

From:

To:

CC:

EPSO DATA PROTECTION COORDINATOR (EC) <epso-data-protection-coordinator@ec.europa.eu>;
SUPERVISION <supervision@edps.europa.eu>

Sent at:

14/03/24 20:42:37

Subject:

RE: EPSO's reply to Complaint EDPS ref. 2022-1189 and
2024-0230 - the way forward- documents

Dear

I have already sent to you and a webex link for our meeting on Monday at 15h.

Please find attached his allegations and screenshots (most of which EPSO has already received from him directly) as well as
two further access request complaints submitted by him in February 2024:

- 1) 'Request for Review': this is his reaction right after EPSO has provided him with the logs in view of implementing the EDPS order of 31 October 2023 (Although I have not attached your reply to him, we have some questions on EPSO's reply);
- 2) 'Manipulation with Videos': this was an Annex to his reaction alleging 'purges',
- 3) 'Request for access to personal data – Selection procedures...': he alleges unlawful breaches,
- 4) 'Webform submission form: Complaint form': he submitted a complaint on 13 February 2024 with attachments on alleged breaches,
- 5) 'Webform submission form: Complaint form sent on 18 February 2024': he submitted another complaint on 18 February with attachments on access to his personal data with a holding reply from EPSO.

The objective of the meeting is to better understand what he is alleging and seek clarifications from you in order to be able to assess and provide him with a comprehensive (definitive) position.

Many thanks for your availability.

Kind regards,

Legal Officer Supervision & Enforcement

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.

From: [REDACTED]
Sent: 14 March 2024 18:12
To: [REDACTED]
Cc: [REDACTED]; SUPERVISION <supervision@edps.europa.eu>; EPSO DATA PROTECTION COORDINATOR (EC) <epso-data-protection-coordinator@ec.europa.eu>; EC DPO (EC) <ec-dpo@ec.europa.eu>; EPSO SECTEUR JURIDIQUE (EC) <epso-secteur-juridique@ec.europa.eu>
Subject: RE: EPSO's reply to Complaint EDPS ref. 2022-1189 - the way forward-some questions

Dear [REDACTED]

Thank you, I would appreciate it if you could send a Webex link. Also, I would be grateful if you could send us the complainant's allegations and screenshots tomorrow at the latest, so that we have time to assess them before the meeting.

Kind regards,

[REDACTED]

From: [REDACTED]
Sent: Thursday, March 14, 2024 5:47 PM
To: [REDACTED]
Cc: [REDACTED]
SUPERVISION Xxx (EDPS) <supervision@edps.europa.eu>; EPSO DATA PROTECTION COORDINATOR <EPSO-DATA-PROTECTION-COORDINATOR@ec.europa.eu>; EC DPO <EC-DPO@ec.europa.eu>; EPSO SECTEUR JURIDIQUE <EPSO-SECTEUR-JURIDIQUE@ec.europa.eu>
Subject: RE: EPSO's reply to Complaint EDPS ref. 2022-1189 - the way forward-some questions

Dear [REDACTED]

Many thanks for your prompt reply.

If you want I can send you a webex link for Monday 18/03 for 45 mins at 15h.

I will send you later the complainant's allegations and screenshots.

Kind regards,

[REDACTED]

From: [REDACTED]
Sent: 14 March 2024 17:11
To: [REDACTED]
Cc: [REDACTED]; SUPERVISION <supervision@edps.europa.eu>; EPSO DATA PROTECTION COORDINATOR (EC) <epso-data-protection-coordinator@ec.europa.eu>; EC DPO (EC) <ec-dpo@ec.europa.eu>; EPSO SECTEUR JURIDIQUE (EC) <epso-secteur-juridique@ec.europa.eu>
Subject: RE: EPSO's reply to Complaint EDPS ref. 2022-1189 - the way forward- some questions

Dear [REDACTED]

Thank you for your message.

[REDACTED] and I would like to propose to meet online on Monday 18/3 at 15h; hopefully a 30-45' minute meeting should be sufficient. Please let us know if this suits you, and we'll send you an invitation.

Kind regards,
[REDACTED]

From: [REDACTED]
Sent: Monday, March 11, 2024 1:18 PM
To: [REDACTED]
Cc: [REDACTED]
SUPERVISION Xxx (EDPS) <supervision@edps.europa.eu>; EPSO DATA PROTECTION COORDINATOR <EPSO-DATA-PROTECTION-COORDINATOR@ec.europa.eu>; EC DPO <EC-DPO@ec.europa.eu>
Subject: FW: EPSO's reply to Complaint EDPS ref. 2022-1189 - the way forward- some questions

Dear [REDACTED]
Dear [REDACTED]

I hope this e-mail finds you both well.

We would like to have a meeting with you, as we have some specific questions regarding EPSO's implementation of the EDPS order of 31 October 2023 regarding the complaint of [REDACTED] Case 2022-1189 (in attachment), in particular due to the fact that

- the complainant is not satisfied with EPSO's reply and the logs he was provided,
- he has sent screenshots and allegations that EPSO has unlawfully erased and 'purged' his data and
- he has submitted two more complaints v EPSO on access request and potential breaches (on 13th Feb and on 18 Feb 2024).

We would be grateful if you could suggest some dates from now until 26 March 2024, so that we can hopefully clarify all his allegations as soon as possible.

Once we find a specific date, I will send you his allegations and screenshots before the meeting.

Many thanks for your prompt reply.

Kind regards,

A solid black rectangular box used to redact the sender's name and signature.

TO: EDPS@edps.europa.eu

To whom might it concern,

Thanks for your time replying my complaint.

I have just received EPSO's logs at the very end of the deadline breaching Article 14(3) "[...]The controller shall provide information on action taken on a request under Articles 17 to 24 to the data subject without undue delay[...]" As I requested the logs more than 1 year ago.

