This is a draft version of the complaint. The final version filed with the relevant authority may depart from this draft and will include all exhibits and personal details that are not included here.

Complaint under Article 77 GDPR

Our Case Number: [redacted]
Complainant: [The identity of the Complainant will be made available in the final complaint]
Controller: [redacted]
Currently Assumed LSA: Datatilsynet (Denmark)

The Complainant is represented by the Austrian non-profit *noyb* – European Center for Digital Rights, Goldschlagstraße 172/4/3/2, 1140 Vienna, Austria under Article 80(1) GDPR. The representation agreement is attached as Exhibit 1.

noyb has contacted the Controller to highlight the issues in this complaint. To limit the workload for all parties we have offered to abstain from filing this complaint, if the Controller chose to comply with the law. Regrettably, the Controller has not followed our suggestion.

1. Basic Facts

From 21-05-2021 to 21-05-2021 the Complainant visited the Controller's website [redacted]. The web page presented a "banner" of a Consent Management Platform ("CMP") provided by OneTrust. Screenshots of the website and the banner are attached as Exhibit 2.

A summary of all relevant settings within the OneTrust configuration files in the JSON format is attached as Exhibit 3.1 to 3.2 ("onetrust-domain.json" and "one-trust-configuration.json"). These files include all settings that the Controller has used to configure the banner.

By using this banner, the Controller tried to establish:

- a legal basis under Article 6(1) GDPR to process personal data of the Complainant and
- a legal basis under Article 5(3) ePrivacy Directive (or the relevant national implementation) and Article 6(1)(a) GDPR to store and/or gain access to information stored in the terminal equipment of the Complainant.

A detailed summary of all HTTP requests and responses ("processing" within the meaning of Article 4(2) GDPR) between the browser and the various servers during the visit of the Controller's website is attached as Exhibit 4 ("traffic.json"). Other forms of processing (other than HTTP requests and responses, like procssing of personal data via JavaScript) may have occurred in addition to these HTTP requests and responses.

In addition, the Complainant identified at least the following data flows that relate to information stored in the terminal equipment of the Complainant, within the meaning of Article 5(3) ePrivacy Directive and contained personal data within the meaning of Article 4(1) GDPR:

Domain	Name	Value	Details
.adnxs.com	icu		Used to select ads and limit the number of times a user sees a particular ad
.adnxs.com	uuid2		This information is used to select advertisements for delivery by the Platform
.doubleclick.net	IDE		Main tracking cookie for Google's

Domain	Name	Value	Details
			Doubleclick
.adform.net	uid		Effortless Modern Marketing - Unique identifier
.casalemedia.com	CMID		Advertisment tracking cookie from Casale Media
.casalemedia.com	CMPS		Advertisment tracking cookie from Casale Media
.casalemedia.com	CMST		Advertisment tracking cookie from Casale Media
.openx.net	i		OpenX uses this cookie to collect information about browsing habits for advertisment
.atdmt.com	ATN		ATDMT is a tracking cookie served by Facebook subsidiary Atlas Solutions and used as a third-party cookie by several websites
.spotxchange.com	audience		Advertisment tracking cookie

A detailed summary of all cookie data is attached as Exhibit 5.

In addition the Complainant was identifiable under a public IP address (188.), which also constitutes personal data.

We further refer to these processing activities as the "**relevant processing activities**".

2. Applicable Law

The Controller preformed a broad set of processing operations to deliver the entire web page. To the extent that the Controller processes personal data of the data subject, the GDPR applies to the relevant processing activities (be it via technologies like HTML code, various scripts, iframes, tracking pixels, local storage or cookies).

To the extent the Controller stored or gained access to data (be it personal or non-personal data) in the Complainant's terminal equipment, Article 5(3) ePrivacy Directive may apply as lex specialis instead of Article 6(1) GDPR to these limited processing operations, but not any processing thereafter.

The relationship between the GDPR and the ePrivacy Directive (or its national implementations) and the jurisdiction of Supervisory Authorities may be different for each processing operation and in each EU Member State (see EDPB Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR). We therefore rely on both legal instruments, their national implementations and all relevant processing activities for the purposes of this complaint.

3. Claimed Legal Basis

According to the banner the Controller relied on consent under Article 6(1)(a) GDPR and Article 5(3) ePrivacy, as well as legitimate interests under Article 6(1)(f) GDPR, to justify the relevant processing activities. However, no valid consent had been given by the Complainant and no legitimate interest existed.

