Feedback to the European Data Protection Board's Guidelines 3/2025 on the interplay between the DSA and the GDPR (Version 1.1)

Dr. Lex Zard, Independent, The Netherlands, lex.zard@proton.me
Dr. Oana Goga, Inria, France, oana.goga@inria.fr
Asmaa El fraihi, Inria, France, asmaa.el-fraihi@inria.fr
Dr. Nataliia Bielova, Inria, France, nataliia.bielova@inria.fr

Dr. Lex Zard is an independent researcher focused on the *EU policy of online advertising*. He is a 2024-2025 Technology and Human Rights Fellow at Harvard Carr-Ryan Center for Human Rights Policy (United States), where he focused on the impact of online advertising on democracy. He defended his PhD thesis about the EU law of online advertising in May, 2024 at Leiden University (the Netherlands), where he also worked as a researcher and teacher since 2019. Lex has also worked as an external consultant to AWO, a digital rights agency, and is a major contributor of the forthcoming study on online advertising commissioned by the EU Commission.

Dr. Oana Goga is a Research Director at Inria (French Institute for Research in Computer Science and Automation) and a member of the Inria CEDAR team and the Laboratoire d'Informatique d'Ecole Polytechnique (LIX). She investigates risks for humans and society brought by online platforms and their deployments of AI, such as advertising technologies. She looks at risks ranging from privacy to disinformation and manipulation to child protection. Her research is interdisciplinary, and she works with economists, social scientists, and legal scholars. Her work has influenced European law, and she has served as an external expert for the European Commission on problems related to data access in the Digital Services Act (DSA). She received the CNRS Bronze Medal in 2024, the Lovelace-Babbage Award from the French Science Academy and the French Computer Society in 2023, and she received an ERC Starting Grant in 2022 that aims to measure and mitigate the impact of AI-driven information targeting. Her recent research received several awards, including the Andreas Pfitzmann Best Student Paper Award at PETS 2024, the Honorable Mention Award at The Web Conference in 2020, and the CNIL-Inria Award for Privacy Protection 2020.

Asmaa El fraihi is a PhD. Candidate at the computer science laboratory of the École Polytechnique in France, under the supervision of Oana Goga, specializing in algorithm auditing of online advertising systems. Her research combines experimental methods, data-driven analysis and real-world platform measurements to study how AI-driven targeting and delivery technologies exploit user data, influence behavior, and raise societal risks.

Dr. Nataliia Bielova is a Research Director in Computer Science at Inria (French Institute for Research in Computer Science and Automation). She is a privacy expert with a multidisciplinary background in *computer science and regulation*, investigating privacy and data protection on the Web. Dr. Bielova was a Senior Privacy Fellow at the French Data Protection Authority (CNIL) and an External Expert for the EU Commission for its implementation of the EU Digital Services Act (DSA). She received a Young Researcher Award from the French National Research Agency (ANR), the Rising Star award by Women at Privacy in 2023, the CNIL–Inria Privacy Award in 2025 and the Lovelace-Babbage Award from the French Science Academy and the French Computer Society in 2025.

Hereunder is our feedback to the EDPB Guidelines 3/2025 on the interplay between the DSA and the GDPR[1]. Our comments are presented after a quotation from the proposed text in a box. The highlights in **bold** were added by the authors.

> ## 2.4 Advertising transparency and prohibition of presenting advertisements based on profiling using special categories of data (Article 26)
>
> 48. Article 26 DSA lays down transparency rules for providers of online platforms regarding advertising and **prohibits providers of online platforms from presenting advertisements to recipients based on profiling using special categories of data** referred to in Article 9(1) GDPR.
>
> 49. Recital 68 of the DSA clarifies that the requirements under Article 26 DSA are without prejudice to the GDPR, ”in particular those regarding the right to object, automated individual decision-making, including profiling, and specifically the need to obtain consent of the data subject prior to the processing of personal data for targeted advertising”. It is also without prejudice to the provisions in the ePrivacy Directive, ”in particular those regarding the storage of information in terminal equipment and the access to information stored therein”.

Online advertising based on profiling

The DSA introduces the concept of **“online advertising based on profiling” (OABP)** for the first time. This notion requires further elaboration, as legal uncertainty remains regarding its scope. Under Article 4(4) GDPR, *profiling* is defined as *“any form of automated processing of personal data to evaluate certain personal aspects relating to an individual”.* We believe that OABP effectively encompasses **all forms of personalized advertising**, where user data is analyzed or inferred to tailor ad content or delivery. **Contextual advertising**—while it may also involve some processing of personal data—does not typically do so for the purpose of evaluating *personal aspects of the individual*, and therefore falls outside the scope of OABP. The key distinction, then, lies between:

- *contextual advertising*, which targets content based on the environment or context of display, and
- *personalized advertising*, which targets based on user-related data or inferred characteristics.

However, as we discuss further, advertising also comes in various forms that contain **significant risk to the individuals**. These include targeting based on inferred demographic, or interest traits, but also retargeting, lookalike targeting, and AI-based ad targeting and delivery methods (e.g. Performance Max campaigns). Without this clarification, the industry may continue to apply the DSA rules narrowly, excluding the most high-risk advertising practices from the scope of the regulation.

[1] https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/guidelines-32025-interplay-between-dsa-and-gdpr_en

Contextual micro-targeting

Our recent empirical work[2] on contextual advertising shows that advertisers can reach audiences associated with **special categories** of attributes as per GDPR (such as *religion*, *health conditions*, or *political orientation*) without processing personal data, and, therefore, engaging in *profiling* as legally defined under the GDPR. This is achieved by identifying content-based proxies—pieces of content that implicitly reveal sensitive traits, without singeling out users For instance, this research found that:

- An advertiser promoting a health supplement can target YouTube videos titled *"Coping with depression"*, which are likely to attract audiences experiencing or seeking information about the condition.
- A political advertiser can target curated YouTube channels (or online blogs) oriented toward *Christian*, *Muslim*, or *Jewish* audiences, with tailored or divisive political messages.

Such targeting uses contextual placement rather than *personal data*, we refer to it as **contextual micro-targeting.** The advertiser does not process or infer personal information; instead, they use the **content environment as a signal for audience characteristics**, which are not tied to the unique user. Technically, these proxies are easily discoverable (e.g. through search queries or APIs) and can be curated at scale, including with assistance of generative AI systems.

