WOJCIECH RAFAŁ WIEWIÓROWSKI
ASSISTANT SUPERVISOR

Mr (...)
Executive Director
European Banking Authority (EBA)
Floor46, One Canada Square,
Canary Wharf,
London, E14 5AA,
UK

Brussels,
WW/XK/sn/D(2018)1720 **C 2017-1083**
Please use edps@edps.europa.eu for all correspondence

Subject: **EDPS prior-check Opinion on *"administrative inquiries and disciplinary proceedings"* at EBA (case 2017-1083)**

Dear Mr (...),

We have analysed the notification on the processing operations in the context of administrative inquiries and disciplinary proceedings at EBA 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 EBA 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) Lawfulness of administrative inquiries

The DPO sent to the EDPS a copy of the "Decision of the Management Board concerning the terms and conditions for internal investigations in relation to the prevention of fraud, corruption and any illegal activity detrimental to the Union's interests" as well as a copy of the "Accession of EBA to the Interinstitutional Agreement of 25 May 1999 concerning internal investigations by OLAF". The DPO informed the EDPS that in June 2015 there was a request from EBA to the European Commission for agreement to the draft decision on administrative inquiries and disciplinary proceedings. There have been some informal updates in the meantime from the Commission, but there has been no formal agreement received as yet and therefore there is no implementing rule yet at EBA, nor a manual of procedures.

The EDPS highlights that the lawfulness of a processing must be justified on the basis of one of the five legal grounds under Article 5 of the Regulation.

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

Article 5 (a) of the Regulation requires two elements: the processing must be based on the Treaties or on an EU legal instrument based on the Treaties (a specific legal basis must be provided) and it must be necessary for the performance of a task carried out in the public interest (the necessity test must be established).

Legal basis

Article 86 of the Staff Regulations and their Annex IX do not on their own provide a legal basis for the conduct of administrative inquiries and disciplinary proceedings[4]. A legal basis means a legally binding decision, policy or implementing rules regarding administrative inquiries and disciplinary proceedings. The EDPS therefore recommends that EBA 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 will allow EBA to carry out a lawful processing operation related to an inquiry or a disciplinary proceeding.

Necessity test
Provided that EBA 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:
1. EBA 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.

[4] See paragraphs 9 and 10 of the EDPS Guidelines.

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

2) Necessity and proportionality when collecting data

On the basis of the information provided, it seems that EBA 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[5] as further outlined by the Guidelines[6], 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[7].

EBA 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.

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

---

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

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

[7] 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:
2. EBA should provide specific guidance on applying the data protection rules when using different means for collecting potential evidence for the investigation.

3) 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 distinction of retention periods applicable in three possible cases. It also refers to a period of 20 years from the date of the Executive Director's decision closing the disciplinary proceedings.

As to the personal data kept in the disciplinary file, EBA 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, 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. In any case, EBA could grant the possibility to the person concerned to submit a request for the deletion of their disciplinary file 10 years after the adoption of the final decision. The Appointing Authority should assess whether to grant this request in light of the severity of the misconduct, the nature of the penalty imposed and the possible repetition of the misconduct during that period of 10 years.

Recommendation:
3. EBA is invited to re-consider the different retention periods according to the possible scenarios as explained in the EDPS revised Guidelines[8].

4) Information to be given to the individuals concerned

Informing individuals concerned

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

Content of the data protection notice

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

Recommendation:

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

4. Under Articles 11(1)(f)(ii) and 12(1)(f)(ii) of the Regulation, EBA should indicate clearly in the privacy statement the different scenarios and their respective retention periods, in light of the revised EDPS Guidelines.

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

EBA 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 EBA 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)[9], such decision should be taken strictly on a case by case basis. In all circumstances, **EBA 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[10].

5) Security measures

EBA has indicated in the notification some security measures.

In accordance with Article 22 of the Regulation, both technical and organisational measures need to be implemented in order to prevent, in particular, any unauthorised disclosure or access, accidental or unlawful destruction, accidental loss or alteration, as well as any other form of unlawful processing. These measures must ensure "a level of security appropriate to the risks represented by the processing" [11].

From the information received from EBA, (....)

Conclusion

The EDPS stresses that EBA should adopt a specific legal basis and implement all the above recommendations in order to be in conformity with the provisions of the Regulation.

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

[9] under Article 20(5) of the Regulation.
[10] This is the kind of documentation the EDPS requests when investigating complaints relating to the application of Article 20.
[11] See pages 19 and 20 of the EDPS Guidelines: https://edps.europa.eu/sites/edp/files/publication/16-11-18_guidelines_administrative_inquiries_en.pdf.

Yours sincerely,

(signed)

Wojciech Rafał WIEWIÓROWSKI

Cc: Mr (...), Data Protection Officer, EBA
Ms (...), Head of Human Resources, EBA