4. Background: Deceptive Banners and "Dark Patterns"

Industry representative themselves claim that only about 3% of all data subjects genuinely want to consent to the use of their personal data for marketing purposes while independent studies show acceptance rates of 0.16% for neutral banners.[1] However, Controllers record consent rates of more than 90%.[2]

To achieve this staggering discrepancy, data subjects are confronted with hundreds of different banners that often have hundreds of individual options and links to endless legal texts. Reading each of these options and texts would take hours every day for the average user.

To navigate the internet efficiently, data subjects have to develop a standard "clicking strategy" to get rid of banners in a reasonable time, often within seconds. As data subjects are not realistically able to read the details of each and every banner, they instinctively identify common patterns (such as "highlighted button allows you to access the page"). Such deliberate information overload combined with only one easy way out ("accept all") leads to the often-discussed "consent fatigue". Contrary to some industry narratives, this is not a defect of the GDPR's consent model, but a deliberate attack on the idea of "freely given, specific, informed and unambiguous" consent.

The differences in consent rates based on design are mind-blowing: For example, the UK ICO has reported that it received about 90% less consents from users of ico.org.uk when it implemented its own guidance on GDPR compliant consent banners.[3] A whitepaper by the German CMP Usercentrics even explains how to increase consent rates by 39% with five simple changes,[4] meaning that 4 in 10 data subjects can be tricked into consenting by these design changes alone.

Contrary to any attempt to identify the true and accurate wishes of data subjects, controllers have developed various forms of deceptive practices to gain wholly unrealistic consent rates of up to 90%, through so-called "dark patterns".

In summary, Controllers follow a strategy to provide one easy way out ("accept all") while making every other option complicated. Such small design changes will lead to click rates that are at odds with anything that any reasonable Controller could understand as an accurate reflection of data subjects' true wishes.

Some of these approaches are systemic, like the fact that 25% of data subjects think that a website cannot be used without giving consent[5] or that users have had so many negative experiences when clicking anything but "accept all" on other pages that they do not even try these options anymore.

Other approaches are specific to a page, like when controllers actively use various tools (such as "A/B testing") and generate lots of data to develop increasingly deceptive systems on their specific page, with the sole aim of increasing the number of data subjects that are tricked into clicking "accept all". A whole profession has developed around so-called "consent optimization" (the industry's latest euphemism for deceptive configurations).

It is the use of countless small design configurations ranging from colors used to text chosen to button alignments that lead to a combined result of transforming the wishes of up to 9 of 10 data subjects to the opposite of what they truly are. The data subjects' free will is dying a "death by a thousand cuts".

The industry is shockingly open about all the options to obstruct any reasonable way for data subjects to exercise their rights under the GDPR. We have therefore collected various internal industry resources to show the systematic, deliberate and intentional development, as well as use of dark patterns with the sole aim to process the personal data of vast numbers of data subjects against their free will.[6]

---

1 See Usercentrics Webinar at about 30:00 (https://youtu.be/oux9uBUtscE?t=1800) and Utz, Degeling, Fahl, Schaub and Holz, (Un)informed Consent, Table 2

2 "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/

3 Average of 119,417 tracked users before the implementation compared to 10,967 after the implementation, see 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", June 2020, page 17;

5 Usercentrics Webinar at about 30:00, https://youtu.be/oux9uBUtscE?t=1800 – likely referring to Utz, Degeling, Fahl, Schaub and Holz, (Un)informed Consent, § 4.5.1

6 [Will be made available in final complaint]

Finally, there are no technical, ethical or otherwise valid reasons for using these dark patterns. The Controller has every possibility to design banners in a fair and transparent way and which complies with the GDPR. A demonstration of how the controller has the option to configure Consent Management Platforms ("CMPs") or other banners to comply with the law with a couple of simple clicks can be found in *noyb*'s guidelines for controllers.[7]

5. Concrete Violations

While not all practices that are debated as "dark patterns" may always constitute a clear violation of the GDPR, the Controller subject to this complaint, has clearly violated the GDPR and/or Article 5(3) of the ePrivacy Directive (or the national implementing law) in the following ways:

Violation Type D: Deceptive Button Colors

The Controller has used different colors for the various options that were presented to the complainant. The HEX-Code of the clickable options within the banner were the following:

Banner Background: #FFFFFF
Accept Button: #FFFFFF (Text Color) #008000 (Button Color)
Reject Button: #696969 (Text Color) #FFFFFF (Button Color)
More Details Button: #696969 (Text Color) #FFFFFF (Button Color)

This leads to a clear highlight of the "accept all" button over the other available options, which indicates to a data subject that this is the expected action and the only "easy way out", especially when taking only a short look at the banner.