Long story short they are useless and don't allow me to verify EPSO/EUIPO's processing activities lawfulness as they are basically dates with no context and the purpose is not there (as it should be as per Pannki S, Case C-579/21).

ON THE SUBJECT

Regarding EPSO's reply

As regards your personal data processed for the purposes of the selection procedures EUIPO/CAST/1/16-6, OIHM/CAST/10/2014 FG III, and EPSO/TA/IT/06 IT, the retention periods had already expired at the time of your initial application of 18 June 2022. EPSO informed you of this in its reply of 5 August 2022, with regard to each of the three abovementioned procedures: *"The processing period of your personal data within the framework of this selection procedure, including the retention period, ended."*

It follows that for these three procedures EPSO no longer processes any of your personal data. Consequently, I hereby confirm that for these procedures no log data exist, therefore EPSO is not in a position to communicate such data to you.

EUIPO and/or EPSO deleted my profile after my complaints.

I recorded (**Annex A.02** with a snipped version of the videos embedded) my EPSO profile status using a third party witness before and after my complaints. The selection procedures were there before my complaint and were deleted unlawfully after my complaint.

EPSO should be ready to restore my data and my logs or would be breaching Article 33(1)(1a)(1b)(1c)(1d)(2)(3):

Security of processing

1. Taking into account the state of the art, the costs of implementation and 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, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including, inter alia, as appropriate:

- (a) the pseudonymisation and encryption of personal data;
- (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union law.

By an email thread between 23/01/2023 and 14/06/2023 (**Annex A.01**), I tried to follow up the complaint with the EDPS providing more information, background and some recitals from EDPB's guideline on right of access and already informed EDPS that EUIPO/EPPO deleted unlawfully my data **advancing factual evidence** of EUIPO's/EPPO's wrongdoings:

“[...]EUIPO nor the European Commission have ever provided me with a single line of logs and even they have deleted the data which I requested the logs about. By doing so they have prevented me to verify EUIPO and European Commission lawfulness of their processing[...]” (emphasis added)

It seems that EUIPO and the EC have inspired recital 39 of EDPB's Guideline on right of access (this comment was already on my follow up emails page 5, **Annex A.01**)

39. Furthermore, the controller shall not deliberately escape the obligation to provide the requested personal data by erasing or modifying personal data in response to a request for access (see 2.3.2). If, in the course of processing the access request, the controller discovers inaccurate data or unlawful processing, the controller has to assess the state of the processing and to inform the data subject accordingly before complying with its other obligations. In its own interest, to avoid the need of further communication on this as well as to be compliant with the transparency principle, the controller should add information about the subsequent rectifications or deletions.

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.

In order to comply with the principle of transparency, controllers should inform the data subject as of the specific point in time of the processing to which the response of the controller refers. In some cases, for example in contexts of frequent communication activities, additional processing or modifications of the data may occur between this time reference point, at which the processing was assessed, and the response of the controller. If the controller is aware of such changes, it is recommended to include information about those changes as well as information about additional processing necessary to reply to the request.

It is also worthy noting that AG Campos Sánchez-Bordona stated in paras 64-65 of his Opinion on case C-579/21 as most probably a dishonest employee deleted my data:

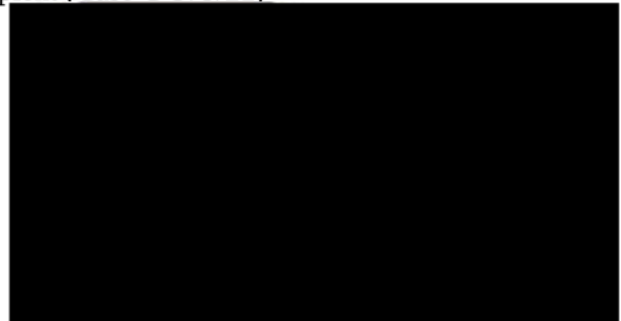
“[...] 64. However, there may be situations in which an employee does not comply with the procedures established by the controller and, on his or her own initiative, accesses the data of customers or other employees in an unlawful manner. In such a case, the dishonest employee would not have acted for and on behalf of the controller.

65. To that extent, the dishonest employee could be described as a ‘recipient’ to whom personal data of the data subject was ‘communicated’ (figuratively speaking). (25) either by his or her own hand and thus unlawfully, or even as a data controller in his or her own right (26)[...]”.

REQUEST

Under Articles 57, 58 I Request to the EDPS the following:

1. To start an investigation due EPSO’s blatant EUDPR non compliance.
2. To order EPSO to restore all the unlawfully deleted data.
3. To order EPSO set all my data as read only and do not delete nor modify again my data.
4. To treat this as a data breach and handle this accordingly.
5. To provide me the name of the dishonest employee that unlawfully deleted my data as due his/her unlawful behaviour has become a recipient (Case C-579/21)
6. To report the dishonest employee to OLAF.



ANNEXES

A.01.All_Emails_Correo de elsotanillo.net - Our ref. 2022-1189 - D(2023) 0200.pdf

A.02.ProfOfCASTManipulationWithVideosEmbedded-Annex.pdf

Table 1: Applications on the applicant's EPSO profile before the 'purge'

Application number	Description	Primary Data Controller	Status
4220689	EUIPO/CAST/1/16 - 6 – INFORMATION TECHNOLOGY/PROJECT MANAGEMENT SPECIALIST - Function Group IV (FG IV)	EUIPO	ERASED
3921833	OHIM/CAST/10/2014 FG III - FG III	EUIPO	ERASED
700311	EPSO/CAST27/5/07 CAST27 (RELEX) - FG III	EC	OK
539001	EPSO/TA/IT/06 IT Temporary Agents IT	EC	ERASED

The three applications now marked "ERASED" existed on the applicant's EPSO profile when he exercised his right of access and other rights through a DSR. The following is a screenshot of the applicant's EPSO profile taken on 2022 (before the 'purge') where his EUIPO/CAST/1/16 can be seen as the last application on his EPSO profile:



The following is the same screenshot taken in 2023 (after the 'purge') where a very old application from 2007 EPSO/CAST27/5/07 can be seen as the last application, as all newer applications were 'purged' after his DSR.