Similar mechanisms have been demonstrated in prior research[3] showing that contextual micro-targeting can be used to approximate age and **effectively target minors**. By selecting videos or channels clearly intended for children, advertisers can deliver ads without processing personal data, thereby **circumventing the legal restrictions on profiling-based advertising directed at children**.

Because **contextual micro-targeting** does not involve *automated processing of personal data* it may fall outside the current scope of the GDPR Article 9(1) and DSA Article 26. Yet, the outcome—reaching vulnerable audiences or audiences defined by special categories of attributes—is functionally equivalent to advertising based on profiling.

Implications of Contextual micro-targeting for Political advertising

This mechanism creates multiple avenues for potential abuse with significant societal implications. Contextual placements can be used for **ideological manipulation**, isolating audiences already engaged with fringe or polarizing material—such as conspiracy-theory content—thereby reinforcing echo chambers and amplifying extreme narratives.

Our analysis of **YouTube's advertising ecosystem** further illustrates these risks. We observed that political ads appear within the platform's Political Ads Transparency Center without disclosing the use of contextual targeting or the specific contextual signals applied (e.g.,

[2]Work under review: https://openreview.net/forum?id=AW3eMRqCya

[3] Medjkoune, Tinhinane, Oana Goga, and Juliette Senechal. "Marketing to children through online targeted advertising: Targeting mechanisms and legal aspects." Proceedings of the 2023 ACM SIGSAC conference on computer and communications Security. 2023. Available at https://www.lix.polytechnique.fr/Labo/Oana.GOGA/papers/children_ads_CCS2023.pdf

keywords or topics). In an empirical study[2] focusing on high-risk content environments, we found that **political ads were more likely to appear alongside conspiracy-theory videos** than in control environments, and that such ads more frequently *included references to "contextual" signals in their ad explanations*. While this analysis focused on a single platform, it underscores the broader potential of contextual micro-targeting and the ongoing opacity of ad-delivery mechanisms, even after the DSA has entered into effect.

Our recommendation
We conclude that the current definition of online advertising based on profiling, even when encapsulating all personalized advertising,is **narrow** and propose that the notion be revised to encompass not only the automated processing of personal data, but also any process undertaken by an advertiser or the platform (data controller) that aims to estimate, infer, or approximate a user's association with an attribute, whether the estimation relies on: • Direct personal data; • Inferred behavioral or contextual signals; • Probabilistic associations between the content, environment, or other proxies.

2.4.1 General advertising transparency obligations

50. Articles 13 and 14 GDPR define the information to be provided to the data subjects when their personal data are processed, and the modalities for doing so. These general rules are applicable to any data processing, including processing that could occur in the context of advertising on online platforms.

51. Article 26(1) DSA lays down transparency rules for providers of online platforms specifically regarding advertising. This provision states that information regarding each specific advertisement should be provided to the recipients of the service in real time. Additionally, meaningful information regarding **the main parameters** used to determine the recipient to whom the advertisement is presented and, where applicable, information about **how to change those parameters** as specified in Article 26(1)(d) DSA must be directly accessible from the advertisement.

52. It means that the elements of information mentioned in Article 26 DSA should be provided **in real time**, **directly accessible from the advertisement**, while information related to transparency obligations as set out in Articles 13 and 14 GDPR could be presented through the means of a privacy policy (e.g., one click away).

53. It also means that information required under Article 26 DSA would be provided after a processing of personal data may have occurred.

54. This is an important difference between Article 26 DSA and the transparency requirements under the GDPR, since the latter provides that in case of personal data collected directly from the data subject, information shall be provided at the time when personal data are obtained, as set out in Article 13(1) and 13(2) GDPR, before the processing takes place.

55. The transparency requirements under Article 26 DSA apply **irrespectively of the**

legal basis for processing under Article 6(1) GDPR by the provider of the online platform.

56. Moreover, if processing for advertising purposes is based on consent (Article 6(1)(a) GDPR), certain information regarding processing (including profiling) must already be provided to the individual before consent is collected. Additional information pursuant to Article 26(1)DSA would later be directly and easily accessible to the recipient from the advertisement.

57. According to Article 26(1)(d) DSA, "providers of online platforms that present advertisements on their online interfaces shall ensure that, for each specific advertisement presented to each individual recipient, the recipients of the service are able to identify, in a clear, concise and unambiguous manner and in real time […] **meaningful information** directly and easily accessible from the advertisement about the **main parameters used to determine the recipient to whom the advertisement is presented** and, where applicable, about how to **change those parameters**".

58. In its Recital 68, the DSA indicates that "Such explanations should include information on the method used for presenting the advertisement, for example whether it is contextual or other type of advertising, and, where applicable, the main profiling criteria used; it should also inform the recipient about any means available for them to change such criteria".

59. Article 4(4) GDPR defines profiling as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability behaviours, location or movements".

60. Indeed, providers of online platforms and other actors that gather information on preferences of users of an online platform in order to enable advertisements to be presented to them accordingly, often conduct profiling under the definition set out in Article 4(4) GDPR.

61. However, **Article 26(1) DSA also applies to forms of advertising that do not involve profiling and that may involve the processing of less (or no) personal data, e.g. general advertising**.

General comments on paragraphs 50-61

Article 26(1)(d) DSA establishes an important rule with significant societal implications: it seeks to ensure that users of online platforms understand how data about them is used for targeted advertising purposes, and, where possible, enables them to influence such use.
While the EDPB opinion on this provision usefully cites relevant articles and recitals of both the DSA and the GDPR, it offers *little concrete guidance* on how these legal norms should be interpreted and operationalised by online platforms and the ad tech intermediaries supporting them. This lack of specificity is problematic.

We believe that the i**ndustry standardisation initiatives** developed in response to Article 26(1)(d) DSA c**urrently fail to meet the rule's substantive requirements**. Absent further regulatory clarification, these initiatives risk creating an *illusion of compliance* and *trustworthiness*, leaving users worse off than before the DSA entered into force.

