noyb – Europäisches Zentrum für digitale Rechte
Goldschlagstraße 172/4/3/2
1140 Wien
ÖSTERREICH

Datenschutzbehörde
Barichgasse 40-42,
1030 Wien

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

Wien, 13.06.2024

noyb Fallnummer: C-083

Beschwerdeführer: [redacted]

vertreten gemäß Artikel 80(1) DSGVO durch: *noyb* – Europäisches Zentrum für digitale Rechte Goldschlagstraße 172/4/3/2, 1140 Wien

Beschwerdegegnerin:

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

wegen:

Artikel 5(1)(a) DSGVO
Artikel 6(1)(a) DSGVO

BESCHWERDE

1. VERTRETUNG

1. *noyb* – Europäisches Zentrum für digitale Rechte ist eine Organisation ohne Gewinnerzielungsabsicht, die im Bereich des Schutzes der Rechte und Freiheiten von betroffenen Personen in Bezug auf den Schutz ihrer personenbezogenen Daten tätig ist, mit Sitz in Goldschlagstraße 172/4/2, 1140 Wien, Österreich und mit Registrierungsnummer ZVR: 1354838270 (iwF: „noyb“) (**Beilage 1**).

2. Der Beschwerdeführer wird gemäß Artikel 80(1) DSGVO durch *noyb* vertreten (**Beilage 2**).

2. SACHVERHALT

3. Am 07.09.2023 veröffentlichte Google LLC (im Folgenden: Google) seine "Privacy Sandbox" API (im Folgenden: die Sandbox API).

4. Vor diesem Datum erlaubte Google sogenannte third-party Cookies im Chrome-Browser, um die Suchhistorie der Nutzer zu verfolgen, personenbezogene Daten zu erfassen und gezielte Werbung (targeted advertisements) zu schalten. Third-party Cookies wurden bereits in anderen Browsern wie Safari von Apple und Firefox von Mozilla weitgehend blockiert, nicht aber in dem von Google bereitgestellten Chrome.[1]

5. Die Sandbox API zielt darauf ab, third-party Cookies - die gängigste Form der Tracking-Technologie - durch das zu ersetzen, was Google "Topics" nennt.[2]

6. Das System hinter der Sandbox API ist weit davon entfernt, ein Werkzeug zur Wahrung der Privatsphäre zu sein, und verfolgt nach wie vor den Browserverlauf eines Nutzers. Der Unterschied besteht darin, dass jetzt der Chrome-Browser selbst das Nutzerverhalten verfolgt und eine Liste von Werbe-"Topics" auf der Grundlage der von den Nutzern besuchten Websites erstellt. Bei der Markteinführung gab es fast 500 Werbekategorien wie "*Student Loans & College Financing", "Undergarments"* oder *"Parenting"*, denen die Nutzer aufgrund ihrer Online-Aktivitäten zugeordnet wurden.[3] Ein Werbetreibender, der auf einer Website präsent ist, die die Sandbox API aktiviert, fragt den Chrome-Browser, zu welchen Topics ein Nutzer gehört, und zeigt dann potenziell eine entsprechende Werbung an.

7. Der Chrome Browser verfolgt also nach wie vor Nutzer für targeted advertising von Google. Die wichtigste Änderung besteht darin, dass dies nur durch den Browser eines Unternehmens (Google) geschieht und nicht mehr durch unzählige serverseitige Tracking-Systeme Dritter. Der Chrome-Browser blockiert jetzt lediglich einige third-party Cookies (was andere Browser

[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> abgerufen am 01.01.2024.

[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> abgerufen am 01.01.2024.

[3] Diese Topics können hier abgerufen werden https://github.com/patcg-individual-drafts/topics/blob/main/taxonomy_v2.md, abgerufen am 01.01.2024.

bereits standardmäßig tun) und verwendet die Daten für targeted advertising.[4] Daher ist es irreführend, wenn Google dieses System als "Privatsphäre"-Tool bezeichnet.[5]

8. Google führte bei der Implementierung der Sandbox API A/B-Tests[6] durch, um eine hohe Einwilligung der Nutzer sicherzustellen. Dieses Vorgehen stellt einen Branchenstandard für jede UI/UX-Änderung dar. Tatsächlich wurde die Einführung der Sandbox-API sogar für 3% der Chrome-Nutzer hintangehalten, um Google die Durchführung von A/B-Tests zu ermöglichen.[7] Normalerweise werden A/B-Tests eingesetzt, um herauszufinden, welche Versionen eines Textes oder eines Schnittstellendesigns aus Unternehmenssicht die besten Ergebnisse liefern. Wenn es um Einwilligungsoptionen für Werbung geht, manipulieren Unternehmen in der Regel die Schnittstelle (mithilfe sogenannter "*dark patterns*"), um extreme Einwilligungsraten wie 90% oder mehr zu erreichen,[8] obwohl wir wissen, dass nur etwa 3% der Nutzer tatsächlich getrackt werden wollen.[9] Es ist daher anzunehmen, dass die Schnittstelle der Eingabeaufforderung "optimiert" wurde, um eine hohe Einwilligungsrate zu erhalten.

