



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

Datenschutzbehörde
Barichgasse 40-42, 1030
Wien, Austria

Per E-Mail: dsb@dsb.gv.at

Vienna, 13.06.2024

noyb Case-No: C-083

Complainant:



represented under
Article 80(1) DSGVO by:

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

Respondent:

Google LLC
1600 Amphitheatre Parkway
Mountain View, California 94043, USA

Regarding:

Article 5(1)(a) GDPR
Article 6(1)(a) 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 172/4/2, 1140 Vienna, Austria, registry number ZVR: 1354838270 (hereinafter: "*noyb*") (**Annex 1**).
2. *noyb* is representing the complainant under Article 80(1) GDPR (**Annex 2**).

2. FACTS PERTAINING TO THE CASE

3. On 07.09.2023, Google (hereinafter: the respondent) released its "Privacy Sandbox" API (hereinafter: the Sandbox API).
4. Prior to this date, Google allowed third-party cookies to track users' search histories on Chrome, acquire personal data, and provide targeted advertisements. Third party cookies were already largely blocked in other browsers such as Apple's Safari and Mozilla's Firefox, but were not in Google's Chrome.¹
5. The Sandbox API aims to replace third-party cookies — the most common form of tracking technology — for what Google calls "topics."²
6. Far from any "privacy" tool, the system behind the Sandbox API still tracks a user's web browsing history. The difference is that now the Chrome browser itself tracks user behaviour and generates a list of advertising "topics" based on the websites users visit. At launch there were almost 500 advertising categories like "*Student Loans & College Financing*," "*Undergarments*" or "*Parenting*" that users were associated with based on their online activity.³ An advertiser that has a presence on a website enabling the Sandbox API will ask the Chrome browser what topics a user belongs to, and then potentially display an advertisement accordingly.
7. The Chrome browser, therefore, still track users for Google's behavioural advertising. The main change is that it is just done by the browser of one company (Google) instead of countless servers-side third-party tracking system. The Chrome browser now "*only blocks some third-party cookies (which other browsers already do by default) and repackages the data for targeted advertisement.*"⁴ Therefore, Google referring to this system as a "privacy" tool is deceiving.⁵

¹ Thorin Klosowski, *How to turn off google's privacy sandbox ad tracking – and why you should*, <<https://www.eff.org/deeplinks/2023/09/how-turn-googles-privacy-sandbox-ad-tracking-and-why-you-should>> accessed 01.01.24

² Thorin Klosowski, *How to turn off google's privacy sandbox ad tracking – and why you should*, <<https://www.eff.org/deeplinks/2023/09/how-turn-googles-privacy-sandbox-ad-tracking-and-why-you-should>> accessed 01.01.24

³ These topics can be found here https://github.com/patcg-individual-drafts/topics/blob/main/taxonomy_v2.md, accessed 01.01.24

⁴ Ben Wolford, *Google's Privacy Sandbox is privacy quicksand*, <<https://proton.me/blog/google-privacy-sandbox>> accessed 11.12.2023

⁵ Thorin Klosowski, *How to turn off google's privacy sandbox ad tracking – and why you should*, <<https://www.eff.org/deeplinks/2023/09/how-turn-googles-privacy-sandbox-ad-tracking-and-why-you-should>> accessed 01.01.24

8. Google conducted A/B testing⁶ when implementing the Sandbox API to ensure a high consent rate from users, which is an industry standard for any UI/UX change. In fact, the roll-out of the Sandbox API was even halted for 3% of Chrome users to “allow [Google] to run A/B tests.”⁷ Usually A/B testing is used to identify which versions of a text or interface design is yielding the best results from a company perspective. When it comes to consent boxes for advertisement, companies usually manipulate the interface (“dark patterns”) to gain extreme consent rates like 90% or more⁸ when we know that only about 3% of users actually want to be tracked.⁹ It can therefore be assumed that the interface of the prompt was “optimized” to get a high consent rate.
9. Rather than making it clear that they were asking for consent to have their browser track users, Google sold the Sandbox API as a “privacy feature” to users. It is understood that this was a conscious choice to manipulate user understanding and ensuring a high consent rate, as users thought that their browser is now protecting them against tracking for advertisement.
10. It should be stressed that so far Google has not phased out third party cookies for most of its users, as both the UK market authority and the UK data protection authority are investigating this shift in Google's business model as a potential infringement of data protection and competition law provisions.¹⁰ If the Sandbox API was designed to counter-balance the elimination of third party tracking for Chrome users, it seems that Google was faster in implementing its own tracking tool than in actually removing existing threats to users' privacy.
11. On the 18.10.23 the data subject (hereinafter: the complainant) received a pop-up box called “turn on an ad privacy feature” when opening google chrome:

⁶ A/B testing is a method of testing two variants of the same web page or cookie banner to website visitors in order to compare which variation drives the highest number of opt-ins.

