

From: SUPERVISION [REDACTED]
To: [REDACTED]
Sent at: 31/05/24 17:16:31
Subject: Our ref.: 2022-1189 - D(2024) 1786

Dear [REDACTED]

We acknowledge receipt of your email of 20 May 2024.

In our email of 15 May 2024, the EDPS informed you that we had come to the conclusion that EPSO has complied with the EDPS order to grant you access to all your log data available in the systems used for the purpose of managing selection procedures, and that we had consequently decided to close case 2022-1189.

In a separate email of 15 May 2024, the EDPS referred to EPSO's reply to you of 3 May 2024, following up on the abovementioned EDPS order in case 2022-1189, and informed you that EPSO's reply to you suggests that there might be additional potential infringements under Regulation (EU) 2018/1725. We therefore informed you that we would open a new complaint case and investigate the new elements and potential violations brought to our attention.

In your email of 20 May 2024, you express your disagreement both with the decision to close case 2022-1189, and the decision not to investigate these new elements and potential infringements under this case.

As regards the closure of case 2022-1189, we refer to our email of 15 May 2024, and reiterate that case 2022-1189 is closed.

As regards the new elements and potential infringements by EPSO, we note that you seem to agree with the EDPS investigating the matter as a complaint. In this context, we remind you that it is for the EDPS to decide how to investigate matters brought to our attention. We would also like to draw your attention to the fact that these new elements concern a separate issue to the infringement identified in case 2022-1189, as it is about the deletion of personal data rather than about the right of access.

In light of the above, the EDPS has decided to open a new complaint case against EPSO. The case number is Case 2024-0500, please refer to this number in your future correspondence with the EDPS.

We will keep you duly informed of any new developments in this case.

Yours sincerely,

S&E Secretariat on behalf of Thomas Zerdick, Head of Unit

SUPERVISION & ENFORCEMENT UNIT



| Tel. (+32) 228 31900 | Fax +32(0)22831950 | ›

Email Supervision@edps.europa.eu

European Data Protection Supervisor

Postal address: Rue Wiertz 60, B-1047 Brussels

Office address: Rue Montoyer 30, B-1000 Brussels

@EU_EDPS www.edps.europa.eu

This email (and any attachment) may contain information that is internal or confidential. Unauthorised access, use or other processing is not permitted. If you are not the intended recipient please inform the sender by reply and then delete all copies. Emails are not secure as they can be intercepted, amended, and infected with viruses. The EDPS therefore cannot guarantee the security of correspondence by email.



Data Protection Notice

According to Articles 15 and 16 of Regulation (EU) 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, please be informed that your personal data will be processed by the EDPS, where proportionate and necessary, for the purpose of investigating your complaint. The legal basis for this processing operation is Article 57(1)(e) of Regulation (EU) 2018/1725. The data processed will have been submitted by you, or from other sources during the inquiry of your complaint, and this may include sensitive data. Your data will only be transferred to other EU institutions and bodies or to third parties when it is necessary to ensure the appropriate investigation or follow up of your complaint. Your data will be stored by the EDPS in electronic and paper files for up to ten years (five years for prima facie inadmissible complaints) after the case closure, unless legal proceedings require us to keep them for a longer period. You have the right to access your personal data held by the EDPS and to obtain the rectification thereof, if necessary. Any such request should be addressed to the EDPS at edps@edps.europa.eu. Your data might be transferred to other EU institutions and bodies or to any third parties only where necessary to ensure the appropriate handling of your request. You may also contact the data protection officer of the EDPS (DPO@edps.europa.eu), if you have any remarks or complaints regarding the way we process your personal data. You can find the full version of our data protection notice on complaint handling at: https://edps.europa.eu/data-protection/our-role-supervisor/complaints-handling-data-protection-notice_en.

From: [REDACTED]

Sent: 20 May 2024 18:17

To: SUPERVISION <supervision@edps.europa.eu>; European Data Protection Supervisor <EDPS@edps.europa.eu>

Subject: Your ref: 2022-1189 and emails of 14/05/2023 and 15/05/2023

Importance: High

Dear EDPS and Supervision,

Thanks four your emails of (attached):

14/05/2023 with subject:"Our ref.: 2022-1189 - D(2024) 1540 - Webform submission from: Complaint form sent on 13 February 2024 - to be linked with Case 2022-118"

15/05/2023 with subject:"Our ref.: 2022-1189 - D(2024) 1552 - Closure of Case 2022-1189"

On your email of 14/05/2023 you stated:

"[...]Thank you for your e-mail of 6 May 2024, informing us of the EPSO's reply of 3 May 2024, which follows up on the EDPS order of 31 October 2023 (Case 2022-1189).

