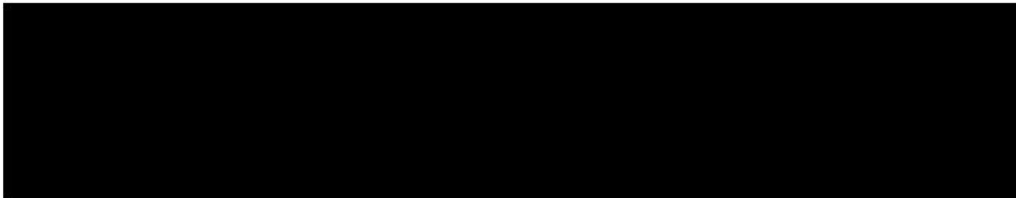noyb – European Center for Digital Rights
Goldschlagstraße 172/4/3/2
1140 Vienna
Austria

Garante per la protezione dei dati personali
Piazza Venezia 11
00187, Rome, Italy

Per E-Mail: protocollo@gpdp.it

Vienna, 09.07.2024

noyb Case-No: C-084

██████████████████████████████████████
██████████████████████████████████████
██████████████████████████████████████

<u>represented under</u>   noyb – European Center for Digital Rights
<u>Article 80(1) DSGVO by:</u>   Goldschlagstraße 172/4/3/2
                                   1140 Vienna
                                   Austria

<u>Defendant:</u>   **Xandr Inc.**
                                   28 West 23ʳᵈ Street, Fl 4
                                   New York, NY 10010
                                   United States of America

<u>Regarding:</u>   Article 5(1)(c) and (d) GDPR
                                   Article 12(2) GDPR
                                   Articles 15 and 17 GDPR

COMPLAINT

noyb – European Center for Digital Rights | Goldschlagstr. 172/4/3/2, 1140 Wien, Austria | ZVR: 1354838270
www.noyb.eu | general requests: info@noyb.eu ████████████████

page 1 of 14

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

2. *noyb* is representing the complainant under Article 80(1) GDPR (**Attachment 2**).

2. FACTS PERTAINING TO THE CASE

2.1. The processing of personal data by Xandr Inc.

3. Xandr Inc. ('Xandr' or 'the Defendant') manages a Real Time Bidding ('RTB') platform that connects multiple actors in the digital advertising ecosystem. RTB systems enable advertisers to buy space for ads ('ad inventory') from online publishers in real time and in a fully automated way. As soon as a user visits a website implementing this technology (for example, an online newspaper), an algorithmic auction takes place among advertisers in order to decide which company will display an impression to the user.

4. In particular, Xandr owns its own Demand Side Platform ('DSP').[1] A DSP brings together hundreds of advertisers and facilitates the auction of ad inventory. As interests and features of a user play a crucial role in determining advertisers' willingness to bid on and buy slots for their ads, DSPs collect and share a massive amount of personal data. Among other data, DSPs process extremely detailed and granular 'market segments' that aim at profiling the users and facilitate targeting.

5. This processing, in short, consists of attaching the segments to a string of code (stored in a cookie, for example) that uniquely identifies the user that is visiting a webpage or using an app or a service. Data is then broadcast to hundreds of companies that may be interested in advertising their products to the user. Even though just one advertisement will be ultimately displayed, *all the advertisers* receive the segments, alongside countless other pieces of information about the user (e.g. IP address, browser and device type, device language etc.).

6. For example, advertisers X, Y, Z decide to display ads to people interested into cars. Xandr links the user x to market segments like 'cars', 'motors', 'vehicles' etc. Even though only Advertiser X will win the auction and display an impression to the user x, the data linked to that user is sent to both X, Y, Z, in order for them to take part in the auction. Of course, ad targeting is much more complex and usually involves multiple segments at the same time.

7. In June 2023, investigative journalists in both the US and Europe uncovered tens of thousands of segments collected by Xandr for targeting purposes.[2] These profiles, originally disclosed by

---

[1] For the technical documentation, see: https://learn.microsoft.com/en-us/xandr/monetize/about-monetize. Xandr, previously known as Appnexus, was acquired by Microsoft from the US telecommunication giant AT&T in 2021.

[2] See The Markup (https://themarkup.org/privacy/2023/06/08/from-heavy-purchasers-of-pregnancy-tests-to-the-depression-prone-we-found-650000-ways-advertisers-label-you) and Netzpolitik (https://netzpolitik.org/2023/microsofts-datenmarktplatz-xandr-das-sind-650-000-kategorien-in-die-uns-die-online-werbeindustrie-einsortiert/)

Xandr itself to promote its products with advertisers,[3] revealed an impressive level of granularity and the potential to draw detailed inferences on personal lives of consumers.