⁷ <https://www.theverge.com/2023/9/7/23862743/google-chrome-privacy-sandbox-milestone-availability>, accessed 01.01.24.

⁸ According to Quantcast's own analysis, more than 10,000 domains worldwide have deployed Quantcast Choice, generating an average consent rate among consumers of more than 90 percent, see: <https://www.quantcast.com/press-release/quantcast-choice-powers-one-billion-consumer-consent-choices/>

⁹ See Usercentrics Webinar at about 30:00 (<https://youtu.be/oux9uBUtscE?t=1800>) and Utz et al., (Un)informed Consent, in *arxiv* (Cornell University), Table 2, Page 10: <https://arxiv.org/abs/1909.02638>.

¹⁰ <https://www.wsj.com/tech/google-cookies-replacement-not-enough-to-protect-uk-consumer-privacy-580d1b16>



Turn on an ad privacy feature

We're launching new privacy features that give you more choice over the ads you see.

Ad topics help sites show you relevant ads while protecting your browsing history and identity. Chrome can note topics of interest based on your recent browsing history. Later, a site you visit can ask Chrome for relevant topics to personalize the ads you see.



You can see ad topics in settings and block the ones you don't want shared with sites. Chrome also auto-deletes ad topics that are older than 4 weeks.

More about ad topics



You can change your mind any time in Chrome settings


Turn it on

No thanks

12. The box gave the complainant the option to “Turn on” the feature or “No Thanks.”


13. The wording that “Chrome can note topics of interest based on your recent browsing history” is presented as a fact of what Chrome is able to do, rather than a choice to the user over whether Chrome should track their browsing history in the first place. It is a factual claim which provides mere information rather than posing a question to the complainant.

14. The complainant clicked *“Turn it on”*. Subsequently, another page appeared which could only be dismissed by clicking *“Got it”*.




Other ad privacy features now available

We're launching new ways to limit what sites can learn about you when they show you personalized ads, for example:



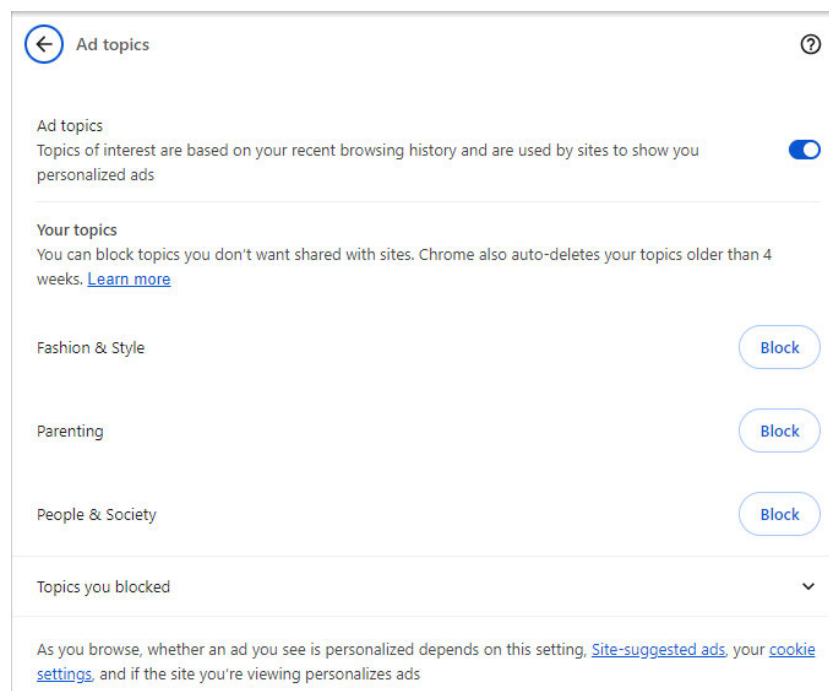
- Site-suggested ads help protect your browsing history and identity while enabling sites to show you relevant ads. Based on your activity, a site you visited can suggest related ads as you continue browsing. You can see a list of these sites and block the ones you don't want in settings.
- With ad measurement, limited types of data are shared between sites to measure the performance of their ads, such as the time of day an ad was shown to you.

