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

Valstybinė duomenų apsaugos inspekcija
L. Sapiegos str. 17
10312 Vilnius
Lithuania

Per E-Mail: [redacted]

Vienna, 29.09.2025

noyb Case-No:	C-102
Complainant 1 :	[redacted], born on [redacted]
Complainant 2:	[redacted], born on [redacted]
represented under Article 80(1) DSGVO by:	*noyb* – European Center for Digital Rights Goldschlagstraße 172/4/3/2, 1140 Vienna
Respondent:	**UAB Whitebridge.ai** Krivių str. 5, Vilnius LT-01204, Lithuania
Regarding:	Articles 5(1)(a), (b) and (d), 6(1), 9, 12(1), (2), (3), (5) and (6), 14, 15(1), (3) and 16 GDPR

COMPLAINT

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 172/4/3/2, 1140 Vienna, Austria, registry number ZVR: 1354838270 (hereinafter: *„noyb")* (**Attachment 1**).

2. *noyb* is representing the Complainants under Article 80(1) GDPR (**Attachments 2 and 3**).

1.1. Respondent

3. The Respondent, UAB Whitebridge.ai (hereafter: "*Whitebridge*", the "*Controller*" or "*the Respondent*"), is a Lithuanian Limited Liability Company with legal entity code 306680556, and registered office at Krivių str. 5, Vilnius LT-01204, Lithuania.

4. Whitebridge provides two main AI-powered services upon payment: (i) the issuance and provision of reports about the "online presence" of individuals and the (ii) real-time monitoring of the individuals' online activities with the provision of notifications when new information appears online.

5. The former include the collection of all types of information on the individuals, such as images of them available on their social media profiles and articles about them on news outlets, leisure and hobbies, data breaches concerning them and social media performance analysis.[1]

6. Whitebridge collects social media data regardless of the fact that social networks expressly prohibit the collection of data through automated means.[2]

7. Furthermore, Whitebridge generates AI generated texts and alleged analysis on each person, that seems to be based on information previously collected from third party sources.

8. Whitebridge's processing activities involve two categories of data subjects:

   - The first category includes the data subjects who use the controller's services to buy reports (hereafter, the "*users*").
   - The second category includes the data subjects who are the subject of the reports or monitoring services provided by Whitebridge (hereafter, as in the Respondent's privacy notice, the "*searched persons*").

9. It is possible for data subjects to fall into both categories when buying the report concerning them. In this case, the Complainants fall into the second category as they have not purchased any of the Respondent's reports or monitoring services.

10. In August 2025, the Controller claimed to have had, since it was launched, about 2.6 million people searched on its website, 560.000 reports generated and almost 80.000 registered users.[3]

---

[1] https://whitebridge.ai/, accessed on 17 September 2025.

[2] See for example on Facebook: https://www.facebook.com/robots.txt, Instagram: https://www.instagram.com/robots.txt, LinkedIn: https://www.linkedin.com/robots.txt, accessed on 17 September 2025.

[3] Data from 7 August 2025 https://whitebridge.ai/.

1.2. The Complainants

11. In December 2024, the Complainants searched their names on the Controller's website. They realised that anyone could buy a report on them - without them being aware.

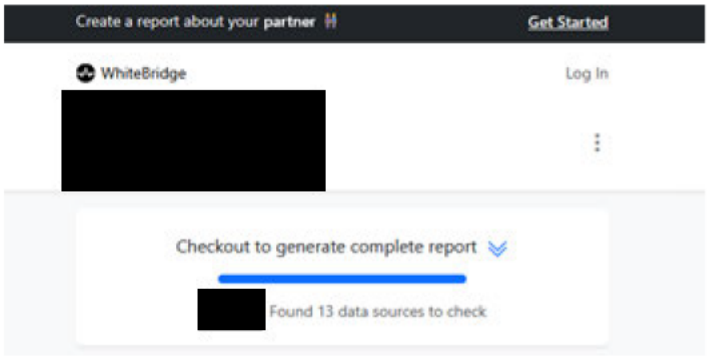


Figure 1 - Screenshot of the search page

12. The scope of this complaint is limited to the searched persons and the processing activities in relation to the issuance and provision of the reports and the monitoring of the data subjects' online activities.

1.3. Access requests

13. On 09.12.2024, both Complainants contacted Whitebridge, requesting access to their data, pursuant to Article 15 GDPR. They both included a copy of their national ID cards to help the Controller to authenticate them. These requests were sent to [redacted] (**Attachments 4 and 5**), as provided in the Respondent's privacy policy.