9. Anstatt klarzustellen, dass es um die Einwilligung zum Tracking der Nutzer durch den Browser ging, verkaufte Google den Nutzern die Sandbox API als „*privacy feature*" – also eine Funktion zur Gewährleistung der Privatsphäre. Es wird davon ausgegangen, dass dies eine bewusste Entscheidung war, um das Verständnis der Nutzer zu manipulieren und eine hohe Einwilligungsrate sicherzustellen, da die Nutzer dachten, dass ihr Browser sie nun vor Tracking für Werbung schützt.

10. Es sollte betont werden, dass Google bisher Third-Party Cookies für die meisten seiner Nutzer nicht abgeschafft hat, da sowohl die britische Marktaufsichtsbehörde als auch die britische Datenschutzbehörde diese Änderung des Geschäftsmodells von Google als möglichen Verstoß gegen datenschutz- und wettbewerbsrechtliche Bestimmungen untersuchen. Auch wenn die Sandbox API als Ausgleich für die Abschaffung des Tracking durch Dritte für Chrome-Nutzer gedacht war, scheint es, dass Google bei der Implementierung seines eigenen Tracking-Tools schneller war als bei der tatsächlichen Beseitigung bestehender Bedrohungen für die Privatsphäre der Nutzer.

---

[4] *Ben Wolford*, Google's Privacy Sandbox is privacy quicksand, <https://proton.me/blog/google-privacy-sandbox> abgerufen am 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> abgerufen am 01.01.2024.

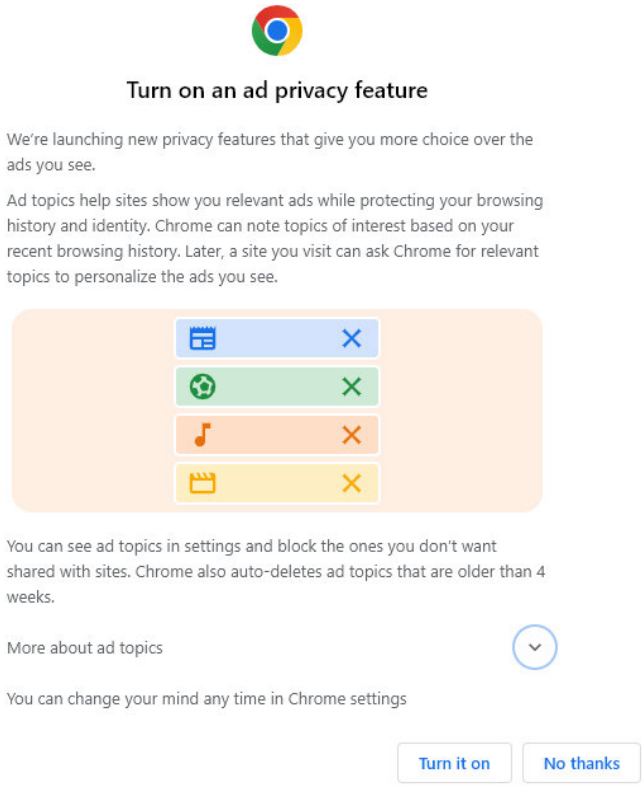
[6] A/B-Testing ist eine Methode, bei der zwei Varianten derselben Webseite oder desselben Cookie-Banners für Website-Besucher getestet werden, um zu vergleichen, welche Variante die höchste Anzahl von Opt-Ins erzielt.

[7] https://www.theverge.com/2023/9/7/23862743/google-chrome-privacy-sandbox-milestone-availability , abgerufen am 01.01.2024.

[8] Laut der eigenen Analyse von Quantcast haben mehr als 10.000 Domains weltweit Quantcast Choice eingesetzt und damit eine durchschnittliche Einwilligung der Verbraucher von mehr als 90% erreicht, siehe:
https://www.quantcast.com/press-release/quantcast-choice-powers-one-billion-consumer-consent-choices/

[9] Siehe Usercentrics Webinar um ca. Minute 30:00 Uhr (https://youtu.be/oux9uBUtscE?t=1800) und *Utz*, et al., (Un)informed Consent, in *arxiv* (Cornell University), Tabelle 2, Seite 10: https://arxiv.org/abs/1909.02638.