More about site-suggested ads and ad measurement 

You can make changes in Chrome settings

[Got it](#) [Settings](#)

15. As a consequence of the interaction with these pop-ups, the complainant's browser started to track him. For example, on 29.05.2024, the complainant checked in his browser settings and found out that the Topics *“Fashion & Style”*, *“Parenting”* and *“People & Society”* have been linked to him.



← Ad topics ⓘ

Ad topics
Topics of interest are based on your recent browsing history and are used by sites to show you personalized ads

Your topics
You can block topics you don't want shared with sites. Chrome also auto-deletes your topics older than 4 weeks. [Learn more](#)

Fashion & Style	Block
Parenting	Block
People & Society	Block

Topics you blocked ▾

As you browse, whether an ad you see is personalized depends on this setting, [Site-suggested ads](#), your [cookie settings](#), and if the site you're viewing personalizes ads

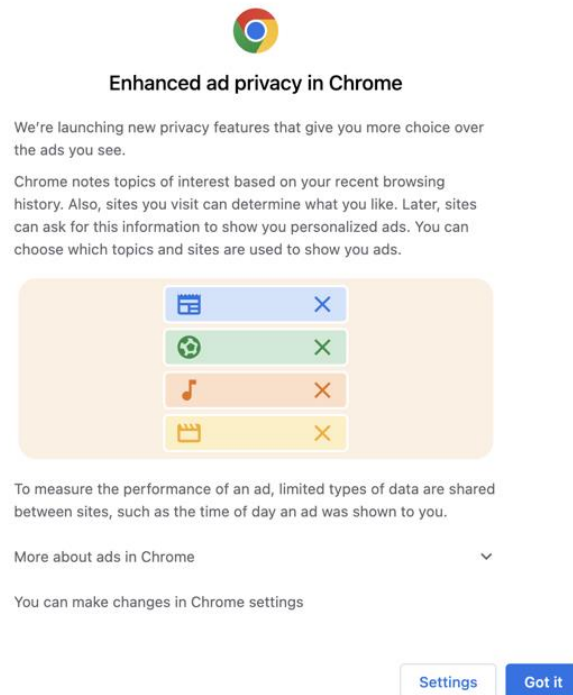
16. The pop-ups marketed themselves as an “*ad privacy feature*” with “*other ad privacy features available.*” The wording marketed the Sandbox API as a privacy feature rather than a consent banner targeted advertising by repeating phrases such as “*protect*”, “*limit*” and “*privacy features*”. This does not reflect what is commonly understood by consumers to be “*Privacy Features*” (such as Cookie or Tracking Blockers) which work to fully shield users rather than track them further through alternative, locally installed means, and share data with advertisers.
17. The design of the first pop-up showed benign topics related to sports, music and film. These do not reflect the actual topics which are far more sensitive, specific, and include sub-topics. For example, “*/Jobs & Education/Jobs/Job Listings/Government & Public Sector Jobs*” and “*/Finance/Credit & Lending/Credit Reporting & Monitoring*”.¹¹ Equally, the second pop-up displayed a “privacy shield” as the central image, again communicating that the main purpose of the Sandbox API is to shield from processed and privacy rather than targeted advertisements in a different form. An adequate icon would have been a camera spying on the browser content or alike.
18. Despite having more context than an average user would typically receive, the intended legal meaning of the pop-up was uncertain to *noyb*’s trained GDPR lawyers when data subjects raised the new pop-up with them. To clarify their understanding, *noyb* had to send a letter to Google to understand if they were seeking consent under Article 6(1)(a) GDPR to process personal data (**Annex 3**).
19. Concerning the first Pop-up window, Google replied stating that:

“Google is seeking consent for the purposes of Article 6(1)(a) GDPR for the generation of ad topics within Chrome. Users can give or refuse consent by clicking “Turn it on” or “No thanks” ... The consent relates to the creation of ad topics within the browser”.
20. Equally, the complainant was unsure as to whether the pop-up was about consent, a change in software settings or a mere information from Google about a feature that did not leave any choice anyway. This was because, as evidenced above, the wording and design of the pop-up failed to make this clear.
21. Upon *noyb* asking about the meaning of the “*Got it*” button on the second Pop-up window, Google stated that:

“The second screen informs users of the new controls within Chrome regarding two other Privacy Sandbox APIs [“App-suggested ads” and “Ad Measurement”], which allow retargeting and ads measurement... The “Got it” button on the second screen simply closes the dialogue box, enabling the user to acknowledge the notice” (**Annex 3**).

