

An:

---

Sehr geehrtes XXXX GmbH-Team,

wir vertreten eine betroffene Person, die Ihre Website ([xyz.de](http://xyz.de)) besucht hat, gemäß Artikel 80 DSGVO. Während dieses Besuchs wurde ein DSGVO-widriges Einwilligungsbanner angezeigt.

### **Beschwerde gemäß Artikel 77 DSGVO**

Wir planen eine formelle Beschwerde gemäß Artikel 77 DSGVO bei der zuständigen Datenschutzbehörde (HmbBfDI (Hamburg)) einzureichen, wenn dieser Fall nicht einvernehmlich gelöst wird.

Weitere Details zu den identifizierten Rechtsverstößen können Sie dem beigefügten Beschwerdeentwurf und dem Leitfaden entnehmen.

Die Höchststrafe beträgt bis zu € 20 Millionen oder 4% Ihres Jahresumsatzes.

### **WeComply! - Möglichkeit zur einvernehmlichen Lösung binnen 30 Tagen**

Um eine formelle Beschwerde zu vermeiden, bieten wir Ihnen eine einfache und kostenlose Möglichkeit, die aufgezeigten Probleme zu beheben und Ihre Compliance auf unserer [WeComply!-Plattform](#) zu melden.

Wenn Sie die aufgezeigten Probleme binnen 30 Tagen beheben, führen wir eine abschließende Prüfung durch und verzichten auf die Einreichung der Beschwerde.

Ihre vorab zugewiesenen Falldetails sind:

- **Fallnummer:** C-037-xxxxxxx
- **Passwort:** z5xxxxxxx
- **Login:** <https://wecomply.noyb.eu/>

Weitere Informationen über uns, die vollständige Einhaltung der gesetzlichen Vorschriften und diese E-Mail finden Sie in unseren [FAQs](#) oder wenn Sie online nach uns suchen.

Bitte haben Sie Verständnis dafür, dass wir keine direkten Antworten auf diese E-Mail bearbeiten können.

Mit freundlichen Grüßen

Max Schrems  
Vorsitzender von *noyb*

#### Über uns:

NOYB - European Center for Digital Rights  
Goldschlagstraße 172/4/3/2, 1140 Vienna, AUSTRIA

(ZVR): 1354838270

[noyb.eu](http://noyb.eu) | [Twitter](#) | [LinkedIn](#) | [Facebook](#) | [RSS](#)

Dies ist ein Beschwerdeentwurf. Die endgültige Fassung dieser Beschwerde, die bei der zuständigen Behörde eingebracht wird kann sich von diesem Entwurf unterscheiden und wird Beweise und Details zur betroffenen Person enthalten, die hier noch fehlen.

## Beschwerde gemäß Artikel 77 DSGVO

**Unsere Fallnummer:** C-037-

**Beschwerdeführer:** [Die Identität des Beschwerdeführers wird in der endgültigen Fassung der Beschwerde ersichtlich sein]

**Verantwortlicher:**

**Gegenwärtig vermutete federführende Aufsichtsbehörde (Lead Supervisory Authority – „LSA“):**  
HmbBfDI (Hamburg)

Der Beschwerdeführer wird von dem österreichischen gemeinnützigen Verein *noyb* – Europäisches Zentrum für digitale Rechte, Goldschlagstraße 172/4/3/2, 1140 Wien, Österreich, gemäß Artikel 80(1) DSGVO vertreten. Die Vertretungsvollmacht ist als Anlage 1 angehängt.

*noyb* hat den Verantwortlichen kontaktiert, um die Themen dieser Beschwerde aufzuzeigen. Um die Arbeitsbelastung für alle Parteien zu begrenzen, haben wir angeboten, auf die Einreichung dieser Beschwerde zu verzichten, sollte der Verantwortliche seine Verarbeitungstätigkeiten rechtskonform gestalten. Bedauerlicherweise ist der Verantwortliche unserem Vorschlag nicht gefolgt.

### 1.G rundsätzliche Fakten

Vom 07-05-2021 13:56:00 bis 07-05-2021 13:56:34 besuchte der Beschwerdeführer die Webseite des Verantwortlichen. Die Webseite zeigte in Form eines „Banners“ eine von OneTrust zur Verfügung gestellten Consent Management Platform („CMP“). Screenshots der Webseite und des Banners sind als Anlage 2 beigelegt.

Eine Zusammenfassung aller relevanten Einstellungen innerhalb der OneTrust-Konfigurationsdateien im JSON-Format ist als Anlage 3.1 bis 3.2 („onetrust-domain.json“ und „one-trust-configuration.json“) beigelegt. Diese Dateien enthalten alle Einstellungen, die der Verantwortliche zur Konfiguration des Banners verwendet hat.

Durch die Verwendung dieses Banners hat der Verantwortliche versucht,

- eine Rechtsgrundlage gemäß Artikel 6(1) DSGVO zu etablieren, um die personenbezogenen Daten des Beschwerdeführers zu verarbeiten, und
- eine Rechtsgrundlage gemäß Artikel 5(3) ePrivacy-Richtlinie (bzw. der relevanten nationalen Umsetzung) und Artikel 6(1)(a) DSGVO zu etablieren, um Informationen am Endgerät des Beschwerdeführers zu speichern und/oder darauf zuzugreifen.

Eine detaillierte Zusammenfassung aller HTTP-Anfragen und -Antworten („Verarbeitung“ im Sinne von Artikel 4(2) DSGVO) zwischen dem Browser und den verschiedenen Servern während des Besuchs der Website des Verantwortlichen ist als Anlage 4 („traffic.json“) beigelegt. Neben diesen Verarbeitungen können auch andere Formen der Datenverarbeitung (andere als HTTP-Anfragen und -Antworten, wie die Verarbeitung personenbezogener Daten über JavaScript) stattgefunden haben.