The applicant has recorded using a third party digital witness his EPSO profile before and after the 'purge' and has attached two snips on this PDF.

The files (a snipped version) are named **AfterThePurge.mp4** and **BeforeThePurge.mp4** are embedded on this document and can be opened from the PDF file.

The authenticity and the timestamp of the videos can be checked by the Court as they (the full version) were recorded via a third party digital witness. The applicant can provide the full version and the methods to authenticate both videos.

From: [REDACTED]
EPSO SECTEUR JURIDIQUE (EC) <epso-secteur-juridique@ec.europa.eu>; EPSO DATA PROTECTION COORDINATOR (EC) <epso-data-protection-coordinator@ec.europa.eu>; [REDACTED]
To: [REDACTED]; EC DPO (EC) <ec-dpo@ec.europa.eu>; [REDACTED]
CC: European Data Protection Supervisor <EDPS@edps.europa.eu>; <mailedsigned@pro.egarante.com>
Sent at: 08/02/24 15:21:44
Subject: Re: Case 2022-1189 - Request for access to personal data - Selection procedures EUIPO/CAST/1/16-6, OIHM/CAST/10/2014 FG III, EPSO/CAST27/5/07, CAST27(RELEX) FG III, EPSO/TA/IT/06 IT - EPSO reply

To whom might it concern,

On my letter of 1/2/2024 I informed you about a data breach and requested

2. That the unlawful storage of my personal data beyond the retention period and the unlawful deletion of my personal data after my DSR are handled as two Personal Data Breaches and therefore, that both data breaches are reported to:
 1. the EDPS (without undue delay and not later than 72 hours) as per Art 34(1) EUDPR;
 2. me (as a data subject) as per Art. 35(1) EUDPR in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 35(3).

I have waited 7 days, which I think is a reasonable time for a notification that has the "without undue delay" requirement, as stated on Art 35(1): "1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, **the controller shall communicate the personal data breach to the data subject without undue delay.**"

Any news on the two data breaches?

Art 34(1) states:

"

1. In the case of a personal data breach, **the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it**, notify the personal data breach to the European Data Protection Supervisor, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the European Data Protection Supervisor is not made within 72 hours, it shall be accompanied by reasons for the delay.

"

Has EPSO informed (at least) the [@EUROPEAN DATA PROTECTION SUPERVISOR](#)?

I haven't received any acknowledgement either.

Thanks for your time

Best regards

[REDACTED]

El jue, 1 feb 2024 a las 15:35 [REDACTED] escribió:

To whom might it concern,

Please find attached my Letter after the actions taken by EPSO after EDPS revised decision.

Thanks for your time and consideration

Best regards

[REDACTED]

El jue, 30 nov 2023 a las 17:17, EPSO-SECTEUR-JURIDIQUE@ec.europa.eu (<EPSO-SECTEUR-JURIDIQUE@ec.europa.eu>) escribió:

Dear [REDACTED]

Please find attached our reply concerning the above request.

Best regards,

[REDACTED]
Legal Affairs



European Personnel
Selection Office

[REDACTED]
Facebook [EU Careers](#)
Twitter [EU Careers](#)
www.eu-careers.eu

||

From: European Data Protection Supervisor <edps-edps@fpfis.tech.ec.europa.eu>
To: SUPERVISION <supervision@edps.europa.eu>
Sent at: 13/02/24 12:07:48
Subject: Webform submission from: Complaint form

<p>Submitted on Tue, 02/13/2024 - 12:00</p>

<p>Submitted values are:</p>

1. Are you:

(a) personally affected by the issue(s) at stake in your complaint

2. Which EU institution, body, office or agency do you wish to complain about?

European Personnel Selection Office

3. Please describe your complaint and specify which personal data protection rule(s) you believe have been infringed by the EU institution, body, office, or agency concerned.

EPSO, In the context of case 2022-1189 and court case T-546/23 hasn't provided any EUDPR or Pankki compliant logs.

By email of 1/02/2023 (LetterAfterRevisedDecision-ANNEXES-signed.pdf EDPS was in CC) I informed EPSO that the provided logs were not compliant and also informed it about a Data Breach (hereinafter 'The purge'). 'The purge' is basically two personal data protection breaches that should have been thoroughly investigated:

1. EPSO was storing applicant's data far beyond any reasonable date. Some data was from 2006 as seen on the Request for review Eg: EPSO/TA/IT/06 IT Temporary Agents IT from 2006.

2. EPSO/EUIPO instead of providing the logs and the data decided to purge applicant's data and claim compliance.

As a matter of fact I already informed the EDPS about the same very Data Breach by emails of 1/04/2023 , 21/04/2023 (Annexes 2023-04-01_Correo de elsotanillo.net - Our ref. 2022-1189 - D(2023) 0200.pdf and 2023-04-21_Correo de elsotanillo.net - Our ref. 2022-1189 - D(2023) 0200.pdf). It seems that the EDPS didn't understand the emails properly as no action was taken at that moment.

I also included the deletion of my personal data on my request for review but the EDPS ignored it again.

I have a certified (by a third party witness eGarante) web session from 15/05/2022 where the purged application EUIPO/CAST/1/16 - 6 - INFORMATION TECHNOLOGY/PROJECT MANAGEMENT SPECIALIST - Function Group IV (FG IV) can be seen. The log clearly state that the web session was from 15/05/2022

2022-05-15 09:49:39.820571

<https://europa.eu/epso/application/passport/login.cfm?islo=true>

2022-05-15 09:50:01.203219 <https://europa.eu/epso/application/base/index.cfm>

2022-05-15 09:50:01.203219

https://europa.eu/epso/application/cv_new/index.cfm

2022-05-15 09:50:04.413404

<https://europa.eu/epso/application/passport/index.cfm?action=pdplegal>

I cannot provide the PDF nor the video as the complaint form only allows me to upload 3 files with less than 3MB. I will provide them by email when I receive your reference number by email

4. Please explain what you would like the EU institution, body, office, or agency to do in order to remedy the alleged violation.