¹¹ These topics can be found here https://github.com/patcg-individual-drafts/topics/blob/main/taxonomy_v2.md, accessed 01.01.24

22. This meant that the “Ad topics” API was controlled by the “Turn it on” pop-up and that the “App-suggested ads” and “Ad Measurement” API’s were basically pre-ticked options for data subjects in Europe, for which no consent was asked by Google.¹²
23. As an example to compare, the non-European version of the first pop-up (Enhanced ad privacy in Chrome) which did not give any user choice, activated the Sandbox API after users clicked “got it”.¹³



3. COMPETENT AUTHORITY

24. The complainant has in Austria his habitual residence and place of work and the pop-up appeared when he was using Chrome in Austria. Therefore, the complainant may lodge his complaint with the Austrian supervisory authority under Article 77 GDPR.
25. As the tracking occurs the level of the data subject’s browser, there is no cross-border element that would justify the competence of a Lead Supervisory Authority pursuant to Article 56 GDPR. As Google itself declares: “The Privacy Sandbox APIs require web browsers to take on a new role. Rather than working with limited tools and protections, the APIs allow a user’s browser to act on the user’s behalf—locally, on their device—to protect the user’s identifying information as they navigate the web. This is a shift in direction for browsers.”¹⁴

¹² An example of “App-suggested ads” and “Ad Measurement” being pre-ticked, even with a data subject clicking “No Thanks”, can be seen here: <https://youtu.be/ogXc8Zi7PCA?feature=shared>

¹³ Thorin Klosowski, *How to turn off google’s privacy sandbox ad tracking – and why you should*, <<https://www.eff.org/deeplinks/2023/09/how-turn-googles-privacy-sandbox-ad-tracking-and-why-you-should>> accessed 01.01.24.

¹⁴ <https://developers.google.com/privacy-sandbox/overview>

26. Topics were originally created by Google and are standardized all over the world, the actual processing is performed by the browser itself. Google explains that when the Sandbox APIs are on, Chrome infers Topics from the websites that a user visits while browsing the internet. The browser then stores topics on the user's device. Topics are not directly transferred to Google's or third parties' servers. The disclosure will only take place in case the user subsequently visits websites where advertisers can access the topics.
27. In other words, the sharing of personal data takes place between the user's browser and the server of an advertiser that embedded the Sandbox API.
28. Therefore, the processing does not take place "*in the context of the activities of establishments in more than one Member State*". In the present case, the processing takes place in the context of a browser's activities. In light of Article 4(23)(a) GDPR, the essential condition for a processing to be qualified as "cross-border" is thus not satisfied.
29. The lack of a cross-border element pursuant to Article 4(23)(a) entails that Article 56(1) is also not applicable. The Austrian supervisory authority remains the competent supervisory authority under Article 55 GDPR and the cooperation mechanism envisaged by Article 60 does not apply.
30. Even if the definition of Article 4(23) GDPR would be fulfilled, we want to highlight that Google currently argues that Google LLC in the US and Google Ireland Limited are separate controllers. Google Ireland Limited is - according to Google - controlling all EU Google subsidiaries. Obviously Google Ireland Limited and its subsidiaries cannot be a "main establishment" of another controller and a separate controller at the same time. Given that this complaint is, as of now, only targeting Google LLC as an opponent, we see no basis to apply Article 56(1) GDPR to this complaint.

4. GROUNDS FOR THE COMPLAINT

4.1. Violations

31. The respondent violated the following provisions of the GDPR:
- (a) Violation of Article 5(1)(a) GDPR: Fairness and Transparency
 - (b) Violation of Article 6(1)(a) GDPR: Consent as a Legal Basis

4.2. Violation of Article 5(1)(a) GDPR

32. Article 5(1)(a) GDPR requires that personal data is processed "*lawfully, fairly and in a transparent manner*". Data was processed neither in a fair, nor in a transparent way.
33. Article 12(1) GDPR further specifies the principle and requires that information is provided in a "*concise, transparent, intelligible and easily accessible form, using clear and plain language*".
34. Recital 60 further clarifies that "*the principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes*".