Darüber hinaus hat der Beschwerdeführer zumindest die folgenden Datenflüsse identifiziert, die sich auf im Endgerät des Beschwerdeführers gespeicherte Informationen im Sinne von Artikel 5(3) ePrivacy-Richtlinie beziehen und personenbezogene Daten im Sinne von Artikel 4(1) DSGVO enthalten:

Domain	Name	Value	Details
.facebook.com	fr	0cylRFm65yFDLQfJb..BglSrU..9.0.BglSrX.	The 'fr' cookie is used to deliver, measure and improve the relevancy of ads, according to Facebook

Eine detaillierte Zusammenfassung aller Cookie-Daten ist als Anlage 5 angehängt.

Zusätzlich konnte der Beschwerdeführer anhand einer öffentlichen IP-Adresse (77.119.XX.XX), identifiziert werden, die ebenso ein personenbezogenes Datum ist.

Im Folgenden beziehen wir uns auf diese Verarbeitungstätigkeiten als „**relevante Verarbeitungstätigkeiten**“.

## 2. Anwendbares Recht

Der Verantwortliche hat eine breite Palette von Verarbeitungsvorgängen durchgeführt, um die gesamte Webseite bereitzustellen. Soweit der Verantwortliche personenbezogene Daten der betroffenen Person verarbeitet, gilt die **DSGVO** für die relevanten Verarbeitungstätigkeiten (sei es über Technologien wie HTML-Code, verschiedene Scripts, iframes, Zählpixel, lokale Speicherung oder Cookies).

In dem Maße, in dem der Verantwortliche Daten (seien es personenbezogene oder nicht-personenbezogene Daten) am Endgerät des Beschwerdeführers speichert oder darauf zugreift, kann Artikel 5(3) ePrivacy-Richtlinie als *lex specialis* anstelle von Artikel 6(1) DSGVO auf diese begrenzten Verarbeitungen Anwendung finden; dies gilt jedoch nicht für darauf folgende Verarbeitungen.

Das Verhältnis zwischen der DSGVO und der ePrivacy-Richtlinie (bzw. deren nationalen Umsetzungen) und die Zuständigkeit der Aufsichtsbehörden kann für jeden Verarbeitungsvorgang und in jedem EU-Mitgliedstaat unterschiedlich sein (siehe EDPB-Stellungnahme 5/2019 zum Zusammenspiel zwischen der ePrivacy-Richtlinie und der DSGVO). Wir stützen uns daher für die Zwecke dieser Beschwerde auf beide Rechtsinstrumente und ihre nationalen Umsetzungen in Bezug auf alle relevanten Verarbeitungstätigkeiten.

## 3. Behauptete Rechtsgrundlage

Dem Banner zufolge berief sich der Verantwortliche auf die Einwilligung gemäß Artikel 6(1)(a) DSGVO und Artikel 5(3) ePrivacy sowie auf berechtigte Interessen gemäß Artikel 6(1)(f) DSGVO, um die relevanten Verarbeitungstätigkeiten zu rechtfertigen. Es lag jedoch keine wirksame Einwilligung des Beschwerdeführers vor und es bestand kein berechtigtes Interesse.

## 4.H Intergrund: Täuschende Banner und „Dark Patterns“

Branchenvertreter geben selbst zu, dass nur etwa 3 % aller Betroffenen in die Verwendung ihrer personenbezogenen Daten für Marketingzwecke wirklich einwilligen wollen, während unabhängige Studien Einwilligungsraten von 0,16 % für neutrale Banner zeigen.<sup>1</sup> Dennoch verzeichnen Verantwortliche Einwilligungsraten von über 90 %.<sup>2</sup>

Um diese schwindelerregende Diskrepanz zu erreichen, werden die betroffenen Personen mit Hunderten von verschiedenen Bannern konfrontiert, die oft Hunderte von individuellen Optionen und Links zu endlosen Rechtstexten enthalten. Das Lesen jeder dieser Optionen und Texte würde den durchschnittlichen Nutzer jeden Tag Stunden kosten.

1 Siehe Usercentrics Webinar ca. bei 30:00 (<https://youtu.be/oux9uBUtscE?t=1800>) and Utz, Degeling, Fahl, Schaub and Holz, (Un)informed Consent, Tabelle 2.

2 „Den eigenen Analysen von Quantcast zufolge, setzen über 10,000 Domains weltweit Quantcast Choice ein und erreichen unter Konsumenten eine durchschnittliche Einwilligungsrate von über 90%“, siehe: <https://www.quantcast.com/press-release/quantcast-choice-powers-one-billion-consumer-consent-choices/>.

Um effizient im Internet zu navigieren, müssen die betroffenen Personen eine „Standard-Klickstrategie“ entwickeln, um die Banner in einer angemessenen Zeit, oft innerhalb von Sekunden, loszuwerden. Da die betroffenen Personen realistischerweise nicht in der Lage sind, die Details jedes einzelnen Banners zu lesen, erkennen sie instinktiv allgemeine Muster (wie z. B. „Mit der hervorgehobenen Schaltfläche können Sie die Seite aufrufen“). Eine solche absichtliche Informationsüberlastung in Kombination mit nur einem einfachen Ausweg („Alles akzeptieren“) führt zu der oft diskutierten „Einwilligungsmüdigkeit“. Im Gegensatz zu einigen Branchenerzählungen ist dies kein Defekt des Einwilligungsmodells der DSGVO, sondern ein bewusster Angriff auf die Idee der „freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebenen“ Einwilligung.

Die Unterschiede in den Einwilligungsraten basierend auf dem Design sind verblüffend: Die britische ICO hat zum Beispiel berichtet, dass sie etwa 90 % weniger Einwilligungen von Nutzern von ico.org.uk erhalten hat, nachdem sie ihre eigene Anleitung für GDPR-konforme Einwilligungsbanner umgesetzt hat.<sup>3</sup> Ein Whitepaper der deutschen CMP Usercentrics erklärt sogar, wie man mit fünf einfachen Änderungen die Einwilligungsraten um 39% steigern kann,<sup>4</sup> d.h. 4 von 10 Betroffenen können allein durch diese Designänderungen zur Einwilligung überredet werden.

Entgegen jedem Versuch, die wahren und genauen Wünsche der betroffenen Personen zu ermitteln, haben die Verantwortlichen verschiedene Formen von Täuschungspraktiken entwickelt, um durch sogenannte „Dark Patterns“ völlig unrealistische Einwilligungsraten von bis zu 90 % zu erreichen.