Some particularly very large online platforms (VLOPs) —such as **Facebook**, **Instagram**, **X**, and **YouTube**—operate as *"walled gardens."* These platforms provide advertisers or their media partners (e.g., agencies) with a **closed-loop advertising interface** that can be used to select audiences and apply various targeting methods. Such walled gardens typically do not rely on any third parties to deliver ads to users and therefore hold centralized, meaningful information about the methods and criteria used for ad delivery. In contrast, **smaller online platforms** generally depend on one or several third parties—such as **publisher ad servers**, **ad networks**, **supply-side platforms (SSPs)**, and **demand-side platforms (DSPs)**—to deliver advertising. In these cases, the **selection of targeting methods and criteria** takes place outside the online platform, typically on the DSP's side. To enable compliance with the transparency obligations under **Article 22(1) DSA**, these third parties must then pass relevant information back to the platform so that it can be shown to users.While Article 22(1) DSA formally applies to all online platforms, this structural distinction means that **compliance is a technically different process** for two types of platforms: (i) VLOPs who operate as "*walled gardens*" and (ii) for open-web platforms. Therefore, we address these two cases separately.

VLOPs and their implementation of main parameters for advertising

While the DSA has increased the visibility of ad parameters, user-facing transparency remains fragmented and insufficiently detailed among Very Large Online Platforms (VLOPs). Standardized, multi-layered disclosures are needed to make *"meaningful information"* operational and verifiable.

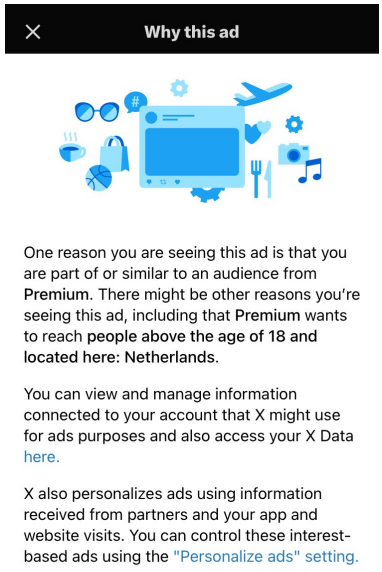


Figure 1. Screenshot of X ad transparency interface in the EU Oct 15, 2025

Our recent analysis of ad transparency interfaces[4] of several VLOPs (YouTube, X, Facebook and Instagram) shows that implementation of the provisions in DSA Article 26(1)(d) is inconsistent and incomplete:

- **Granularity:** the level of detail provided to users about the targeting criteria used to deliver the ads varies significantly across interfaces. For instance, on YouTube, Google provides only generic explanations (e.g. *"Because of your interests")*

- **Attribution of targeting and delivery choices:** users are almost never informed whether the targeting parameters stem from *advertiser-selected criteria* or from *platform-level inferences* and *optimizations*.

[4] Work under review: https://osf.io/596jx/files/srmtn?view_only=12e8946fc0f9465fa2b289e5c5d0f985

- **Data source clarity:** references to off-platform data such as cross-site behavioral data are seldom included.

- **Accuracy:** in several cases, we found that user-facing ad explanations omitted targeting types that are evidently used. For example, in an experiment conducted on YouTube, user profiles that had opted out of personalization (i.e. profiling and behavioral targeting) were presented ad explanations disclosing only "age" and "general location" as targeting parameters. However, the ads shown were found to be triggered by the search terms entered by the user profile, indicating the use of *contextual targeting that was not included* in the accompanying explanation.

Overall, these gaps demonstrate that the concept of **"meaningful information" is being interpreted differently across VLOPs.** Users therefore receive uneven, and sometimes misleading accounts of how ads are personalized.

Our recommendation

To align with the intent of DSA Article 26(1)(d), user facing ad explanations should at least:

- **Disaggregate targeting components**, distinguishing between:
  - Advertiser-declared parameters (e.g. demographic or interest-based criteria);
  - Platform-inferred signals (e.g. interests or affinities derived from user engagement or social connections);
  - Algorithmic delivery factors (e.g. performance-based optimization).
- **Specify provenance of each parameter** — whether derived from user-provided data, behavioral inference, or contextual cues.
- **Ensure completeness** even for contextual or non-personalized ads by disclosing the parameters (e.g. content topics, keywords) used to determine ad placement.

A harmonized schema of transparency—covering **parameter type**, **source**, and **decision-maker**—would make disclosures comparable across platforms and more intelligible to users.

It is also advisable that the **EDPB consider requiring disclosure of the actual values of the targeting criteria used**, rather than merely their general categories. Without this, transparency remains largely formal: users can see *which types* of parameters were applied, but not *how* those parameters were instantiated in practice. Disclosing the concrete values (for example, "location: Amsterdam" or "interest: budget travel") would enable meaningful scrutiny of targeting logic, facilitate detection of discriminatory or sensitive-data-based targeting, and ensure that Article 22(1) DSA delivers genuine rather than nominal transparency.

Open-web platforms and their implementation of main parameters for advertising

Often online platforms rely on third parties for ad delivery, especially when ad inventory is sold programatically on open auctions using OpenRTB protocol[5], proposing a concrete

[5] https://www.iab.com/guidelines/openrtb/

implementation of the *Real-Time Bidding or RTB*. Another group of protocols, called *Header Bidding (HB)* were recently introduced and is currently being significantly used.

Real-Time Bidding (RTB) is well-described in this 2012 publication[6]: "In the mid-2000s publishers began seeking ways to monetize the "remnant" inventory they were not able to sell through an ad network. Ad exchanges offered to fill the slots, in real time, taking bids from many advertisers via many advertising networks ("real-time bidding" or "RTB"). Ad exchanges quickly extended beyond remnants, and a number of intermediary business models now exist in the exchange ecosystem:

- *Demand-side platforms (DSPs)*, which are replacing ad networks as "virtual on-ramps" for advertisers to place bids in multiple ad exchanges.
- *Supply-side platforms (SSPs)* and yield optimizers, which assist publishers in strategically making inventory offerings to networks and exchanges so as to maximize revenue.
- *Data providers*, which sell ad targeting data to advertisers in real time. Data providers often base their targeting recommendations on tracking (e.g. Quantcast), information purchased from publishers (e.g. BlueKai), and offline consumer databases (e.g. Datalogix)."