8. Just to mention some examples out of the many hundreds of sensitive profiles concerning data subjects in Europe, Xandr offers:

    - data concerning health: 'french_disability', 'diabetes_german', 'italy dieting and weight loss', 'pregnant';
    - data revealing sex life or sexual orientation: 'spain > interest > lgbt', 'Sexy Center'; 'paedophilie';
    - data revealing political or philosophical opinions: 'mentality-nieuwe-conservatieven', 'germany environmentalism', 'gender_equality';
    - data revealing religious believes: 'greek orthodox', 'jewishfrench', 'ramadan';
    - data on financial status: 'italy credit level – poor', 'struggling families', 'fragile seniors retirees over 65'.

9. Typically, segments are not created directly by Xandr but rather bought from third companies – Xandr's 'data partners' (data brokers) – that track users' online activities for the purpose of targeted advertising.

10. One of these data brokers is Emetriq GmbH ('Emetriq'). A contractual relationship between Xandr and Emetriq is evident from the documents disclosed by Xandr itself, where Emetriq is classified as both 'data provider's partner' and 'ad server partner'.[4] Emetriq also confirms to partner with Xandr since 2021.[5]

2.2   Complainant's access and erasure requests

11. On 19.02.2024, the data subject made an access request with Emetriq, specifically asking for segments created about him and the recipients his data was shared with. The data subject attached the value of some cookies set by Emetriq on his device while visiting the website www.paradisi.de. The visit occurred on the same day of the access request (**Attachment 3**).

12. On 27.02.2024, the data subject also made access and erasure requests with Xandr (**Attachment 4** and **4-bis**, concerning access and erasure requests respectively). The data subject attached the value of a cookie that was set by Xandr on his device when the user visited a website embedding Xandr's tracking technology, the name of the website and the date of the visit. The visit occurred on the same day of the access request. This aimed at enabling Xandr to authenticate the data subject and address his access and erasure requests.

13. From a technical perspective, 'uui2' is a tracking cookie that uniquely identifies a user for the purpose of targeted advertising, as declared by Xandr itself: "*This cookie contains a unique randomly-generated value that enables the Platform to distinguish browsers and devices. It is*

---

[3] After the media reports, Xandr removed this list from its website. However, the database can still be consulted on The Markup's website: https://themarkup.org/privacy/2023/06/08/from-heavy-purchasers-of-pregnancy-tests-to-the-depression-prone-we-found-650000-ways-advertisers-label-you.

[4] See Xandr's 'Policy and Regulations' section and specifically the 'Third Party Providers' page: https://learn.microsoft.com/en-us/xandr/policies-regulations/third-party-providers.

[5] https://www.emetriq.com/wp-content/uploads/2021/09/2021_09_07_Xandr_emtriq_PM.pdf

matched against information – such as advertising interest segments and histories of ads shown in the browser or device – provided by clients or other third parties and stored on the Platform."[6] This cookie is set by the domain .adnxs.com, which belongs to Xandr.

14. On 11.03.2024, Xandr replied that they were not able to identify the data subject and therefore could not provide access, nor erase data related to him: "*Please note that our advertising platform only contains consumers' pseudonymous personal data and not personally identifiable information (such as name or plain text email address). Therefore, we could not match your identifying information to any consumer personal data in our possession, nor could we locate any personal data associated with you in our other records*". (**Attachment 4**)

15. On 18.03.2024, Xandr provided an additional, partially conflicting reply, in the form of a single sentence email: "*We have re-evaluated your submission. Although we remain unable to confirm whether we maintain any personal data relating to you, if the identifier you provided exists in our database, we will delete it.*" (**Attachment 4**)

16. Meanwhile, on 28.03.2024, the data subject got a reply to his access request with Emetriq (**Attachment 5**). The data broker provided a copy of over 200 market segments linked to the data subject ('*usersegmentnames*' or 'List 1' - **Attachment 6**) and a list of about 70 'profiling events' on the basis of which the segments were created ('*userevents*' or 'List 2' - **Attachment 6**).

17. According to the information provided by Emetriq in List 2, the websites where tracking occurred are: www.imodium.at, www.paradisi.de, www.9monate.de, www.leben-und-erziehen.de, www.babelli.de, www.donaukurier.de, www.bgland24.de, www.baby-vornamen.de. It is also clear from the same document that the entire browsing activity took place in just one day (19.02.2024) – and more specifically, for less than two hours.

18. Of the 8 websites, 7 embed Xandr cookies, as clearly stated in the second or third layer of the cookie banners. Only www.imodium.at has recently changed its cookie policy and no longer implements cookies by Emetriq or Xandr – although it is manifest from List 2 that at least Emetriq's cookies were present on the website at the time of the events.

19. Concerning the recipients of this data, Emetriq declares that the segments (and their link with a given cookie ID) are shared with DSPs on the basis of the user's consent. This consent is said to be collected when the user visits websites that rely on DSPs to show ads (**Attachment 5**).

