launch an administrative inquiry, the DPO should be consulted before any personal data are processed for the inquiry.

3) Necessity and proportionality when collecting data

On the basis of the information provided, it seems that ESA 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 Decision[10] and as further outlined by the Guidelines[11], 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 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[12].

ESA 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.

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

---

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

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

[12] 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:
3. ESA should provide specific guidance on applying the data protection rules when using different means for collecting potential evidence for the investigation.

4) Retention periods

In accordance with Article 4(1)(e) of the Decision, 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 period of six years after the conclusion of the investigation for all data collected for the purposes of conducting any investigation. This is in order to allow for any recurrent patterns or multiple cases to be identified during the typical employment term of an ESA staff member.

The EDPS invites ESA to consider some possible scenarios in light of the revised Guidelines[13] and apply them, where appropriate:

1) Pre-inquiry file: For cases in which ESA makes a preliminary assessment of the information collected and the case is dismissed, ESA 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.

2) Inquiry file: When ESA launches an inquiry including the collection of evidence and interviews of individuals, there could be three possibilities: i) the inquiry is closed without follow-up, ii) a sanction under Article 44 of ESA's SF and Rules has been decided, iii) the "Responsible Member" 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), ESA 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: In principle, ESA 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.

Furthermore, the notification states that where the final outcome of any investigation and associated appeals procedure is the imposition of a disciplinary sanction, the data collected will be retained for a period of 5 years after the end of employment of the individual(s) concerned. The reason is so that any relevant information may be used to inform reference checks for individuals returning to ESA.

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

The EDPS invites ESA to consider the possibility that a staff member might want to exercise their right of erasure and submit a request for deletion[14]. In such cases, ESA should set up different time-limits, that a staff member may submit a request in light of each disciplinary measure imposed. ESA 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. In cases where ESA grants the request and the decision on the penalty stored in the personal file is deleted, the disciplinary file, which led to the penalty, should also be deleted.

Recommendation:
4. ESA should distinguish between different retention periods according to the possible scenarios explained above.

5) Rights of access and rectification

The notification refers to the following: "Authority procedure for data subject requests (DSR) (document 863894)". It is a general document on how data subjects can exercise their rights regarding a processing operation. It does not mention any information how the individuals may exercise their right of access and rectification specifically in the context of an administrative inquiry and a disciplinary proceeding.

For example, a person under investigation should be entitled to comment on the facts concerning them. They should be sent a summary of the facts and preliminary conclusions and be allowed to send comments within a specific deadline[15].

Recommendation:
5. ESA should put in place modalities in order to ensure that all individuals concerned in the context of an administrative inquiry or disciplinary proceeding may exercise their right of access and rectification within the meaning of Articles 13 and 14 of the Decision and in light of the EDPS Guidelines. This information should be provided in the privacy statement (see below).

6) Information to be given to the individuals concerned

Informing individuals concerned and content of the privacy statement

ESA has provided a privacy statement entitled "new starters, staff and leavers". This privacy statement is irrelevant to the processing operations under analysis.

ESA should prepare a privacy statement, which should refer to all relevant information related to administrative inquiries and disciplinary proceedings following the list of elements stated in Articles 11 and 12 of the Regulation in a clear, comprehensive and plain language. This privacy statement should be posted where ESA will publish all the relevant documents about

[14] For example, under Article 27 of Annex IX to the EU Staff Regulations, a staff member may request 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.
[15] See further pages 11, 12 and 14 of the EDPS Guidelines: https://edps.europa.eu/sites/edp/files/publication/16-11-18_guidelines_administrative_inquiries_en.pdf.

administrative inquires and disciplinary proceedings (ESA's Rules and Manual). The privacy statement should also which is communicated to the individuals concerned before an administrative inquiry[16].

Recommendation:
6. Under Articles 11 and 12 of the Decision, ESA should prepare a privacy statement regarding the processing operations under analysis, as explained above.

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

ESA should also refer in the privacy statement to possible restrictions to the right of information, access and rectification in light of Article 20 of the Regulation[17].

Reminder:

In cases where ESA decides to apply a restriction of information, access, rectification etc. under Article 20(1) of the Decision, or to defer the application of Article 20(3) and 20(4)[18], such decision should be taken strictly on a case by case basis. In all circumstances, **ESA 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 Decision and they should be documented before the decision to apply any restriction or deferral is taken[19]**.**

7) Security measures

(...)

Conclusion

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

In light of the accountability principle, the EDPS **expects ESA to consult the EDPS Guidelines and implement the above recommendations** accordingly.

The EDPS has therefore decided to **close the case**.

Yours sincerely,

[16] See further page 12 of the EDPS Guidelines: https://edps.europa.eu/sites/edp/files/publication/16-11-18_guidelines_administrative_inquiries_en.pdf.
[17] See further pages 13, 14 and 15 of the EDPS Guidelines: https://edps.europa.eu/sites/edp/files/publication/16-11-18_guidelines_administrative_inquiries_en.pdf.
[18] under Article 20(5) of the Decision.
[19] This is the kind of documentation the EDPS requests when investigating complaints relating to the application of Article 20.

(signed)

Wojciech Rafał WIEWIÓROWSKI

Cc: (...), Data Protection Officer, ESA