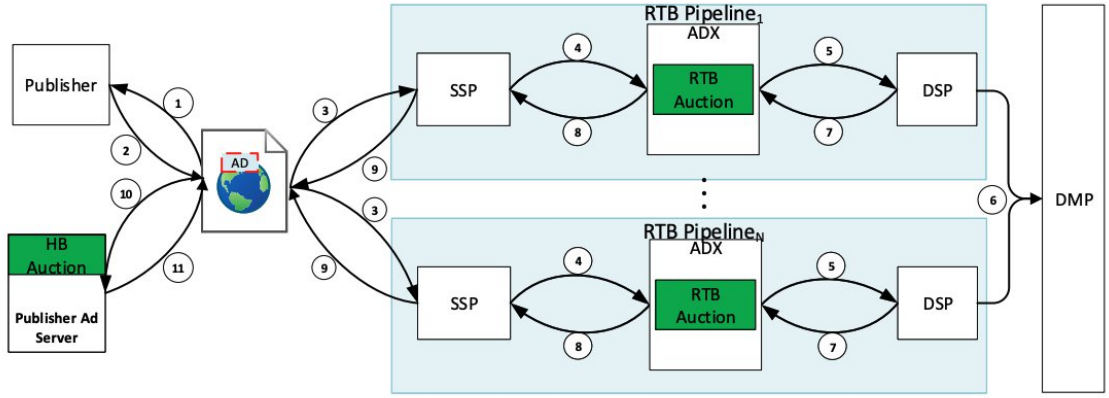


Fig. 1. Online advertising workflow using Real-Time Bidding (RTB) and Header Bidding (HB).

Figure 2. Source: Inferring Tracker-Advertiser Relationships in the Online Advertising Ecosystem using Header Bidding. John Cook, Rishab Nithyanand, Zubair Shafiq. Privacy Enhancing Technologies Symposium (PETS), 2020.

This system has then evolved introducing more actors — such as AdX and DMPs, whose roles are thoroughly described in another publication[7] and demonstrated in the Figure 2.

- *Ad Exchanges (AdX)*, to whom SSPs manage submit the publisher's ad inventory up for auction, and who "collects bid responses from multiple DSPs and uses an auction mechanism (typically a second price auction) to determine the winning bid. If the

[6] Jonathan R. Mayer and John C. Mitchell. Third-party web tracking: Policy and technology. In Proc. of IEEE Symposium on Security and Privacy, 2012. See Section V.A.2), page 7. Available at https://jonathanmayer.org/publications/trackingsurvey12.pdf

[7] Inferring Tracker-Advertiser Relationships in the Online Advertising Ecosystem using Header Bidding. John Cook, Rishab Nithyanand, Zubair Shafiq. Privacy Enhancing Technologies Symposium (PETS), 2020. Available at https://petsymposium.org/popets/2020/popets-2020-0005.pdf

winning bid value surpasses the impression's minimum sale price set by the publisher, the winning bid and the associated ad is forwarded to the SSP , which places the ad on a browser page"

- *Data Management Platforms (DMPs)* receive the user identifiers from the DSP and synchronizes them with the DSP, who evaluates the bid request using the information sent by the AdX and from the DMPs.

Header Bidding (HB) "is an emerging programmatic process for online advertising that is rapidly gaining popularity due to its promise to increase yield for publishers as compared to traditional RTB [...] In contrast to RTB, where the ad inventory is offered to different ad exchanges (and consequently bidders) in a sequential (or waterfall) manner, HB offers the ad inventory to multiple bidders simultaneously."[8]

In such protocols, the **logic determining ad targeting resides not primarily with the publisher, but with ad tech intermediaries**—most notably *Demand-Side Platforms (DSPs)*—acting on behalf of advertisers.

IAB Tech Lab's DSA Transparency Specification. In 2024, IAB Tech Lab, maintaining OpenRTB protocol, introduced the *DSA Transparency Specification*[9] to establish a shared understanding of how parties participating in OpenRTB could transmit Article 26(1)(d) DSA information to online platforms. This specification is accompanied by the "DSA Transparency: Implementation Guidelines" document of the IAB Europe[10]. The IAB Tech Spec on Github reads: "To ensure that the third parties are equipped to provide this support [provide data to populate DSA transparency disclosures], this technical specification standardizes the collection, compilation and transport of the data, leaving Online Platforms free to decide how they wish to make the user-facing disclosures, including if they want to delegate the disclosures to another party." This suggests that online platforms can populate DSA ad disclosures by themselves, or delegate it to the third parties (e.g., SSPs, ad servers) serving them.

IAB DSA Spec entails signaling to the OpenRTB participants "if the bid request belongs to an Online Platform/VLOP, such that a buyer should respond with DSA Transparency information."

[8] *Ibid* 6.

[9] https://github.com/InteractiveAdvertisingBureau/openrtb/blob/main/extensions/community_extensions/dsa_transparency.md

[10] https://iabeurope.eu/wp-content/uploads/IAB-Europe-DSA-Transparency-Implementation-Guidelines-FINAL.pdf

List of User Parameters

The definitions below are not meant to be consumer-facing messages.

User Parameter ID	**User Parameter**	**Definition**	**TCF Purpose IDs**
1	Profiling	Information about the user, collected and used across contexts, that is about the user's activity, interests, demographic information, or other characteristics.	TCF Purposes 4
2	Basic advertising	Use of real-time information about the context in which the ad will be shown, to show the ad, including information about the content and the device, such as: device type and capabilities, user agent, URL, IP address, non-precise geolocation data. Additionally, use of basic cross-context information not based on user behavior or user characteristics, for uses such as frequency capping, sequencing, brand safety, anti-fraud.	TCF Purpose 2
3	Precise geolocation	The precise real-time geolocation of the user, i.e. GPS coordinates within 500 meter radius precision.	TCF Special Feature 1

Figure 2 IAB DSA Specification GitHub, accessed on 31 October 2025; source: https://github.com/InteractiveAdvertisingBureau/openrtb/blob/main/extensions/community_extensions/dsa_transparency.md

As seen in the Figure 2 above, such transparency information includes three user parameters, which are mapped onto purposes within the IAB Europe Transparency and Consent Framework (TCF):

1) "*profiling*" which corresponds to TCF Purpose 4[11], and if the user has consented to this purpose, and the DSP relies on it, the DSP can signal this to the platform, which in turn displays "profiling" as the relevant parameter per ad impression[12].
2) "*basic advertising*," which at first may appear as *contextual* advertising, but its description involves data from the user device, typically used for browser fingerprinting, such as device type and capabilities, user agent, IP address. Moreover, the visited URL (for example, a website with information about *mental disorders*) will typically reveal information about the user's interest as discussed above.
3) "*precise geo-location*" which corresponds to the TCF Special Feature 1 which reads[13] "With your acceptance, your precise location (within a radius of less than 500 metres) may be used in support of the purposes explained in this notice." and therefore can be used for any purpose, including advertising.