Zusammenfassend lässt sich sagen, dass die für die Datenverarbeitung Verantwortlichen die Strategie verfolgen, einen einfachen Ausweg anzubieten („Alles akzeptieren“), während sie jede andere Option so kompliziert wie möglich gestalten. Solche kleinen Design-Änderungen führen zu Klickraten, die im Widerspruch zu allem stehen, was ein vernünftiger Verantwortlicher als genaue Widerspiegelung der wahren Wünsche der Betroffenen verstehen könnte.

Einige dieser Ansätze sind systemisch, wie z. B. die Tatsache, dass 25 % der Betroffenen der Meinung sind, dass eine Website ohne Einwilligung nicht genutzt werden kann<sup>5</sup> oder dass die Nutzer so viele negative Erfahrungen mit dem Anklicken von etwas anderem als „Alles akzeptieren“ auf anderen Seiten gemacht haben, dass sie diese Optionen gar nicht mehr ausprobieren.

Andere Ansätze sind spezifisch für eine Seite, wie z. B. wenn Verantwortliche aktiv verschiedene Tools (wie z. B. „A/B-Tests“) verwenden und viele Daten generieren, um zunehmend trügerische Systeme auf ihrer spezifischen Seite zu entwickeln, mit dem einzigen Ziel, die Anzahl der betroffenen Personen zu erhöhen, die dazu verleitet werden, auf „Alles akzeptieren“ zu klicken. Ein ganzer Berufszweig hat sich um die sogenannte „Einwilligungsoptimierung“ (der neueste Euphemismus der Industrie für trügerische Konfigurationen) entwickelt.

Es ist die Verwendung unzähliger kleiner Designkonfigurationen, die von den verwendeten Farben über die Textauswahl bis hin zur Anordnung der Schaltflächen reichen, die in der Summe dazu führen, dass die Wünsche von bis zu 9 von 10 betroffenen Personen in das Gegenteil von dem verwandelt werden, was sie wirklich sind. Der freie Wille der Betroffenen stirbt einen „Tod durch tausend Stiche“.

Die Branche ist schockierend offen, was alle Möglichkeiten angeht, den betroffenen Personen jeden vernünftigen Weg zur Ausübung ihrer Rechte nach der DSGVO zu versperren. Wir haben daher verschiedene brancheninterne Ressourcen gesammelt, um die systematische, absichtliche und vorsätzliche Entwicklung sowie die Verwendung von „Dark Patterns“ mit dem alleinigen Ziel aufzuzeigen, die personenbezogenen Daten einer großen Anzahl von betroffenen Personen gegen ihren freien Willen zu verarbeiten.<sup>6</sup>

Schließlich gibt es keine technischen, ethischen oder anderweitig gültigen Gründe für die Verwendung dieser „Dark Patterns“. Der Verantwortliche hat jede Möglichkeit, Banner auf faire und transparente Weise zu gestalten, die mit der DSGVO konform sind. Eine Demonstration, wie der Verantwortliche die Möglichkeit hat, Consent

---

3 Durchschnittlich 119.417 erfasste Nutzer vor der Umsetzung im Vergleich zu 10.967 nach der Umsetzung, siehe <https://ico.org.uk/about-the-ico/our-information/disclosure-log/irq0873632/>.

4 Usercentrics: „Optimising the Opt-In Rate – A new discipline in online marketing“, Juni 2020, Seite 17.

5 Usercentrics Webinar bei ca. 30:00, <https://youtu.be/oux9uBUtscE?t=1800> – wahrscheinlich unter Bezug auf Utz, Degeling, Fahl, Schaub and Holz, (Un)informed Consent, § 4.5.1.

6 [Wird in der endgültigen Fassung der Beschwerde verfügbar sein]

Management Platforms („CMPs“) oder andere Banner mit ein paar einfachen Klicks gesetzeskonform zu konfigurieren, finden Sie in *noybs* Leitfaden für Verantwortliche.<sup>7</sup>

## 5. Konkrete Verstöße

Obwohl nicht alle Praktiken, die als „Dark Patterns“ diskutiert werden, immer einen klaren Verstoß gegen die DSGVO darstellen, hat der Verantwortliche, der mit dieser Beschwerde belangt wird, eindeutig gegen die DSGVO und/oder Artikel 5(3) ePrivacy-RL (oder das nationale Umsetzungsgesetz) verstoßen, und zwar auf folgende Weise:

### Verstoß Typ A: Keine „Ablehnen“-Option auf der ersten Ebene

Während das Banner eine Schaltfläche zum Akzeptieren aller relevanten Verarbeitungstätigkeiten und eine Schaltfläche, die der betroffenen Person den Zugriff auf weitere Optionen ermöglicht, bereitstellte, wurde die Option zum „Ablehnen“ der relevanten Verarbeitungstätigkeiten vom Verantwortlichen absichtlich ausgeblendet.

Das Ausblenden der „Ablehnen“-Option auf der ersten Ebene hat enorme Auswirkungen auf das Verhalten der Nutzer: Laut Branchenzahlen besuchen nur 2,18 % der betroffenen Personen die zweite Ebene,<sup>8</sup> was bedeutet, dass 97,82 % der betroffenen Personen nie die Option zur Ablehnung ihrer Einwilligung angezeigt wird. Genau wie 97,82 % der Nutzer wurde dem Beschwerdeführer auf der ersten Ebene nur die Option der Einwilligung angezeigt.

Was für den Beschwerdeführer nicht klar war: Bei der Konfrontation mit der ersten Ebene des Banners waren tatsächlich alle relevanten Verarbeitungstätigkeiten vorausgewählt - wenngleich nicht sichtbar für den Beschwerdeführer, sondern versteckt in der zweiten Ebene des Banners. Als der Beschwerdeführer akzeptierte, behandelte der Verantwortliche dies als Einwilligung zu allen versteckten vorausgewählten Optionen, auf der zweiten Ebene des Banners.

