noyb – European Center for Digital Rights
Goldschlagstraße 172/4/3/2
1140 Vienna
Austria

European Data Protection Supervisor
Rue Wiertz 60
B-1047 Bruxelles

Per E-Mail: edps@edps.europa.eu

Vienna, 22 August 2024

noyb Case-No:	**C-086-01**
Complainant:	[redacted]
represented pursuant to Article 67 of the EU GDPR by:	*noyb* - European Center for Digital Rights Goldschlagstraße 172/4/3/2 1140 Vienna Austria
Respondent:	European Parliament Directorate-General for Personnel Rue Alcide de Gasperi L-1615 Luxembourg
Regarding:	Data breach resulting from the infringement of Articles 4(1)(c), (e) and (f) and 33(1) of Regulation (EU) 2018/1725

COMPLAINT
UNDER ARTICLE 63 OF REGULATION (EU) 2018/1725

1. REPRESENTATION

1. *noyb* – European Center for Digital Rights is a not-for-profit organisation active in the field of the protection of data subjects' rights and freedoms with its registered office in Goldschlagstraße 172/4/2, 1140 Vienna, Austria, registry number ZVR: 1354838270 (hereinafter: *"noyb"*) (**Annex 1**).

2. The Complainant is represented by *noyb* pursuant to Article 67 of Regulation (EU) 2018/1725 (hereinafter: "EU GDPR") (**Annex 2**).

2. FACTS PERTAINING TO THE CASE

2.1. Occurrence and discovery of the breach

3. In a data breach that occurred on an unidentified date in early 2024, the personal data of over 8,000 EU Parliament (hereinafter "Parliament" or "controller") job applicants was compromised on the Parliament's staff recruitment application, "PEOPLE".

4. PEOPLE is controlled by the Parliament. The Directorate-General for Personnel (hereinafter "DG-PERS"), which is a part of the Parliament and manages the institution's human resources (HR) services, processes PEOPLE's data.

5. The complainant is an [redacted] at the European Parliament who underwent recruitment in [redacted] Along with other Parliament staff, the complainant used the PEOPLE portal to submit documents as part of the hiring process. The complainant has not used the portal since 2019.

6. The documents uploaded to the portal included identity cards and passports, extracts of criminal records, civil status certificates, documents related to residence or domicile, education and experience supporting documents, declarations of honour, documents establishing individual entitlements and additional administrative documents. The breach compromised every single document pertaining to the Complainant that was hosted in the portal.

7. The Parliament did not become aware of the breach until months after it occurred. It is unclear exactly when the Parliament realised the breach, but after conducting an internal investigation, it formally confirmed on 24 April 2024 that PEOPLE experienced a breach.

8. According to its communications with the affected data subjects, the Parliament has not yet uncovered the cause of the breach.

2.2. Notifications to authorities and data subjects

9. On 26 April 2024, the Parliament informed the European Data Protection Supervisor (EDPS) of the breach. It subsequently also reported the incident to the Luxembourg police.

10. On 6 May 2024, the Parliament informed data subjects that a data breach occurred in early 2024.

11. On 22 May 2024, the Parliament sent data subjects further information concerning the categories of data accessed. All 23 documents corresponding to the complainant were implicated in the breach.

Category of document	Number of documents available	Number of documents accessed
Identity card or passport	2	2
Extract of criminal records	1	1
Civil status certificates	3	3
Certificates and other documents to determine the residence or domicile	8	8
Education or experience supporting documents	6	6
Military obligations certificate	0	0
Declaration of honour documents made by data subject	0	0
Documents to establish the individual entitlements	2	2
Contract and additional administrative documents	1	1

Screenshot of information sent to the complainant on 22 May 2024.

12. On 31 May 2024, the Parliament advised data subjects to replace their IDs and passports as a precautionary measure and offered to reimburse those costs. It stated that the investigation was ongoing and that there were no further findings concerning the cause of the breach.