20. With two subsequent communications on 02.04 and 23.04.2024, the data subject asked Emetriq to disclose the identity of specific recipients, with regard in particular to the single DSPs, including Xandr's (**Attachment 7**). With these messages the data subject was seeking formal confirmation of a fact that seemed manifest. On its website, Emetriq explicitly declares that its segments can be found on several DSPs, including Xandr's.[7]

---

[6] This description was available on Xandr's 'Digital Platform Cookie Policy', now removed by the Defendant: https://about.ads.microsoft.com/en-us/solutions/xandr/digital-platform-cookie-policy. This choice is puzzling to say the least, as Xandr still makes use of this cookie for the same purposes.

[7] It is sufficient to visit the 'Segmentfinder' page and click on any of the segments to see Xandr's logo under the sentence "*Available on these DSPs*" (in German: "*Verfügbar auf diesen DSPs*"): https://www.emetriq.com/segmentfinder/
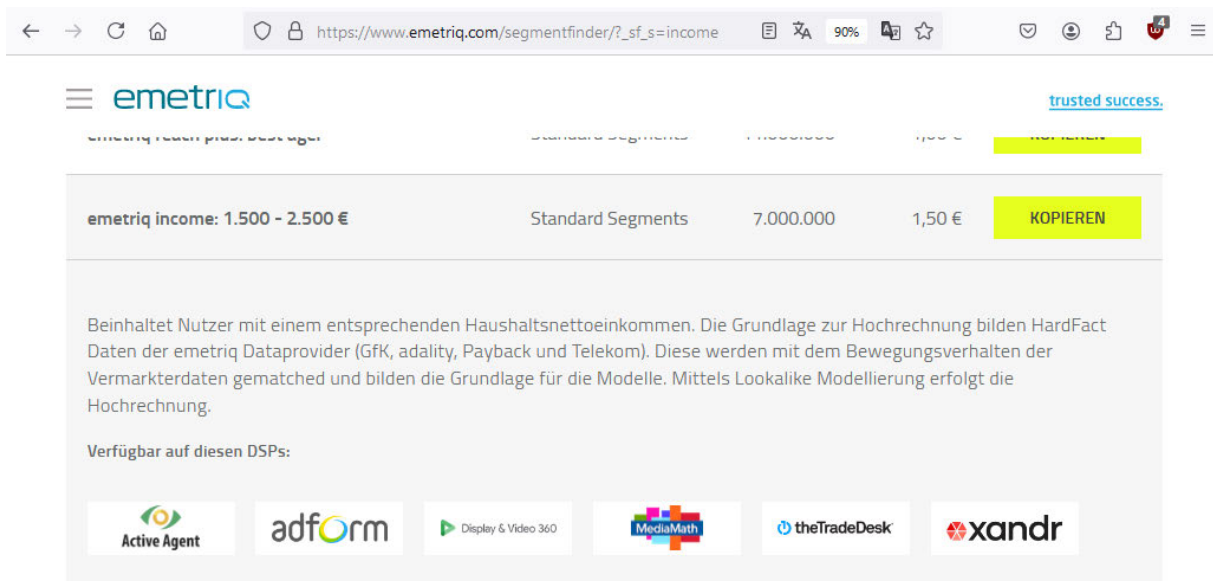
From the Emetriq website, where the data broker states that its segments are available on various DSPs (in German: *'Verfügbar auf diesen DSPs'*), including Xandr's (bottom right). Note incidentally how the segment in question 'emetriq income: €1,500 - €2,500' is one of those also referred to the complainant.

21. On 24.04.2024, Emetriq confirmed that Xandr, alongside with other 6 DSPs, is among the recipients of the data subject's segments, *provided that the data subject consented to the processing on the visited websites* (**Attachment 7**). The data subject, when visiting the said websites, accepted all cookies and trackers, including Xandr's. Therefore, it is clear that Emetriq shared the segments with Xandr.

3. COMPETENT AUTHORITY

22. According to the Defendant's privacy policy, "*Xandr is a global company headquartered in the United States with data centers located in the United States, Europe and Asia*".[8] In particular, decisions relating to purposes and means of the processing are undoubtedly taken in the US.

23. This was confirmed by the Defendant's privacy policy, which uniquely mentions Xandr's New York office. However, Xandr admits to process data of data subjects in the EEA and that the GDPR is applicable to them. In the sub-section 'Questions or complaints', section 'Information for residents of European countries', Xandr states that "*you have the right to lodge a complaint with the data privacy authority where you reside.*"[9]

24. The Complainant is Italian and resides and works in Italy. Therefore, the Garante is the competent authority pursuant to Article 55(1) GDPR and Recital 122 Sentence 2 GDPR.