We bring the attention of the EDPB to the fact that none of these "user parameters" **do not provide meaningful information** directly and easily accessible from the advertisement about the **main parameters used to determine the recipient to whom the advertisement is presented** required by the Article 26(1)(d): "profiling" and "basic advertising" are very high-

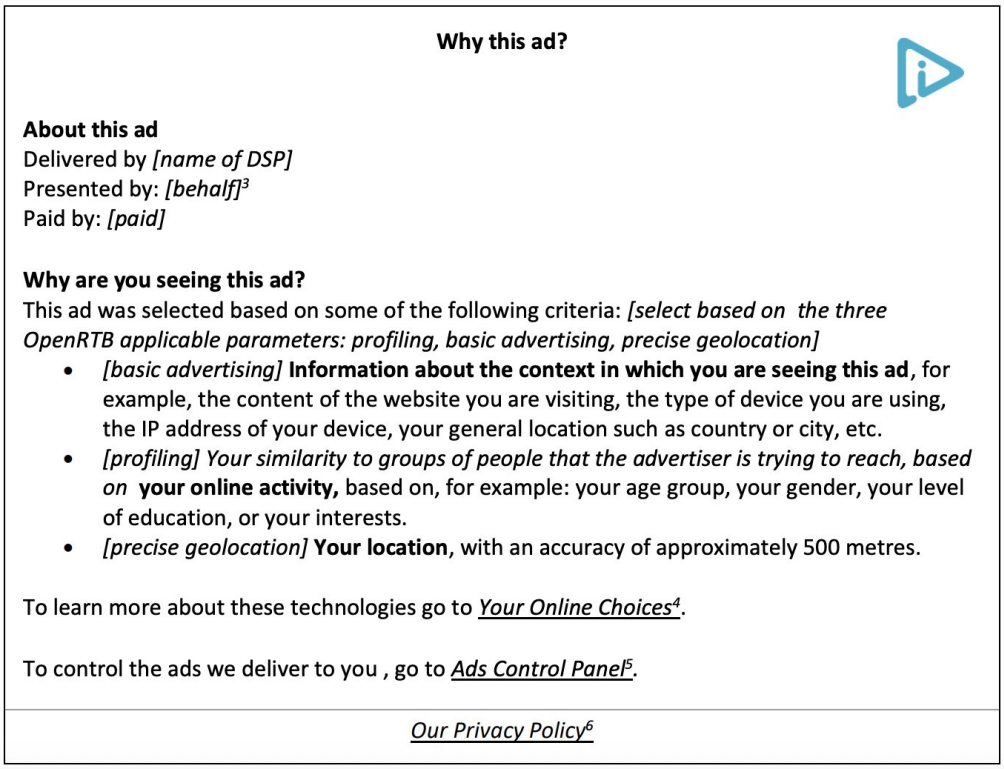
[11] This purpose is defined as "Advertising presented to you on this service can be based on your advertising profiles, which can reflect your activity on this service or other websites or apps (like the forms you submit, content you look at), possible interests and personal aspects.", source: IAB Europe Transparency & Consent Framework Policies, Version 2025-01-16.5.0.a, accessed 31 October 2025 at https://iabeurope.eu/iab-europe-transparency-consent-framework-policies/

[12] https://iabeurope.eu/wp-content/uploads/IAB-Europe-DSA-Transparency-Implementation-Guidelines-FINAL.pdf

[13] IAB Europe Transparency & Consent Framework Policies, Version 2025-01-16.5.0.a, accessed 31 October 2025 at https://iabeurope.eu/iab-europe-transparency-consent-framework-policies/

level and do not inform the user of the parameters used to determine the user, while "precise geo-location" does not specify at all the parameters, but only a presence of a potential use of the geolocation of the user, without explaining which location was used, whether it's the current location or one of the past locations the user has been to (for example, if the user has visited a political or religious place in the past, could be considered a special category of personal data of this user).

Consumer-facing standardization of DSA ad disclosures is led by the European Digital Advertising Alliance (EDAA), which developed the *Advanced Advertising Transparency Programme (AATP)*.[14] EDAA AATP guidance is largely based on IAB DSA Spec, suggesting that the three parameters prescribed by the IAB DSA spec provide baseline transparency. EDAA notes "that the parameters above [from IAB DSA Spec] are not exclusive or exhaustive and should be considered a baseline; the party that renders the Enhanced Transparency Page may choose to add other parameters to the list above." Figure 3 below shows an example of Enhanced Transparency Page:



Why this ad?

About this ad
Delivered by *[name of DSP]*
Presented by: *[behalf]*[3]
Paid by: *[paid]*

Why are you seeing this ad?
This ad was selected based on some of the following criteria: *[select based on the three OpenRTB applicable parameters: profiling, basic advertising, precise geolocation]*

- *[basic advertising]* **Information about the context in which you are seeing this ad**, for example, the content of the website you are visiting, the type of device you are using, the IP address of your device, your general location such as country or city, etc.
- *[profiling] Your similarity to groups of people that the advertiser is trying to reach, based on* **your online activity,** based on, for example: your age group, your gender, your level of education, or your interests.
- *[precise geolocation]* **Your location**, with an accuracy of approximately 500 metres.

To learn more about these technologies go to *Your Online Choices*[4].

To control the ads we deliver to you , go to *Ads Control Panel*[5].

Our Privacy Policy[6]

Figure 3. EDAA Enhanced Transparency Page (EDAA AATP Guidance, pg. 12)

AATP guidance suggests that online platforms should consider what other parameters to consider based on the audience characteristics that were selected by an advertiser for targeting (e.g., age, location, etc.). Yet, in practice, **because the IAB specification does not technically enable seamless transmission of this information, many platforms will simply fall back on displaying only the three default parameters**.

Similar to the VLOP's walled gardens, this approach falls short of compliance with the Art 26 (1) (d) DSA, but to greater extent. As recital 68 DSA clarifies, explanations about the "main

[14] https://edaa.eu/wp-content/uploads/EDAAs-AATP-%E2%80%93-Transparency-for-the-DSA.pdf

parameters" should include "information on the **method** used for presenting the advertisement, for example whether it is contextual or other type of advertising". It further suggests that when the *method* is online advertising based on profiling platforms should disclose "the **main profiling criteria** used", and "it should also inform the recipient about any means available for them to **change such criteria**."