35. This information must be available when the complainant makes the decision and not just hidden in a privacy policy. EDPB Guidelines state that *“when the identity of the controller or the purpose of the processing is not apparent from the first information layer of the layered privacy notice (and are located in further sub-layers), it will be difficult for the data controller to demonstrate that the data subject has given informed consent, unless the data controller can show that the data subject in question accessed that information prior to giving consent.”*¹⁵
36. The first layer in this context was the pop-up described above. The complainant was not informed of the *“purpose of the processing”*, but actually misled by claiming that this is a “privacy” tool - not a tracking tool. While the complainant was allegedly consenting to let Google track his browser, which would still result in a form of targeted advertisement, he was led to believe that this is a privacy feature.
37. As a point of comparison, Brave (another browser akin to Chrome) also describes its *“Brave shields”* as a privacy feature.¹⁶ However, rather than facilitating targeted advertising, the shield blocks online trackers across your browser. Just like with many functions of other browsers or plug-ins, this is what an average user would legitimately expect from a *“privacy”* feature.
38. EU law connects misleading advertising to unfair commercial practices.¹⁷ In the CJEU case C-562/15, deceptive marketing by Carrefour was held to be an act of unfair competition. Recital 42 GDPR also picks up on this link and states that *“a declaration of consent pre-formulated by the controller, should [...] not contain unfair terms”*. In a similar fashion, Google’s pre-formulated consent was misleading and unfair resulting in a breach of Article 5(1)(a) GDPR.
39. In line with Recital 39, the information provided should make it *“transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed”*.
40. The pop-up was not transparent about the fact that Google was asking for consent and using it to track user’s browsing histories and provide versions of this data to third parties. Rather, according to Google, Chrome only *“notes”* topics of interest for the purposes of privacy and works to *“protect your browsing history”*.
41. Article 26(1)(d) Digital Services Act incorporates the transparency requirements of the GDPR and requires providers of very large online platforms (such as Google) to provide recipients of online advertising with meaningful explanations of the underlying logic, including when profiling is used.¹⁸
42. The Sandbox API pop-up did not transparently explain the logic that *“topics”* uses to categorise the complainant, nor the criteria it uses to connect the complainant to advertisers. To the contrary, Google did everything to make the user believe that they now enjoy a new *“privacy”*

¹⁵ https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf at footnote 42.

¹⁶ Brave, *Brave Shields*, <<https://brave.com/shields/>>, accessed 11.12.2023

¹⁷ EU Directives 84/450/EEC (concerning misleading advertising), 93/13/EC (aimed at unfair terms and conditions), 2005/29/EC (aimed at preventing unfair business-to-consumer commercial practices) and 2006/114/EC (governing misleading and comparative advertising).

¹⁸ Recital 68 of the Digital Services Act (DSA).

feature, while - according to Google - they actually agreed to a software tracking every click and move they make online.

43. Google has sold their Sandbox as a better alternative to third-party tracking systems. While this may be true, the Sandbox API nonetheless still works to track users. It is simply in a different form. Tracking invades user's rights and should not be re-framed as "*privacy feature*" when this is clearly not the case.

4.3. Violation of Article 6(1)(a) GDPR

44. With regard to the creation of "Topics" (first pop-up), Google relies on consent as a legal basis for processing under Article 6(1)(a) GDPR **(Annex 3)**.
45. Article 4(11) GDPR states that consent, among others, must be "*specific, informed and unambiguous indication of the data subject's wishes.*"
46. As stated above, the consent could not have been informed given the misleading nature of the pop-up box.
47. The complainant was unaware (until noyb contacted Google) that he was - according to Google - consenting to the processing of his data for targeted advertisement when interacting with the pop-up box.
48. Moreover, the phrase "*turn it on*" is ambiguous and does not resemble the typical consent buttons which follow the wordings of "*agree*", "*consent*" or "*accept*". The CJEU has already ruled on the importance of the text on a button in order to have clear transactions.¹⁹ For example, under Article 8(2) of Directive 2011/83/EU an order button must convey an obligation to pay with the words "*buy now*" or "*order with an obligation to pay.*" Therefore, the phrase "*turn it on*" is insufficient to reflect consent.
49. It follows that the complainants consent could not have been informed nor an unambiguous indication of his wishes, and that Google's reliance on consent does not fulfil the conditions required by Article 4(11) GDPR.
50. With regard to the "Other ad privacy features" (second pop-up), Google only informs the user about the existence of re-targeting and ad measurement processing activities. Google states in the pop-up that, when these "privacy features" are turned on, "*a site you visited can suggest related ads as you continue browsing*" and "*limited types of data are shared between sites to measure the performance of their ads*".
51. According to Google's own interpretation of this second pop-up, the purpose of the "Got it" button is not to collect consent: "*The "Got it" button on the second screen simply closes the dialogue box, enabling the user to acknowledge the notice.*" **(Annex 3)** "Site-suggested ads" (re-targeting) and ad measurement are by default turned on, unless the user goes to the settings and manually disables them.