EPSO has ignored all my attempts to get access to the logs even after being ordered to comply with my request by 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)

5. When did you become aware of the alleged violation?

2023-04-01

6. If you have supporting documents to substantiate your claim, please upload them here.

- [screenshot_before_afterthepurge_1.pdf](#)
- [2023-04-21_correo-de-elsotanillo.net---our-ref.-2022-1189---d\(2023-0200_0.pdf](#)
- [2023-04-01_correo-de-elsotanillo.net---our-ref.-2022-1189---d\(2023-0200_0.pdf](#)

7. Have you already contacted the EU institution, body, office or agency you want to complain about concerning the alleged violation?

Yes

Please provide details, including the reply of the EU institution, body, office or agency.

EPSO has ignored all my attempts to get the logs and has deleted my data. The EDPS has already all the supporting documents and emails shared between me and the EPSO.

8. Have you submitted the same matter to other bodies (Court of Justice, European Ombudsman, etc.)?

No

9. Your Name

Please note:

If you are a lawyer acting on behalf of a client, please enter your client's name here, not yours - please enter your details under "contact information" below and attach a power of attorney.

If you are a not-for-profit body, organisation or association, please enter your client name here, not yours - please enter your details under "contact information" below and attach a mandate from the individual.

First name(s)

[REDACTED]

Family name(s)

[REDACTED]

10. Contact information

[REDACTED]

11. E-mail address

[REDACTED]

The EDPS treats all complaints confidentially. However, the investigation of your complaint may require disclosing your identity and the allegations you made to the EU institution, body, office, or agency against which you complained. If necessary for the investigation, the identity of the third parties involved, including national data protection authorities may be disclosed. The EDPS will also copy the Data Protection Officer (DPO) of the EU institution, body, office or agency concerned into all correspondence between the EDPS and the EU institution, body, office or agency concerned. Any public summaries of cases (e.g. in the Annual Reports of the EDPS) will be completely anonymous.

12. Do you accept this standard confidential treatment of your complaint?

Yes

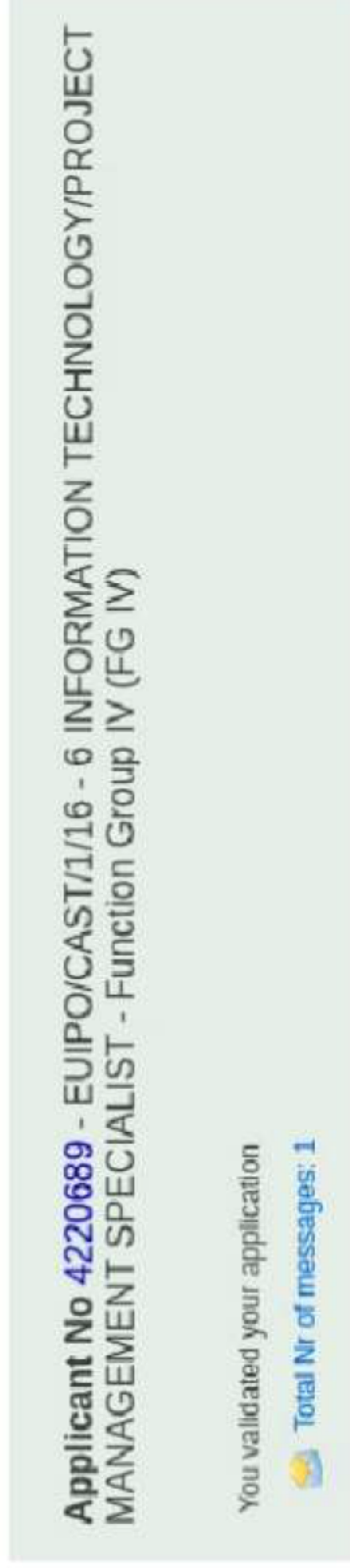
13. Do you agree that your complaint may be passed to another institution, body, office or agency (European or national), if the EDPS is not competent?

Yes

14. I acknowledge having read and understood the Data protection notice.

Yes

The following is an screenshot of my EPSO profile taken on 2022 (before the purge) where my EUIPO/CAST/1/16 can be seen as the last application on my EPSO profile :



The following is the same screenshot taken in 2023 (after the deletion) where a very old application from 2007 can be seen as the last application as all newer applications were deleted after my request for access.

ANNEX C.06 21

**Applicant No 700311 - EPSO/CAST27/5/07 CAST27 (RELEX) -
FG III → Access CAST27 RELEX CV**

EPSO and EUIPO

As seen before, EDPB guideline's recital 39 and Example 6 explains clearly EUIPO's wrongdoing by denying me my personal data, documents and logs.



Our ref.: 2022-1189 - D(2023) 0200

21 de abril de 2023, 11:37

Para: SUPERVISION <supervision@edps.europa.eu>, edps@edps.europa.eu

Dear SUPERVISION

The EDPB released a guideline on right of access (Guidelines 01/2022 on data subject rights - Right of access)
https://edps.europa.eu/sites/default/files/publication/09-10-01_olaf_right_access_en.pdf

It seems that EUIPO and the EC have inspired recital 39 with their unlawful behavior.

39. Furthermore, the controller shall not deliberately escape the obligation to provide the requested personal data by erasing or modifying personal data in response to a request for access (see 2.3.2). If, in the course of processing the access request, the controller discovers inaccurate data or unlawful processing, the controller has to assess the state of the processing and to inform the data subject accordingly before complying with its other obligations. In its own interest, to avoid the need of further communication on this as well as to be compliant with the transparency principle, the controller should add information about the subsequent rectifications or deletions.