Um die Bearbeitung abzulehnen, hätte der Beschwerdeführer auf die Schaltfläche klicken müssen, die zu weiteren Optionen führt, was faktisch zwei Vorgänge auslöst: Zunächst (I.) deaktiviert er die vorausgewählten Optionen, die auf der zweiten Ebene angezeigt werden, und dann (II.) öffnet er die zweite Ebene. Nur der zweite Schritt ist für die betroffenen Personen sichtbar. Mit einem weiteren Klick kann der Beschwerdeführer dann die nun deaktivierten Optionen bestätigen. Mit anderen Worten: Der Beschwerdeführer kann die betreffende Verarbeitung mit einem Klick akzeptieren, benötigt aber zwei (oder mehr) Klicks, um die betreffenden Verarbeitungstätigkeiten zu deaktivieren und abzulehnen.

Der Verantwortliche hat die CMP absichtlich so eingestellt, dass eine „Ablehnen“-Option in der ersten Ebene des Banners ausgeblendet wird, obwohl eine „Ablehnen“-Schaltfläche im CMP-Setup vorhanden ist und mit einem einfachen Klick ein- und ausgeschaltet werden kann.<sup>9</sup> Es gibt keinen logischen, technischen oder ethischen Grund, die Option „Ablehnen“ zu verstecken, außer die betroffenen Personen zu verwirren oder Ablehnungen aufwändiger und unwahrscheinlicher zu machen.

Der Verantwortliche hat damit gegen die folgenden gesetzlichen Bestimmungen und Gerichtsentscheidungen verstoßen und die personenbezogenen Daten des Beschwerdeführers unrechtmäßig verarbeitet:

1. Das Verstecken einer „Ablehnen“-Option auf der ersten Ebene verstößt gegen die Grundsätze der „Verarbeitung nach Treu und Glauben“ und „Transparenz“ (Artikel 5(1)(a) DSGVO).
2. Das Ausblenden der vorausgewählten Optionen auf der zweiten Ebene und das Nichtanzeigen in der ersten Ebene verstößt ebenfalls gegen „Treu und Glauben“ und „Transparenz“ (Artikel 5(1)(a) DSGVO).
3. Eine Einwilligung ohne die Kenntnis der Möglichkeit, die Verarbeitung auf der zweiten Ebene abzulehnen, kann keinesfalls als „informiert“ angesehen werden (Artikel 4(11) DSGVO) und daher ist Artikel 6(1)(a) DSGVO als Rechtsgrundlage unwirksam.
4. Eine Einwilligung, auf der ersten Ebene, in alle Optionen, die auf der zweiten Ebene versteckt sind, ist eindeutig nicht „für den bestimmten Fall“ (Artikel 4(11) DSGVO) und daher ist Artikel 6(1)(a) DSGVO als Rechtsgrundlage unwirksam.

<sup>7</sup> Siehe Leitfaden unter <https://wecomply.noyb.eu/FAQs>.

<sup>8</sup> Usercentrics: „Optimising the Opt-In Rate – A new discipline in online marketing“, Juni 2020, Seite 5.

<sup>9</sup> Siehe Leitfaden unter <https://wecomply.noyb.eu/FAQs>.

5. Das Verstecken einer „Ablehnen“-Option (die von 97 % aller Besucher, einschließlich des Beschwerdeführers, nicht einmal aufgesucht wird) kann keine echte Anzeige von Wahlmöglichkeiten darstellen. Dies hat zur Folge, dass die eingeholte Einwilligung nicht „freiwillig“ gegeben wurde (Artikel 4(11) DSGVO) und daher ist Artikel 6(1)(a) DSGVO als Rechtsgrundlage unwirksam.
6. Eine Einwilligung auf der ersten Ebene (i) ohne Kenntnis der vorausgewählten Optionen auf der zweiten Ebene (ii) ohne zu wissen, um welchen Zweck es bei der Verarbeitung geht, ist eindeutig nicht „in informierter Weise“ (Artikel 4(11) und 13(1)(c) DSGVO), wie der EUGH in Randnummer 55 von C-673/17- Planet 49 entschieden hat und daher ist Artikel 6(1)(a) DSGVO als Rechtsgrundlage unwirksam.
7. Eine Einwilligung in vorausgewählte Optionen (auf der zweiten Ebene) ist zudem keine „Willensbekundung“ der betroffenen Person, wie der EuGH in C-673/17- Planet 49 entschieden hat und ist daher unwirksam gemäß Artikel 4(11) und 6(1)(a) DSGVO.
8. In Analogie zu Artikel 7(3) DSGVO (wonach die Einwilligung genauso leicht zu widerrufen wie zu erteilen sein muss) ist es erforderlich, dass die Verweigerung der Einwilligung genauso einfach ist wie die Erteilung der Einwilligung. Andernfalls ist die betroffene Person gezwungen, zunächst ihre Einwilligung zu erteilen, bevor sie dann die Möglichkeit hat, diese Einwilligung einfach zu widerrufen. Dies kann vernünftigerweise nicht die Absicht des Gesetzgebers sein. Folglich muss im Wege der Analogie die Verweigerung einer erbetenen Einwilligung genauso einfach sein wie die Erteilung der Einwilligung selbst.
9. Gemäß Artikel 12(2) DSGVO muss der Verantwortliche die Ausübung der Rechte des Beschwerdeführers „erleichtern“, was den Widerruf der Einwilligung gemäß Artikel 17(1)(b) DSGVO und analog auch die Verweigerung der Einwilligung einschließt (siehe (8) oben). Der Verantwortliche hat gegen diese Verpflichtung verstoßen, indem er auf der ersten Ebene des Banners keine „Ablehnen“-Option angeboten hat.
10. Schließlich hat der EuGH in Randnummer 50 des Urteils C-61/19 - Orange Romania festgestellt, dass die freie Entscheidung sich der Sammlung und Aufbewahrung von Daten zu widersetzen, durch einen Verantwortlichen ungebührlich beeinträchtigt wird, wenn dieser Verantwortliche verlangt „dass der betroffene Kunde schriftlich erklärt, weder in die Sammlung noch in die Aufbewahrung [...] [seiner Daten] einzuwilligen“.