EPSO's reply suggests that there might be additional potential infringements under Regulation (EU) 2018/1725.

The EDPS will therefore open a new complaint case and investigate the new elements and potential violations brought to our attention.

In case you disagree, please inform us accordingly by 21 May 2024.[...] " (bold added by me)

I disagree with the EDPS opening a new complaint. I request that the already existing case 2022-1189 is used instead as the EDPS shouldn't have closed it (see below).

On your email of 15/05/2023 you stated:

"We have carefully analysed EPSO's reply to you of 30 November 2023, and its further clarifications provided by letter of 3 May 2024. The EDPS concludes that EPSO has provided you with the logs generated by consultation operations of your EPSO profile that it had in its possession. This means that EPSO has complied with the EDPS order to grant you access to all your log data available in the systems used for the purpose of managing selection procedures.

In light of the above, the EDPS has decided to close Case 2022-1189."

By filling a complaint form of 13/02/2024 I lodged a complaint that you linked (your email of 7/03/2024) to the case number 2022-1189:

"[...]The file will be linked to your complaint case number 2022-1189.

The EDPS will assess your complaint of 13 February 2024 (below) as well as EPSO's reply sent to you on 30 November 2023 regarding the EDPS order of 31 October 2023 that EPSO provide you access to all your log data, the time and purpose of each access[...]"

On my complaint of 13/02/2024:

- I informed you (again) about the purge and provided logs and a video (I provided the video later by email as the complaint form didn't allow me to upload it)
- I informed the EDPS: "EPSO has ignored my request to inform me (as a data subject) and to the EDPS the two data breaches from my letter from 1/02/2023 (LetterAfterRevisedDecision-ANNEXES-signed.pdf EDPS was in CC)"

In the Letter LetterAfterRevisedDecision-ANNEXES-signed.pdf (attached), I thoroughly explained why EPSO's provided logs were not EUDPR compliant nor Pankki compliant and made some requests under the EUDPR that EPSO ignored.

Also, I thoroughly analysed EPSO's reply against its ROPA and demonstrated how EPSO's reply was not EUDPR nor Pankki nor ROPA compliant (see 4 LOGs provided in my letter LetterAfterRevisedDecision-ANNEXES-signed.pdf). EPSO's ROPA document mentions the existence of more logs.

In paragraph 6.7 and 6.11 to 6.16 of his Review Decision of 31 October 2023, the EDPS stated the following:

"6.7. However, the EDPS notes that EPSO has not submitted any evidence or documentation

to support its statement in the reply of 26 October 2023 that this type of logfile does not exist."

6.11. In this context, the EDPS draws the attention of EPSO to the principle of accountability

laid down in Article 4(2) of the Regulation, which states that "the controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."

Moreover, Article 26(1) EUDPR requires the controller "to implement appropriate technical

and organisational measures to ensure and to be able to demonstrate that processing is

performed in accordance with that Regulation, taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for

the rights and freedoms of natural persons. Those measures shall be reviewed and updated

where necessary" (emphasis added).

6.12. In relation to Article 5(2) of the GDPR the Court has recently confirmed its case-law:

"The controller, in accordance with the principle of 'accountability' laid down in that provision, is responsible for compliance with paragraph 1 of that article and must be able to

demonstrate its compliance with each of the principles set out in paragraph 1 of that article,
the burden of such proof thus being placed on it".¹⁰ On 4 July 2023, the Grand Chamber

clarified even further that "in accordance with Article 5 of the GDPR, the controller bears

the burden of proving that those data are collected, inter alia, for specified, explicit and legitimate purposes and that they are processed lawfully, fairly and in a transparent manner

in relation to the data subject." (emphasis added).¹¹

6.13. In his Opinion of 27 April 2023 in Case C 340/21, Natsionalna agentsia za prihodite, Advocate General Pitruzella confirmed that "[t]he principle of accountability is one of the central pillars of the GDPR and one of its most significant innovations. It places responsibility firmly on the controller to take proactive action to ensure compliance and to be ready to demonstrate that compliance."