Our research[15] already showed that purposes defined in the IAB Europe TCF are questionable and **not specific enough to be mapped to the legal basis** of processing (mostly consent or legitimate interest. Moreover, even grouped purposes that IAB Europe TCF proposes as "Stacks", such as "Personalized Advertising", "Personalized Content", are not understood by the users: the recent research[16] found out that "**most purpose descriptions were not informative enough, according to participants**. Descriptions do not often tell users the specifics about an organization's data handling procedures, such as how long their data is retained, nor outline the data deletion process. Overall, participants wanted descriptions to provide more transparency and reassurance."

Nevertheless, it seems that current IAB and EDAA frameworks **tie the "change" function to the TCF purposes**. Thus, users can only opt out of profiling by withdrawing consent for Purpose 4 rather than modify specific profiling criteria. However, it is not clear what happens in terms of profiling if the consent is given for TCF purpose 3 "Create profiles for personalised advertising". Neither the IAB DSA specification nor the EDAA AATP presently enables users to view or adjust the concrete values of interests or segments used to target them.

This shortcoming is especially concerning as artificial intelligence (AI) systems increasingly determine targeting and ad delivery decisions. Whereas traditional advertising systems at least rely on human-defined audience segments recorded somewhere in the ad tech stack (usually DSPs), **AI-based targeting often does not explicitly represent such criteria** but rather infers and applies them dynamically. Without appropriate transparency mechanisms, users—and regulators—will have no visibility into how such automated decisions are made.

Our recommendation
The EDPB should address these questions in future guidance, as passing along and displaying profiling criteria will inevitably involve the processing of personal data and raise complex issues of data confidentiality, security, and fairness. Providing clarity on how these obligations intersect with the GDPR, especially regarding the lawful basis, data minimisation, and user rights, would be of great value. Without such guidance, self-regulatory standards may continue to underdeliver on the transparency and user agency that Article 26(1)(d) DSA was designed to achieve. EDPB can suggest, for example, that transparency interface includes *any and all* demographic, or interest groups, assigned to the user or otherwise targeted by an advertiser, including when ad targeting or/and delivery happens solely by using AI. This may require application of explainable AI.

[15] Purposes in IAB Europe's TCF: which legal basis and how are they used by advertisers? Célestin Matte, Cristiana Santos, Nataliia Bielova. Annual Privacy Forum (APF 2020). Available at https://www-sop.inria.fr/members/Nataliia.Bielova/papers/Matt-Sant-Biel-20-APF.pdf

[16] Kyi L., Mhaidli A., Santos C., Roesner F., Biega A., It doesn't tell me anything about how my data is used": User Perceptions of Data Collection Purposes, 2024. Available at https://dl.acm.org/doi/pdf/10.1145/3613904.3642260

2.4.2 Legal framework on automated individual decision-making and profiling

62. The provisions in Article 26(1) DSA on advertising transparency also may, depending upon the particular characteristics of the case, relate to data processing practices that might fall within the scope of automated individual decision-making and profiling that fulfil the criteria of Article 22(1) GDPR, if the profiling in question leads to a decision that produces legal effects or similarly significantly affects data subjects. To assess whether an automated decision to present a specific advertisement to an individual produces legal effects or similarly significantly affects him or her, several (non-exhaustive) characteristics of the personal data processing activity (including at the level of each individual advertisement delivery) should be taken into account, including the intrusiveness of the profiling process, the tracking of individuals across different websites, devices and services; the expectations and wishes of the individuals concerned; the way the advert is delivered; or using knowledge of the vulnerabilities of the data subjects targeted.

63. According to Article 22(1) GDPR, the data subject has "the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her".

64. However, such processing can be lawful if it relies on specific legal bases as defined in Article 22(2) GDPR necessary for the performance of a contract, authorised by Union or Member State law or based on the data subject's explicit consent.

65. Whether or not the data has been obtained directly or indirectly, the GDPR mandates that the data subject shall be properly informed, according to Articles 13 and 14 GDPR, of "the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing". Recital 71 GDPR also indicates that processing within the scope of Article 22 GDPR "should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision (…)". Moreover, Recital 60 GDPR states that "the data subject should be informed of the existence of profiling and the consequences of such profiling" even where profiling does not fall within the scope of Article 22 GDPR.

66. Some of the elements or parts of the elements mentioned in Article 26 DSA should therefore already be provided to the data subject under the GDPR especially where Article 22 GDPR applies, in particular regarding the main parameters of the profiling.

67. Therefore, the DSA and the GDPR both include transparency obligations that are relevant to the delivery of advertisements on online platforms. The DSA lays down additional obligations, as it specifies the manner in which the relevant information

must be provided and the expected level of information and control, for instance providing the main parameters for determining that a specific advertisement is presented to the recipient and providing information on possibilities to change said parameters, where such possibilities exist.

While the EDPB already draws an important connection between Article 26(1) DSA and Article 22(1) GDPR, it should go further and provide **concrete examples** of cases in which *online advertising based on profiling (OABP)* may trigger Article 22 GDPR safeguards. EDPB may choose to include instances of targeting in which automated decision determines users who see(1) professional opportunities (**employment ads**); (2) property listings, rentals, or mortgage offers (**housing ads**); (3) loan, credit card, or insurance premiums offers (**financial-services ads**); or that applies (4) dynamic pricing that presents different offers or conditions to different users (**personlised pricing**). In all these cases, the automated decision to display—or withhold—an advertisement may produce legal or similarly significant effects on the individual, thus falling within the scope of Article 22(1) GDPR.

In paragraphs 63 of the opinion, the EDPB points out that in case of OABP with significant effects, the user has "the right not to be object to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her". In par 64, the EDPB clarifies that OABP with significant effects be lawful if it relies on specific legal bases as defined in Article 22(2) GDPR necessary for the performance of a **contract**, **authorised** by Union or Member State law or based on the data subject's **explicit consent.** In case of online platforms, this will almost always be explicit consent. However, the EDPB does not clarify how is this Article 22(2) GDPR "explicit consent" different from the general consent requirement of the GDPR. This is a great opportunity for the EDPB to clarify this, proposing, for example, that online platforms ask for additional consent separately if they wish to engage in such targeting with significant effects.

2.4.3 Legal framework on profiling using special categories of data

72. Processing of special categories of data, including profiling based on these data, are subject to a specific legal regime as set out in Article 9 GDPR. Processing of such special categories of data is prohibited in principle, unless it relies on specific derogations, as set out in Article 9(2) GPDR. The scope of the special categories of data under Article 9(1) GDPR is very broad. In particular, it may include data derived or inferred from profiling activity or indirect disclosure of such data. Moreover, it does not matter if the information revealed by the processing operation in question is correct and if the controller is acting with the aim of obtaining information that falls in that category.