Wir verweisen unter anderem auch auf die Leitlinien der französischen CNIL,<sup>10</sup> die ausdrücklich betonen, dass eine „Alle ablehnen“-Option in der ersten Ebene der Banner bereitgestellt werden muss oder sollte.

## Verstoß Typ C: Irreführendes Linkdesign

Der Button, der zu der Option führt, die relevanten Verarbeitungstätigkeiten abzulehnen, verwendet ein „Linkdesign“ (hervorgehobener oder unterstrichener Text), während die Schaltfläche „Alles akzeptieren“ ein typisches „Button-Design“ (rechteckiges Feld mit Text darauf) verwendet.

Es ist gängige Praxis, dass Links verwendet werden, um einen bloßen Verweis auf eine andere Seite anzuzeigen (z. B. eine Datenschutzerklärung oder andere Informationen), aber in der Regel nicht auf eine Auswahl oder ein interaktives Element hinweisen, wie eine Schaltfläche. Indem „Alles akzeptieren“ als einzige eindeutig interaktive Option in einem „Button-Design“ angezeigt wurde, wurde die betroffene Person folglich zu der Annahme verleitet, dass es keine andere Option als „Alles akzeptieren“ gibt, insbesondere wenn sie nur einen kurzen Blick auf das Banner wirft.

Der Verantwortliche hat die CMP bewusst so eingestellt, dass sie Links anstelle von Schaltflächen anzeigt, um diesen Effekt zu erzielen, was mit einem einfachen Klick geändert werden könnte.<sup>11</sup> Es gibt keinen anderen logischen, technischen oder ethischen Grund, der eine solche Gestaltungsoption erklären könnte, außer die betroffenen Personen zu verwirren oder Ablehnungen aufwändiger und unwahrscheinlicher zu machen.

Der Verantwortliche hat damit gegen die folgenden Rechtsvorschriften verstoßen und die personenbezogenen Daten des Beschwerdeführers unrechtmäßig verarbeitet:

<sup>10</sup> Délibération n° 2020-092 « recommandation » (<https://www.cnil.fr/sites/default/files/atoms/files/recommandation-cookies-et-autres-traceurs.pdf>).

<sup>11</sup> Siehe Leitfaden <https://wecomply.noyb.eu/> unter „FAQs“.

1. Eine „Ablehnen“-Option als bloßen Link zu gestalten, während die „Alles akzeptieren“-Option als Button gestaltet ist und dadurch suggeriert wird, dass dies die einzige interaktive Option ist, verstößt gegen die Prinzipien von „Treu und Glauben“ und „Transparenz“ (Artikel 5(1)(a) DSGVO).
2. Eine Einwilligung ohne klare Kenntnis einer interaktiven Möglichkeit, die Verarbeitung abzulehnen, ist eindeutig nicht „in informierter Weise“ oder „unmissverständlich“ (Artikel 4(11) DSGVO) und daher ist Artikel 6(1)(a) DSGVO als Rechtsgrundlage unwirksam.
3. Wenn die betroffene Person eindeutig dazu verleitet wird, ihre Einwilligung zu geben, anstatt sie zu verweigern, ist der geäußerte Wunsch offensichtlich nicht „unmissverständlich“ (Artikel 4(11) DSGVO) und daher ist Artikel 6(1)(a) DSGVO als Rechtsgrundlage unwirksam.
4. Das Verstecken einer Option vor der betroffenen Person, einschließlich des Beschwerdeführers, hat zur Folge, dass die eingeholte Einwilligung nicht „freiwillig“ erteilt wurde, da keine echte Wahlmöglichkeit angezeigt wurde (Artikel 4(11), Artikel 5(1)(a) DSGVO).

## Verstoß Typ D: Irreführende Button-Farben

Der Verantwortliche hat unterschiedliche Farben für die verschiedenen Optionen verwendet, die dem Beschwerdeführer präsentiert wurden. Der HEX-Code der anklickbaren Optionen innerhalb des Banners war der folgende:

**Banner-Hintergrund:** #3A1443

**„Annehmen“-Button:** #FFFFFF (Textfarbe) #30A93F (Buttonfarbe)

**„Weitere Details“-Button:** #DD97DD (Textfarbe) #3A1443 (Buttonfarbe)

Dies führt zu einer deutlichen Hervorhebung der Schaltfläche „Alles akzeptieren“ gegenüber den anderen verfügbaren Optionen, was einer betroffenen Person signalisiert, dass dies die erwartete Aktion und der einzige „einfache Ausweg“ ist, vor allem, wenn sie nur einen kurzen Blick auf das Banner wirft.

Der Verantwortliche hat die CMP absichtlich so eingestellt, dass solche Farben verwendet werden, auch wenn die CMP es ermöglicht, diese Farben mit einem einfachen Klick in ein ausgewogenes Design zu ändern. Es gibt keinen logischen, technischen oder ethischen Grund für die Verwendung solcher Schaltflächenfarben, außer dass sie die betroffenen Personen verwirren oder Ablehnungen aufwändiger machen.

Der Verantwortliche hat damit gegen die folgenden Rechtsvorschriften verstoßen und die personenbezogenen Daten des Beschwerdeführers unrechtmäßig verarbeitet:

- Die Hervorhebung der Option „Alle akzeptieren“ gegenüber anderen Optionen verstößt gegen die Prinzipien von „Treu und Glauben“ und „Transparenz“ (Artikel 5(1)(a) DSGVO).
- Wenn die betroffene Person eindeutig dazu veranlasst wird, die Einwilligung zu erteilen, anstatt sie zu verweigern, ist der geäußerte Wunsch offensichtlich nicht „unmissverständlich“ (Artikel 4(11) GDPR) und daher ist Artikel 6(1)(a) DSGVO als Rechtsgrundlage unwirksam.