14. On 02.01.2025, the Respondent replied that it had no "*registered users*" and that it does not process data in relation to the email addresses of the Complainants. In both replies, the Controller specified that "*aspects related to the specific natural person personal data information disclosure will not be provided as an answer to the received email request*". Finally, the Controller redirected the data subjects to another email address that the Complainant would have to contact with a qualified electronic signature. The reply was signed by the DPO [redacted], who is also the [redacted]. (**Attachments 4 and 5**).

15. On 10.01.2025, *noyb* purchased the reports relating to the complainants (**Attachments 6 and 7**). In case of Complainant 1, the report contained a warning for "*sexual nudity*", while for Complainant 2, reference was made to "*dangerous political content*".

16. On 15.01 and 17.01.2025 Complainant 2 and Complainant 1 both contacted the email address referred, requesting access to their data under Article 15 GDPR and rectification under Article 16 GDPR regarding respectively the "*dangerous political content*" and the "*sexual nudity*" items. They explained that these records are inaccurate. They both attached a copy of their ID and explained that they do not have a qualified electronic signature (**Attachments 8 and 9**).

17. On 24.01.2025, the Respondent replied with a reference to its privacy notice and added that under Article 12(6) GDPR, it could request an electronic signature to verify data subjects' identities. No comment on the request to exercise their right of rectification was given (**Attachment 8 and 9**).

18. On 17.02.2025, Complainant 1 insisted, stating that she does not have a qualified electronic signature and that as she provided a copy of her ID, she does not see any doubt about her identity that would allow the Controller to request additional information – and specifically an eID that most people in the EU do not possess - under Article 12(6) GDPR (**Attachment 8**). Given that the Controller processed data of data subjects globally – it seems even more absurd to insist only on an eID, which many countries in the world do not even issue.

19. On 04.03.2025, the Controller replied that "*modern AI technologies make it increasingly easy to generate highly convincing forged documents. Given this, and in line with GDPR Article 12(6) we are entitled to request documentation to verify your identity*" (**Attachment 8**).

20. To this date, the incorrect information has not been rectified and the Respondent did not handle either of the Complainants' access requests.

2. COMPETENT AUTHORITY/ LEAD AUTHORITY

21. The Lithuanian State Data Protection Inspectorate is competent to handle this complaint pursuant to Article 77 GDPR as the Controller is registered in Lithuania and most of the violations take place there. Whitebridge confirms being subject to the authority of the Lithuanian State Data Protection Inspectorate in its privacy policy.

3. GROUNDS FOR THE COMPLAINT

3.1. Violations

22. The Respondent violated the following provisions of the GDPR:

    (a) The Controller's processing activities lack a legal basis, in violation of Articles 5(1)(a), 6(1) and 9(2) GDPR;

    (b) The Controller processes data from third party sources in violation of the purpose limitation principle in Article 5(1)(b) GDPR;

    (c) The Controller failed to provide information to the Complainants under Article 14 GDPR upon collection of their personal data;

    (d) The Controller failed to handle the Complainants' access requests, in violation of Articles 15(1), (2) and (3) and 12(1), (2), (3), (5) and (6) GDPR;

    (e) The Controller failed to handle the Complainants' rectification requests, in violation of Articles 16 GDPR and 12(1), (2), (3), (5) and (6) GDPR;

    (f) The Controller generated inaccurate data, in violation of Article 5(1)(b) GDPR.

3.2. Violation of Articles 5(1)(a), 6(1) and 9(2) GDPR

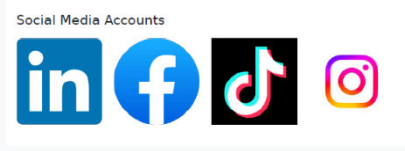
23. The privacy policy of the Controller contains references to multiple legal bases regarding processing activities concerning the personal data of users. As the complainants qualify as searched persons, but not as users, this complaint will not examine the processing activities in relation to "users".

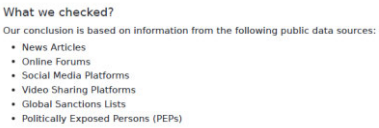
24. The Controller claims, in its privacy notice that the searched persons' data "*is available in public information sources*", and comes "*from public sources such as Facebook, LinkedIn, Instagram, Google, media outlets, other social media networks, websites, etc.*". It claims that, when reports contain sensitive personal data, it is only data manifestly made public under Article 9(2)(e) GDPR.

25. The Complainants specifically asked what was the legal basis for the processing of their data but their request remained unanswered (**Attachments 5 and 6**).