73. Moreover, automated individual decision-making within the scope of Article 22 GDPR shall not be based on special categories of personal data referred to in Article 9(1) GDPR unless such processing relies on the explicit consent of the data subject (Article 9(2)(a)) GDPR or is necessary for reasons of substantial public interest (Article 9(2)(g) GDPR) pursuant to Article 22(4) GDPR.

74. However, according to Article 26(3) DSA, "Providers of online platforms shall not present advertisements to recipients of the service based on profiling as defined in Article 4, point (4), of Regulation (EU) 2016/679 using special categories of personal data referred to in Article 9(1) of Regulation (EU) 2016/679".

75. This means that the GDPR requires specific derogations regarding profiling by online platforms using special categories of data for advertising purposes. On the other side, the DSA prohibits the presentation of any advertising based on profiling using such special categories of personal data by providers of online platforms to recipients of the service, regardless of whether this profiling is carried out by providers of online platforms or by others.

Example 2 – Profiling based on special categories of data A company uses inferred religious beliefs from geolocation (e. g. visiting places of worship) or shopping habits (e. g. purchase of specific food products) to predict lifestyle and shopping patterns and then presents an advertisement based on those predictions.

76. These special rules laid down by the DSA complement the rules laid down in Article 9(2) GDPR and Article 22(4) GDPR when they apply. The presentation of advertisements based on profiling using special categories of personal data by providers of online platforms to recipients of the service is prohibited by the DSA even in situations where the provider of an online platform or another entity would rely on an appropriate legal basis under Article 6(1) GDPR and an appropriate derogation under Article 9(2) GDPR for this processing.

In paragraphs 72–76, the EDPB Guidelines discusses the relationship between Article 9 GDPR, which concerns special categories of personal data, and Article 26(3) DSA, which prohibits online advertising based on profiling using such data. Article 26(3) is among the most consequential provisions of the DSA. It has significant implications for the online advertising industry and has therefore become one of the most contested provisions in scholarly, industry, and policy debates. While it is commendable that the EDPB has explicitly addressed this issue, the precise boundaries of the prohibition remain insufficiently clear.

Broadly, three interpretations can be identified. The narrowest reading limits the prohibition to explicit targeting based on sensitive categories (e.g., an advertiser selecting "Christian" as a targeting criterion). A broader interpretation extends the ban to criteria that indirectly reveal sensitive information (e.g., "frequently visits a Christian church"). The broadest interpretation would prohibit any data processing that could—even unintentionally or through inference—reveal sensitive attributes (e.g., the use of all geo-location data).

The EDPB's guidelines currently suggest that the scope of Article 9(1) GDPR is *"very broad"* and covers *"data derived or inferred from profiling activity"* (referring to the C-252/21 Meta judgment), as well as *"indirect disclosure of such data"* (referring to C-184/20 OT). Yet this explanation remains ambiguous. Building on the EDPB's statement and the OT judgment, data should be regarded as *special categories of personal data* whenever, *"by means of an intellectual operation involving comparison or deduction,"* they can reveal information about a protected attribute. Under this interpretation, narrow geo-location targeting—for instance,

at the level of specific neighbourhoods—could fall within the scope of special categories of data, as it may indirectly expose a person's racial, ethnic, or religious affiliation.

This issue becomes even more complex when targeting and ad delivery are no longer based on human-defined audiences but are determined by algorithmic systems, such as *lookalike audiences* or *Performance Max* campaigns, in which selection of similarity of users is identified by an algorithmic systems. For example, algorithms may use geo-location data to target users visiting places of worship without a data controller explicitly inferring that person has religious affiliation. Similarly, algorithms may rely on cursor-movement patterns or other behavioural signals to target elderly users or those with neurological conditions—again, without such criteria being explicitly recorded or recognisable. These systems can infer sensitive attributes from data in ways that may be incomprehensible to humans, in a way that may be difficult to verify. EDPB is welcome to comment weather such cases fall within the meaning of processing *"by means of an intellectual operation involving comparison or deduction,"* or create another additional criteria.

Without further clarification, it remains uncertain where EU law draws the line. Given that algorithmic targeting entails high opacity and heightened risks of exploitation, the EDPB should consider such practices prohibited in principle, unless online platforms can, through explainable-AI tools, disclose the precise criteria used to determine targeting. In the absence of such transparency and safeguards ensuring that targeting does not exploit vulnerabilities or rely on sensitive attributes, there should be no place for these practices in European society.

2.4.4 Security and confidentiality of data resulting from advertising transparency obligations

77. Article 26(1)(d) DSA states that information must be provided about the main parameters used to determine the recipient to whom each advertisement is presented. As per Recital 68 of the DSA, "recipients of the service should have information directly accessible from the online interface where the advertisement is presented, on the main parameters used for determining that a specific advertisement is presented to them, providing meaningful explanations of the logic used to that end, including when this is based on profiling". **In practice, that information likely often constitutes personal information as it can reveal alleged user preferences and prior navigation.**

78. As recalled in Recital 107 DSA, "The provision of online advertising generally involves several actors, including intermediary services that connect publishers of advertisements with advertisers". For the relevant information to reach the recipient of the service, those intermediaries need to facilitate the transmission of information. Appropriate technical and organisational measures need to be implemented to ensure that the presentation of that information and the ability to change parameters – where such possibilities exist – **does not allow any intermediary to access or collect any additional information about the recipient of the service**. The associated processing should respect the obligation provided by Article 32 GDPR, as well as data minimisation according to Article 5(1)(c) GDPR, and

data protection by design and default under Article 25 GDPR. Compliance with the transparency obligations set out in Article 26 DSA should not entail further sharing of personal data with intermediaries: access or collection of information regarding the recipient of the service through intermediary companies requires an appropriate legal basis under Article 6 GDPR and must respect the principles laid out in Article 5 GDPR.

79. Additionally, providers of intermediary services should, where possible and without leading to an increased collection of personal data, take appropriate steps to ensure that the information is provided to the one recipient of the service that is subject to such profiling.

