noyb - European Centre for Digital Rights
Goldschlagstraße 172/4/3/2
1140 Vienna
Austria

Garante per la Protezione dei Dati Personali
Piazza Venezia 11
00187 - Rome
By E-Mail:

noyb Case-No: [redacted]

Complainant: [redacted]
(see Annex 2 for biographical details)

Represented in accordance with of Article 80(1) GDPR by: *noyb* - European Centre for Digital Rights
Goldschlagstraße 172/4/3/2, 1140 Vienna

Counterparty/owner: **PubMatic, Inc.**
601 Marshall Street
94063, Redwood City
California (USA)

e

any other data **controller** or **processor** that the Data Protection Authority may wish to identify in the context of this complaint.

Concerns: Non-authentication via cookies - Violation Articles 11, 12, 15, 24, 25 GDPR

COMPLAINT UNDER ART. 77 GDPR

1. PROXY FOR LITIGATION

1. *noyb-European* Centre for Digital Rights is a non-profit organisation with its registered office at Goldschlagstraße 172/4/2, 1140 Vienna, Austria [redacted] (hereinafter, "***noyb***") (**Annex 1**, Articles of association) [redacted] Pursuant to Article 80(1) GDPR, the complainant is represented by *noyb* in these proceedings (**Annex 2**).

2. FACTS

2. On 18.8.2022, the complainant browsed the webpage www.my-personaltrainer.it (the 'Site').

3. After accessing the Site, and accepting the cookies presented by the consent management platform on the Site, the complainant browsed for a few minutes, performing searches on the website and consulting various links and articles. At the end of the browsing, the complainant generated two separate session files. The first one consisted of a JSON file generated by a plugin able to extract the first and/or third party cookies installed by the Site within the complainant's browser (**Annex 3**). The second file, generated by means of Chrome's '*Inspect*' function, launched at the beginning of browsing, was a HAR file including all the interactions made by the user while browsing the Site (**Exhibit 4**).

4. The aforementioned JSON file shows that, in the present case, the Site had allowed the installation of a ponderous quantity of cookies developed by the present proprietor ('third-party cookies'), all traceable to the domain of the controller ".*pubmatic.com*" domain, including cookies containing unique identification IDs such as *KADUSERCOOKIE* ([redacted] ("[redacted]") and, from "*.ads.pubmatic.com*", *pubsyncexp* ("[redacted]") (see Annex 3).

5. On 29.8.2022, the complainant sent, to the email address specified by the owner in its privacy policy (**Annex 5**), a request for access pursuant to Article 15 GDPR (**Annex 6**).[1] In order to prove that the personal data covered by the request were related to the data subject itself, the latter attached the list of cookies deposited by the Site within its browser and contained in the JSON file in Annex 3.

6. Following receipt of the access request, the controller requested the complainant to perform further steps allegedly necessary to complete the authentication procedure. In particular, on 31.8.2022, Pubmatic invited the complainant to provide the following details: '*First and last name, Home address, Business address (if claiming on behalf of a business), Email address*'. On 23.9.2022, the complainant replied, among other things, that the request for this additional information was unreasonable: '*Since you take your responsibility under the GDPR seriously, I want to emphasise that your request for additional information is unreasonable. In order to process my access request, you ask me to give you (a data broker) even more information about my residence, including home (and business) address, as well as my email address. I do not intend to share this information with you*'. The information requested by the owner, the complainant claimed, did not add any identifying value to the cookies already transmitted with the request. On 24.9.2022, the holder invoked the time extension under Article 12(3) GDPR for a period of two months. On 11.10.2022, the holder laconically replied that "*We have run specific searches against our products and data storage centres and have confirmed that no instances of the provided identifiers remain within our systems.*" (**Annex 7**).