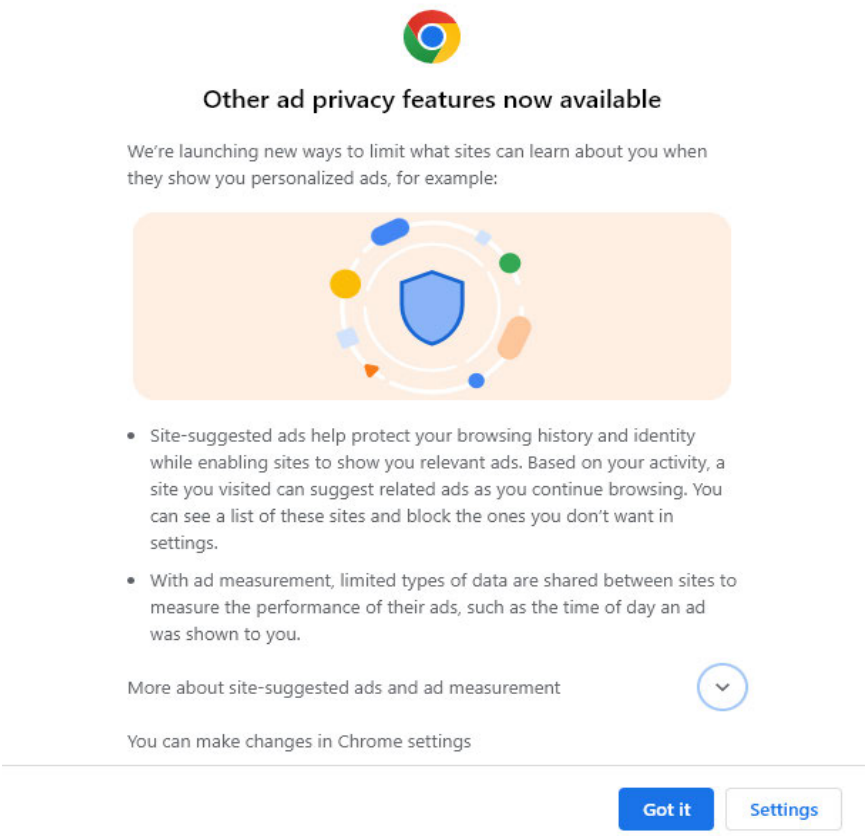
11. Am 18.10.2023 erhielt der Beschwerdeführer beim Öffnen von Google Chrome ein Pop-up-Fenster mit der Überschrift: *„turn on an ad privacy feature*", zu Deutsch: *„Aktivieren Sie eine Funktion zur Wahrung der Privatsphäre bei Werbeanzeigen*":



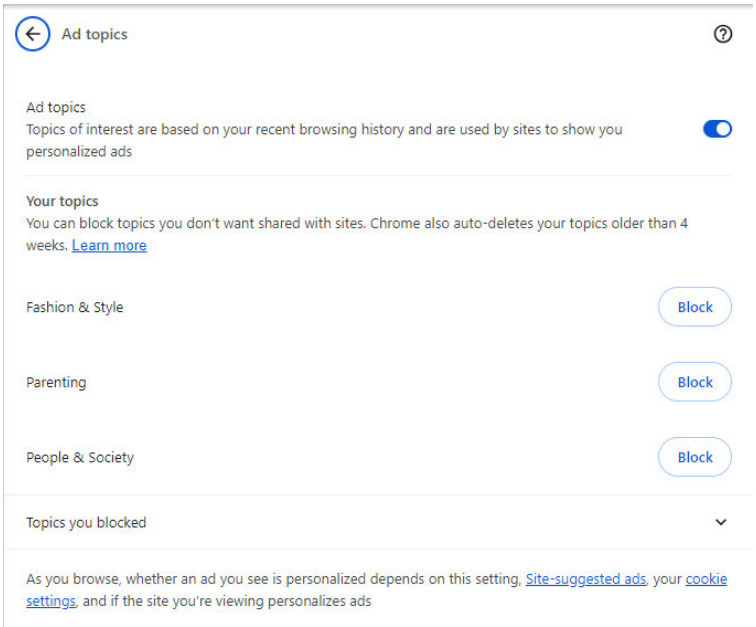
12. Das Pop-Up-Fenster gab dem Beschwerdeführer die Möglichkeit, die Funktion einzuschalten („*Turn on*") oder es abzulehnen („*No Thanks*").

13. Die Formulierung, „*Chrome can note topics of interest based on your recent browsing history*" (zu Deutsch: "*Chrome kann der Grundlage Ihres jüngsten Browserverlaufs Themen von Interesse erkennen*"), wird als Tatsache dessen dargestellt, was Chrome tun kann, und nicht als Wahlmöglichkeit für den Nutzer, ob Chrome seinen Browserverlauf überhaupt verfolgen soll. Es handelt sich um eine Tatsachenbehauptung, die eher eine bloße Information darstellt, als eine Frage an den Beschwerdeführer.

14. Der Beschwerdeführer klickte auf *"Turn it on"*. Daraufhin erschien eine weitere Seite, die nur durch Anklicken einer Verstanden-Schaltfläche (*"Got it")* verlassen werden konnte:



15. Als Folge der Interaktion mit diesen Pop-ups begann der Browser des Beschwerdeführers, Informationen zu dessen Surfverhalten aufzuzeichnen und sein Profil mit Themen zu verknüpfen. Am 29.05.2024 überprüfte der Beschwerdeführer beispielsweise seine Browsereinstellungen und stellte fest, dass die Themen "*Fashion & Style*", "*Parenting*" und "*People & Society*" mit ihm verknüpft wurden.



16. Der in den Pop-Ups verwendete Wortlaut ("*ad privacy feature*") versucht die Sandbox API als eine Funktion zur Wahrung der Privatsphäre zu vermarkten und nicht als Einwilligung in targeted advertising, indem Formulierungen wie „*schützen*" („*protect*"), „einschränken" („*limit*") und „*Funktionen zur Wahrung der Privatsphäre*" („*privacy features*") wiederholt verwendet wurden. Dies entspricht nicht dem, was Verbraucher gemeinhin unter Funktionen zum Schutz der Privatsphäre (wie Cookie- oder Tracking-Blocker) verstehen, die darauf abzielen, Nutzer vollständig abzuschirmen, anstatt sie durch alternative, lokal installierte Mittel weiter zu verfolgen und Daten mit Werbetreibenden zu teilen.