3. GROUNDS FOR THE COMPLAINT

3.1. Violations

13. The Parliament has infringed the EU GDPR as follows:

(a) The Parliament lacked adequate security measures given the risks associated with the data it processed, including sensitive data, and its cybersecurity system, infringing Article 33 EU GDPR.
(b) The breach compromised the confidentiality of the data subjects' personal data in violation of Article 4(1)(f) EU GDPR.
(c) The collection and storage practices for the processed data infringe data minimisation and storage limitation principles pursuant to Article 4(1)(c) and (e) EU GDPR.

3.2. Applicable legal framework

14. The processing of personal data by EU institutions is governed by the EU GDPR. Recital 5 of the EU GDPR states that:

> *"Whenever the provisions of this Regulation follow the same principles as the provisions of Regulation (EU) 2016/679, those two sets of provisions should, under the case law of the Court of Justice of the European Union (the 'Court of Justice'), be interpreted homogeneously, in particular because the scheme of this Regulation should be understood as equivalent to the scheme of Regulation (EU) 2016/679."*

15. Therefore, interpretations of both Regulation (EU) 2016/679 (hereinafter "GDPR") principles and CJEU case law are applicable to the EU institutions.

3.3. Lack of appropriate security measures under Article 33 EU GDPR

3.3.1. Parliament was long aware of cybersecurity vulnerabilities and high risks

16. In November 2023, the Parliament's IT department conducted an institutional cybersecurity review. The internal report (hereinafter "November 2023 report") concluded that the Parliament's cybersecurity "*has not yet met industry standards*" and that existing measures were "*not fully in-line with the threat level*" posed by state-sponsored hackers.[1]

17. By early 2024, the Parliament was on notice of (1) the high risk of future cyberattacks, particularly from state actors; (2) the high risk of targeting directed to MEPs and staff; and (3) the inadequacies in its IT security systems to protect against these kinds of attacks.[2]

18. Indeed, the PEOPLE breach occurred alongside a number of other cyberattacks on EU institutions. Russian hacking groups attacked the Parliament's website in November 2022[3] and numerous European governments in autumn 2023.[4] In February 2024—around the time of the PEOPLE breach—the Parliament suffered a different breach in its security and defence subcommittee when two MEPs and a staffer found Israeli-made spyware on their devices.[5]

19. Targeting of individuals within the Parliament a serious and known risk. Foreign adversaries use a number of techniques to obtain personal data about politicians, including device spyware (see para. 18), bribery,[6] surveillance efforts on family members and 'honeypot' schemes. Such espionage can leverage sensitive personal data (such as sexual orientation[7] and

---

[1] See Politico's coverage on the internal report: https://www.politico.eu/article/european-parliament-election-cybersecurity-problem/.

[2] As acknowledged by the November 2023 internal cybersecurity review as well as other EU institutional representatives such as the Cyber Emergency Response team: https://www.politico.eu/article/european-parliament-election-cybersecurity-problem/; Commission spokesperson Johannes Bahrke: https://www.politico.eu/article/threat-eu-high-russia-hackers-launch-cyberattacks-fancy-bear-election/.

[3] See: https://www.reuters.com/world/europe/pro-kremlin-group-says-responsible-cyberattack-eu-parliament-official-2022-11-23/

[4] See Politico's report on the cyberattack here: https://www.politico.eu/article/threat-eu-high-russia-hackers-launch-cyberattacks-fancy-bear-election/.

[5] See news's coverage of the hack: https://www.lepoint.fr/monde/nathalie-loiseau-mon-telephone-a-ete-infecte-par-le-logiciel-espion-pegasus-17-02-2024-2552661_24.php#11; https://www.politico.eu/article/nathalie-loiseau-elena-yoncheva-pegasus-spyware-european-parliament-security-defense-subcommittee/

[6] Joint Motion for a Resolution on new allegations of Russian interference in the European Parliament, in the upcoming EU elections and the impact on the European Union (2024/2696 (RSP)), points C, E, H, L, 1, 4 https://www.europarl.europa.eu/doceo/document/RC-9-2024-0262_EN.pdf [hereinafter "2024/2696 (RSP)"],