As the EDPB notes in paragraph 77, when meaningful information about the main parameters used to deliver online advertising is shared with users, that information may itself constitute **personal data**. For example, as we previously suggested, profiling criteria should include the *actual values* assigned to a specific user (e.g., "surf enthusiast," "young mother") rather than merely referring to broad categories of targeting (e.g., "interests," "demographics"). We commend the EDPB for emphasizing the importance of **security and confidentiality** when multiple actors exchange such data to comply with **Article 26(1) DSA.** We fully agree that data minimization and data protection by design and by default principles must be respected.

However, we are concerned that security and confidentiality requirements could be invoked by some industry actors to **justify limited compliance** with Article 26(1) DSA—keeping disclosures overly high-level and thereby reducing their usefulness to users. Currently, the **OpenRTB specification** allows participants to broadcast personal data to multiple intermediaries via the **bidstream**, often using fine-grained audience taxonomies. For example, the IAB Audience Taxonomy defines 1,559 audience segments, classified under categories such as *purchase intent*, *demographics*, and *interests*.[17] We see no valid reason **why such audience segments may be freely transmitted along the supply chain for targeting purposes**, yet not for compliance with Article 26(1) DSA. Security and confidentiality considerations should not be invoked as a justification for such non-compliance.

2.8 Codes of conduct, including for online advertising (Articles 45, 46 and 47), and their relationship with codes of conduct under Article 40 GDPR

111. In Article 46 DSA, providers in the advertising value chain are encouraged to contribute to further transparency beyond the requirements of Article 26 and 39 DSA. This could include, for example, the transparency requirements of Chapter 3 GDPR.

Additional considerations around guidelines provided in DSA Article 39 (not specifically mentioned in the EDPB guidelines 3/2025)

[17] https://github.com/katieshell/Taxonomies/blob/main/Audience%20Taxonomies/Audience%20Taxonomy%201.1.tsv

Article 39(1) DSA states that "Providers of very large online platforms or of very large online search engines that present advertisements on their online interfaces shall compile and make publicly available in a specific section of their online interface, through a searchable and reliable tool that allows multicriteria queries and through application programming interfaces, a repository containing the information referred to in paragraph 2, for the entire period during which they present an advertisement and until one year after the advertisement was presented for the last time on their online interfaces[...]
Article 39(2) DSA states, **bolded** by the authors:" The repository shall include at least all of the following information:

> (e) whether the advertisement was intended to be presented specifically to one or more particular groups of recipients of the service and if so, **the main parameters used for that purpose** including where applicable the main parameters used to exclude one or more of such particular groups.

In addition, Recital 95 DSA specifies that "Advertising systems used by very large online platforms and very large online search engines pose particular risks and require further public and regulatory supervision on account of their scale and **ability to target and reach recipients of the service based on their behaviour** within and outside that platform's or search engine's online interface. Very large online platforms or very large online search engines should **ensure public access to repositories of advertisements** presented on their online interfaces to facilitate supervision and research into emerging risks brought about by the distribution of advertising online, for example in relation to illegal advertisements or manipulative techniques and disinformation with a real and **foreseeable negative impact on public health**, **public security, civil discourse, political participation** and **equality**. Repositories should include the content of advertisements, including the name of the product, service or brand and the subject matter of the advertisement, and related data on the advertiser, and, if different, the natural or legal person who paid for the advertisement, and the delivery of the advertisement, in particular where targeted advertising is concerned. This information should include both information about **targeting criteria and delivery criteria**, in particular when advertisements are delivered to persons in vulnerable situations, such as minors."

Recent comparative work[18] on ad repositories (Google, Meta, and X) identified several issues in the current implementation of ad repositories:

- **Meta:**
  - Meta's Ad Library is well-documented and searchable but reveals only limited targeting information (age, gender, location). Broader targeting dimensions, such as interests, lookalike audiences, and other delivery criteria, are not disclosed. A separate "Ad Targeting Dataset" applies only to political ads and is based on Meta's internal determination of what counts as political content.
  - The repository provides no information on whether algorithmic delivery factors were included in ad targeting.
- **Google:**
  - Google's Transparency Center does not enable keyword search and *lacks identifiers linking user-facing ads to repository entries*.

[18] Work under review: https://osf.io/596jx/files/srmtn?view_only=12e8946fc0f9465fa2b289e5c5d0f985

  - The repository discloses only high-level targeting categories (e.g. “contextual signals,” “demographics”) without specifying the exact values selected.
  - Moreover, the range of targeting parameters available to advertisers in Google Ads interfaces is not consistent with the parameters disclosed in the repository. For example, categories such as lookalike audiences and schedule-based targeting are absent from the list of available options in the repository.
  - The repository attributes all targeting criteria to advertiser selections, even when this is not the case. In a test ad campaign conducted on Google products, the corresponding repository entry indicated that the advertiser had chosen to target ads based on contextual signals, despite no such selection being made during campaign setup.
  - We also identified inaccuracies in the targeting parameters disclosed in the repository. A comparison between user-facing ad explanations collected from YouTube users in Germany and their corresponding repository entries revealed numerous instances where “interests—that is, profiling or behavioral targeting—were referenced in the user-facing explanations but were absent from the associated repository records.
- **X (Twitter):**
  - X’s ad repository offers only minimal search functionality. Searches can be filtered by advertiser, country, and date range, but not by keyword or topic.
  - Targeting parameters are presented as unstructured text tokens (e.g. “computer games”), without clear labeling or distinction of what those tokens stand for in terms of advertiser choices (interests, keywords, etc.).
  - Furthermore, the repository provides no information on whether algorithmic delivery factors were included in ad targeting.
  - In terms of accuracy, data shows inconsistencies between the explanations and the corresponding repository entries, particularly with regard to lookalike and behavioral targeting. These inconsistencies stemmed either from omissions of specific parameters or from mismatches in labeling—cases where users were shown delivery criteria not selected by the advertiser, or where repository labels differed from those presented in the ad explanations.

Overall, the information disclosed in ad repositories often lacks:

- **Completeness:** Key targeting and delivery parameters are missing or overly aggregated.
- **Attribution:** It remains unclear which actor (advertiser or platform) determined each parameter.
- **Linkability:** Users and researchers cannot easily relate repository entries to actual ads they encounter.

Our recommendation
To achieve the transparency objectives of Article 39, repositories should: • disclose all main targeting and delivery parameters with sufficient granularity; • clearly attribute targeting decisions to advertisers or platform systems; • include identifiers enabling cross-reference with user-facing ad explanations; and • **standardize** data formats to support independent auditing and comparative research.