6.14. The European Commission refers to the principle of accountability as one of the shared concepts and principles on which the GDPR, the EUDPR and Directive 2016/680" are based, resulting in the consistent interpretation and application of EU data protection rules."

6.15. The principle of accountability therefore places on the controller the duty to prove its compliance with the Regulation. Any uncertainties in that regard must be borne by the responsible controller.

"6.16. In accordance with the principle of accountability, it is thus for EPSO to demonstrate

its compliance with the complainant's right to access in accordance with Article 17(1) of the Regulation and EPSO must bear the burden of proof that some of the logfiles that the complainant requested in his email of 20 November 2022 do not exist."

EPSO's ROPA clearly states that the logs exist.

It is EPSO's task to demonstrate compliance.

EPSO:

- hasn't submitted yet any evidence or documentation to support all its statements
- hasn't provided any recipient. (see 3.2 Recipients of my letter LetterAfterRevisedDecision-ANNEXES-signed.pdf)
- has acknowledged the purge but hasn't provided the disloyal employee details.
- has acknowledged the purge but hasn't informed me nor the EDPS about this data breach.
- hasn't fulfilled any of my requests (pages 12-14 of my letter LetterAfterRevisedDecision-ANNEXES-signed.pdf).
- hasn't restored the unlawfully purged data (see 3.4 Backups and Logs of my letter LetterAfterRevisedDecision-ANNEXES-signed.pdf).

I would like to bring to your attention that EPSO and EUIPO were joint controllers on some of the purged selection procedures and both should share the responsibility of The Purge.

From your Monitoring and enforcing compliance with Regulation (EU) 2018/1725[1]:

"Example: a person complains that an EUI unlawfully withheld personal data it held about her when replying to a request for access to one's own personal data under Article 17 of the Regulation. Following an on-site check, the EDPS decision establishes that the EUI indeed unlawfully withheld the data and orders it to provide a complete reply to the complainant by a specified deadline. **The EUI fails to comply with the order by that deadline. This is a situation in which the EDPS may decide to impose a fine.**" (bold added by me)

From EDPB's guideline on right of access:

"Example 6: On the occasion of replying to an access request a controller realises, that an application of the data subject for a vacancy in the company of the controller has been stored beyond the retention period. **In this case the controller cannot delete first and then reply to the data subject that no data (concerning the application) is processed. It has to give access first and delete the data afterwards.** In order to prevent a subsequent request for erasure it would then be recommended to add information about the fact and time of the deletion. [...]" (bold added by me)

EDPS' closing decision lacks of any substance as EPSO hasn't granted "access to all your log data available in the systems" as clearly and thoroughly explained on my letter LetterAfterRevisedDecision-ANNEXES-signed.pdf and on EPSO's ROPA.

EDPS' closing decision ignores completely my complaint of 13/2/2024. It was

It was EDPS decision (not mine) to link my complaint to case 2022-1189 **"The file will be linked to your complaint case number 2022-1189."** and has closed it without addressing the complaint and the Purge.

EDPS has recognized EPSO's non-compliances by its email of 14/05/2024: **"EPSO's reply suggests that there might be additional potential infringements under Regulation (EU) 2018/1725."** but yet decides to close the 2021-1189.

Therefore I request:

1. that the EDPS reviews its decision to close the case 2022-1189 and keep it open and not open a new complaint. All investigations must be carried out under the already existing 2022-1189
2. that the EDPS orders EPSO to comply with all my request on my letter LetterAfterRevisedDecision-ANNEXES-signed.pdf
3. an on-the-spot investigation on EPSO's facilities to thoroughly investigate the purge and all EPSO non-compliances.
4. to be present in the on-the-spot investigation while the EDPS gathers all the evidence.

I would also like to bring your attention to your case 2024-0230 where EPSO ignored my all requests too.

Finally I would like to remind you of Article 22a of the staff regulations:

"Article 22a

1. Any official who, in the course of or in connection with the performance of his duties, becomes aware of facts which give rise to a presumption of the existence of possible illegal activity, including fraud or corruption, detrimental to the interests of the ► M128 Union ◀ , or of conduct relating to the discharge of professional duties which may constitute a serious failure to comply with the obligations of officials of the ► M128 Union ◀ , shall without delay inform either his immediate superior or his Director-General or, if he considers it useful, the Secretary-General, or the persons in equivalent positions, or the European Anti-Fraud Office (OLAF) direct.[...]" (bold added by me).

Thanks for your time

Best regards

[Redacted signature block]