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.

In order to comply with the principle of transparency, controllers should inform the data subject as of the specific point in time of the processing to which the response of the controller refers. In some cases, for example in contexts of frequent communication activities, additional processing or modifications of the data may occur between this time reference point, at which the processing was assessed, and the response of the controller. If the controller is aware of such changes, it is recommended to include information about those changes as well as information about additional processing necessary to reply to the request.

Activity logs are personal data too. Yet EUIPO and EC have decided to denied it to me

97. Thus, subject to the specific facts of the case, when assessing a specific request for access, the following types of data are, *inter alia*, to be provided by controllers without prejudice to Art. 15(4) GDPR:
- Special categories of personal data as per Art. 9 GDPR;
 - Personal data relating to criminal convictions and offences as per Art. 10 GDPR;
 - Data knowingly and actively provided by the data subject (e.g. account data submitted via forms, answers to a questionnaire)⁵⁶;
 - Observed data or raw data provided by the data subject by virtue of the use of the service or the device (e.g. data processed by connected objects, transaction history, activity logs such as

access logs, history of website usage, search activities, location data, clicking activity, unique aspects of a person's behaviour such as handwriting, keystrokes, particular way of walking or speaking)⁵⁷;

- Data derived from other data, rather than directly provided by the data subject (e.g. credit ratio, classification based on common attributes of data subjects, country of residence derived from postcode)⁵⁸;
- Data inferred from other data, rather than directly provided by the data subject (e.g. to assign a credit score or comply with anti-money laundering rules, algorithmic results, results of a health assessment or a personalization or recommendation process)⁵⁹;
- Pseudonymised data as opposed to anonymized data (see also section 3 of these guidelines).

Example 16: Elements that have been used to reach a decision about e.g. employee's promotion, pay rise or new job assignment (e.g. annual performance reviews, training requests, disciplinary records, ranking, career potential) are personal data relating to that employee. Thus such elements can be accessed by the data subject on request and respecting Art. 15(4) GDPR in case personal data for example, also relate to another individual (e.g. the identity or elements revealing the identity of another employee whose testimony about the professional performance is included in an annual performance review may be subject to limitations under Art. 15(4) GDPR and hence it is possible that they cannot be communicated to the data subject in order to protect the rights and freedoms of said employee). Nevertheless, national labour law provisions may apply for instance regarding the access to personnel files by employees or other national provisions such as those concerning professional secrecy. Under all circumstances, such restrictions to the exercise of the right of access of the data subject (or other rights) provided in a national law must respect the conditions of Art. 23 GDPR (see section 6.4).

108. If appropriate, internal connection logs can be used to hold record about accesses to a file and to trace back which actions were performed in connection with accesses to a record, such as printing, copying, or deleting personal data. These logs may include the time of logging, the reason for the access to file as well as information identifying the person having had access. Questions related to this topic are at issue in a case currently pending before the CJEU (C-579/21). The putting in place and the supervision and revision of connection logs fall within the controller's responsibility and are liable to be checked by the supervisory authorities. The controller should thus make sure that the persons acting under its authority who have access to personal data do not process personal data except on instructions from the controller, as per Art. 29 GDPR. If the person nevertheless processes the personal data for other purposes than fulfilling the controller's instructions, it may become controller for that processing and subject to disciplinary or criminal proceedings or administrative sanctions issued by supervisory authorities. The EDPB notes that it is part of the employer's responsibility under Art. 24 GDPR to make use of appropriate measures, extending from education to disciplinary procedures, to ensure that processing is in compliance with the GDPR and that no infringement occurs.

Regarding EUIPO and EC claims on unfounded or excessive requests.

6.3 Article 12(5) GDPR

175. Art. 12(5) GDPR enables controllers to override requests for the right of access that are manifestly unfounded or excessive. These concepts have to be interpreted narrowly, as the principles of transparency and cost free data subjects rights must not be undermined.
176. Controllers must be able to demonstrate to the individual why they consider that the request is manifestly unfounded or excessive and, if asked, explain the reasons to the competent supervisory authority. Each request should be considered on a case by case basis in the context in which it is made in order to decide if it is manifestly unfounded or excessive.

6.3.1 What does manifestly unfounded mean?

177. A request for the right of access is manifestly unfounded, if the requirements of Art. 15 GDPR are clearly and obviously not met when applying an objective approach. However, as explained especially

in section 3 above, there are only very few prerequisites for requests for the right of access. Therefore, the EDPB emphasises that there is only very limited scope for relying on the "manifestly unfounded" alternative of Art. 12(5) GDPR in terms of requests for the right of access.

Summarizing it:

- * EUIPO nor EC DPOs provide me with the requested data (data and logs)
- * They delete my data
- * They accuse me of sending unfounded or excessive request

Can you please give me any indication? Is EDPS taking any action?

Thanks for your time

Best regards



[El texto citado está oculto]



Our ref.: 2022-1189 - D(2023) 0200



1 de abril de 2023, 7:39

Para: SUPERVISION <supervision@edps.europa.eu>, edps@edps.europa.eu

Errata, I started in 2022, not in 2021 as stated before

Btw: all the selection procedure that I wanted the logs have disappeared from my EPSO profile. How convenient...

After 10 month of ignoring the undue delay, when I finally received a reply denying my request I found that all is gone

All transparence and fairness

[El texto citado está oculto]

From: SUPERVISION <supervision@edps.europa.eu>
To: [REDACTED]
Sent at: 07/03/24 16:06:43
Subject: Webform submission from: Complaint form sent on 18 February 2024 - Case 2024-0230

Dear [REDACTED]

The EDPS acknowledges receipt of your complaint submitted through the online complaint form on 18 February 2024 against EPSO regarding your access request to your personal data (second attachment).

The file has been given the case number 2024-0230. Please refer to this number and use supervision@edps.europa.eu when corresponding with the EDPS.