---

[8] See Xandr's privacy policy, section 'Where do we operate': https://about.ads.microsoft.com/en-us/solutions/xandr/platform-privacy-policy

[9]See Xandr's privacy policy, section 'Information for residents of European countries': https://about.ads.microsoft.com/en-us/solutions/xandr/platform-privacy-policy

25. The fact that Xandr is part of the Microsoft Advertising group does not play a role in determining the competence of the Garante to deal with this complaint.

26. As a matter of fact, Xandr was bought by Microsoft in 2021 but retained its structural autonomy. Xandr has its own 'Platform privacy policy' (**Attachment 8**).[10] Xandr has also specific webpages dedicated to the exercise of data subject rights[11] (that the Complainant used) and to the technical documentation for developers.[12]

27. Xandr is also mentioned as a separate entity at least twice in Microsoft general Privacy Policy, and more specifically in the 'Advertising' section. Microsoft also explains that Xandr is involved in its targeted advertising activities:[13]

    • "*We may share data we collect with internal and external partners, such as Xandr, Yahoo, or Facebook (see below), so that the ads you see in our products and their products are more relevant and valuable to you.*"
    • "*Additionally, Microsoft partners with [Xandr](), a Microsoft company, and third-party ad companies to help provide some of our advertising services* [...]"

28. Microsoft advertising and Xandr Inc. are therefore at most joint controllers. Article 26(3) GDPR allows data subject to file a complaint against both joint controllers, regardless of their internal agreements.

4. GROUNDS FOR THE COMPLAINT

4.1. Violations

29. The Defendant violated the following provisions of the GDPR:

    (a) the principles of **data minimisation** and **accuracy** (Article 5(1)(c) and (d) GDPR). The large amount of conflicting information processed by Xandr is not only unnecessary to achieve a targeted form of advertising, but even defeats the purpose of genuine ad personalisation;

    (b) the complainant's **rights to access** (Article 15(1) and (3) GDPR) and **erasure** (Article 17 GDPR) and the **duty to facilitate** the exercise of such rights (Article 12(2) GDPR). Xandr has a global response rate to access and erasure requests of 0% and actively hinders the exercise of data protection rights.

---

[10] https://about.ads.microsoft.com/en-us/solutions/xandr/platform-privacy-policy

[11] https://monetize.xandr.com/privacy-center/

[12] https://learn.microsoft.com/en-us/xandr/

[13] https://privacy.microsoft.com/en-gb/privacystatement

4.2. Violation of the general principles of accuracy and data minimisation

4.2.1. Accuracy

30. Article 5(1)(d) GDPR states that data shall be accurate with regard to the purpose for which it is processed.

Profile data is intrinsically contradictory and defeats the purpose of personalised advertising

31. A quick look at List 1 ('*usersegmentnames*' in **Attachment 6**) shows that the segments concerning the complainant are nothing else than inferences on users' interests and habits, to be used for ad targeting. This is ultimately the core of Xandr's business model. Therefore, in the case at hand, the purpose of the processing is advertising, to be achieved by means of behavioural targeted advertising.

32. When the purpose of the processing is to target users with personalised ads, sharing a huge amount of conflicting information violates the principle of accuracy, as users that consented to profiling will not receive 'personalised' content. It can be assumed that a user who *genuinely* consents to such an intrusive form of tracking and profiling is motivated by the desire to get tailored ads. Unfortunately, List 1 shows a different reality. The segments broadcast by the Defendant do not enable advertisers to bid on ad slots in an accurate way. In other words, there is extensive processing but no benefit for the user.

33. More in details, tens of segments are in manifest contradiction with each other and, far from facilitating personalisation, they only create confusion on the Complainant's interests and features. We reproduce here some examples but we strongly invite the competent authority to directly examine List 1 to appreciate of how chaotic and contradictory information is.

- The Complainant's gender is considered to be both woman *and* man (while the Complainant is in fact a ▮▮▮▮

```
11987 : emq gender: Frau HR @AdA
11988 : emq gender: Mann HR @AdA
```

- His estimated age spans between 16 and 60+ ▮▮▮▮▮▮▮▮▮▮▮▮

```
13187 : age_16-19_ida2_high_reach_one_classifier_intersection @classifier
13188 : age_20-29_ida2_high_reach_one_classifier_intersection @classifier
13189 : age_30-39_ida2_high_reach_one_classifier_intersection @classifier
13190 : age_40-49_ida2_high_reach_one_classifier_intersection @classifier
13191 : age_50-59_ida2_high_reach_one_classifier_intersection @classifier
13192 : age_60plus_ida2_high_reach_one_classifier_intersection @classifier
```

- His estimated income spans between 500 and 4000 €/month (at the time of the events the Complainant had ▮▮▮▮▮▮▮▮▮▮

```
21779 : emetriq income: 500 - 1.500 €_ctv
21776 : emetriq income: 1.500 - 2.500 €_ctv
21777 : emetriq income: 2.500 - 4.000 €_ctv
```