The Controller has deliberately set the CMP to use such colors, even when the CMP allows changing these colors to a balanced design with a simple click. There is no logical, technical or ethical reason to use such button colors other than confusing data subjects or making refusals more burdensome.

The Controller has thereby violated the following legal provisions and unlawfully processed the Complainant's personal data:

- Highlighting the "accept all" option over other options violates the principle of “fairness” and “transparency” (Article 5(1)(a) GDPR).
- When the data subject is clearly led to give consent rather than refusing it, the expressed wish is obviously not "unambiguous" (Article 4(11) GDPR) and is therefore invalid under Article 6(1)(a) GDPR.

Violation Type E: Deceptive Button Contrast

The Controller has used different contrast ratios for the various options that were presented to the complainant. The HEX-Code of the options within the banner were the following:

Banner Background: #FFFFFF
Accept Button: #FFFFFF (Text Color) #008000 (Button Color)
Reject Button: #696969 (Text Color) #FFFFFF (Button Color)

The contrast ratio between the accept button and the background is 5.14 and the contrast ratio between the reject button and the background is 1.0. This lead to a clear highlight of the "accept all" option over the "reject all" option.

It is notable that the contrast ratio that the Controller uses is even below the extremely permissive (and regularly unlawful) self-imposed industry standard that the interactive advertising bureau (IAB) has set at 5:1 as a bare minimum in it's "Transparency and Consent Framework" (TCF) for texts,[8] which can be equally applied for buttons.

7 See guidelines available at https://wecomply.noyb.eu/FAQs;
8 See https://iabeurope.eu/wp-content/uploads/2020/11/TCF_v2-0_Policy_version_2020-11-18-3.2a.docx-1.pdf at page 68: “a minimum contrast ratio of 5 to 1”;

The contrast ratio that the Controller uses is further below the W3C's minimum standards for web content accessibility (WCAG 2.0), which requires a bare minimum contrast rate of 4.5:1 for texts ,[9] which can be equally applied for buttons.

There is no logical, technical or ethical reason to use such contrast rates, other than confusing data subjects or making refusals more burdensome.

The Controller has thereby violated the following legal provisions and unlawfully processed the Complainant's personal data:

1. Highlighting the "accept all" option over other options violates the principle of “fairness” and “transparency” (Article 5(1)(a) GDPR).
2. When the data subject is clearly led to give consent rather than refusing it, the expressed wish is obviously not "unambiguous" (Article 4(11) GDPR) and therefore invalid under Article 6(1)(a) GDPR.

Violation Type H: Legitimate Interests

The Controller relied on legitimate interests under Article 6(1)(f) GDPR for the relevant processing activities (namely [redacted]), when in fact no overriding legitimate interest exists for such processing activities. The EDPB has repeatedly clarified that there is generally no legitimate interest in these purposes (see EDPB Guidelines 8/2020 on the targeting of social media users, para 43 to 50, Article 29 Working Party, Opinion on profiling and automated decision making, WP 251, rev. 01, p. 15 or Article 29 WP, Opinion on legitimate interest, p. 32 and 48).

While the option to consent features prominently on the banner, there was no option to "object" on the first layer and no other way to facilitate the exercise the right to object. The only way of objecting to such an alleged legitimate interest, was hidden in the deeper layers of the banner, which are hardly reviewed by data subjects. According to industry numbers, only 2,18% of data subjects visit the second layer,[10] meaning that 97,82% of data subjects are never shown the option to object. Just like 97,82% of users, the Complainant was only shown the acceptance option on the first layer. In summary, the Controller greatly "facilitated" the options to give up the right to data protection, but is deliberately hiding the option to exercise the right to data protection.

As the banner only highlights the options under Article 6(1)(a) on the first layer but does not feature an option to object under Article 21 GDPR, the Controller further leads the data subject to believe that it has no options in respect of Article 6(1)(f) GDPR.