Regarding your access request to EPSO, please inform us of the outcome when EPSO replies on 12 March 2024 (EPSO's holding reply - third attachment).

Yours sincerely,

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](https://twitter.com/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: European Data Protection Supervisor <no-reply@web.edps.europa.eu>

Sent: 18 February 2024 23:00

To: SUPERVISION <supervision@edps.europa.eu>

Subject: Webform submission from: Complaint form

<p>Submitted on Sun, 02/18/2024 - 22:49</p>

<p>Submitted values are:</p>

1. Are you:

(a) personally affected by the issue(s) at stake in your complaint

2. Which EU institution, body, office or agency do you wish to complain about?

European Personnel Selection Office

3. Please describe your complaint and specify which personal data protection rule(s) you believe have been infringed by the EU institution, body, office, or agency concerned.

By email (page 1, EmailThread.pdf and EC_DataSubjectRequest-signed.pdf) of 4/1/2024, I sent a DSR to <mailto:data-protection-officer@ec.europa.eu>

By email (page 2, EmailThread.pdf) of 12/1/2024, <mailto:data-protection-officer@ec.europa.eu> acknowledged the email and informed me that my DSR was forwarded to the European Personnel Selection Office (EPSO)

By email (page 4, EmailThread.pdf) of 29/1/2024, <mailto:epso-data-protection-coordinator@ec.europa.eu> acknowledged my DSR:

"[...]We refer to your e-mail of 04/01/2024 registered on 12/01/2024 under reference number Ares(2024)213926. Received by EPSO on 16/01/2024. [...]"

By email (page 5 EmailThread.pdf) of 29/1/2024, I requested to EPSO's DPO a confirmation on the deadline.

By email (page 5 EmailThread.pdf) of 29/1/2024, EPSO's DPO confirmed me that the deadline was 16/02/2024

Today is 18/2/2024 and I haven't received any reply.

EPSO has denied my rights under Art. 16 and 17 EUDPR

This is not the first time EPSO denies my rights under the EUDPR. Please link this complaint to your Case 2022-1189 and to the complaint I lodged on 13/2/2024 (case number still pending) where I informed the EDPS about two Personal Data Breaches.

4. Please explain what you would like the EU institution, body, office, or agency to do in order to remedy the alleged violation.

Provide me with the requested data and conduct an internal investigation under Article 69 as this is not the first time EPSO denies my rights and fails to investigate a Personal Data Breach.

5. When did you become aware of the alleged violation?

2024-12-02

6. If you have supporting documents to substantiate your claim, please upload them here.

- https://www.edps.europa.eu/system/files/webform/complaint_form/11907/emailthread.pdf
-

https://www.edps.europa.eu/system/files/webform/complaint_form/11907/ec_datasubjectrequest-signed.pdf

7. Have you already contacted the EU institution, body, office or agency you want to complain about concerning the alleged violation?

Yes

Please provide details, including the reply of the EU institution, body, office or agency.

See EmailThread.pdf

8. Have you submitted the same matter to other bodies (Court of Justice, European Ombudsman, etc.)?

No

9. Your Name

Please note:

If you are a lawyer acting on behalf of a client, please enter your client's name here, not yours - please enter your details under "contact information" below and attach a power of attorney.

If you are a not-for-profit body, organisation or association, please enter your client name here, not yours - please enter your details under "contact information" below and attach a mandate from the individual.

First name(s)

[REDACTED]

Family name(s)

[REDACTED]

10. Contact information

[REDACTED]

11. E-mail address

[REDACTED]

The EDPS treats all complaints confidentially. However, the investigation of your complaint may require disclosing your identity and the allegations you made to the EU institution, body, office, or agency against which you complained. If necessary for the investigation, the identity of the third parties involved, including national data protection authorities may be disclosed. The EDPS will also copy the Data Protection Officer (DPO) of the EU institution, body, office or agency concerned into all correspondence between the EDPS and the EU institution, body, office or agency concerned. Any public summaries of cases (e.g. in the Annual Reports of the EDPS) will be completely anonymous.

12. Do you accept this standard confidential treatment of your complaint?

Yes

13. Do you agree that your complaint may be passed to another institution, body, office or agency (European or national), if the EDPS is not competent?

Yes


14. I acknowledge having read and understood the Data protection notice.

Yes



Request under Articles 16 and 17 EUDPR

1 mensaje


Para: data-protection-officer@ec.europa.eu

4 de enero de 2024, 22:24

Dear DPO,

Please find attached my DSR.

Thanks for your time

Best regards



EC_DataSubjectRequest-signed.pdf
188K



DPO-DSR-2024-01-EP SO_ Request under Articles 16 and 17 EUDPR

2 mensajes

DATA-PROTECTION-OFFICER@ec.europa.eu <DATA-PROTECTION-OFFICER@ec.europa.eu>

12 de enero de 2024,

12:08

Para: [REDACTED]

Dear [REDACTED]

Thank you for your email of 04 January 2024.

We hereby acknowledge receipt of your request to exercise your rights under [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.

The Data Protection Officer of the European Commission does not process your personal data for the purpose of your query.

Consequently, we have referred your request to the European Personnel Selection Office (EP SO) competent in that area. Pursuant to Article 14(3) of Regulation (EU) 2018/1725, they will reply to you without undue delay and in any event within one month. In case this time limit needs to be extended, they will inform you in due course.

Yours faithfully,



Administrative Assistant to the Data Protection Officer



European Commission
Data Protection Office

B-1049 Brussels/Belgium

data-protection-officer@ec.europa.eu

https://ec.europa.eu/info/departments/data-protection-officer_en

From: [REDACTED]
Sent: Thursday, January 4, 2024 10:24 PM
To: DATA PROTECTION OFFICER <DATA-PROTECTION-OFFICER@ec.europa.eu>
Subject: Request under Articles 16 and 17 EUDPR

Dear DPO,

Please find attached my DSR.