- His employment status covers almost any possible option (the Complainant is ▮▮▮▮ ▮▮▮▮

```
11838 : emetriq status: pupil
11836 : emetriq status: student
```

```
11847 : emetriq job: job seeker
11850 : emetriq job: employed
11851 : emetriq job: self-employed
```

- His estimated company size spans between 1 and 5,000 people (the Complainant's employe ███████████████████████████████████

```
12191 : emq empl: 1-10 @iqd
12195 : emq empl: 1000+ @iqd
23209 : emetriq job: company size: 1001-5000 @XING
```

- His estimated consumption of TV varies greatly, he is categorized as a "lightviewer [light viewer]", "mediumuser [medium user]" and a "heavy tv watcher" at the same time:

```
17210 : emetriq custom: tv lightviewer <90 min. 50 mio. @GfK extended
17212 : emetriq custom: tv lightviewer <42 min. 30 mio. @GfK extended
22817 : emetriq custom: CCS2022_TV-MEDIUMUSER_E1869
22465 : emetriq entertainment: heavy tv watcher @magentatv extended_ctv
```

34. It is hard to see how an accurate targeting could take place on the basis of these categories. As a matter of fact, the Complainant may be a man or a woman, anything in between a teenager and a retired person, an individual below the poverty threshold or a very affluent one, a (school or university) student, a job seeker or a worker (both employed or self-employed). Xandr seems to have no clear idea about the Complainant's company's size or about his TV consumption. Nevertheless, this data is sold to advertisers, so that they can bid on it to "tailor" their products.
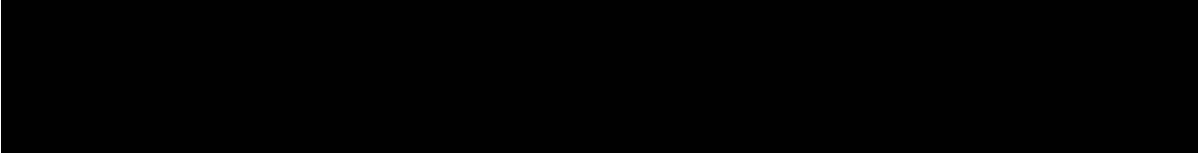
35. The fact that the Defendant did not directly create these segments is not a justification, as Xandr still processes the profiles and broadcasts them to hundreds of companies without any check on their accuracy. Personal data is simply disseminated in the digital ads ecosystem. In any case, in light of the principle of accountability (Article 5(2) GDPR), it is up to the Defendant to prove otherwise.

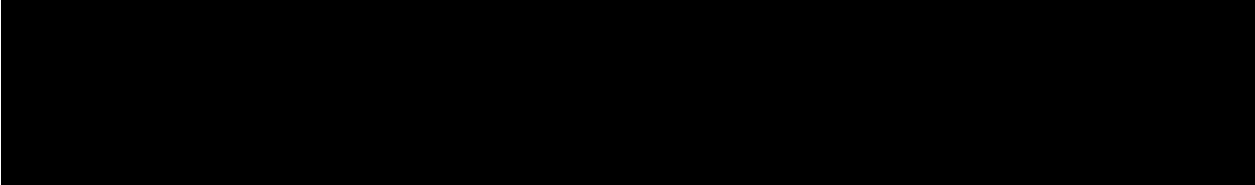Xandr's profit from grossly inaccurate information and "business to business" unfairness

36. Obviously Xands profits from pretending to have information about users that are in fact not accurate.

37. Normally, advertisers bidding through DSPs like Xandr's set certain criteria to target potential audiences. For example, they can decide that they want to bid only on users whose income is "above X/month". If a user is marked as "above X" and "below X" at the same time, Xandr can thereby offer a larger inventory and it will have more chances to find advertisers willing to bid (and pay). Unfortunately, this is the opposite of what advertisers would expect, namely that profiles and market segments will help them to take part in the auction with an informational advantage.

███
███
███
███
███
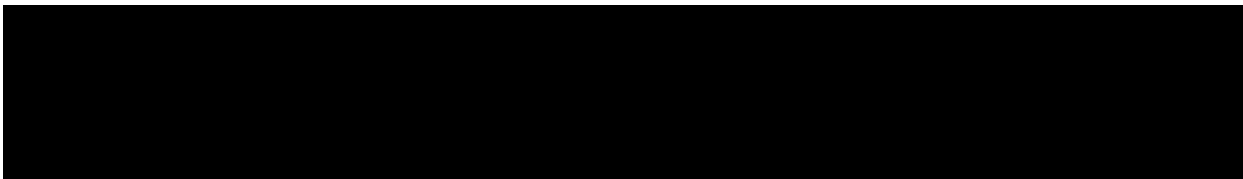
39. Even if Xandr receives the profiles from third parties, it seems unlikely that the Defendant is not aware of this accuracy issue when it further broadcasts them to further entities. As shown by List 1, the scale of the inaccuracy is macroscopic and cannot be easily ignored.