It is further wholly absurd to assume that a data subject that would e.g. reject to give consent to these processing operations but would not also object to the processing under Article 21 GDPR. However the banner seems to assume that data subjects need to express the same wish to not have their data processed twice: Once as a rejection of consent, and then as an additional objection, on the very same processing activity (constituting a "double opt-out"). Finally, since the legal basis for the use of cookies which are not necessary should always be consent, the legitimate interest of the controller is not relevant in this instance.

There is no logical, technical or ethical reason to rely on legitimate interests, other than preventing the data subjects' right to express their wishes in an "opt-in" system based on Article 6(1)(a) and instead unlawfully shift to an "opt-out" system under Article 6(1)(f) GDPR.

The Controller has thereby violated the following legal provisions and court decisions and unlawfully processed the Complainant's personal data:

1. Under Article 5(3) ePrivacy Directive, the legal basis for the storing and the gaining access to information stored in terminal equipment is always consent as per Article 6(1)(a) GDPR. In the absence of consent,

9 See https://www.w3.org/TR/WCAG20-TECHS/G18.html: “Ensuring that a contrast ratio of at least 4.5:1 exists between text (and images of text) and background behind the text.”;

10 Usercentrics: „Optimising the Opt-In Rate – A new discipline in online marketing”, June 2020, page 5;

the processing of data and the use of the cookie is illegal. The only exception are processing for the purpose of transmission or provision of the service.

2. The legal basis that the Controller claims to fall under (Article 6(1)(f) GDPR) is not available for the relevant processing activities. There is neither a legitimate interest at the outset, not in any form any interest that would be overriding the interests of the Complainant in any balancing test. Therefore, the Controller violated Article 6(1) GDPR.
3. The Controller has not facilitated the objection to the processing, but instead hid the relevant options in secondary layers, and thereby violated Article 12(2) GDPR.
4. The Controller has not explicitly, clearly and separately brought the right to object to the attention of the data subject at the time of the first communication and thereby violated Article 21(4) GDPR.
5. Hiding the option to object to processing based on Article 6(1)(f) GDPR as a legal basis, while prominently displaying the option to consent as per Article 6(1)(a) GDPR, violates the principles of “transparency” and “fairness” under Article 5(1)(a) GDPR.
6. Interpreting a rejection as only a rejection to consent under Article 6(1)(a) GDPR, but not as a rejection to any processing for the said purposes, including an objection under Article 21 GDPR is evidently ignoring the clear wishes by the data subject and therefore violates the principle of “fairness” under Article 5(1)(a) GDPR.

Violation Type I: Inaccurate Classification of Processing Activities and Cookies

The Controller has classified at least the following cookies and processing operations as "essential" or "strictly necessary":

Domain	Name	Value	Purpose
[redacted]	_gfp_64b	[redacted]	doubleclick.net

In fact, all of these processing operations and cookies use personal data and serve purposes which are evidently not "strictly necessary" within the meaning of Article 5(3) ePrivacy Directive or the ordinary meaning of "strictly necessary" or "essential" under the GDPR.

This classification seems to have also resulted in the processing of personal data and the storing and gaining access to information before the data subject had any interaction with the banner.

The Controller has thereby violated the following legal provisions and unlawfully processed the Complainant's personal data:

1. Storing and gaining access to information in terminal equipment that is not "strictly necessary" without consent of the data subject violates Article 5(3) ePrivacy Directive.
2. Conducting any (further) processing activities as "necessary" and without consent of the data subject violates Article 6(1) GDPR, as there is no legal basis for the said processing activities.
3. Misclassifying cookies and processing operations as "essential" or "strictly necessary" violates the principles of “fairness” and “transparency” (Article 5(1)(a) GDPR).
4. Misclassifying cookies and processing operations as "essential" or "strictly necessary" violates the transparency and information obligations of the Controller under Article 13(1)(c) GDPR.

Violation Type K: Not as easy to withdraw as to give consent

The option to agree to the relevant processing activities features prominently in the banner, however the Complainant was unable to easily find an option to withdraw consent. There was no prominent “withdraw” banner or any similar option.

While OneTrust provides an option to show a small icon on all pages that allows data subjects to return to their privacy settings, where they can withdraw their consent, the Controller has deliberately not activated this option.

There is no logical, technical or ethical reason to deactivate the option to withdraw consent, other than preventing data subjects to exercise their right to withdraw under Article 7(3) GDPR.