1. In addition to a full explanation of the processing of personal data resulting from the acquisition via cookies (Article 15(1) and (2) GDPR), the request sought clarification of certain aspects so to speak typical of processing via cookies, requesting for example the precise details of the recipients of the personal data (Articles 15(1)(c) and 19 GDPR) as well as the sources of the same, where available (Article 15(1)(g) GDPR). It also required a perfect copy of all data processed in any way related to the user (Article 15(3) GDPR).

7. Apart from the conduct just described, it was not possible in any other way to submit the request and obtain further information with respect to the processing of personal data. For example, the controller's website did not present any procedure within or outside the CMP to be able to submit a request to exercise the right in a user-friendly manner.

8. In the complainant's view, the facts set out above constitute the violations listed in the following paragraphs.

3. ELEMENTS OF THE COMPLAINT

9. The complainant considers that, by its conduct, the controller has, at the very least, committed the following violations of the GDPR, as further set out in the following paragraphs:

    1) Failure to facilitate the exercise of the right of access and violation of the principle of data minimisation by requesting to perform steps and provide additional information not required for user authentication in violation of Articles 11, 12(2) and (6), 15 and 24 GDPR;

    2) Failure and/or incomplete response to the request for access in violation of Article 15 GDPR;

    3) Any other breach relating to cookie authentication systems that the Garante, with its powers of investigation, may ascertain as a result of the analysis and investigation of this complaint.

1) ***Failure to facilitate the exercise of the complainant's right of access by requesting him to take steps and provide information in addition to that required for user authentication***

10. After receiving the request, the controller replied by requesting further elements allegedly necessary to complete the user's authentication. However, none of the requested elements, including the data subject's country of residence, abode, and other e-mail addresses, was really necessary to authenticate the complainant (see § 6).

11. When there is no account between the user and the service, as in this case, the only possible authentication factor is the cookies installed within the complainant's browser. All other possible identification factors including, for example, the signature or copy of an identity document, the address of residence or habitual abode are absolutely irrelevant. In this case, in fact, the controller does not possess (or at least should not possess) any of these elements, so that further requests by the latter for alleged authentication purposes are unlawful and lacking justification (see, among others, WP29, *Guidelines on the right to data portability*, pp. 13-14).

12. On this point, the EDPB has expressly clarified how, in the case of data processing for the purpose of behavioral advertising, "*identification by means of an identity card does not necessarily help in the online context (e.g. with the use of pseudonyms) if the person concerned cannot contribute any other evidence, e.g. further characteristics matching to the user account*". For example, in the case where "*A controller C processes personal data with the purpose of addressing behavioral advertising to its web users. Personal data collected for behavioral advertising are usually collected by cookies and associated with pseudonymous random identifiers. A data subject Mr. X exercises his right of access with C via C's website.* ***C is able to precisely identify Mr. X to show the data subject's behavioral advertising, by linking the terminal equipment of Mr. X to its advertising profile with the cookies dropped in the terminal. C should then also be able to precisely identify Mr. X to grant him access to his personal***'. More precisely, in the above example, '*the purposes of C require the identification of the data subjects, while Art. 11 GDPR addresses the situation of a controller who would process additional data within the meaning of Art. 11(1) GDPR for the sole purpose of being able to comply with the GDPR. Accordingly, Art. 11 should be interpreted in particular in the light of the principle of fairness. This, in some cases, may mean that no additional data should be requested in order to exercise the rights of the data subject.* ***However, if Mr. X tries***

to exercise his access right by e-mail or by regular mail, then in this context C will have no other choice to ask Mr. X to provide "additional information" *(Art. 12(6)) in order to be able to identify the advertising profile associated with Mr. X.* ***In this case, the additional information will be the cookie identifier stored in the terminal equipment of Mr. X.***". [emphasis added] (EDPB, Guidelines 01/2022 on data subject rights - Right of access**,** pp. 24-25).