17. Das Design des ersten Pop-ups zeigte harmlose Topics aus den Bereichen Sport, Musik und Film. Diese spiegeln nicht die tatsächlichen Topics wider, die viel sensibler und spezifischer sind und Sub-Topics umfassen. Zum Beispiel: *"/Jobs & Education/Jobs/Job Listings/Government & Public Sector Jobs"* and *"/Finance/Credit & Lending/Credit Reporting & Monitoring".*[10] Das zweite Pop-up zeigte als zentrales Bild ein „Datenschutzschild" an, was wiederum impliziert, dass der Hauptzweck der Sandbox-API darin bestünde, die Verarbeitung und die Privatsphäre zu schützen, und nicht darin, gezielte Werbung in anderer Form zu schalten. Ein angemessenes Symbol wäre eine Kamera gewesen, die den Inhalt des Browsers ausspioniert, oder ähnliches.

18. Obwohl den geschulten Datenschutzjuristen von noyb ein genauerer Kontext bekannt war, als das bei einem durchschnittlichen Nutzer der Fall ist, war ihnen die beabsichtigte rechtliche Bedeutung des Pop-ups unklar, als betroffene Personen das neue Pop-up gegenüber noyb aufbrachten. Um sich Klarheit zu verschaffen, musste *noyb* erst ein Schreiben an Google senden, um zu verstehen, ob Google die Einwilligung nach Artikel 6(1)(a) DSGVO zur Verarbeitung personenbezogener Daten einholen möchte (**Beilage 3**).

19. Zum ersten Pop-up Fenster antwortete Google wie folgt:

> *"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".*
>
> Auf Deutsch:
>
> *"Google bittet um Einwilligung im Sinne von Artikel 6(1)(a) DSGVO für die Erstellung von Werbethemen in Chrome. Nutzer können ihre Einwilligung geben oder verweigern, indem sie auf ‚Einschalten' oder ‚Nein Danke' klicken. […] Die Einwilligung bezieht sich auf die Erstellung von Werbe-Topics innerhalb des Browsers".*

20. Für den Beschwerdeführer war es nicht nachvollziehbar, ob es sich bei dem Pop-up um eine Einwilligung, eine Änderung der Softwareeinstellungen oder eine bloße Information von Google über eine Funktion handelte, die ohnehin keine Wahlmöglichkeit ließ. Dies lag daran, dass, wie oben dargelegt, Wortlaut und Gestaltung des Popup-Fensters dies nicht klar erkennen ließen.

21. Auf die Frage *von noyb* nach der Bedeutung der *"Got it"*-Schaltfläche im zweiten Pop-up Fenster erklärte Google **(Beilage 3)**:

---

[10] Diese Topics finden sich hier: https://github.com/patcg-individual-drafts/topics/blob/main/taxonomy_v2.md, abgerufen am 01.01.2024.

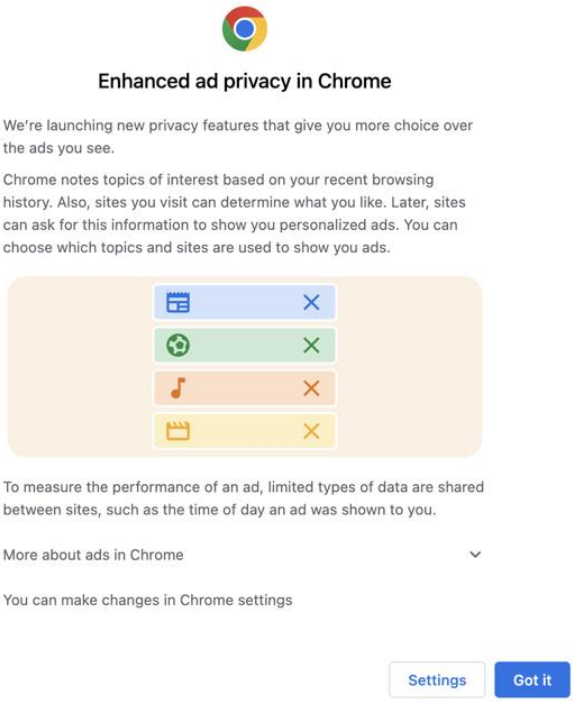
"The second screen informs users of the new controls within Chrome regarding two other Privacy Sandbox APIs ['App-suggested ads' and *'Ad Measurement'], which allow retargeting and ads measurement. […] The 'Got it' button on the second screen simply closes the dialogue box, enabling the user to acknowledge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

Auf Deutsch:

"Das zweite Fenster informiert die Nutzer über die neuen Kontrollen innerhalb von Chrome in Bezug auf zwei andere Privacy Sandbox APIs [‚App-suggested ads' und *‚Ad Measurement'], die Retargeting und Werbemessung ermöglichen. [...] Die Schaltfläche ‚Got it' auf dem zweiten Bildschirm schließt einfach das Dialogfeld und ermöglicht es dem Nutzer, den Hinweis zu bestätigen".*

22. Dies bedeutete, dass die API Ad Topics durch die Schaltfläche *"Turn it on"* gesteuert wurde und dass die APIs *"App-suggested ads"* und *"Ad Measurement"* für die betroffenen Personen in Europa im Grunde vorangekreuzte Optionen waren, für die keine Einwilligung von Google eingeholt wurde.[11]

23. Zum Vergleich: Die außereuropäische Version des ersten Pop-up-Fensters („*Enhanced ad privacy in Chrome*"), das keine Wahlmöglichkeit für den Nutzer bot, aktivierte die Sandbox-API, nachdem die Nutzer auf *"got it"* geklickt hatten.[12]



[11] Ein Beispiel dafür, dass *"App-suggested ads"* und *"Ad Measurement"* bereits angekreuzt sind, auch wenn die betroffene Person auf *"No Thanks"* klickt, findet sich hier: https://youtu.be/ogXc8Zi7PCA?feature=shared.