3.2.1. Publicly available data

26. In the present case, the reports on the Complainants are allegedly based, among others, on the content of the Complainants' social media accounts, in particular Instagram, Facebook, LinkedIn and TikTok (**Attachments 6 and 7**). See for example the following screenshots for Complainant 1.





27. According to its privacy policy, Whitebridge appears to be of the view that any data visible on social media is publicly available and hence qualifies as "manifestly made public" in the sense of Article 9(1)(e) GDPR. However, social media accounts and their content, including any personal data under Article 4(1) GDPR are only accessible to other users through the creation of an account with the respective social media platform. Data displayed on social media therefore usually belongs to the private and not a public sphere.

28. Even though data displayed on social media is private irrespective of users' privacy settings, the private nature of data displayed on social media becomes even more obvious regarding Complainant 2 who has a private Instagram account, meaning it is only accessible to the followers he accepted. Nonetheless, the Respondent claims that this account has been a source used to generate the report.

29. The CJEU confirmed in C-252/21 that entering information on a social networking application does <u>not</u> equate to manifestly making this data public.

> "*if no such individual setting are available, it must be stated […] that where users voluntarily enter information in to a website or app or tap on buttons integrated into the, they must, in order to be deemed to have manifestly made those data public, have explicitly consented, on the basis of express information provided by that site or app prior to any such entering or clicking or tapping, to the data being viewed by any person having access to that site or app*".[4]

30. The initial consideration that any data on social media platforms are publicly available is hence already unfounded. Even if one was to consider that this data has been manifestly made public by the data subject under Article 9(2)(e) GDPR and is thus not subject to the prohibition

[4] C-252/21, 4 July 2023, *Bundeskartellamt*, §83.

under Article 9(1) GDPR, its processing is thus still subject to the requirements of the GDPR, including the need for a legal basis under Articles 5(1)(a) and 6(1) GDPR.[5]

3.2.2. Primary argument - right to conduct a business does not constitute a legal basis

31. According to the Controller, "*processing of personal data from publicly available sources is both legal and appropriate. This is supported by Recital 4 of the GDPR, Article 16 of the EU Charter of Fundamental Rights* [hereinafter the CFR]*, and Article 48 of the Constitution of the Republic of Lithuania, along with other relevant laws. It aligns with the freedom to conduct business and complies with GDPR requirements.*"[6]

32. The Controller bases its argument on the following fundamental misunderstandings of the law:

    (a) The GDPR is already the result of the balancing between the rights to data protection under Article 8 CFR and other interests – such as business interests. Recital 4 of the GDPR makes clear that the balancing was the legislators work – not the future work of controllers. This means, the GDPR cannot be "*balanced*" again and again – to delude the legislator's decision on the right balance between Article 8 CFR and other rights in the interest of businesses. The non-binding Recital 4 of the GDPR does not allow a controller to make itself a co-legislator that can just "reinterpret" the text of the GDPR until it does not interfere with his commercial interests anymore.

    (b) The "freedom to conduct a business" under Article 16 CFR is extremely narrow, as it (i.) is not a "right" under the CFR, but merely a "freedom", (ii.) is aimed at allowing people to pursue an economic activity without being subject to discrimination or disproportionate restrictions[7] (e.g. inheritance of the right to be conduct a certain business from the parents that conducted the same business). It is not a "right to make money" or a "right to be profitable" and (iii.) most importantly, it is limited to the conduct of any business "*in accordance with Union law*", such as the GDPR. In other words: The freedom to conduct a business ends where any tax, hygiene, worker protection or privacy law starts.

    (c) The fact that data is allegedly "*publicly available*" is not a legal basis under Article 6(1) GDPR. The controller clearly attempts to create a new legal basis that does not exist.

33. Consequently, the freedom to conduct a business cannot be used as a pretext to legitimize an economic activity carried out in violation of fundamental rights or legal obligations. A simple parallel can be drawn with the example of a company operating a factory where dangerous substances are produced. The company could not realistically rely on its freedom to conduct a business to waive any employee safety measures or a legal prohibition to produce certain chemicals under Article 31 CFR. In the same vein, the Respondent cannot deny the complainant's fundamental rights under Article 7 and 8 CFR and cannot waive its mandatory legal obligations under the GDPR by invoking the freedom to conduct a business

34. Contrasting the legal view of the controller with the legal reality shows that Whitebridge is acting entirely outside of the framework of EU law and the GDPR. In conclusion, the freedom

---

[5] See e.g. C-34/21, *SCHUFA II*, 30 March 2023, §68 with further references,

[6] Whitebridge's privacy notice, https://whitebridge.ai/legal/privacy-policy, last updated on 12 April 2024, consulted on 12 September 2025.