13. This line of reasoning has already been followed by several decisions on the merits. For example, the Finnish DPA held that requiring a signature on a paper form for identification was not necessary, since the data subject was able to provide the access data with which he had established contact with the controller. In fact, not only was it considered that **requiring a signed paper form from the controller made it more difficult for the data subject to exercise his rights**, but it was also considered to increase, rather than decrease, the potential risk of abuse (DPA Finland, 6097/161/21). Faced with a similar case, in a joint decision under Article 60 GDPR, the DPAs of Berlin and Malta ruled that the request to verify identity by means of an identity document was disproportionate, since, among other things, **the data minimisation principle under Article 5(1)(c) GDPR prohibits requesting a wider range of personal data than those already processed prior to the request**, unless this is strictly necessary (§§ 21 and 26). Rather, the DPAs considered that the controller should have used **other measures**, such **as matching the information and personal data provided by the data subject with the information already available to the controller** (DPA Berlin/Malta, no. *EDPBI:MT:OSS:D:2022:341*). Again, in another Article 60 GDPR procedure, the Irish DPC ruled that it was unlawful to request additional information that was not necessary for authentication (DPC, case number not available, decision in annex). Finally, the Belgian DPA (APD, No 145/2022) and the Dutch DPA (AP, procedure number not available, decision in annex) were of the same opinion (**Annex 8**).

14. Accordingly, in the present case, the controller clearly violated several principles and specific provisions of the Regulation. In particular, by requiring the data subject to provide additional information entirely superfluous for the purposes of authentication, it has, among other things, clearly breached the principles of fairness, minimisation and facilitation of the exercise of the data subject's rights and thus Articles 5(1)(a), (c), 11, 12(2) and (6), 15 and 24 GDPR.

2) ***Failure and/or incomplete response to the request for access in violation of Article 15 GDPR.***

15. On 11 October 2022, the controller reported the following: "*Thank you for your patience.* ***We have run specific searches*** *against our products and data storage centres and have confirmed that no instances of the provided identifiers* ***remain*** *within our systems*' (emphasis added) (see Exhibit 7d). The tenor of the reply is definitely ambiguous.

16. Let us assume that the authentication of the data subject has actually taken place.[2] The logical consequence would be for the controller to provide all the information requested by the complainant under Article 15 GDPR. However, as it can easily be seen, the controller's response **does not provide any substantive information about** the content of the access request (see Exhibit 6). For instance, but not limited to, none of the information prescribed by Article 15(1) GDPR, including elements on the sources and recipients of personal data, was provided. [3]

17. The same applies to the requested copy of personal data pursuant to Article 15(3) GDPR. On this point, the controller merely states that '*no instances of the provided identifiers* ***remain*** *within our systems*'. It must be emphasised that this statement **may not correspond to reality**. Many of the cookies installed by Pubmatic, in fact, had expired **after** the date of the company's last reply (11

[2] Otherwise, it would not have been possible to '*run specific searches*' and state that '*no instances of the provided identifiers* ***remain*** *within our systems*' (emphasis added).

[3] On this point, the complainant refers to the recent CJEU, 12 January 2023, No -C154/21. The decision rules on the interpretation of Article 15(1)(c) GDPR and clarifies that, where the data subject so requests, as was undoubtedly the case here, the data controller is obliged to communicate details of the recipients of the personal data. Such details were entirely omitted by the present data controller.

October 2022). For example, *KADUSERCOOKIE* and *DPSync3* both expired on 16 November 2022. In relation to other cookies, however, **the response is certainly late**. For example, just to mention a few, *SpugT*, *KRTBCOOKIE_* 699, *KRTBCOOKIE_279* and *KRTBCOOKIE_153 expired* on 17 September 2022, and thus after the submission of the request (**Annex 9**).

18. The retention of this information in Pubmatic's systems was essential to ensure proper fulfilment of the access request. A world-class data broker cannot 'wait' for cookies to expire and then simply report that no information '*remains*' in the storage systems. Slowness and disorganisation cannot be a valid excuse in such cases.