¹⁹ C-249/21 Fuhrmann-2-GmbH

52. Re-targeting, however, is a form of personalised advertising. Ad measurement is an essential part of personalised advertising, too, as it enables advertisers to monitor the effectiveness of their campaigns. Personalised advertising can be based on legitimate interest under Article 6(1)(f) GDPR only insofar as it does not go beyond the “reasonable expectations” of the data subject (CJEU, C-252/21, Meta Platforms Inc., par. 116).
53. As the purpose of the “Privacy Sandbox” initiative is *precisely* to phase out third party cookies and substitute them with the “Topics API”, a user may not expect that their browser will continue to enable re-targeting and ad measurement unless they opt-out.
54. The only valid legal basis for these processing activities would thus be consent. However, Google does not offer the user a free choice, but only an opt-out mechanism which is incompatible with consent requirements pursuant to Article 4(11) GDPR.
55. Therefore, the respondent violates Article 6(1) GDPR also with regard to both the first and second pop-up.

4.3 Burden of Proof

56. Article 7(1) and Recital 42 of the GDPR states that the burden of proof to demonstrate consent rests on the data controller (Google).
57. It is for the respondent to demonstrate that the complainant has given consent to the processing of their data within the meaning of Article 4(11) GDPR.
58. If the controller cannot demonstrate that consent was obtained “*in full compliance of the GDPR*” then the complainant’s consent becomes “*illusory and consent will be an invalid basis for processing rendering the processing activity unlawful.*”²⁰ Which would, in turn, result in a breach of Article 6(1) GDPR.
59. Given that the burden of proof rests on Google, it follows that Google should disclose the consent rate for the Sandbox API, as well as any results from A/B testing or other methods that allow to see that Google has in fact provided the most transparent information to data subjects and has not - as alleged - used these tools to intentionally mislead data subjects.

5. REQUESTS AND SUGGESTIONS

5.1. Request to investigate

60. The complainant hereby requests that the competent supervisory authority fully investigates the complaint under Article 58(1) GDPR, including the internal design and decision process that lead to the misleading interface provided by Google.

²⁰ EDPB Guidelines 05/2020, para 62.

5.2. Request to compel respondent to:

61. The complainant requests that the complaint be upheld and that Google be found to have infringed Article 5(1)(a) and Article 6(1) GDPR.
62. The complainant requests that the competent supervisory authority orders the respondent to:
 - (a) Bring processing operations, in particular with regard to the collection of consent, in compliance with the GDPR (Article 58(2)(d) GDPR)
 - (b) Stop the processing of the data collected under invalid consent (Article 58(2)(f) GDPR);
 - (c) Stop the processing of personal data in connection with any of the Sandbox APIs, including but not limited to the “Topics API”, the “Attribution Reporting API”, the “Protected Audience API”, the as well as any measurement or statistics processing.
 - (d) Inform each recipient to whom the data subject’s personal data have been disclosed of the illegal processing and the need to stop any processing by recipients (Article 58(2)(g) GDPR).

5.3. Suggestion to impose an effective, proportionate and dissuasive fine

63. The complainant recommends, according to Articles 58(2)(i) and 83(5) GDPR, the imposition of an effective, proportionate and dissuasive fine.
64. Due regard should be paid to the deceptive nature of the collection of consent and the 3 billion estimated chrome users affected.²¹

6. CONTACT

65. Communications between *noyb* and the DSB in the course of this procedure can be done by email at [REDACTED] with reference to the **Case-No C083** oder [REDACTED]

²¹ Rohit Shewale, 35+ Chrome Statistics for 2024 (Users, Data & Facts), <<https://www.demandsage.com/chrome-statistics/>>, accessed 01.01.24