[7] European Union Agency for Fundamental Rights, "*Freedom to conduct a business: exploring the dimensions of a fundamental right*", 2015, p.21 and caselaw cited.

to conduct a business cannot be relied on to avoid the requirement of legal basis under Article 5(1)(a) and 6(1) GDPR.

3.2.3. Subsidiary argument – The legal basis possibly invoked by the Controller is invalid

35. The above shows that the processing of the Complainants' data was performed without legal basis. The Controller does not refer to any legal basis for the processing of the searched persons' data, putting the complainants in a position where they can only speculate on the applicable legal basis.[8]

36. The Complainants, and more generally the searched persons have not given consent under Article 6(1)(a) GDPR nor entered into a contract with the Controller within the meaning of Article 6(1)(b) GDPR that would justify the processing of their personal data. Article 6(1)(c), (d) and (e) GDPR cannot possibly constitute a legal basis in the case at hand as there is neither a legal obligation to process the data, nor a vital interest of the data subject, nor a public interest However, the Controller repeatedly refers to its economic interest in its privacy notice. These elements allow for the speculation that the Controller relies on legitimate interest under Article 6(1)(f) GDPR to process the searched persons' data.

37. For this legal basis to be valid, three cumulative conditions must be met:

    (i) The pursuit of a legitimate interest by the Controller or by a third party;
    (ii) The processing must be necessary for the pursued legitimate interest. This condition must be examined in light of the data minimization principle[9];
    (iii) The interests or fundamental freedoms and rights of the person concerned must not outweigh the legitimate interest of the controller or of a third party.[10]

38. These conditions are not met for the processing at stake:

39. As regards condition (i), the CJEU clearly confirmed that the mere commercial purpose does not constitute a legitimate interest to scrape the internet.[11] This reasoning is applicable *mutatis mutandis* to the case at stake.

40. Overall Recitals 47 to 49 largely refer to "defensive" actions as a legitimate interest, such as ensuring network security from hackers. There is no "offensive" examples of a legitimate interest in the GDPR. In fact, WhiteBridge.ai is not just "offensive" but nothing but a "*people spy page*" on other individuals, which cannot possibly be a legitimate interest. If it would be one – literally any processing would be a legitimate interest.

41. When it comes to the necessity requirement (ii), the CJEU explains that it should be ascertained "*whether the legitimate interest pursued by the processing of the data can reasonably be achieved just as effectively by other means less restrictive of the fundamental*

[8] See Section 2.3 on the violation of Article 14(1)(c) GDPR following this lack of transparency.

[9] EDPB, *Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR,* 8 October 2024, §29 and caselaw cited.

[10] CJEU, C-621/22, *Koninklijke Nederlandse Lawn Tennisbond*, 4 October 2024, §37; CJEU, C-252/21, *Meta Platforms and Others*, §106; EDPB, *Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR,* 8 October 2024, §6.

[11] CJEU, C- 131/12, *Google Spain,* 13 May 2014, §81.

freedoms and rights of data subjects"[12]. In this case, the interest is already not legitimate and no measures have been put in place by the Controller to minimize the data processed.

42. To the extent that the processing is limited to information available publicly on news outlets, it could be justified under the principle of necessity, provided that it also passes the obligatory balancing test. However, when the processing extends to a data subject's personal account on social media data, something that belongs to their private sphere it becomes unnecessary and disproportionate.

43. The relevant pages all use a "robots.txt" file to limit the scraping of data by third parties.[13] The relevant files all contain a string of "*User-agent: **" and "*Disallow: /*", which sets that the relevant data of these pages may not be scraped or used by third parties. This ensures that data on these social media pages is not "public" as in available on web search engines. The Respondent clearly ignores these settings and unlawfully "scrapes" the relevant data from these Social Media pages. The Complainants on the other hand did not make the relevant data "public" as on a normal website, but were merely sharing it within a social network, where such data could only reasonably be seen by relevant connections.

44. Regarding the balance between the legitimate interest of the controller and the fundamental rights and freedoms of the data subject (iii), the CJEU considers that account must be taken of the reasonable expectations of the data subjects, the scope of the processing in question and the impact of the processing on the data subjects.[14] In this case, the searched persons do not have any relationship (contractually or otherwise) with the Controller, have not even been informed of the reports being issued and could therefore not reasonably expect the Controller to process their data. Given the potentially unlimited scope of the processing (especially with the profile monitoring feature) and the significant impact on the data subjects (the reports can be accessed by anyone and used for many purposes[15]), the rights of data subjects clearly outweigh the Controller's commercial interest in this case.