4.2.2.   Data minimisation

41. Article 5(1)(c) GDPR states that data shall be "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*".

Data is not limited to what necessary: the amount of data is massive and disproportionate

42. Data processed by Xandr is not "*limited to what is necessary*". After less than two hours of browsing activities on just 7 or 8 websites, the Defendant received around 200 profiles from Emetriq alone, which is only one of Xandr's many 'data providers'.

43. As a matter of fact, the use of segments by Xandr is likely much broader. Xandr itself provides a list of 50 official 'data providers' (**Attachment 9**).[14] Many of these entities are active on a website at the same time to profile the user. On each of the 7 websites embedding the Defendant's technology, for example, 7 to 11 of these 'data providers' are listed in the cookie banners.[15] Assuming a processing comparable in scale with Emetriq's, a very conservative calculation suggests that the number of segments received by Xandr easily goes beyond 1,400. This – it should be stressed once more – in the course of one day.

44. Admittedly, this is only a rough estimate. However, it was not possible for the Complainant to get precise data due to Xandr's refusal to comply with the access request, as further discussed in this complaint.

45. These numbers, already impressive, shall be considered then in the context of the RTB system managed by Xandr. Xandr's DSP shares the segments (and many other personal data) with countless entities in order to enable advertisers to bid. On its website, Xandr discloses the

---

[14] Pdf downloaded from https://learn.microsoft.com/en-us/xandr/policies-regulations/third-party-providers. According to data obtained directly from Xandr (and now only available on a journalistic database: see Note 3), this list is not even exhaustive, as other data brokers would also provide segments for the purpose of targeted advertising.

[15] Adsquare GmbH, Amnet GmbH, DoubleVerify Inc.; Emetriq GmbH; GumGum Inc; Integral Ad Science, Meetrics GmbH; Nano Interactive Group Ltd.; Playground xyz Emea LTD; Seedtag Advertising S.L.; Semasio GmbH.

names of hundreds of 'Ad-server partners' "*which may receive Platform Data and other Information* [...] *as a result of their partnership with Xandr or due to their partnership with Xandr customers using Xandr's technology*" (**Attachment 9**).[16]

46. This merely quantitative element should finally be evaluated in light of the type of data actually processed. In his Opinion in the CJEU case C-446/21, Advocate General Rantos found that 'necessity' for the purpose of targeted advertising, to fulfil the principle of data minimisation, shall be assessed distinguishing between 'static' and 'behavioural' data. In particular, the processing of behavioural data - *such as the monitoring of users' browsing habits* – shall be regarded as more intrusive. The Advocate General goes further and even argues that, within the category of 'behavioural data', the collection of data relating to 'passive' behaviour – *such as simply visiting a website* – is the most intrusive form of processing.[17]

47. Xandr therefore carries out highly intrusive processing with an enormous amount of data. The data processing does not seem in any way limited – also not in relation to the purpose. It is thus incontestable that the data processing is not 'necessary'.

<u>Data is not adequate nor relevant for the purpose of targeted advertising, but rather defeats it.</u>

48. Even though the significant amount of behavioural data was considered 'necessary' in light of the principle of data minimisation, the analysis of the segments linked to the Complainant shows that data is by no means 'adequate' nor 'relevant' to the purpose of targeted advertising.

49. As a matter of fact, if the function of targeted advertising is to personalise the 'ad experience' of the user and enable advertisers to buy ad inventory that better fits their campaigns, the processing at issue seems to defeat the purpose. As already discussed, tens of segments are in manifest contradiction with each other and, far from facilitating personalisation, they only create confusion on the Complainant's interests and features.

50. Too many conflicting pieces of information are *by definition* not relevant and inadequate to achieve the purpose of personalising ads. It does not appear realistic that the Defendant, after receiving the profiles from its data providers, operates some kind of filtering or monitoring of necessity, adequacy and relevance. This is because the auction occurs in real time and in the fraction of a second data is broadcasted to Xandr's partners. In any case, it is up to the controller to prove otherwise pursuant to Article 5(2) GDPR.

## 4.3. Violation of the Complainant's rights to access and erasure

4.3.1. Systemic nature of the violations

51. Preliminary, it is important to notice that the violations discussed in this section are particularly concerning as they do not exclusively affect the Complainant. Xandr processes data of millions of users in Europe, including detailed profiles that enable to draw precise inferences

---

[16] Pdf downloaded from https://learn.microsoft.com/en-us/xandr/policies-regulations/third-party-providers.