## Verstoß Typ E: Irreführender Button-Kontrast

Der Verantwortliche hat unterschiedliche Kontrastverhältnisse für die verschiedenen Optionen verwendet, die dem Beschwerdeführer präsentiert wurden. Der HEX-Code der Optionen innerhalb des Banners war der folgende:

**Banner Hintergrund:** #3A1443

**„Akzeptieren“-Button:** #FFFFFF (Textfarbe) #30A93F (Buttonfarbe)

**„Weitere Einstellungen“-Button:** #DD97DD (Textfarbe) #3A1443 (Buttonfarbe)

Das Kontrastverhältnis zwischen dem „Akzeptieren“-Button und dem Hintergrund ist 5.05 und das Kontrastverhältnis zwischen dem Button „Weitere Einstellungen“ und dem Hintergrund ist 1.0. Dies führte zu einer deutlichen Hervorhebung der Option „Alle akzeptieren“ gegenüber der Option „Weitere Einstellungen“.

Es ist bemerkenswert, dass das vom Verantwortlichen verwendete Kontrastverhältnis sogar unter dem extrem großzügigen (und ebenfalls rechtswidrigen) selbst auferlegten Branchenstandard liegt, den das Interactive

Advertising Bureau (IAB) in seinem „Transparency and Consent Framework“ (TCF) mit 5:1 als absolutes Minimum für Texte festgelegt hat,<sup>12</sup> was für Buttons gleichermaßen gelten muss.

Das Kontrastverhältnis, das der Verantwortliche verwendet, liegt zudem unter den Mindeststandards des W3C für die Zugänglichkeit von Webinhalten (WCAG 2.0), die bei Texten zumindest einen Mindestkontrast von 4,5:1 fordern,<sup>13</sup> was für Buttons gleichermaßen gelten muss.

Es gibt keinen logischen, technischen oder ethischen Grund für die Verwendung solcher Kontraststraten, außer dass sie die betroffenen Personen verwirren oder Ablehnungen aufwändiger machen.

Der Verantwortliche hat damit gegen die folgenden gesetzlichen Bestimmungen verstoßen und die personenbezogenen Daten des Beschwerdeführers unrechtmäßig verarbeitet:

1. Die Hervorhebung der Option „Alle akzeptieren“ gegenüber anderen Optionen verstößt gegen die Prinzipien von „Treu und Glauben“ und „Transparenz“ (Artikel 5(1)(a) DSGVO).
2. Wenn die betroffene Person eindeutig dazu veranlasst wird, die Einwilligung zu erteilen, anstatt sie zu verweigern, ist der geäußerte Wunsch offensichtlich nicht „unmissverständlich“ (Artikel 4(11) DSGVO) und daher ist Artikel 6(1)(a) DSGVO als Rechtsgrundlage unwirksam.

## Verstoß Typ H: Vermeintliche berechnete Interessen

Der Verantwortliche hat sich für die relevanten Verarbeitungstätigkeiten (nämlich "Select basic ads", "Create a personalised ads profile", "Select personalised ads", "Create a personalised content profile", "Select personalised content", "Measure ad performance", "Measure content performance", "Apply market research to generate audience insights", "Develop and improve products", "Personalised ads and content, ad and content measurement, audience insights and product development", "Use precise geolocation data", "Actively scan device characteristics for identification") auf berechnete Interessen gemäß Artikel 6(1)(f) DSGVO berufen, obwohl in Wirklichkeit kein überwiegendes berechnetes Interesse für diese Verarbeitungstätigkeiten besteht. Der EDSA hat wiederholt klargestellt, dass an diesen Zwecken generell kein berechnetes Interesse besteht (siehe EDSA-Leitlinien 8/2020 „on the targeting of social media users“ (zum Zeitpunkt der Beschwerdeerstellung bestand noch keine offizielle Übersetzung ins Deutsche), Randummern 43 bis 50; Artikel-29-Datenschutzgruppe, WP 251 rev.01, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling, Seite 16 oder WP 217, zum Begriff des berechneten Interesses, Seite 41 und 62).

Während die Option zur Einwilligung an prominenter Stelle auf dem Banner erscheint, gab es auf der ersten Ebene keine Option zum „Widerspruch“ und keine andere Möglichkeit, die Ausübung des Widerspruchsrechts zu erleichtern. Die einzige Möglichkeit, einem solchen angeblichen berechneten Interesse zu widersprechen, war in den tieferen Ebenen des Banners versteckt, die von den betroffenen Personen kaum überprüft werden. Nach Zahlen der Branche besuchen nur 2,18 % der betroffenen Personen die zweite Ebene,<sup>14</sup> was bedeutet, dass 97,82 % der betroffenen Personen nie die Option zum Widerspruch angezeigt wird. Wie 97,82 % der Nutzer wurde dem Beschwerdeführer nur die Option „Annehmen“ auf der ersten Ebene angezeigt. Zusammenfassend lässt sich sagen, dass der Verantwortliche die Möglichkeiten, auf das Recht auf Datenschutz zu verzichten, stark „erleichtert“ hat, die Möglichkeit, das Recht auf Datenschutz auszuüben, jedoch bewusst verbirgt.

Da das Banner nur die Optionen nach Artikel 6(1)(a) DSGVO auf der ersten Ebene hervorhebt, aber keine Option zum Widerspruch nach Artikel 21 DSGVO enthält, verleitet der Verantwortliche die betroffene Person weiterhin zu der Annahme, dass sie keine Optionen in Bezug auf Artikel 6(1)(f) DSGVO hat.

Es ist außerdem völlig absurd anzunehmen, dass eine betroffene Person, die z.B. die Einwilligung zu diesen Verarbeitungsvorgängen verweigern würde, nicht auch der Verarbeitung gemäß Artikel 21 DSGVO widersprechen würde. Das Banner scheint jedoch davon auszugehen, dass betroffene Personen denselben Wunsch, ihre Daten nicht verarbeiten zu lassen, zweimal äußern müssen: Einmal als Ablehnung der Einwilligung und dann als zusätzlicher Widerspruch zu derselben Verarbeitungstätigkeit (was ein „Double Opt-out“ darstellt). Da die

---

12 Siehe [https://iabeurope.eu/wp-content/uploads/2020/11/TCF\\_v2-0\\_Policy\\_version\\_2020-11-18-3.2a.docx-1.pdf](https://iabeurope.eu/wp-content/uploads/2020/11/TCF_v2-0_Policy_version_2020-11-18-3.2a.docx-1.pdf) Seite 68: „ein minimales Kontrastverhältnis von 5 zu 1“.