[12] *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> abgerufen am 01.01.2024.

3. ZUSTÄNDIGE AUFSICHTSBEHÖRDE

24. Der Beschwerdeführer hat seinen gewöhnlichen Aufenthalt und seinen Arbeitsplatz in Österreich, und das Pop-up erschien, als er Chrome in Österreich verwendete. Daher kann der Beschwerdeführer seine Beschwerde bei der österreichischen Aufsichtsbehörde gemäß Artikel 77 DSGVO einreichen.

25. Da das Tracking auf der Ebene des Browsers der betroffenen Person erfolgt, gibt es kein grenzüberschreitendes Element, das die Zuständigkeit einer federführenden Aufsichtsbehörde gemäß Artikel 56 DSGVO rechtfertigen würde. Wie Google selbst erklärt:

> "*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*."[13]
>
> Auf Deutsch:
>
> "*Die Privacy Sandbox APIs verlangen von Webbrowsern die Einnahme einer neuen Rolle. Anstatt mit begrenzten Werkzeugen und Schutzmechanismen zu arbeiten, ermöglichen die APIs dem Browser eines Nutzers, im Namen des Nutzers zu handeln - vor Ort, auf seinem Gerät -, um die identifizierenden Informationen des Nutzers zu schützen, während er im Internet surft. Dies ist ein Richtungswechsel bei den Browsern*.

26. Die Topics wurden ursprünglich von Google erstellt und sind weltweit standardisiert; die eigentliche Verarbeitung erfolgt durch den Browser selbst. Google erklärt, dass Chrome – bei aktivierten Sandbox-APIs – Topics aus den Websites ableitet, die ein Nutzer beim Surfen im Internet besucht. Der Browser speichert die Topics dann auf dem Gerät des Nutzers. Die Topics werden nicht direkt auf die Server von Google oder Dritten übertragen. Die Offenlegung erfolgt nur dann, wenn der Nutzer anschließend Websites besucht, auf denen Werbetreibende auf die Topics zugreifen können.

27. Mit anderen Worten, der Austausch personenbezogener Daten findet zwischen dem Browser des Nutzers und dem Server eines Werbetreibenden statt, der die Sandbox-API eingebettet hat.

28. Daher findet die Verarbeitung nicht "*im Rahmen der Tätigkeiten von Niederlassungen […] in mehr als einem Mitgliedstaat*" statt. Im vorliegenden Fall findet die Verarbeitung im Rahmen der Tätigkeit eines Browsers statt. In Anbetracht von Artikel 4(23)(a) DSGVO ist die wesentliche Voraussetzung für die Einstufung einer Verarbeitung als "*grenzüberschreitend*" somit nicht erfüllt.

29. Das Fehlen eines grenzüberschreitenden Elements gemäß Artikel 4(23)(a) DSGVO hat zur Folge, dass auch Artikel 56(1) DSGVO nicht anwendbar ist. Die österreichische Aufsichtsbehörde bleibt die zuständige Aufsichtsbehörde nach Artikel 55 DSGVO und der in Artikel 60 DSGVO vorgesehene Kooperationsmechanismus findet keine Anwendung.

[13] https://developers.google.com/privacy-sandbox/overview.

30. Selbst wenn die Definition von Artikel 4(23)(a) DSGVO erfüllt wäre, möchten wir darauf hinweisen, dass Google derzeit argumentiert, dass Google LLC in den USA und Google Ireland Limited getrennte Verantwortliche sind. Google Ireland Limited kontrolliert - laut Google - alle Google-Tochtergesellschaften in der EU. Offensichtlich können Google Ireland Limited und seine Tochtergesellschaften nicht gleichzeitig eine „Hauptniederlassung" eines anderen für die Verarbeitung Verantwortlichen und ein separater für die Verarbeitung Verantwortlicher sein. Da sich diese Beschwerde bisher nur gegen Google LLC als Beschwerdegegner richtet, sehen wir keine Grundlage für die Anwendung von Artikel 56(1) DSGVO auf diese Beschwerde.

4. BESCHWERDEGRÜNDE

4.1. Rechtsverletzungen

31. Google hat die folgenden Vorschriften der DSGVO verletzt:

    (a) Verletzung von Artikel 5(1)(a) DSGVO: Treu und Glauben und Transparenz

    (b) Verletzung von Artikel 6(1)(a) DSGVO: Einwilligung als Rechtsgrundlage

4.2. Verletzung von Artikel 5(1)(a) DSGVO

32. Artikel 5(1)(a) DSGVO verlangt, dass personenbezogene Daten " *auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise*" verarbeitet werden. Die Daten wurden weder nach Treu und Glauben noch in transparenter Weise verarbeitet

33. Artikel 12(1) DSGVO präzisiert den Grundsatz und verlangt, dass die Informationen in "*präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache*" bereitgestellt werden.