Thanks for your time

Best regards

[REDACTED]

[REDACTED]
Para: DATA-PROTECTION-OFFICER@ec.europa.eu

23 de enero de 2024, 18:54

Dear DPO,

I haven't received any acknowledgement from your EPSO counterpart.
Should I expect any acknowledgement?

Thanks for your time.

Best regards

[REDACTED]

[El texto citado está oculto]



image001.gif
4K



(Re) DPO-DSR-2024-01-EP SO_Request under Articles 16 and 17 EUDPR - Ares(2024)657919

3 mensajes

EP SO DATA PROTECTION COORDINATOR <epso-data-protection-coordinator@ec.europa.eu>29 de enero de 2024,
15:16

Cc: "ve_epso.data protection coordinator (EP SO)" <epso-data-protection-coordinator@ec.europa.eu>, "ve_sg.dpo (SG)" <data-protection-officer@ec.europa.eu>

[\(Re\) DPO-DSR-2024-01-EP SO_Request under Articles 16 and 17 EUDPR - Ares\(2024\)657919](#) (Please use this link only if you are an Ares user – Svp, utilisez ce lien exclusivement si vous êtes un(e) utilisateur d'Ares)

Dear 

We refer to your e-mail of 04/01/2024 registered on 12/01/2024 under reference number Ares(2024)213926. Received by EP SO on 16/01/2024.

We hereby acknowledge the receipt of your request pursuant to Articles 16 and 17 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 (hereinafter: 'Regulation (EU) 2018/1725').

We will reply to your request within one month from its receipt. In case this time limit needs to be extended, you will be informed in due course.

Yours sincerely,

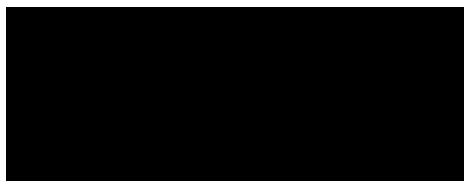


image001

Corporate Services**Facebook** [EU Careers](#)**Twitter** [EU_Careers](#)www.eu-careers.eEuropean Personnel
Selection Office image001.png
4K

29 de enero de 2024, 15:24

Para: EPSO DATA PROTECTION COORDINATOR <epso-data-protection-coordinator@ec.europa.eu>
Cc: "ve_sg.dpo (SG)" <data-protection-officer@ec.europa.eu>

Dear DPO,

Can you please confirm the deadline?
There are many dates on your reply.

Thanks for your time.

Best regards

[El texto citado está oculto]



European Personnel
Selection Office

image001.png
4K

EPSO-DATA-PROTECTION-COORDINATOR@ec.europa.eu <EPSO-DATA-PROTECTION-COORDINATOR@ec.europa.eu>

29 de enero de
2024, 15:27

Para: [Redacted]
Cc: "DATA-PROTECTION-OFFICER@ec.europa.eu" <DATA-PROTECTION-OFFICER@ec.europa.eu>, "EPSO-DATA-PROTECTION-COORDINATOR@ec.europa.eu" <EPSO-DATA-PROTECTION-COORDINATOR@ec.europa.eu>

Dear [Redacted]

The deadline is 16/02/2024.

Best regards

[El texto citado está oculto]

To:data-protection-officer@ec.europa.eu

Dear DPO,

Request under Articles 16 and 17 EUDPR:

Can you please provide:.

1. Copy of all data being currently processed by the EPSO/EC that has not been obtained from the data subject, specifically (but not exclusive) all the data that EUIPO or EDPS (or any other body) has provided to the European Commission.
2. The categories of personal data concerned;
3. Access logs with the time and the purpose of each access generated by consultations operations.
4. The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
5. Where the personal data are not collected from the data subject, any available information as to their source;
6. Any minutes of meetings as per [EDPB Right of access guideline](#)¹ and cases C-141/12 and C-372/12:

95. In joint cases C-141/12 and C-372/12⁵¹ the CJEU ruled that the right of access covered personal data contained in minutes, namely the “name, date of birth, nationality, gender, ethnicity, religion and language of the applicant” “and, “where relevant, the data in the legal analysis contained in the minute”, but not the legal analysis itself⁵². The legal analysis was in this context not liable in itself to be the subject of a check of its accuracy by the data subject nor of rectification. Furthermore, providing access to the legal analysis does not fulfil the purpose of guaranteeing privacy but access to administrative documents.

7. Any communication (eg: Teams’ chats, emails, etc.) between the EC and others third parties as per [EDPB Right of access guideline](#)

Scope of the right of access

The scope of the right of access is determined by the scope of the concept of personal data as defined in Art. 4(1) GDPR. Aside from basic personal data like name, address, phone number etc. a broad variety of data may fall within this definition like medical findings, history of purchases, creditworthiness indicators, activity logs, search activities etc. Personal data which have undergone pseudonymisation are still personal data as opposed to anonymised data. The right of access refers to personal data concerning the person making the request. This should not be interpreted overly restrictively and may include data that could concern other persons too, for example communication history involving incoming and outgoing messages.

Please have in mind the following Case law before replying:

CJEU C-141/12

CJEU C-307/22

CJEU C-372/12

CJEU C-340/21

CJEU C-579/21


Please use my GPG public key (see below) to encrypt your reply.