[17] AG Opinion, case C-446/21 of 25 April 2024, *Schrems v Meta Platforms Ireland Limited*, par. 25.

on citizens' life habits and interests. Nevertheless, astonishingly, data published by the De-
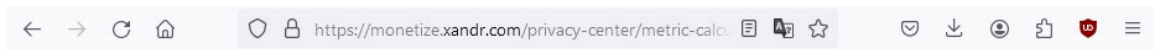
Consumer Request Metrics

The following metrics calculate the number of consumer data requests received from consumers, globally the past calendar year, via our Privacy Center. This information will be updated on an annual basis. The metrics below are for January 1, 2022 - December 31, 2022:

*Access and deletion requests are denied when we are unable to verify the identity and jurisdiction of the requestor. Due to the pseudonymous nature of the data Xandr collects on its Platform, we are unable to verify the identity of the consumers who made access and deletion requests when such requests are not tied to any other identifiers, and therefore we denied such requests. Xandr recognizes the opt-out requests from its clients on our platform when a client forwards a consumer opt-out request to Xandr.

	Number Received	Number Complied with, in whole or in part	Number Denied	Average Average number of days to respond
Access Requests*	1294	0	1294	2 Bus. Days
Deletion Requests*	660	0	660	2 Bus. Days
Opt-out of Sale Requests	Do not sell requests are recognized from Xandr's clients and calculated by the client. California consumers interacting directly with Xandr's website can also opt-out of sale or sharing their personal data			

fendant on their website shows that in 2022 the <u>response rate to access and erasure requests worldwide was 0%</u>.[18] Several other data subjects supported by *noyb* unsuccessfully tried to exercise their rights under Articles 15 and 17 in 2023 and 2024, too. There is no element suggesting that the Defendant is now following a different approach.

52. It is thus manifest that the Defendant, despite processing a massive amount of granular data, does not do enough to facilitate the exercise of data subject rights but rather seems to actively hinder such exercise.

4.3.2. Right to access and duty to facilitate the exercise of data subjects' rights

53. According to Article 12(2) GDPR, the controller shall facilitate the exercise of data subject rights under Articles 15 to 22 GDPR.

54. The Complainant tried to exercise his right to access under Article 15(1) and (3) GDPR. So far, the Defendant has not replied to the Complainant's access request.

55. In refusing to act on the Complainant's access request pursuant to Article 15 GDPR, the Xandr claims not to be in the position to identify the data subject, implicitly invoking the second sentence of Article 12(2) GDPR.

56. However, this is simply not true. The Complainant provided the Defendant with the value of a Xandr cookie ('uuid2') that uniquely identifies him, the URL of the website where this cookie was set and the date of the visit. These pieces of information enable Xandr to single out a specific user and to ascertain that the latter is not pretending to be someone else. As a matter of fact, a data subject could not match these three highly specific pieces of information if they were not the person to which the data belongs.

---

[18] See Xandr's website, section 'Consumer Request Metrics', consulted on 03.05.2024: https://monetize.xandr.com/privacy-center/metric-calculations

57. Even if the data provided by the Complainant was not sufficient for authentication purposes, the combination of Article 12(6) GDPR and the duty to facilitate would impose on Xandr an obligation to communicate to the data subject what additional information the controller needs.

58. The violation is particularly serious as List 1 disclosed by Emetriq shows how information collected about the Complainant is extensive and very specific. It shall be stressed again that Emetriq is just one of several data brokers partnering with Xandr. Most likely, the 200 profiles attached to this complaint are just a fraction of the Complainant's data processed by the Defendant. The Complainant has a right to have this information disclosed, including its sources and recipients.

4.3.3.   Erasure

59. The Complainant's erasure request has not been answered or fulfilled, either. Xandr simply states, with regard to the cookie provided: "*if your identifier is present in our database, we will erase it.*" This statement seems to contradict the previous claim that the Defendant is not in the position to authenticate the Complainant. If that was true (and it is not), Xandr should *not* erase this data, as it could not confirm that the erasure request actually came from the person to whom the identifier refers to.

60. Moreover, the statement, formulated as a mere possibility in the future - by an entity that at the same time declares "*we remain unable to confirm whether we maintain any personal data relating to you*" - cannot be considered confirmation that the erasure took place pursuant to Article 12(3) GDPR.

61. Most importantly, the erasure request did not (only) concern the identifier – which was provide only for authentication purposes – but *any* data, including segments or profiles.

4.3.4.   Data is not pseudonymous and the GDPR fully applies

62. The argument that Xandr cannot identify the Complainant as they only process pseudonymous data is not correct, either. Article 4(5) GDPR states that is pseudonymous when data "*can no longer be attributed to a specific data subject without the use of additional information, <u>provided that such additional information is kept separately</u>*".

63. It should be recalled here what Xandr declares in its privacy policy about the uuid2 cookie: "*This cookie contains a unique randomly-generated value that enables the Platform to distinguish browsers and devices. It is matched against information – such as advertising interest segments and histories of ads shown in the browser or device – provided by clients or other third parties and stored on the Platform*". The fact that profiles and segments processed by Xandr are linked to a "randomly-generated" value only means that such a value is a string of numbers and letters, instead of a name or email address. However, importantly, such a code is <u>unique</u> – namely it singles out only one data subject and their browser – and it is "matched against" segments <u>stored within the same database</u> (or at most in a strictly linked database).