13 Siehe <https://www.w3.org/TR/WCAG20-TECHS/G18.html>: „Sicherstellen, dass ein Kontrastverhältnis von zumindest 4.5:1 zwischen Text (und Bildern von Text) und dem Hintergrund unter dem Text besteht.“

14 Usercentrics: „Optimising the Opt-In Rate – A new discipline in online marketing“, Juni 2020, Seite 5.

Rechtsgrundlage für die Verwendung von Cookies, die nicht notwendig sind, immer die Einwilligung sein sollte, ist das berechtigte Interesse des Verantwortlichen in diesem Fall nicht relevant.

Es gibt keinen logischen, technischen oder ethischen Grund, sich auf berechtigte Interessen zu berufen, außer dass das Recht der betroffenen Personen, ihre Wünsche in einem „Opt-in“-System auf der Grundlage von Artikel 6(1)(a) DSGVO zu äußern, verhindert wird und stattdessen unrechtmäßig zu einem „Opt-out“-System gemäß Artikel 6(1)(f) DSGVO übergegangen wird.

Der Verantwortliche hat damit gegen die folgenden gesetzlichen Bestimmungen und Gerichtsentscheidungen verstoßen und die personenbezogenen Daten des Beschwerdeführers unrechtmäßig verarbeitet:

1. Rechtsgrundlage für die Speicherung von und den Zugriff auf Informationen, die in Endgeräten gespeichert sind, ist gemäß Artikel 5(3) ePrivacy-Richtlinie immer die Einwilligung gemäß Artikel 6(1)(a) DSGVO. Liegt keine Einwilligung vor, ist die Verarbeitung der Daten und die Verwendung des Cookies rechtswidrig. Einzige Ausnahme sind Verarbeitungen zum Zwecke der Übermittlung oder Erbringung des Dienstes.
2. Die Rechtsgrundlage, auf die sich der Verantwortliche beruft (Artikel 6(1)(f) DSGVO), ist für die betreffenden Verarbeitungen nicht gegeben. Es liegt weder ein berechtigtes Interesse vor, noch in irgendeiner Form ein Interesse, das die Interessen des Beschwerdeführers bei einer Abwägung überwiegen würde. Daher hat der Verantwortliche gegen Artikel 6(1) DSGVO verstoßen.
3. Der Verantwortliche hat den Widerspruch gegen die Verarbeitung nicht erleichtert, sondern die entsprechenden Optionen in tieferen Ebenen versteckt und damit gegen Artikel 12(2) DSGVO verstoßen.
4. Der Verantwortliche hat die betroffene Person bei der ersten Mitteilung nicht ausdrücklich, klar und gesondert auf das Widerspruchsrecht hingewiesen und damit gegen Artikel 21(4) DSGVO verstoßen.
5. Das Ausblenden der Option, der Verarbeitung auf der Grundlage von Artikel 6(1)(f) DSGVO als Rechtsgrundlage zu widersprechen, während die Option der Einwilligung gemäß Artikel 6(1)(a) DSGVO deutlich sichtbar angezeigt wird, verstößt gegen die Prinzipien von „Treu und Glauben“ und „Transparenz“ gemäß Artikel 5(1)(a) DSGVO.
6. Die Auslegung einer Ablehnung nur als Ablehnung der Einwilligung gemäß Artikel 6(1)(a) DSGVO, nicht aber als Ablehnung jeglicher Verarbeitung für die genannten Zwecke, einschließlich eines Widerspruchs gemäß Artikel 21 DSGVO, ignoriert offensichtlich die klaren Wünsche der betroffenen Person und verstößt daher gegen das Prinzip von „Treu und Glauben“ gemäß Artikel 5(1)(a) DSGVO.

## **Verstoß Typ K: Widerruf der Einwilligung ist nicht so einfach wie ihre Erteilung**

Die Möglichkeit, in die relevanten Verarbeitungstätigkeiten einzuwilligen, ist im Banner prominent dargestellt. Der Beschwerdeführer konnte jedoch nicht ohne Weiteres eine Option zum Widerruf der Einwilligung finden. Es gab kein auffälliges „Widerruf“-Banner oder eine ähnliche Möglichkeit.

OneTrust bietet zwar die Möglichkeit, auf allen Seiten ein kleines Symbol einzublenden, mit dem betroffene Personen zu ihren Datenschutzeinstellungen zurückkehren können, wo sie ihre Einwilligung widerrufen können. Der Verantwortliche diese Option jedoch bewusst nicht aktiviert.

Es gibt keinen logischen, technischen oder ethischen Grund, die Option zum Widerruf der Einwilligung zu deaktivieren, abgesehen davon, dass die betroffenen Personen daran gehindert werden soll, ihr Recht auf Widerruf gemäß Artikel 7(3) DSGVO auszuüben.

Der Verantwortliche hat damit gegen die folgenden gesetzlichen Bestimmungen verstoßen und die personenbezogenen Daten des Beschwerdeführers unrechtmäßig verarbeitet:

1. Das Fehlen einer auffälligen und ständig sichtbaren Option zum Widerruf der Einwilligung verstößt gegen die Grundsätze der Transparenz und der Verarbeitung nach Treu und Glauben gemäß Artikel 5(1) (a) GDPR.
2. Das Fehlen einer auffälligen und ständig sichtbaren Option zum Widerruf der Einwilligung verstößt gegen das Erfordernis gemäß Artikel 7(3) DSGVO, den Widerruf so einfach zu gestalten wie die Erteilung der Einwilligung.
3. Das Fehlen einer Option zum Widerruf der Einwilligung in „leicht zugänglicher Form“ verstößt gegen Artikel 12(1) und 17(1)(b) DSGVO.

## **6. Anträge**

### **6.1. Untersuchung**

Der Beschwerdeführer beantragt hiermit, dass die zuständigen Aufsichtsbehörden die Beschwerde gemäß Artikel 58(1) DSGVO vollständig und zügig untersuchen.