45. The CJEU also points out that "*according to Article 13(1)(d) of the GDPR, it is the responsibility of the controller, at the time when personal data relating to a data subject are collected from that person, to inform him or her of the legitimate interests pursued where that processing is based on* [Article 6(1)(f)]".[16] Here, even in the hypothesis that the Controller relied on legitimate interest as a legal basis, it also failed to inform the Complainants that it processed their data and about the legal basis.

46. Therefore, the Controller violates Articles 5(1)(a) and 6(1) by lacking legal basis or alternatively by relying on an invalid legal basis.

---

[12] CJEU, C-394/23, *Mousse,* 9 January 2025, §48; see also EDPB, *Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR,* 8 October 2024, p. 2.

[13] On Facebook: https://www.facebook.com/robots.txt, Instagram: https://www.instagram.com/robots.txt, LinkedIn: https://www.linkedin.com/robots.txt, accessed on 17 September 2025.

[14] CJEU, C-252/21, *Meta Platforms and Others*, §116.

[15] For example, the Controller promotes the use of its service for hiring decisions, which undoubtedly has a major impact on data subjects' rights and freedoms.

[16] CJEU, C-621/22, *Koninklijke Nederlandse Lawn Tennisbond*, 4 October 2024, §41.

3.2.4. Article 9(2) GDPR

47. Article 9(1) GDPR prohibits the processing of special categories of personal data which benefit from a protected status under the GDPR due to its particularly sensitive nature (Recital 51 GDPR).

48. As explained, Complainants' reports respectively included warnings for "sexual nudity" and "dangerous political content".

49. Political content is explicitly mentioned in Article 9(1) GDPR, which prohibits processing of personal data "*revealing* [...] *political opinions*". While the GDPR does not define "political opinion", the term political content is necessarily included in this category. Article 29 Working Party confirms this broad understanding by stating that this term is to be understood to include not only data containing sensitive information in itself, but also data by which "*sensitive information with regard to an individual can be concluded*".[17]

50. Similarly, nudity also falls under the category of sensitive personal data. Article 9(1) GDPR prohibits processing of personal data "*concerning a natural person's sex life or sexual orientation*". The terms are also understood broadly to include data related to sexual practices, as well as other acts that may reveal sexual orientation.[18] Considering the fact that the Respondent includes the warning regarding "sexual nudity", this data may reasonably be associated with the Complainant's sex life.

51. By allegedly processing sensitive data within the meaning of Article 9(1) GDPR without applicable exemption under Article 9(2) GDPR, the Respondent also violated Article 9 GDPR.

3.3. Violation of Article 5(1)(b) GDPR

52. Under Article 5(1)(b) GDPR, personal data shall be "*collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes*".

53. Whitebridge's activity includes the processing of data shared by data subjects on social medias to generate reports. Recital 18 of the GDPR specifically considers the sharing of data on social medias as a household activity. As explained in section 3.2.1., data subjects share data on social medias with a restricted amount of users. Social media being private sphere, data subjects are active on it with private purposes.

54. By processing data shared by the data subjects on their social media for their private purposes to generate its reports, Whitebridge further processes this data for its own (commercial) interest of building a "spy website", in a manner totally incompatible with the initial purpose of exchanging with friends and online connections. Consequently, the processing in relation to the issuance of the reports violates the principle of purpose limitation under Article 5(1)(b) GDPR.

---

[17] WP29, "*Advice paper on special categories of data ("sensitive data")", 4 April 2011, p. 6*. Available here.

[18] *Petri*, in Simitis, Horning, Spiecker gen. Döhmann, Datenschutzrecht, Article 9 GDPR margin number 23 (C.H. Beck 2019).

3.4. Violation of Article 14 GDPR

55. Article 14(1), (2) and (3) GDPR provides that where personal data have not been obtained from the data subject, certain information must be provided to the data subjects. This includes information about the data subjects' rights; information, if applicable, about the legitimate interest pursued by the controller; and the recipients of the personal data, if any.

56. Article 12(1) GDPR specifies that the Respondent is obliged to take appropriate measures to provide information referred to in Article 14 GDPR. In particular, "*the information shall be provided in writing, or by other means, including, where appropriate, by electronic means"*.

57. As shown above, the Controller did not take any measure to provide information under Article 14 GDPR.

3.4.1. Article 14(3) – Timing to provide the information

58. This information must be provided within a reasonable period after obtaining the personal data, at the latest within one month under Article 14(3)(a) GDPR. Article 29 Working Party adds that "*The general one-month time limit in Article 14.3(a) can also be curtailed under Article 14.3(c) which provides for a situation where the data are being disclosed to another recipient (whether a third party or not). In such a case, the information must be provided at the latest at the time of the first disclosure*".[19]

59. In this case, it is clear that the Complainants' data have been disclosed to at least one recipient as Whitebridge issued a report for each of them. Given that the Respondent did not give any information to the Complainants under Article 14 GDPR, *a fortiori,* it did not provide the information in the required timeframe.