34. Erwägungsgrund 60 stellt weiter klar: „*Die Grundsätze einer fairen und transparenten Verarbeitung machen es erforderlich, dass die betroffene Person über die Existenz des Verarbeitungsvorgangs und seine Zwecke unterrichtet wird."*

35. Diese Informationen müssen dann verfügbar sein, wenn der Beschwerdeführer seine Entscheidung trifft, und dürfen nicht einfach in einer Datenschutzerklärung versteckt sein. In den EDSA-Leitlinien heißt es*: „Es wird darauf hingewiesen, dass es für den Verantwortlichen schwer sein wird, nachzuweisen, dass die betroffene Person ihre Einwilligung in informierter Weise erteilt hat, wenn die Identität des Verantwortlichen oder der Zweck der Verarbeitung im Fall einer mehrschichtigen Datenschutzerklärung nicht in der ersten Informationsschicht mitgeteilt wird (sondern wenn sie sich in weiteren Unterebenen befinden), es sei denn, der Verantwortliche kann nachweisen, dass die jeweilige betroffene Person Zugriff auf diese Informationen hatte, bevor sie ihre Einwilligung erteilt hat."*[14]

36. Die erste Informationsschicht in diesem Zusammenhang war das oben beschriebene Pop-up. Der Beschwerdeführer wurde nicht über den *"Zweck der Verarbeitung"* informiert, sondern

[14] https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_de.pdf Fußnote 42.

tatsächlich in die Irre geführt, indem behauptet wurde, es handele sich um eine Funktion zur Wahrung der Privatsphäre („*privacy feature*“) - und nicht um ein Tracking-Tool. Während der Beschwerdeführer angeblich seine Einwilligung zum Tracking durch seinen Browsers bzw. durch Google gab, was immer noch zu einer Form von targeted advertising führen würde, wurde ihm vorgegaukelt, dass dies eine Funktion zur Wahrung der Privatsphäre erfolgen würde.

37. Zum Vergleich: Brave (ein anderer Browser, der mit Chrome verwandt ist) beschreibt seine *"Brave Shields"* ebenfalls als privacy feature.[15] Das „*Brave Shield*“ erleichtert jedoch nicht targeted advertising, sondern blockiert Online-Tracker im jeweiligen Browser. Wie bei vielen Funktionen anderer Browser oder Plug-ins ist dies das, was ein durchschnittlicher Nutzer berechtigterweise von einer Funktion zur Wahrung der Privatsphäre erwarten würde.

38. Das EU-Recht ordnet irreführende Werbung den unlauteren Geschäftspraktiken zu.[16] In der Rechtssache C-562/15 wertete der EuGH das irreführende Marketing von Carrefour als unlautere Geschäftspraktik. Erwägungsgrund 42 der DSGVO greift diesen Zusammenhang ebenfalls auf führt aus, dass "*eine vom Verantwortlichen vorformulierte Einwilligungserklärung [...] keine missbräuchlichen Klauseln beinhalten"* sollte*.* Die von Google vorformulierte Einwilligung war allerdings irreführend und missbräuchlich, was zu einem Verstoß gegen Artikel 5(1)(a) der DSGVO führt.

39. Erwägungsgrund 39 hält außerdem fest: „*Für natürliche Personen sollte Transparenz dahingehend bestehen, dass sie betreffende personenbezogene Daten erhoben, verwendet, eingesehen oder anderweitig verarbeitet werden und in welchem Umfang die personenbezogenen Daten verarbeitet werden und künftig noch verarbeitet werden*“.

40. Das Popup-Fenster war allerdings nicht transparent in Bezug auf die Tatsache, dass versucht wird, eine vermeintliche Einwilligung einzuholen und diese dazu verwendet wird, die Browserverläufe der Nutzer zu verfolgen und Ausgestaltungen dieser Daten an Dritte weiterzugeben. Vielmehr behauptet Google, Chrome generiere nur gewisse Topics, die Interessen der Nutzer wiederspiegeln und würde dies machen, um die Privatsphäre und den Browserverlauf der Nutzer zu schützen.

41. Artikel 26(1)(d) Gesetz digitaler Dienste greift die Transparenzanforderungen der DSGVO auf und verlangt, dass Anbieter sehr großer Online-Plattformen (wie Google) den Empfängern von Online-Werbung aussagekräftige Erläuterungen zur zugrunde liegenden Logik bereit stellen, einschließlich der Angabe, wann Profiling genutzt wird.[17]

42. Das Pop-up zur Sandbox API hat weder transparent über die Logik aufgeklärt, auf der die gegenständlichen Topics beruhen, und die den Beschwerdeführer kategorisieren, noch die Kriterien dargelegt, die verwendet werden, um den Beschwerdeführer mit Werbekunden zu verbinden. Im Gegenteil, Google versuchte alles, um den Beschwerdeführer das Gefühl zu geben, dass er nun in den Genuss einer neuen Privatsphäre-Funktion kommt, während er - laut Google - in Wirklichkeit zustimmte, dass eine Software jeden Klick und jede Bewegung, die er online macht, verfolgt.