¹ https://edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf

-----BEGIN PGP PUBLIC KEY BLOCK-----

mQGNBGSmavIBDADFnXX7LfU14W9hJ0pcz2BG1sEvVfdxa9PwBH2xhBRG5n7WLvpz
DdCWON8dnCNnAIVNj8ILBmZVie9sjEiafuXcjUHMwaTgxgotkVp6LQwk1tWRCF0Q
o5qiOSCzqWf92/B8o0xqZGC3ap3CuLc9pFvA7vnJZgkVogWfQn0h+Ji+hUYLWnVB
pkj0z55iGpXf4JPcYzLOIxti2lwCjzcApqXxkQVIxkdoKdVADmbA2bZ3OgA/K+1i
Pye6ZMJ7b8U/sfa+AC0rtTGuRE6oIDRbTTN7xL53sUmRdqUPnpbSs0z4QNHpgWcK
kDLXdgHG+sFHN1qc4y9Eb4wYy2eEFIKSaBT95qApRi8OS/iYztNaA7vcwgPbT1F9
JszZ3RfgZhBhACAUXps0dRb6v+h44S/kug9j2mbJ2Vr0ysaTbxhDqV5BgcWfeWKj
ee3zEEGL3IPOWMJN42IeV2/0tLiDcd0B1+CDt7W1IpZ9JWBhUX9KWfR32i0jgs4
MH9TTkwPYDaYjE8AEQEAAbQnSnVhbiBTaWVycmEgUG9ucyA8anVhbKBlbHNvdGFu
aWxsby5uZXQ+IQHUBBMBCgA+FiEECTpZ243lGDOUiCJj/EKTde8hsT8FAmSmavIC
GwMFCQPCZwAFCwkIBwIGFQoJCAasCBBYCAwECHgECF4AACgkQ/EKTde8hsT9FigwA
mqxM56Qe6L+Qo/7A5O9jXllupWtLCwkrRElKred5DAGgZRRo7SJnaprHVArhPr2F
bZ2VjMYGvxFA2YB8eOaV/z+oRmF62PmCQTkN94jyc0/zjLq6RGjx43S151JUoJoZ
yf9/TGfZ/T9urQmR20rZ1kExfBo0WXnB9rjwLLvMfzm8ETOhr0shtwBPvauqg2FZ
KnztWDFVGE5zJM5UQQglCQMF8FidMPKb4KZnRQ8DSVM9N7HRr0fkQmuZ/mNVVFP
ie2zwCaDKJICL01XLPXGlgzfu2tL63XsrgUhCqMPM4Md+Spr9lX3pjkWvcLGFayg
aSENY4bao90orkjt193zF0/qtiY+2We3VkV1QVNoFcJ2USFV+OhwV9/FkOH7ulrc
E2d/a6dvMMS/KIKottNgY++dVLxJVMk2Iv6HGx0u9xGkEBbWDcwmr0Rv3SAyKJyQ
Xz1G90AZyP02lGlxnHq2jOmqiOWjhl641zBJgbrN9VcQAmsAgSrpv654ftLv4Ydq
uQGNBGSmavIBDAC9mXDCqNZPBBfspmAedmGwl4YDRapGfCFHmEiQroUC24w36swS
oet+mau7TbhY1mzFWpgf5vnhfXQXwgxphsctFwxm+p2Rn90hU2hE+FAGizDYvUF3
IdsMEtmkEbIzgfuk5zCZR8FCj2lm3G6Hdwy9n+37EO+yZkKHfNmVi8QWcQwJ9k0E
9o5GZPyUyiUtwCMnqZjGQ/OO6sOy8e0jIULTp2cbnJTPSepiWXRT/sNB7TzreD8T
qIFY3DD0WQ+H6atpfleXEBQH7SMv7beU5val8xgkihjFvxUgiHx/OmN7REyiNu/8
+hcM5VBBRQJ5An+yZJVOKJzG4+j/1sjyVZZPYjuiPPeOn86r93KolS/fAoNLGar
entxqMGkxwOZvqSeZ8r8+cqz75SHhgZ1jjEUxMT8rCmwG4y/XwjUrAGazXF7L5fl
eFsde2Og+y8LptjJW5BJKBiZFJTW0N7lQ7eVvrd+aM+cso6vqCSZZpY+l8U5kR19
EPaMV+5sWGBi2m8AEQEAAYkBVaQYAQoAJhYhBArT89uN5RgzlIgiY/xCk3XvIbE/
BQJkpmryAhsMBQkDwmcAAAOJEPxCK3XvIbE/hvkMAJ11hYYGKuRC5uuWR27NPJKU
eYuCd+Uz755wwSYkGQIjE0uyzS81z/iIUTJKuugtrJnFThjqmeesY2tpBFjLMrnF
HffF3y4llVo3oaRLYdDDo/wSdK3U8yJnG+fqIlAPUJioxwXuXN3+zTCxZd/IjBV
yq8+FmTr2DTPj+6Aup+MvWBDsr9xr1c5vjFX2UUCWWDPPi9ABdo24PfXTsq+uw7s
ZxJLl1u4+MVfVq5woJ9vUXYDbAczz+3u4zqdqu5VQ4Edsvd8y8D23fC3YRdlIG9
berrS4JPbNpn5PeCoifFh1e8rcDjnrXUj+vBQbnLo/f+BYLqOHGdD9xYeDgif4As
vpLzVQL5mVSMcWgFAMPBaQzl2XHqJ3exU9AK/wONvYFu7bz85FGgjKBrUF6e+sP4
Zhwc0oV3KJGEJdovKDXxL6ILVh3liWzYvOH/P6I5gGQIJrrBAPeiK71w9lAvWEBe
Tntoni1Ut/hO0EfpRHHydsqRBoFHZWeEviXKca9Tfg==
=LKi8

-----END PGP PUBLIC KEY BLOCK-----

Brussels, 28/02/2024
EPSO.001.  ARES (2024)s. 1780160



Subject: Request for access to personal data ref. DPO-DSR-2024-01-EPSO

Dear 

We refer to your message of 04/01/2024 in which you make a request for access to personal data pursuant to Article 17 of Regulation (EU) 2018/1725.

Your application was registered on 12/01/2024 under the above mentioned reference number and is currently being handled. However, since we were regrettably not in a position to complete the handling of your application within the time limit of 1 month from the date of registration, we have to extend the time limit with 1 month in accordance with Article 14(3) of Regulation (EU) 2018/1725. The new time limit expires on 12/03/2024.

We apologize for this delay and for any inconvenience this may cause.

Yours sincerely,