3.4.2. No exemption under Article 14(5)(a) and (b) applies

60. Article 14(5)(a) and (b) GDPR provide that such information is not necessary when (a) the data subject already has the information or (b) if providing "*such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes*".

61. The Respondent claims, in its privacy notice, that it does not have the direct contact details of the searched person and as a result, that the "*information proves to be impossible or would involve a disproportionate effort, and therefore, in compliance with Article 14(5)(a-b)*".[20]

62. Unlike alleged by the Respondent, Article 14(5)(a) is not possibly applicable. The Complainants are not informed elsewhere that their data is being processed by the Controller.

63. Second, the Respondent cannot convincingly claim that the provision of information to data subjects proves to be impossible. The impossibility is easy to assess: "*something is either impossible or it is not; there are no degrees of impossibility*".[21] As a matter of fact, because the Controller precisely identifies the social networks and contact details of the searched persons to issue its reports (**Attachments 6 and 7**). It could then very easily contact the searched persons in order to inform them about its processing activities

---

[19] WP29, 'Guidelines on Transparency under Regulation 2016/679', 11 April 2018 (available here), p. 15.
[20] https://whitebridge.ai/legal/privacy-policy.
[21] WP29, 'Guidelines on Transparency under Regulation 2016/679', 11 April 2018 (available here), p. 29.

64. Third, the claim that such information would involve a disproportionate effort cannot be upheld. The exemption under Article 14(5)(b) GDPR must be subject to particular caution: if its scope is too broad, it would deprive Article 14 GDPR of its essence. Article 29 Working Party points out that "*this exception should not be routinely relied upon by data controllers who are not processing personal data for the purposes of archiving in the public interest, for scientific or historical research purposes or statistical purposes*".[22]

65. The ICO also examined the scope of the exemption in relation to data brokers and considered, in substance, that processing very large amounts of data "*cannot be a deciding factor against it being proportional to notify people about the processing*". It outlined that it would create a "*perverse incentive to gather as much data as possible in order to reduce the burden* […] *to notify people*". In conclusion, "*it would not be 'disproportionate'* […] *to comply with Article 14 and proactively tell people that they are processing their personal data*". [23] It goes without saying that the considerations of the ICO concerning data brokers, who process much more data than the Respondent, apply here *mutatis mutandis*.

66. In addition, when seeking to rely on the disproportionate effort exemption, controllers must carry out a balancing test and document it in accordance with their accountability obligations. They also must take appropriate measures to protect the data subjects' rights.[24]

67. In this case, the Respondent does not pursue purposes of archiving in the public interest, for scientific or historical research purposes or statistical purposes nor has carried out a balancing test. There is also no evidence of any measure taken to protect the data subjects' rights. As explained above, the Respondent also processes the contact details of the researched persons and can therefore easily contact them. These elements bring to the conclusion that the Respondent cannot reasonably rely on a disproportionate effort under Article 14(5)(b) GDPR.

68. As none of the information necessary under Article 14 GDPR have been provided, and no exemption under Article 14(5) GDPR is applicable, the Respondent has violated Article 14 GDPR.

3.5. Violation of Articles 15(1) and (3) and 12(2), (3), (5) and (6) GDPR

69. Under Article 15(1) and (3), the Controller shall handle data subjects' access requests. Article 12(2) and (3) further specifies the modalities of the exercise of the data subjects' rights and provides that the controller should facilitate the exercise of the data subject rights and cannot refuse to act on data subjects' request unless it demonstrates that it is not in a position to identify the data subject. The controller should also handle access and rectification requests without undue delay and at the latest within one month.

70. In this case, the Respondent, as explained in Section 1.3 of this complaint, provided mere references to its privacy notice in reply to the Complainants' access requests.

---

[22] WP29, 'Guidelines on Transparency under Regulation 2016/679', 11 April 2018 (available here), p. 30.

[23] Vgl ICO, Investigation into data protection compliance in the direct marketing data broking sector (October 2020), (available here), accessed on 12 September 2025.

[24] WP29, 'Guidelines on Transparency under Regulation 2016/679', 11 April 2018 (available here), p. 31.

3.5.1. Violation of Article 12(2) GDPR

71. The Respondent also asked the Complainants to contact another email than the one provided in the privacy notice and then refused to respond without a qualified electronic signature.[25] This attitude clearly obstructs the exercise of the data subjects' right, in violation of Article 12(2) GDPR.