---

[15] Brave, *Brave Shields,* <https://brave.com/shields/>, aufgerufen am 11.12.2023.

[16] EU-Richtlinien 84/450/EWG (über irreführende Werbung), 93/13/EWG (über missbräuchliche Klauseln in Verbraucherverträgen), 2005/29/EG (über unlautere Geschäftspraktiken von Unternehmen gegenüber Verbrauchern) und 2006/114/EG (über irreführende und vergleichende Werbung).

[17] Erwägungsgrund 68 des Gesetzes über digitale Dienste (Digital Services Act).

43. Google hat seine Sandbox API als bessere Alternative zu third-party-tracking-Systemen verkauft. Das mag zwar stimmen, aber die Sandbox-API nimmt weiterhin ein Tracking der Nutzer vor - nur eben in einer anderen Form. Tracking ist ein Eingriff in die Rechte der Nutzer und sollte nicht als *"privacy feature"* umgedeutet werden, wenn dies eindeutig nicht der Fall ist.

4.3. Verletzung von Artikel 6(1)(a) DSGVO

44. In Bezug auf die Erstellung von Topics (wie im ersten Pop-up angekündigt) stützt sich Google auf die Einwilligung als Rechtsgrundlage für die Verarbeitung gemäß Artikel 6(1)(a) DSGVO **(Beilage 3).**

45. Artikel 4(11) DSGVO besagt, dass die Einwilligung unter anderem eine *"für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung"* der betroffenen Person sein muss.

46. Wie bereits erwähnt, konnte die Einwilligung angesichts des irreführenden Charakters des Pop-up-Fensters nicht in informierter Weise erfolgen.

47. Der Beschwerdeführer war sich (bis noyb Kontakt mit Google hergestellt hat) nicht bewusst, dass er durch die Interaktion mit dem Pop-up- - laut Google - der Verarbeitung seiner Daten für gezielte Werbung zustimmte.

48. Außerdem ist die Formulierung *"turn it on"* zweideutig und ähnelt nicht den typischen Einwilligungsschaltflächen, die Formulierungen wie *"zustimmen"*, *"einwilligen"* oder *"annehmen"* beinhalten. Der EuGH hat bereits über die Bedeutung des Textes auf einer Schaltfläche für den Abschluss eines Fernabsatzvertrages geurteilt.[18] So muss nach Artikel 8(2) der Richtlinie 2011/83/EU eine Schaltfläche mit den Worten *"zahlungspflichtig bestellen"* oder einer entsprechenden eindeutigen Formulierung gekennzeichnet sein, um zu vermitteln, dass eine Zahlungspflicht besteht. Dementsprechend ist eine mit „*turn it on*" beschriftete Schaltfläche nicht geeignet, eine Einwilligung einzuholen.

49. Daraus folgt, dass die Einwilligung des Beschwerdeführers weder in informierter Weise abgegeben wurde, noch in unmissverständliche Willensbekundung gewesen sein kann und dass Googles Berufung auf die Rechtsgrundlage der Einwilligung nicht die in Artikel 4(11) DSGVO geforderten Bedingungen erfüllt.

50. In Bezug auf das zweite Pop-up („*Other ad privacy features*") informiert Google den Nutzer lediglich über die das Bestehen der Verarbeitungen Re-Targeting und Anzeigenmessung. Google weist in dem Pop-up darauf hin, dass, wenn diese „*privacy features"* aktiviert sind, bereits besuchte Websites, für die Auswahl ähnlicher Anzeigen herangezogen werden und gewisse Arten von Daten zwischen Websites ausgetauscht werden, um die Leistung ihrer Anzeigen zu messen.

[18] C-249/21 Fuhrmann-2-GmbH.

51. Nach Googles eigener Interpretation besteht der Zweck der Schaltfläche "*Got it*" auf diesem zweiten Pop-up-Fenster nicht darin, eine Einwilligung einzuholen. Im Schreiben an noyb hält Google fest: "the '*Got it' button on the second screen simply closes the dialogue box, enabling the user to acknowledge the notice.*" Auf Deutsch: „*Die Schaltfläche ‚Got it' auf dem zweiten Bildschirm schließt einfach das Dialogfeld und ermöglicht es dem Nutzer, den Hinweis zu bestätigen*" (**Beilage 3**) "Site-suggested ads" (Re-Targeting) und Anzeigenmessung sind also standardmäßig aktiviert, es sei denn, der Nutzer geht zu den Einstellungen und deaktiviert sie manuell.

52. Re-Targeting ist jedoch eine Form der personalisierten Werbung. Auch die Werbemessung ist ein wesentlicher Bestandteil der personalisierten Werbung, da sie es Werbetreibenden ermöglicht, die Wirksamkeit ihrer Kampagnen zu überwachen. Personalisierte Werbung kann gemäß Artikel 6(1)(f) DSGVO nur dann auf ein berechtigtes Interesse gestützt werden, wenn sie nicht über die vernünftigen Erwartungen der betroffenen Person hinausgeht (EuGH, C-252/21, Meta Platforms Inc., Rn 116).