[7] For instance, in April 2024, UK PM William Wragg disclosed that he was targeted by a honeytrap plot. Allegedly, someone on Grindr whom he sent intimate photos to blackmailed him, demanding the personal phone numbers of other MPs. See https://www.bbc.com/news/uk-politics-68773702; https://www.lbc.co.uk/politics/william-wragg-resigns-commons-posts-honeypot/ . Such examples are neither new nor rare. In the 20th century, a "Lavender Scare" emerged as a moral panic leading to mass dismissal of suspected gay politicians in US government; see: https://digitalcommons.georgiasouthern.edu/cgi/viewcontent.cgi?article=1113&context=aujh ; https://www.nbcnews.com/id/wbna52158960 (discussing a particular blackmail case against US Senator Lester Hunt if he did not withdraw his bid for re-election, threatening to publicize Senator Hunt's son's sexuality as a gay man). Other cases of political blackmail and extortion due to sexuality cases can be seen in Australia and Bosnia; see

infidelity[8]) to "pressure" politicians and enables nefarious actors to solicit information from political leaders. In its Joint Motion 2024/2696 (RSP),[9] the Parliament acknowledged numerous espionage incidents attempting to exploit MEPs and other European political leaders, including the arrest of MEP Maximilian Krah's APA on suspicion of spying for China,[10] the arrest of Russian and Chinese spies in Germany,[11] and incidents involving the provision of Austrian officials' mobile phone data to Russian intelligence officials.[12]

20. The Parliament was aware of these security risks. The November 2023 report noted the number of cyberattacks on EU institutions was "*increasing sharply*" and that the Parliament should prepare to face cyber threats. Contemporaneous breaches across Europe clearly indicated vulnerabilities for both MEP and staff data,[13] as well as for HR information.[14]

3.3.2. Parliament's security measures were not appropriate given the known risks

21. In its Data Protection Notice relating to the recruitment and management of Accredited Parliamentary Assistant contracts (hereinafter "Data Protection Notice"), the Parliament informed data subjects of its security measures as follows:

> *"Relevant 'physical and/or IT security' measures have been applied. Suitable safeguards are in place. (Please note that the exact details cannot be published, in order to protect the process)."*[15]

22. Given the controller's vague description, it is unclear precisely what security measures were put in place. This merits further investigation by the EDPS pursuant to Article 57(e) and (f) EU GDPR.

23. The CJEU has stated that the appropriateness of security measures must be assessed *"in a concrete manner"* (C-687/21 *MediaMarktSaturn*, para. 38; C-340/21 *Natsionalna agentsia za prihodite,* para. 30) and that a two-stage analysis must be conducted.

24. The first step of this analysis is to identify the risks of a personal data breach caused by the processing concerned and their possible consequences for the rights and freedoms of natural

---

https://www.brisbanetimes.com.au/national/mp-blackmail-attempt-on-gay-sex-film-20090222-geauj3.html; https://www.fairplanet.org/editors-pick/homophobic-extortion-targets-politicians-in-bosnia/

[8] Canada (https://www.theglobeandmail.com/politics/article-tony-clement-admits-to-multiple-acts-of-infidelity/) ; US (https://www.nbcnews.com/politics/politics-news/missouri-gov-eric-greitens-admits-affair-after-blackmail-accusations-surface-n836736); UK (https://www.theguardian.com/politics/2015/nov/16/robert-halfon-tory-minister-admits-cheating-on-partner-blackmail)

[9] 2024/2696 (RSP)

[10] See 2024/2696 (RSP), point J, https://www.europarl.europa.eu/doceo/document/RC-9-2024-0262_EN.pdf

[11] See 2024/2696 (RSP), points K, 6, 7 https://www.europarl.europa.eu/doceo/document/RC-9-2024-0262_EN.pdf

[12] See 2024/2696 (RSP), points I, 14 https://www.europarl.europa.eu/doceo/document/RC-9-2024-0262_EN.pdf

[13] The February 2024 breach in Parliament's defense subcommittee indicated vulnerability of staff data as well.