3.5.2. Violation of Article 12(6) GDPR

72. Regarding the request for a qualified electronic signature, Article 12(6) provides that if a controller has reasonable doubts concerning the identity of the natural person making a request, it may request additional information to identify them.

73. The EDPB clarifies that the request for additional information to confirm a data subject's identity cannot lead to "*excessive demands and to the collection of personal data which are not relevant or necessary to strengthen the link between the individual and the personal data requested*".[26]

74. Furthermore, the EDPB states that in cases where a controller imposes measures that are burdensome, it must "*adequately justify this and ensure compliance with all fundamental principles*".[27]

75. In this sense, the higher Court of Graz already confirmed that no specific signature formality could be required for identity verification under the GDPR.[28]

76. In this instance, the Complainants provided a copy of their IDs, their names and their email addresses. This information is complete enough to identify any natural person, especially given that on Whitebridge's website, the Complainants found their 'profiles' by simply entering their name and surname. The Controller nevertheless requested a qualified electronic signature, which neither of the Complainants hold. The Controller also explained that AI tools could create highly convincing forged documents.

77. Given that not everyone possesses a qualified electronic signature, especially since this means is usually provided at a certain cost and that it is not available in every country, the request for a qualified electronic signature is excessive and unfair. In addition, the mere possibility of forged documents does not meet the standard of reasonable doubt under Article 12(6) GDPR.

78. For the remainder, *noyb* is informed that other data subjects have sent an electronic signature in the context of their access request with the Respondent and have not received any further information about the processing of their data (see **Attachment 10**).

79. As the Respondent already had enough information to handle the data subjects' requests, it cannot prove any doubt that could allow it to request a qualified electronic signature. It therefore violated Article 12(6) GDPR.

80. The request for a qualified electronic signature also appears to be absolutely not based on security concerns given that anyone can buy the reports of the Complainants without proving

---

[25] We note here that Whitebridge referred the Complainants to the CEO. As the DPO is also the CEO, it cannot perform its tasks with the required independency, in violation of Article 37 GDPR, read in light of Recital 97 GDPR.

[26] EDPB, 'Guidelines 01/2022 on data subject rights- Right of access' 28 March 2023 (Version 2.1), p. 24. Available here

[27] EDPB, 'Guidelines 01/2022 on data subject rights- Right of access' 28 March 2023 (Version 2.1), pp. 26. Available here

[28] OLG Graz - 2 R 192/24h, https://GDPRhub.eu/index.php?title=OLG_Graz_-_2_R_192/24h

their identity. If WhiteBridge would be that concerned with providing data to the wrong person, it begs the question why it provides this highly personal data to any third party that buys that data from them. It is obvious that the "need" for an eID to provide personal data is merely a tactic to reject access requests under Article 15 GDPR.

3.5.3. Violation of Article 12(5) GDPR

81. It seems like the Controller's business model includes the sale of their data to the data subjects themselves (!) which goes against the requirement of Article 12(5) and 15 GDPR. These articles provide that the data subjects' have the right to access their own data free of charge. WhiteBridge.ai instead tries to profit from the fear of data subjects that a website has collected sensitive information about them – that they cannot see.

82. The Complainants did not obtain an answer to their requests for access. On the contrary, the only way for them to know what data about them was processed by the Respondent was through the purchase of the reports.

83. The Respondent is well aware that data subjects are entitled to access their data free of charge. In addition to being contrary to Article 12(5), it is therefore more than questionable to take advantage of the fact that data subjects would be curious to know what the reports contain (and whether it could harm them) in order to make profit. Again, as developed in section 3.2.2, the Respondent could not reasonably rely on its freedom to conduct a business to justify such an infringement of the data subjects' fundamental right.

84. By providing access to personal data upon purchase of the reports and not free of charge, further to the access requests, the Controller clearly violated Article 12(5) GDPR.

3.5.4. Violation of Article 12(3) GDPR

85. Given that the access requests have not been handled, the one-month delay is undeniably exceeded, in violation of Article 12(3) GDPR.

86. In conclusion, by refusing to act on the Complainants' access requests, the Controller violated Article 15(1) and (3) GDPR as well as Article 12(2), (3), (5) and (6) GDPR.

3.6. Violation of 5(1)(d) GDPR

87. Article 5(1)(d) GDPR provides that personal data shall be "*accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay*".