53. Da der Zweck der "Privacy Sandbox" gerade darin besteht, third-party Cookies abzuschaffen und durch die Topic API zu ersetzen, liegt es nicht in den vernünftigen Erwartungen eines Nutzers wie dem Beschwerdeführer, dass sein Browser weiterhin Re-Targeting und Werbemessung ermöglicht, wenn er sich nicht dagegen entscheidet.

54. Die einzig gültige Rechtsgrundlage für diese Verarbeitungen wäre somit eine Einwilligung der betroffenen Person. Google bietet dem Nutzer jedoch keine freie Wahl, sondern nur einen Opt-out-Möglichkeit, der mit den Anforderungen an die Einwilligung gemäß Artikel 4(11) DSGVO unvereinbar ist.

55. Daher verstößt Google im Hinblick auf das erste und zweite Pop-up gegen Artikel 6(1) DSGVO.

4.3 Beweislast

56. Artikel 7(1) und Erwägungsgrund 42 der DSGVO besagen, dass die Beweislast für den Nachweis der erfolgten Einwilligung beim Verantwortlichen (Google) liegt.

57. Es obliegt daher Google, nachzuweisen, dass der Beschwerdeführer die Einwilligung zur Verarbeitung seiner Daten im Sinne von Artikel 4(11) DSGVO gegeben hat.

58. Wenn Google nicht nachweisen kann, dass die Einwilligung in voller Übereinstimmung mit den dafür vorgesehenen Voraussetzungen eingeholt wurde, ist die vermeintliche Einwilligung des Beschwerdeführers eine ungültige Grundlage für die Verarbeitung, wodurch die Verarbeitungstätigkeit rechtswidrig wird.[19] Dies würde wiederum zu einem Verstoß gegen Artikel 6(1) DSGVO führen.

59. Da die Beweislast bei Google liegt, sollte Google die Einwilligungsrate für die Sandbox API sowie alle Ergebnisse von A/B-Tests oder anderen Methoden offenlegen, die zeigen, dass Google den betroffenen Personen tatsächlich die transparentesten Informationen zur

[19] EDSA-Leitlinien 05/2020, Rn 62.

Verfügung gestellt hat und diese Instrumente nicht - wie behauptet - zur absichtlichen Irreführung der betroffenen Personen eingesetzt hat.

5. BESCHWERDEANTRÄGE

5.1. Ersuchen umfassender Untersuchungen

60. Der Beschwerdeführer fordert hiermit, dass die zuständige Aufsichtsbehörde die Beschwerde gemäß Artikel 58(1) DSGVO vollständig untersucht, einschließlich der internen Prozesse, die zur gegenständlichen Gestaltung, der von Google verwendeten irreführenden Schnittstelle geführt haben.

5.2. Anträge

61. Der Beschwerdeführer beantragt, der Beschwerde stattzugeben und festzustellen, dass Google gegen Artikel 5(1)(a) und Artikel 6(1) DSGVO verstoßen hat.

62. Der Beschwerdeführer beantragt, dass die zuständige Aufsichtsbehörde Google aufträgt:

    (a) die gegenständlichen Verarbeitungen im Hinblick auf die Einholung der vermeintlichen Einwilligung des Beschwerdeführers in Einklang mit der DSGVO zu bringen (Artikel 58(2)(d) DSGVO);

    (b) die Verarbeitung von Daten des Beschwerdeführers, die mit ungültiger Einwilligung erhoben wurden, einzustellen (Artikel 58(2)(f) DSGVO);

    (c) die Verarbeitung von Daten des Beschwerdeführers einzustellen, die in Verbindung mit einer der Sandbox APIs stehen (insbesondere aber nicht ausschließlich "Topics API", "Attribution Reporting API", "Protected Audience API", sowie sämtliche damit zusammenhängende Verarbeitungen zu Mess- oder Statistikzwecken); und

    (d) jeden Empfänger, an den die personenbezogenen Daten des Beschwerdeführers weitergegeben wurden, über die unrechtmäßige Verarbeitung zu informieren und diese auf die Notwendigkeit hinzuweisen, die Verarbeitung ebenfalls einzustellen (Artikel 58(2)(g) DSGVO).

5.3. Anregung eine wirksame, verhältnismäßige und abschreckende Geldbuße zu verhängen

63. Der Beschwerdeführer regt an, gemäß Artikel 58(2)(i) und Artikel 83(5) DSGVO, eine wirksame, verhältnismäßige und abschreckende Geldbuße zu verhängen.

64. Dem irreführenden Vorgehen bei der Einholung der vermeintlichen Einwilligung, sowie dem Umstand, dass etwa 2 Milliarden Chrom-Nutzer betroffen sind,[20] sollte dabei eine entsprechende Berücksichtigung zukommen,

[20] Rohit Shewale, 35+ Chrome Statistics for 2024 (Users, Data & Facts), <https://www.demandsage.com/chrome-statistics/>, aufgerufen am 01.01.2024.

6. KONTAKT

65. Die Kommunikation zwischen *noyb* und der DSB im Rahmen dieses Verfahrens kann per E-Mail an [redacted] unter Bezugnahme auf die **Rechtssache C083** oder per Telefon unter [redacted] erfolgen.