19. On this point, it is worth recalling that, when GDPR rights are exercised, the onus is on the controller, pursuant to Article 24 GDPR, to take appropriate technical and organisational measures to **recognise** the content of the access request and to act accordingly. Confirmation of this can be found in the EDPB's recent guidelines on the right of access: '*the controllers should be proactively **ready to handle requests** for access to personal data. This means that the controller should be prepared to receive the request, **assess it properly*** [...] *and provide an **appropriate reply** without undue delay to the requesting person*". (EDPB, Guidelines 01/2022 on data subject rights - Right of access**,** p. 18). **This did not happen in the present case**.

20. Contrary to what happened in this case, **other data controllers** to whom such a request was made have correctly fulfilled their information obligation under Article 15 GDPR. In one case, for example, after a quick authentication of the user (based solely on the cookies provided in the JSON file), the controller provided a clear representation of the current processing, indicating the data still held and providing clear information about the purpose of the processing, the recipients and the sources of the data (**Annex 10**).

21. The above-mentioned conduct of today's data controller therefore constitutes a clear violation of Article 15 GDPR.

3) ***Other possible breaches relating to the authentication system when using profiling cookies***

22. Finally, it is requested that the Garante make a more general assessment in relation to systems of authentication and exercise of rights by means of cookies. The GDPR, as is well known, places particular emphasis on the effectiveness of the data subject's rights set out in Articles 15-22 (Recital 11) and, in the present case, it is not considered that such effectiveness has been guaranteed. In fact, the complainant had to engage the data controller with the support of lawyers and technical specialists in order to obtain rather meagre results, hence the present complaint. The Garante is therefore asked to verify whether, in the light of an interpretation oriented to the principles of effectiveness and facilitation of rights, the data controller has put in place all the appropriate technical and organisational measures to respond to the requests for the exercise of rights for the specific processing in question (Articles 24 and 25 GDPR).

4. REQUESTS

1) ***Request to carry out any necessary investigation***

23. In light of the above, the complainant requests the Garante to investigate the above facts with particular reference to the controller's authentication practices related to the use of tracking cookies. It is also requested to verify whether, in relation to the type of processing considered, the controller has taken all necessary organisational measures pursuant to, inter alia, Articles 24 and 25 GDPR, in order to properly authenticate the complainant and respond in a complete and timely manner to access requests.

2) ***Request to establish the violation and issue specific orders***

24. The complainant petitions for the Data Protection Authority to ascertain any violation arising from the facts set out and/or ascertained in the investigation and to adopt any remedy deemed appropriate to bring the data processing back into compliance with the GDPR. In particular, the complainant respectfully petitions the Data Protection Authority:

    1) pursuant to Article 58(2)(c) GDPR, orders the data controller to give full effect to the request for access;

    2) having ascertained the lack of adequate technical and organisational measures to authenticate the user through the use of cookies in violation of, inter alia, Articles 12(2), 24 and 25 of the GDPR, orders, pursuant to Article 58(2)(d) of the GDPR to make the operations compliant, in a specific manner, including, where necessary, automatic authentication tools via cookies;

    3) in view of any other breach of the GDPR that the Garante, with its investigative powers, may ascertain as a result of its analysis and investigation of this complaint, adopt any remedy it deems appropriate.

3) ***Request to impose an administrative fine***

25. The complainant suggests the imposition of an effective, proportionate and dissuasive fine for the breaches found. It should be noted in particular that, among other elements, (i) thousands of internet users visit the Website every day that allowed the installation of the tracking cookies developed by the present owner and that (ii) the articles on the Website concern or may concern particular categories of data within the meaning of Article 9 of the GDPR.

5. CONTACTS AND FURTHER INFORMATION

26. Communications between *noyb* and the Guarantor in the course of this procedure may take place by e-mail to [redacted] with reference to the case number indicated in the title of this complaint. We will be happy to assist you with any further factual or legal details you may require to process this complaint.

Signature