88. In this case, the Respondent generated warnings for "*sexual nudity*" and "*dangerous political content*". These are false information that seem to be added by some form of Artificial Intelligence to make the WhiteBridge reports more dramatic or interesting, in violation of the principle of accuracy. This violation exists regardless of - and is also confirmed by - the fact that the Complainants have requested the rectification of the false information. Creating such fake information is a straight-forward violation of Article 5(1)(d) GDPR.

89. In conclusion, Whitebridge knowingly and deliberate generates and processes inaccurate data and also refuses to take any measure to rectify it when requested by the Complainants, in violation of the principle of accuracy of Article 5(1)(d) GDPR.

3.7. Violation of 16 GDPR

90. The Complainants requested rectification to the Respondent of the warning for "*sexual nudity*" and "*dangerous political content*". The data is not only inaccurate, in violation of Article 5(1)(d) GDPR, but also potentially highly damaging to the data subjects as any third party could purchase their Reports with this information on them.

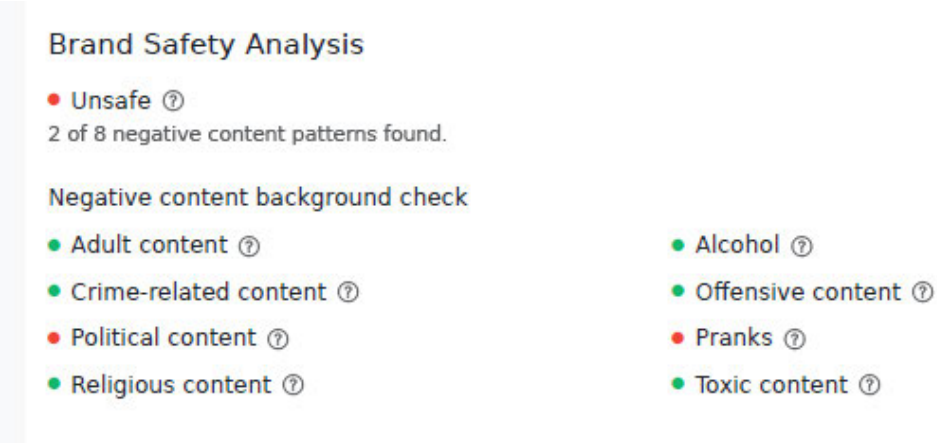


Figure 2 - Extract from Complainant 2's report

91. The correct information would be to mark "political content" for Complainant 2 and "adult content" for Complainant 1 as green.

92. By ignoring the rectification requests, the Controller violated Article 16 GDPR. For the remainder, the violations of Article 12 GDPR explained in section 3.5 are applicable *mutatis mutandis* in the context of the exercise of the right to rectification under Article 16 GDPR.

4. REQUESTS AND SUGGESTIONS

4.1. Request to investigate

93. The Complainants invite the competent authority to investigate the processing that Whitebridge conducts according to Article 58(1) GDPR

4.2. Request to issue a declaratory decision

94. The Complainants request that the complaint be upheld and that Whitebridge be found to have infringed Articles 5(1)(a), (b) and (d), 6(1), 9, 12(1), (2), (3), (5) and (6), 14, 15(1), (3) and 16 GDPR.

4.3. Request to prohibit the controller from processing personal data in violation of the GDPR

95. The Complainants request that the supervisory authority imposes, under Article 58(2)(f) GDPR, a ban on processing of scraped personal data and AI generated false information in violation of Articles 5(1)(a), (b) and (d), 6(1) and 9 GDPR.

4.4. Request to order the Controller to comply with the Complainants' requests

96. The Complainants request that the supervisory authority orders Whitebridge to comply with the access and rectifications requests formed by the Complainants and provides the Complainants with full access to the data concerning them under Article 15 GDPR and rectifies the sections of the reports concerning respectively sexual nudity and political content to include a green mark on these items.

4.5. Request to order the Controller to comply with its notification obligations

97. The Complainant requests that the supervisory authority orders Whitebridge to comply with its notification obligations under Article 19 GDPR. This article places an obligation to the Controller to communicate the outcome of the rectification of personal data to all recipients (as per Article 4(9) GDPR) to whom the personal data have been disclosed.

4.6. Suggestion to impose a fine

98. The Complainants suggest that the competent authority imposes a fine to Whitebridge, as controller, pursuant to Articles 58(2)(i) and 83(5)(a) and (b) GDPR for the infringements of Articles 5(1)(a), (b) and (d), 6(1), 9, 12(1), (2), (3), (5) and (6), 14, 15(1), (3) and 16 GDPR.

5. CONTACT

99. Communications between *noyb* and the Lithuanian State Data Protection Inspectorate in the course of this procedure can be done by email at [redacted] with reference to the **Case-No C102** or [redacted].