[14] For example, in May 2024, Britain's Ministry of Defense revealed a Chinese cyberattack breached troops' personal data via its payroll system: https://www.politico.eu/article/europe-cyberattacks-russia-china-uk-ministry-of-defence-hacks/

[15] https://www.europarl.europa.eu/data-protect/reportPdf/printPreview.do;jsessionid=A279FF297A7C7B676C94F712894A7B62?output=pdf&lang=EN&prefix=V3&nr=321

persons, *"taking into account the likelihood of the risks identified and their severity"* (C-340/21 *Natsionalna agentsia za prihodite,* para. 42).

25. In the present case, Parliament's November 2023 report and recent cyber threats indicated that the likelihood of future attacks on EU institutions was very high. The severity of such an attack was high, given that the controller is one of the main EU institutions, making it a "primary target" for foreign adversaries.

26. Key political institutions face a particularly high risk for the use of personal data. As was discussed in para. 19, personal information about MEPs, staff and their family members can be used to apply political pressure and influence their carryout of duties. As observed in the cases of the defence subcommittee MEP and assistant's device surveillance and MEP Krah's APA's alleged surveillance on behalf of China, foreign adversaries' use of varied surveillance tools on MEPs and staff alike pose high risk for democratic governance and security.

27. The second step of the security measure analysis requires ascertaining "*whether the measures implemented by the controller are appropriate to those risks, taking into account the state of the art* [...]" (C-340/21 *Natsionalna agentsia za prihodite,* para. 42).

28. The controller itself acknowledged the inadequacy of its security measures. The November 2023 report stressed that its cybersecurity system *"has not yet met industry standards"* and that its measures were not proportionate to known risks levels[16] (see above at para. 16). The failure to implement more appropriate security measures as called for in the November 2023 report would indicate that the Parliament's security measures fail the CJEU's two-part test, infringing Articles 33(1) and 4(1)(f) EU GDPR.

29. Moreover, even if the controller had implemented adequate measures, pursuant to Article 26(1) EU GDPR it still *"bears the burden of proving that the personal data are processed in such a way as to ensure appropriate security of those data"* (C-687/21 *MediaMarktSaturn*, para. 42).

30. The EDPS should exercise its investigatory powers to determine precisely what measures were in place and to assess them under the CJEU's two-part test. In particular, the EDPS might consider whether the Parliament used encryption, anonymisation or other privacy enhancing technologies. It should also investigate to what extent, if at all, it implemented the November 2023 report's recommendations.

3.3.3. The need for additional safeguards where sensitive data is processed

31. Several documents in the PEOPLE application processed special categories of the complainants' personal data pursuant to Articles 10(1). In particular, data concerning the Complainant's sexual orientation were processed through this application.

[16] See Politico's coverage on the internal report: https://www.politico.eu/article/european-parliament-election-cybersecurity-problem/.

32. The CJEU has stated that a wide interpretation of the term "special categories of data" must be adopted (C-184/20 *Vyriausioji tarnybinės etikos komisija,* para. 125). The Court has specified that personal data that are liable to disclose indirectly the sexual orientation of a natural person constitutes processing of special categories of personal data (C-184/20 *Vyriausioji tarnybinės etikos komisija,* para. 117-128).

33. In this case, the complainant uploaded a copy of [redacted] certificate on the portal. The document's contents, including the name of the complainant's [redacted] enabled inference of the complainant's sexual orientation. Under the CJEU's jurisprudence, the processing of such civil documents is thus processing of a special category of data.

34. Article 33(1) EU GDPR requires controllers to take into account "*the risks of varying likelihood and severity for the rights and freedoms of natural persons*" in its security measures.

35. The CJEU has ruled that the processing of these sensitive data constitutes "*a particularly serious interference with the fundamental rights to privacy and the protection of personal data*" (C-136/17 *GC and Others (De-referencing of sensitive data*), para. 44).[17] The unlawful disclosure of sensitive data has a more severe impact on the fundamental rights to privacy and the protection of personal data, and thus carries higher risk.

36. However, the controller does not appear to have adopted a higher level of protection for these types of data. The PEOPLE breach implicated *every single* document in the data subject's recruitment file. It is unclear precisely why this happened; this may indicate that the file was stored in full and/or without encryption in a single location (see para. 11). Whatever the cause, the Parliament appears to have stored sensitive data without adopting stronger measures than the ones adopted for non-sensitive personal data. There is no indication of additional security measures, such as encryption, to secure the sensitive data.