64. For sure, Xandr does not have "*measures to ensure that the personal data are not attributed to an identified or identifiable natural person*" (Article 4(5) GDPR): to the contrary, the attribution of profiles and other information to a single user through their uuid2 is at the very core of

Xandr's business model. It is therefore ludicrous that the Defendant claims to process pseudonymous data. This statement probably just means that Xandr does not use names and surnames to target users. However, Xandr singles out users on a regular basis for its targeting purposes and this is incompatible with the definition of pseudonymous data under the GDPR.

65. In addition, even if data was genuinely pseudonymous (and this would lead to the question how Xandr can actually operate its business), the GDPR, including the rights to access and erasure, would still apply. Notably, the Defendant does not even try to argue that data processed by them is anonymous, which Recital 26 GDPR considers to be the only case where the Regulation does not apply.

66. In light of the above, the Defendant does not have any valid reason to refuse the Complainant access and erasure of their personal data.

5. REQUESTS AND SUGGESTIONS

5.1. Request to investigate

67. It must be stressed that, given the limited transparency and cooperation on the Defendan's side, the use of investigative powers by the authority is the only feasible path for the Complainant to understand the processing and exercise his data protection rights.

68. The Complainant requests the supervisory authority to use its powers under Article 58(1) GDPR to investigate the matter, in particular but not limited to:

   a) the type, amount, sources, recipients and retention period of personal data of the Complainant processed by the Defendant;
   b) the legal basis of the data processing carried out by the Defendant;
   c) if the Defendant is a joint controller together with others and in this case if the requirement of Article 26(1) GDPR are complied with;
   d) the authentication procedure deployed by the Defendant when addressing data subjects' rights requests.

5.2. Request to adopt corrective measures

69. The complainant requests that the competent supervisory authority orders the Defendant **to comply with the Complainant's access and erasure requests** (Article 58(2)(c) and (g) GDPR), with regard to *all* profiles and segments processed by Xandr, their sources and recipients.

70. The complainant suggests that the competent supervisory authority orders the Defendant, in relation to all data subjects, to bring processing operations in compliance with the principles of data minimisation and accuracy, and with the duty to facilitate the exercise of data subjects' rights (Article 58(2)(d) GDPR). In particular, Xandr should be ordered:

   (a) **to limit the processing of personal data to what is 'adequate', 'relevant' and 'necessary'** to personalised advertising. This can be achieved for example by collecting less data

from 'data providers' (or from less 'data providers'), by filtering data at the moment of the collection before broadcasting them to advertisers, or a mix of both. <u>When it is not possible to choose between multiple logically incompatible segments</u> (e.g. "pupil", "job seeker", "employed") <u>the Defendant should abstain from using that category</u> (e.g. "employment status") for the bidding, instead of profiting from the confusion;

(b) **to erase or rectify all the inaccurate 'profiles' or 'market segments'** used for targeted advertising. Even though Xandr's inferences concerning users probably rely on statistical methods, the Defendant is not exempted from compliance with the accuracy principle. Statistical models can also be good or bad. The fact that Xandr may not be in the position to offer accurate inferences, far from limiting its responsibility under the GDPR, only shows the questionable quality of Xandr's products. <u>As long as data *cannot* be accurate, it shall be erased;</u>

(c) **to provide an effective tool to users to exercise their rights to access and erasure,** <u>clarifying which piece(s) of information are required for the authentication</u> (e.g. the uuid2 cookie, whose value can be easily found by any user inspecting their browser while on a website that embeds Xandr's technology).

5.3. Suggestion to impose a fine

71. The Complainant also recommends the imposition of an effective, proportionate and dissuasive administrative fine pursuant to Articles 58(2)(i) and 83 GDPR. In the Complainant's view, the necessity to impose a fine is shown by:

a) the general and continuous nature of the violations, as well as the amount of data subjects involved and the scale of the processing, which ultimately constitutes the entire business model of the Defendant (Article 83(2)(a) GDPR);

b) the intentional character of the infringements, as shown by the 0% compliance rate to access and erasure requests (Article 83(2)(b) GDPR);

c) the total lack of technical and organisational measures, at least with regard to the duty to facilitate data subjects, and probably also concerning compliance with the basic principles of the GDPR (Article 83(2)(d) GDPR);

d) the sensitive nature of the behavioural data processed (Article 83(2)(g) GDPR);

e) the relevant financial benefits deriving from the processing, potentially gained in a fraudulent way at the detriment of the Defendant's business clients (Article 83(2)(k) GDPR).

6. CONTACT

72. Communications between *noyb* and the Authority in the course of this procedure can be done by email at [redacted] with reference to the **Case-No C084** or by phone at [redacted]