The Controller has thereby violated the following legal provisions and unlawfully processed the Complainant's personal data:

1. Not providing a prominent and continuously visible option to withdraw consent, violates the principles of “transparency” and “fairness” under Article 5(1)(a) GDPR.
2. Not providing a prominent and continuously visible option to withdraw consent, violates the requirement to make withdrawal as easy as to give consent under Article 7(3) GDPR.
3. Not providing an “easily accessible” option to withdraw consent, violates Articles 12(1) and 17(1)(b) GDPR.

6. Applications

6.1. Investigation

The Complainant hereby requests that the competent supervisory authorities fully and swiftly investigate the complaint under Article 58(1) GDPR.

In the interest of keeping this complaint comprehensive and in line with the applicable procedural law, we have only attached and linked all relevant information to support the complaint as it was filed. Should the Controller make further legal or factual submissions or any Supervisory Authority requires further information, we reserve the right to provide the relevant Supervisory Authorities with further details, legal or factual arguments or evidence that may become relevant in the course of the procedure.

6.2. Finding that the data subjects' rights have been violated

Given the formal requirement under § 24 Abs 2 Z5 of the Austrian Data Protection Act, the Complainant requests a finding that the data subjects' rights have been violated as alleged above.

6.3. Order to stop all unlawful processing and delete existing data

As foreseen in Articles 17, 19 and 58(2)(c) GDPR, the Complainant requests that the competent Supervisory Authority orders the Controller to stop all relevant processing activities, erase all relevant personal data and to communicate the erasure to all recipients to whom the data have been disclosed.

We would like to highlight that the GDPR allows the competent Supervisory Authority to make an order that goes beyond the personal data of the Complainant, given that potentially thousands of other data subjects are equally concerned by the relevant processing activities. An order to broadly delete all relevant data also ensures that the Controller and other third parties cannot further profit from unlawfully obtained personal data.

6.4. Request to impose an effective, proportionate and dissuasive fine

The Complainant requests, according to Articles 58(2)(i) and 83(5) GDPR, the imposition of an effective, proportionate and dissuasive fine of up to € 20 Million or 4% of the worldwide annual turnover, taking into account the following:

1. the gravity of the infringement, considering that the data subjects' rights were structurally and broadly violated (Article 83 (2)(a) GDPR);
2. the potentially large number of data subjects equally affected over a long period of time by the setup of the Controller (Article 83 (2)(a) GDPR);
3. the continuous intentional infringement despite the warning by *noyb* and proposed solution of the violation, which amounts to knowingly violating the law (Article 83(2)(b) GDPR);
4. the simple technical options to remedy the infringement and the software design that violate the very core idea of privacy by design as under Article 25(1) GDPR (Article 83(2)(c) GDPR);
5. the processing and sharing of highly sensitive data about the online communication of the data subject (Article 83(2)(g) GDPR);

6. the fact that the violation only came to the attention of the Supervisory Authority via a complaint, despite the knowledge of the Controller (Article 83(2)(h) GDPR); and
7. the use and sharing of tracking data for a competitive and financial gain (Article 83 (2)(k) GDPR);

In summary, the Controller engaged in an intentional, massive, structural and profound violation, conducted for financial and competitive advantages and which continued despite previous warnings to the Controller along with a "grace period" to overcome the issue. As such, the fine must be effective and dissuasive (Article 83(1) GDPR), which should also send a clear message to other Controllers (general deterrence).

7. Other

7.1. Languages

As different supervisory authorities will most likely deal with this complaint, we have taken the step to provide an informal English translation of this complaint. The translation is only provided for the convenience of the DPA and is not endorsed by *noyb*. Should there be any conflict in the translations, the original version should prevail, as it is legally required language and should be the only one to be taken into account for the sake of this procedure.

7.2. Applicable Procedural Law

We want to highlight, that this complaint was submitted in compliance with the applicable Austrian Procedural Law (AVG) and we reserve the right to rely on all our procedural rights under the AVG at a later stage - independent of the jurisdiction of a possible Lead Supervisory Authority.

7.3. Contact details

Communications between *noyb* and any Supervisory Authority as well as the Controller in the course of this procedure should be done via email at [email will be made available in final complaint], citing the case number (C-037-10924). We are also available at [phone number will be made available in final complaint].