37. The controller's consideration of the sensitive data it processed and the resulting risks it carried was thus insufficiently reflected in its security measures, reiterating its infringement of Article 33(1) EU GDPR.

3.4. Processed more data than necessary, for longer than necessary

38. According to the Data Protection Notice, the Parliament processes data subjects' information for the purpose of recruiting APAs, dismissing APAs and processing contract modifications.[18] The data retention period for the recruitment files is 10 years.[19]

39. Pursuant to Article 26(1) EU GDPR and in line with CJEU case law, controllers must demonstrate that they have sought to minimise the amount of personal data collected as much

---

[17] See also C-184/20 *Vyriausioji tarnybinės etikos komisija*, para. 126.

[18] https://www.europarl.europa.eu/data-protect/reportPdf/printPreview.do;jsessionid=A279FF297A7C7B676C94F712894A7B62?output=pdf&lang=EN&prefix=V3&nr=321

[19] See the Parliament's Data Protection Notice for APA recruitment: https://www.europarl.europa.eu/data-protect/reportPdf/printPreview.do;jsessionid=A279FF297A7C7B676C94F712894A7B62?output=pdf&lang=EN&prefix=V3&nr=321

as possible.[20] The burden thus rests on the Parliament to demonstrate its compliance with Articles 4(1)(c) and (e) GDPR.

40. Data minimisation obligations pursuant to Article 4(1)(c) EU GDPR require controllers to only process data that is "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*". Personal data is limited to "*what is necessary*" when the purpose cannot be reasonably achieved without the processing of that personal data.

41. While the recruitment of APAs might require the documents collected, the dismissal of APAs does not. The Parliament does not specify why the *entire* recruitment file, particularly its sensitive civil documents, is needed to process the dismissal or contractual changes of a temporary staff member. The continued processing of this data beyond the recruitment period is excessive.

42. The 10-year data retention period is also excessive. The storage limitation principle requires data to be "*kept in a form which permits identification of data subjects <u>for no longer than is necessary for the purposes for which the personal data are processed".</u>*

43. The processing of data subject recruitment files, as discussed above in para. 42, is clearly going on for *"longer than is necessary*" for processing purposes, in violation of Article 4(1)(e) EU GDPR. The Data Protection Notice does not justify the complete file's retention period. It also does not contemplate deletion prior to the 10-year period, even where data subjects are dismissed or not hired.

44. If the controller had complied with the principles of data minimisation and storage limitation, and therefore promptly deleted the data, obviously no information about the complainants would have been stolen during this data breach. Therefore, there is a clear causal link between the violation of Articles 4(1)(c) and (e) EU GDPR and the data breach.

[20] See discussion above; see also C-175/20, *Valsts ienemumu dienests,* para. 78.

4. REQUESTS AND SUGGESTIONS

4.1. Request for comprehensive investigation

45. In light of the above, the complainant requests the EDPS to fully investigate this complaint in accordance with the powers conferred on it under Article 58(1) EU GDPR.

4.2. Request for declaratory decision and exercise of corrective powers

46. Given the security shortcomings discussed, the complainant requests the EDPS to find that the respondent has:

    (a) infringed Article 33(1) and 4(1)(f) EU GDPR by processing personal data, including sensitive data, without implementing appropriate security measures;

    (b) infringed Article 4(1)(c) and (e) EU GDPR by processing personal data in violation of the principles of data minimisation and storage limitation.

47. The complainant requests the EDPS to exercise its corrective power under Article 58(2)(e) EU GDPR and order the controller to bring its processing operations into compliance with the EU GDPR.

4.3. Suggestion to impose a fine

48. In light of the above infringements, the complainant suggests that the EDPS impose a fine pursuant to Article 66(2) and (3) EU GDPR.

5. CONTACT

49. Communications between *noyb* and the EDPS in the context of this complaint may be made by e-mail with reference to the case number mentioned in the title of this complaint.

50. We will be happy to assist you if you require further factual or legal details to deal with this complaint. Please contact us at [redacted].