Im Interesse der Vollständigkeit dieser Beschwerde und im Einklang mit dem geltenden Verfahrensrecht haben wir nur alle relevanten Informationen zur Unterstützung der Beschwerde, so wie sie eingereicht wurde, beigefügt und verlinkt. Sollte der Verantwortliche in weiterer Folge rechtliches oder faktisches Vorbringen erstatten oder eine Aufsichtsbehörde weitere Informationen benötigen, behalten wir uns das Recht vor, den zuständigen Aufsichtsbehörden weitere Details, Argumente oder Beweise zu übermitteln, die im Laufe des Verfahrens relevant werden könnten.

### **6.2. Feststellung, dass die Rechte der betroffenen Personen verletzt wurden**

Aufgrund der formellen Anforderung des § 24(2)Z5 DSG beantragt der Beschwerdeführer die Feststellung, dass die Rechte des Beschwerdeführers wie oben behauptet verletzt wurden.

### **6.3. Anordnung, alle unrechtmäßigen Verarbeitungen zu stoppen und vorhandene Daten zu löschen**

Wie in Artikel 17, 19 und 58(2)(f) DSGVO vorgesehen, fordert der Beschwerdeführer, dass die zuständige Aufsichtsbehörde den Verantwortlichen anweist, alle relevanten Verarbeitungstätigkeiten einzustellen, alle relevanten personenbezogenen Daten zu löschen und die Löschung allen Empfängern mitzuteilen, denen die Daten offengelegt wurden.

Wir möchten betonen, dass die DSGVO der zuständigen Aufsichtsbehörde erlaubt, eine Anordnung zu treffen, die über die personenbezogenen Daten des Beschwerdeführers hinausgeht, da potenziell Tausende anderer betroffener Personen gleichermaßen von den relevanten Verarbeitungstätigkeiten betroffen sind. Eine Anordnung zur weitgehenden Löschung aller relevanten Daten stellt auch sicher, dass der Verantwortliche und andere Dritte nicht weiter von unrechtmäßig erlangten personenbezogenen Daten profitieren können.

### **6.4. Antrag auf Verhängung einer wirksamen, verhältnismäßigen und abschreckenden Geldbuße**

Der Beschwerdeführer beantragt gemäß Artikel 58(2)(i) und Artikel 83(5) DSGVO die Verhängung einer wirksamen, verhältnismäßigen und abschreckenden Geldbuße in Höhe von bis zu 20 Millionen Euro oder 4 % des weltweiten Jahresumsatzes, wobei Folgendes zu berücksichtigen ist:

1. Die Schwere des Verstoßes in Anbetracht der Tatsache, dass die Rechte der betroffenen Personen strukturell und umfassend verletzt wurden (Artikel 83(2)(a) DSGVO);
2. Die potenziell große Anzahl betroffener Personen, die über einen langen Zeitraum hinweg gleichermaßen von der technischen Umsetzung des Verantwortlichen betroffen waren (Artikel 83(2)(a) DSGVO);
3. Der fortwährende vorsätzliche Verstoß trotz der Warnung durch *noyb* und der vorgeschlagenen Lösung des Verstoßes, was einem wissentlichen Verstoß gegen das Gesetz gleichkommt (Artikel 83(2)(b) DSGVO);
4. Die einfachen technischen Möglichkeiten zur Behebung des Verstoßes und das Softwaredesign, die den Kerngedanken des „Datenschutz durch Technikgestaltung“ gemäß Artikel 25(1) DSGVO verletzen (Artikel 83(2)(b) DSGVO);
5. Die Verarbeitung und Weitergabe hochsensibler Daten über die Online-Kommunikation der betroffenen Person (Artikel 83(2)(g) DSGVO);
6. Die Tatsache, dass die Aufsichtsbehörde trotz Kenntnis des Verantwortlichen erst durch eine Beschwerde auf den Verstoß aufmerksam wurde (Artikel 83(2)(h) DSGVO); und

7.D ie Verwendung und Weitergabe von Tracking-Daten für einen Wettbewerbsvorteil und finanziellen Gewinn (Artikel 83(2)(k) DSGVO).

Zusammenfassend lässt sich sagen, dass der Verantwortliche einen vorsätzlichen, massiven, strukturellen und tiefgreifenden Verstoß begangen hat, der zu finanziellen und wettbewerblichen Vorteilen durchgeführt wurde und der trotz vorheriger Abmahnungen an den Verantwortlichen zusammen mit einer „Schonfrist“ zur Beseitigung des Problems fortgesetzt wurde. Daher muss die Geldbuße wirksam und abschreckend sein (Artikel 83(1) DSGVO), was auch eine klare Botschaft an andere Verantwortliche senden sollte (Generalprävention).

## **7. Sonstiges**

### **7.1. Sprachen**

Da sich höchstwahrscheinlich verschiedene Aufsichtsbehörden mit dieser Beschwerde befassen werden, haben wir den Schritt unternommen, eine informelle englische Übersetzung dieser Beschwerde bereitzustellen. Die Übersetzung dient nur der Vereinfachung der Arbeit der Aufsichtsbehörde und ist für *noyb* nicht verbindlich. Sollte es einen Konflikt zwischen den Übersetzungen geben, sollte die Originalversion Vorrang haben, da sie in der gesetzlich vorgeschriebenen Sprache abgefasst ist und die einzige sein sollte, die für dieses Verfahren zu berücksichtigen ist.

### **7.2. Anwendbares Verfahrensrecht**

Wir möchten betonen, dass diese Beschwerde in Übereinstimmung mit dem geltenden österreichischen Verfahrensrecht (AVG) eingereicht wurde und wir uns vorbehalten, alle unsere Verfahrensrechte nach dem AVG zu einem späteren Zeitpunkt geltend zu machen - unabhängig von der Zuständigkeit einer möglichen federführenden Aufsichtsbehörde.

### **7.3. Kontakt**

Die Kommunikation zwischen *noyb* und einer Aufsichtsbehörde sowie dem Verantwortlichen im Zuge dieses Verfahrens sollte per E-Mail an [E-Mail-Adresse wird in der endgültigen Fassung der Beschwerde bereitgestellt] unter Angabe der Fallnummer (C-) erfolgen. Wir sind auch unter [Telefonnummer wird in der endgültigen Fassung der Beschwerde bereitgestellt] erreichbar.